

MIA

Eine Methode zur Erreichung von Compliance in flexiblen und
IT-gestützten Geschäftsprozessen

Dissertation

zur Erlangung des Grades

Doktor der Wirtschaftswissenschaft (Dr. rer. pol.)

der Juristischen und Wirtschaftswissenschaftlichen Fakultät
der Martin-Luther-Universität Halle-Wittenberg

vorgelegt von

Tobias Seyffarth, M. Sc. Wirtschaftsinformatik

Halle (Saale),

November 2020

Erstgutachter: Prof. Dr. Stefan Sackmann

Zweitgutachter: Prof. Dr. Ralf Peters

Tag der Verteidigung: 18. Februar 2021

Danksagung

Bei meinem Doktorvater Prof. Dr. Stefan Sackmann möchte ich mich für die Chance und das entgegengebrachte Vertrauen zur Bearbeitung dieses Forschungsthemas bedanken. Ohne die zahlreichen kritischen Debatten wäre es mir nicht möglich gewesen, das Forschungsthema in zu bearbeiten und in seiner letztendlichen Form abzuschließen. Besonders positiv habe ich die Freiheit in der Bestimmung, Ausgestaltung und Umsetzung meines Forschungsvorhabens wahrgenommen. Außerdem gilt mein Dank Prof. Dr. Ralf Peters für seine Bereitschaft zur Übernahme des Zweitgutachtens.

Ich danke meinen Kollegen am Lehrstuhl für Wirtschaftsinformatik, insbesondere Betriebliches Informationsmanagement für die zahlreichen Diskussionen, kritischen Nachfragen und Anregungen in den Forschungskolloquien und Lehrstuhlabenden sowie den schnellen Problemlösungen und Geduld während der Entwicklung meines Softwareprototypens. Außerdem danke ich den Kollegen unseres Nachbarlehrstuhls für Wirtschaftsinformatik, insbesondere E-Business für die ermutigenden Worte während der verschiedenen Schreibphasen dieser Arbeit und der Möglichkeit mich in einige ihrer Publikationsprojekte einbringen zu dürfen.

Weiter danke ich meinem Freundeskreis für die regelmäßigen Kultur- und Konzertbesuche. Es war jedes Mal sehr beruhigend zu wissen, dass es neben Compliance und Geschäftsprozessen auch noch weitere wichtige und spannende Themen gibt. Zuletzt möchte ich meinen Eltern danken, dass sie mich dazu befähigt und unterstützt haben, selbstbestimmt meine eigenen Entscheidungen in meinem akademischen Bildungsweg zu treffen. Mir ist bewusst, dass das keine Selbstverständlichkeit ist.

Zusammenfassung

Die Datenschutzgrundverordnung, das Handelsgesetzbuch, Verträge zwischen Geschäftspartnern und weitere Compliance-Anforderungen können Bedingungen an Geschäftsprozesse stellen. Zur Sicherstellung der Compliance in Geschäftsprozessen können Geschäftsprozessmodelle mit sogenannten Compliance-Prozessen angereichert werden. Compliance-Prozesse, wie bspw. ein Vier-Augen-Prinzip oder die Freigabe durch Vorgesetzte, stellen die Einhaltung von Compliance-Anforderungen sicher. Neben Geschäftsprozessen können IT-Architekturen respektive ihre IT-Komponenten ebenfalls Träger von Compliance-Anforderungen sein. Darüber hinaus ermöglichen IT-Komponenten durch die Unterstützung von Compliance-Prozessen die Sicherstellung von Compliance-Anforderungen, wodurch IT-Komponenten im Zusammenhang mit Compliance eine Doppelrolle haben.

Outsourcing-Entscheidungen, neue Technologien, Prozessverbesserungen oder Restrukturierungen von Geschäftsprozessen und IT-Architekturen können zu Veränderungen von Compliance-Anforderungen, Geschäftsprozessen und IT-Architekturen führen. Eine Outsourcing-Entscheidung kann beispielsweise zum Ersetzen einer IT-Komponente oder Geschäftsaktivität führen. Die Restrukturierung von IT-Architekturen kann wiederum das Entfernen einzelner IT-Komponenten zur Folge haben. Trotz möglicher Veränderungen ist die Erhaltung von Compliance jedoch weiterhin notwendig, wodurch es erforderlich wird die Auswirkungen auf die Erhaltung von Compliance durch das Ersetzen und Entfernen zum Entwurfszeitpunkt zu kennen und die Konsequenzen zu berücksichtigen. Im Falle des Ersetzens gilt es alle relevanten Compliance-Anforderungen zu kennen, um diese berücksichtigen zu können. Im Fall des Entfernens gilt es mögliche Compliance-Verletzungen oder obsoletere Compliance-Anforderungen zu identifizieren.

Bestehende Arbeiten erlauben nur eine eingeschränkte Modellierung von Compliance-Anforderungen, dem Geschäftsprozessmodell und dem Modell der IT-Architektur in einem gemeinsamen Modell. Für eine vollständige Berücksichtigung aller Abhängigkeiten zur Erhaltung von Compliance ist jedoch eine vollständige Modellierung der genannten Modelle notwendig. Daneben gibt es ebenfalls Arbeiten, die automatische Abfragen zwischen einzelnen Elementen der Modelle ermöglichen. Jedoch erlauben sie keine Unterscheidung zwischen den Veränderungsmustern Ersetzen und Entfernen. Für die Identifikation der Auswirkungen auf die Erhaltung von Compliance ist das aber zwingend notwendig, da beim Ersetzen und Entfernen von Elementen jeweils andere Zusammenhänge zwischen den drei Modellen betrachtet werden müssen. Darüber hinaus berücksichtigen aktuelle Ansätze keine notwendigen IT-Komponenten bei der Adaption von Geschäftsprozessmodellen. Für eine Compliance-konforme Adaption von Geschäftsprozessen ist das durch die Doppelrolle der IT allerdings zwingend erforderlich. Letztendlich adressieren bestehende Arbeiten jeweils nur einen Teilaspekt des beschriebenen Problems. Daher ist das Ziel eine Methode zur Erreichung von Compliance in IT-gestützten Geschäftsprozessen beim Ersetzen oder Entfernen von oder Compliance-Anforderungen, Geschäftsaktivitäten oder IT-Komponenten.

Dem Forschungsparadigma des Design Science Research (DSR) entsprechend, wurden verschiedene Modelle, Konstrukte und Methoden entwickelt, die sich zu der Methode MIA zusammenfassen lassen, welche aus drei Schritten besteht:

- Modellieren eines gemeinsamen Modells aus Compliance-Anforderungen, Geschäftsprozessen und IT-Komponenten.
- Identifizieren der Auswirkungen auf die Erhaltung von Compliance aufgrund des Entfernens oder Ersetzens eines Elements aus dem gemeinsamen Modell.
- Adaptieren des Geschäftsprozesses durch die Integration alternativer Compliance-Prozesse.

Die Modellierung des gemeinsamen Modells basiert auf einer Modelltransformation von Compliance-Anforderungen sowie dem Modell des Geschäftsprozesses und der IT-Architektur und ihrer Verbindung in einem gemeinsamen Graphen. Die Identifikation der Auswirkungen auf die Erhaltung von Compliance erfolgt durch verschiedene Suchstrategien, die auf Basis einer Vorwärts- und Rückwärtssuche in dem integrierten Graphen ausgeführt werden. Sollte eine Compliance-Verletzung gegenüber dem Geschäftsprozess festgestellt werden, erfolgt die Compliance-konforme Adaption des Geschäftsprozessmodells. Basis dieser Adaption sind verschiedene, getrennt vom Geschäftsprozess modellierte und gespeicherte Compliance-Prozesse. Eine Compliance-Anforderung kann dabei von mehreren alternativen Compliance-Prozessen sichergestellt werden. Die Unterscheidung zwischen alternativen Compliance-Prozessen erfolgt anhand ihrer Eigenschaften, wie dem Automatisierungsgrad oder ihrer Compliance-Aktivitäten. Compliance-Prozesse können außerdem durch sogenannte Compliance-Prozess-Muster generalisiert werden.

Die Anwendbarkeit von Artefakten kann im Forschungsparadigma DSR durch Softwareprototypen demonstriert werden, weshalb die Demonstration von MIA in dem Softwareprototypen BCIT erfolgte. Zudem wurden die wahrgenommene Nützlichkeit von MIA anhand des Softwareprototypens BCIT in mehreren Fallstudien durch Domänenexpert:innen positiv evaluiert.

Durch die Anpassung bestehende Methoden und Verfahren auf ein neues Problemfeld leisten die entwickelten Artefakte einen Wissensbeitrag des Typs Exaptation. Darüber hinaus können sie als Ausgangspunkt für weitere Forschung dienen. So ist es vorstellbar MIA um die Adaption der IT-Architektur zu erweitern. Ferner ist eine Methode denkbar, die auf Basis existierender integrierter Graphen, Empfehlungen sowohl zur Berücksichtigung von Compliance-Anforderungen als auch zur Integration von Compliance-Prozessen unmittelbar während des Entwurfs des Geschäftsprozessmodells gibt.

Inhaltsverzeichnis

Danksagung.....	II
Zusammenfassung.....	III
Inhaltsverzeichnis.....	V
Abkürzungsverzeichnis.....	VIII
Symbolverzeichnis.....	IX
Abbildungsverzeichnis.....	X
Tabellenverzeichnis.....	XI
1 Einleitung.....	1
1.1 Problem.....	1
1.2 Forschungslücke und Ziel.....	2
1.3 Methode und Ergebnisse.....	3
1.4 Aufbau der Arbeit.....	3
2 Wechselwirkungen zwischen Compliance, Geschäftsprozessen und IT.....	5
2.1 Compliance.....	5
2.1.1 Business Process Compliance.....	5
2.1.2 IT-Compliance.....	7
2.1.3 Fazit.....	8
2.2 Veränderungsmuster.....	8
2.3 Ausgangsszenario.....	9
3 Stand der Forschung.....	12
3.1 Ermittlung des Forschungsstands.....	12
3.2 Methoden zur Modellierung und Identifikation.....	13
3.2.1 Mustersuche in Prozessmodellen.....	13
3.2.2 Modellieren und Identifizieren von Abhängigkeiten zwischen Compliance-Anforderungen.....	13
3.2.3 Modellieren und Identifizieren von Abhängigkeiten zwischen Compliance-Anforderungen und Geschäftsprozessen.....	14
3.2.4 Modellieren und Identifizieren von Abhängigkeiten zwischen Compliance-Anforderungen und IT-Komponenten.....	16
3.2.5 Modellieren und Identifizieren von Abhängigkeiten zwischen Compliance-Anforderungen, Geschäftsprozessen und IT-Komponenten.....	16

3.3	Methoden zur Geschäftsprozessadaption	17
3.4	Ableiten der Forschungslücke.....	17
4	Forschungsdesign	20
5	Entwurf und Entwicklung der Artefakte.....	23
5.1	Konzeptuelles Domänenmodell.....	23
5.2	Modellieren eines integrierten Compliance-Modells.....	24
5.3	Identifizieren von Auswirkungen auf Compliance	26
5.3.1	Anwendung auf das Ausgangsszenario	26
5.3.2	Ersetzen eines Elements	26
5.3.3	Entfernen eines Elements	28
5.4	Adaptieren des Geschäftsprozessmodells	29
5.4.1	Anwendung auf das Ausgangsszenario	30
5.4.2	Eigenschaften von Compliance-Prozessen.....	31
5.4.3	Struktur eines alternativen Compliance-Prozess-Graphs	33
5.4.4	Suchen und integrieren alternativer Compliance-Prozesse.....	34
6	Demonstration und Evaluation der Artefakte	36
6.1	Einordnung der Evaluationsepisoden.....	36
6.2	Erweiterter Softwareprototyp BCIT	37
6.3	Evaluation der wahrgenommenen Nützlichkeit	39
6.3.1	Fallstudienaufbau.....	40
6.3.2	Diskussion der Testgütekriterien	41
6.3.3	Fallstudienresultate und Diskussion der Ergebnisse.....	42
7	Diskussion	45
7.1	Limitationen	45
7.2	Implikationen für Wissenschaft und Praxis	47
8	Schlussbetrachtung	49
9	Literaturverzeichnis.....	X
	Anlage A: Autorenerklärung über die Arbeitsanteile der Artikel.....	XXIV
	Anlage B: Publikation „A Taxonomy of Compliance Processes for Business Process Compliance“	XXVI
	Anlage C: Publikation „Business Process Compliance and Business Process Change“	XLIV

Anlage D: Publikation „Business Process Compliance despite Change“LIX
Anlage E: Publikation „Maintaining Business Process Compliance despite Changes“LXXIII
Eidesstattliche Erklärung über verwendete Hilfsmittel CV

Abkürzungsverzeichnis

BCIT	Business Process, Compliance and IT
BPMN	Business Process Model and Notation
CA	Compliance-Anforderung
CP	Compliance-Prozess
DSGVO	Datenschutzgrundverordnung
DSR	Design Science Research
ERP	Enterprise Resource Planning
ERP FI	ERP Finanzwesen
ERP MM	ERP Materialmanagement
FCL	Formal Contract Logic
FF	Forschungsfrage
IDW	Institut der Wirtschaftsprüfer
IT	Informationstechnologie
ITK	IT-Komponente
LTL	Linear Temporal Logic
MIA	Modellieren, Identifizieren, Adaptieren
PLTL	Past Linear Temporal Logic
TOSCA	Topology and Orchestration Specification for Cloud Applications
UML	Unified Modeling Language
WS-BPEL	Web Services Business Process Execution Language
XML	eXtensible Markup Language

Symbolverzeichnis

<i>AG</i>	Alternativer Compliance-Prozess-Graph
<i>C</i>	Menge von koordinierenden Knoten
<i>CA</i>	Menge von Compliance-Aktivitäten
<i>CAG</i>	Compliance-Anforderungen-Graph
<i>CP</i>	Compliance-Prozess-Graph
<i>c_type</i>	Funktion zum Zuweisen eines eines Koordinationstyps
<i>E</i>	Menge von Kanten
$e_{i,j}$	Gerichtete Kante zwischen zwei Knoten n_i und n_j der Kantenmenge E
<i>G</i>	Integrierter Compliance-Graph
<i>GA</i>	Menge von Geschäftsaktivitäten
<i>ITG</i>	IT-Architektur-Graph
<i>N</i>	Menge von Knoten
n_i	Knoten der Knotenmenge N
$n_{identify}(n)$	Funktion zum Zuweisen eines Identifikators
$n_{type}(n)$	Funktion zum Zuweisen eines Knotentyps
$n_{rule}(n)$	Funktion zum Zuweisen einer Compliance-Regel
<i>PG</i>	Geschäftsprozess-Graph

Abbildungsverzeichnis

Abbildung 1. Interner Bestellprozess	10
Abbildung 2. Kernartefakte von MIA	20
Abbildung 3. Einordnung der Publikationen	21
Abbildung 4. Konzeptuelles Domänenmodell.....	23
Abbildung 5. Auswirkungen auf Compliance durch das Ersetzen und Entfernen.....	26
Abbildung 6. Pseudocode zur Auswirkungsidentifikation beim Ersetzen einer IT-Komponente	27
Abbildung 7. Pseudocode zur Auswirkungsidentifikation beim Entfernen einer IT-Komponente	29
Abbildung 8. Compliance-konforme Varianten des Internen Bestellprozesses.....	30
Abbildung 9. Compliance-Prozess-Taxonomie.....	32
Abbildung 10. Pseudocode für das Adaptieren Compliance-konformer Geschäftsprozesse	35
Abbildung 11. Technologie-Stack von BCIT	38
Abbildung 12. Schritte in BCIT.....	38
Abbildung 13. Verbinden von Elementen und integrierter Compliance-Graph	38
Abbildung 14. Auswirkungen auf Compliance beim Entfernen von „ERP MM“	39
Abbildung 15. Adaptierter Compliance-konformer Geschäftsprozess in BCIT	39
Abbildung 16. Boxplot der Evaluationsergebnisse.....	43

Tabellenverzeichnis

Tabelle 1. Fragen, die durch MIA beantwortet werden können.....	11
Tabelle 2. Ergebnisse der ersten Literatursuche.....	12
Tabelle 3. Ergebnisse der zweiten Literatursuche	13
Tabelle 4. Autorenzentrierte Konzeptmatrix	18
Tabelle 5. Evaluationsepisoden von MIA	37
Tabelle 6. Wahrgenommene Nützlichkeit von BCIT.....	42
Tabelle 7. Eingebachte Publikationen.....	50

1 Einleitung

1.1 Problem

Compliance bezeichnet die Einhaltung sogenannter Compliance-Anforderungen, die aus Gesetzen, Verträgen, Standards oder internen Regelwerken resultieren können.¹ Compliance-Anforderungen können Bedingungen an verschiedene Elemente einer Unternehmensarchitektur stellen.² Die Elemente einer Unternehmensarchitektur können wiederum Sichten zugeordnet werden, wobei eine zentrale Sicht die Steuerungssicht ist. Sie verbindet weitere Sichten wie die Daten-, Ressourcen- oder Organisationssicht miteinander³. Die Steuerungssicht wird über Geschäftsprozesse modelliert, die im Wesentlichen aus einer Menge von Geschäftsaktivitäten zum Erreichen eines unternehmerischen Ziels bestehen.⁴ Komponenten einer Informationstechnologie (IT)-Architektur wiederum ermöglichen durch die explizite Unterstützung oder implizite Abbildung einzelner Geschäftsaktivitäten die Ausführung von Geschäftsaktivitäten.⁵

Aus Compliance-Sicht haben Geschäftsprozesse und IT-Komponenten eine Doppelrolle und sind deshalb im Fokus dieser Arbeit. Einerseits können Geschäftsaktivitäten und IT-Komponenten Träger von Compliance-Anforderungen sein⁶. Andererseits ermöglichen Geschäftsaktivitäten und IT-Komponenten ebenso die Sicherstellung von Compliance-Anforderungen.⁷ Daraus ergeben sich wechselseitige Beziehungen zwischen Compliance-Anforderungen, Geschäftsaktivitäten und IT-Komponenten.⁸

Geschäftsaktivitäten, IT-Komponenten oder bestehende Compliance-Anforderungen können durch viele Faktoren, wie Prozessverbesserungen, neue Technologien oder Outsourcing-Entscheidungen entfernt oder durch andere Geschäftsaktivitäten, IT-Komponenten oder Compliance-Anforderungen ersetzt werden.⁹ Jedoch ist die Einhaltung der betroffenen Compliance-Anforderungen weiterhin notwendig, was Mechanismen zur Sicherstellung von Compliance erfordert.¹⁰ Insofern müssen die Auswirkungen auf Compliance durch Änderungen an den genannten Elementen bereits im Vorfeld erkannt und die Konsequenzen zur Entwurfszeit von Geschäftsprozessmodellen berücksichtigt werden, wenn Compliance weiterhin erreicht werden soll.¹¹

Eine manuelle Sicherstellung von Compliance in Geschäftsprozessen unter Berücksichtigung von IT-Komponenten und ihrer Compliance-Anforderungen ist aus zwei Gründen nur mit sehr

¹ Vgl. Turetken et al. 2011, S. 2; Sadiq et al. 2007, S. 149.

² Vgl. Knuplesch et al. 2013a, S. 110; Sadiq et al. 2007, S. 150 f.

³ Vgl. Scheer 1992, S. 109.

⁴ Vgl. u.a. Hammer und Champy 1993, S. 39.

⁵ Vgl. u.a. Scheer 1992, S. 14.

⁶ Vgl. u.a. Klotz 2007, S. 14; Institut der Wirtschaftsprüfer (IDW) (Hg) 2002, S. 1169; Governatori und Sadiq 2009, S. 427.

⁷ Vgl. Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2012, S. 1.

⁸ Vgl. Seyffarth und Kühnel 2020, S. 2; Seyffarth et al. 2018, S. 178.

⁹ Vgl. Fdhila et al. 2015a, S. 2; Rudzajs und Buksa 2011, S. 96; Rinderle et al. 2004, S. 9.

¹⁰ Vgl. Rudzajs und Buksa 2011, S. 97; Governatori und Sadiq 2009, S. 429.

¹¹ Vgl. Sadiq und Governatori 2010 S. 267.

hohem Ressourceneinsatz möglich. Erstens müssen die Verletzungen von Compliance-Anforderungen durch eine Änderung von Geschäftsprozessen und IT-Komponenten identifiziert werden. Diese Identifikation kann durch viele Geschäftsprozessmodelle, große IT-Architekturen und einer Vielzahl von Compliance-Anforderungen nur mit hohem Aufwand manuell durchgeführt werden.¹² Zweitens müssen alle betroffenen Geschäftsprozessmodelle hin zu einem Compliance-konformen Ablauf adaptiert werden, wenn die Verletzung einer Compliance-Anforderung aufgrund einer Änderung identifiziert wurde. Durch die hohe Anzahl von Abhängigkeiten zwischen Geschäftsaktivitäten, IT-Komponenten und Compliance-Anforderungen und einer stetig steigenden Anzahl von Compliance-Anforderungen sind sowohl eine manuelle Identifikation der Auswirkungen auf Compliance als auch eine manuelle Geschäftsprozessadaption nicht praktikabel.¹³ Dementsprechend bedarf es einer Methode zum Erreichen von Compliance trotz des Ersetzens oder Entfernens dieser Elemente.

1.2 Forschungslücke und Ziel

Die benötigte Methode muss verschiedene Aspekte abbilden können. Erstens müssen, analog zur multiperspektivischen Unternehmensmodellierung, Compliance-Anforderungen, Aktivitäten eines Geschäftsprozesses und IT-Komponenten formal in einem Modell abgebildet werden¹⁴. Zweitens müssen die Auswirkungen auf Compliance beim Ersetzen oder Entfernen von Compliance-Anforderungen, Geschäftsaktivitäten und IT-Komponenten bestimmt werden.¹⁵ Drittens muss das betroffene Geschäftsprozessmodell, im Fall einer Compliance-Verletzung, Compliance-konform adaptiert werden.¹⁶

Existierende Ansätze adressieren nur einzelne Teilaspekte des beschriebenen Problems.¹⁷ Einerseits gibt es vielfältige Ansätze zur Modellierung und automatischen Abfrage von Beziehungen sowohl innerhalb als auch zwischen Compliance-Anforderungen, Geschäftsaktivitäten und IT-Komponenten.¹⁸ Davon losgelöst gibt es andererseits kontrollflussbasierte Ansätze zur automatischen Sicherstellung von Compliance in Geschäftsprozessen.¹⁹ Eine Kombination der bestehenden Ansätze ist jedoch aufgrund der fehlenden Interoperabilität existierender Modelle, Methoden und Softwarewerkzeuge nicht ohne weiteres möglich.²⁰

Das Ziel ist eine Methode zur Erreichung von Compliance in IT-gestützten Geschäftsprozessen beim Ersetzen oder Entfernen von Compliance-Anforderungen, Geschäftsaktivitäten oder IT-

¹² Vgl. u.a. Elgammal et al. 2010, S. 17; Ghanavati et al. 2009, S. 133.

¹³ Vgl. Sackmann und Kittel 2015, S. 249; Dijkman et al. 2012, S. 91; Sadiq und Governatori 2010, S. 265.

¹⁴ Vgl. u.a. Winter und Fischer 2006, S. 33 f.; Frank 2002, S. 1662; Scheer 1992, S. 18 f.

¹⁵ Vgl. Seyffarth et al. 2018, S. 176 f.

¹⁶ Vgl. u.a. Sackmann und Kittel 2015, S. 250.

¹⁷ Vgl. Sackmann et al. 2018, S. 410 ff.; Seyffarth et al. 2018, S. 185 f.

¹⁸ Vgl. u.a. Elgammal et al. 2010, S. 17 ff.; Becker et al. 2014, S. 4 ff.; Knuplesch et al. 2015, S. 100 ff.; Rudzajs und Buksa 2011, S. 96 ff.; Koetter et al. 2016, S. 215 ff.

¹⁹ Vgl. u.a. Kittel 2013, S. 971; Kittel et al. 2013b, S. 154 ff.; Kopp et al. 2011, S. 59 ff.; Schumm et al. 2010a, S. 5 ff.; Awad et al. 2009, S. 13 ff.

²⁰ Vgl. Sackmann et al. 2018, S. 418 f.

Komponenten. In dieser Arbeit erfolgt die Erreichung von Compliance zum Zeitpunkt des Modellentwurfs, wodurch bereits vor der Prozessausführung verschiedene Szenarien von Veränderungen und ihre Auswirkungen auf die Erreichung von Compliance getestet werden können. Zur Konkretisierung des Ziels werden folgende Forschungsfragen (FF) als Teilziele abgeleitet:

- FF 1: Wie können Compliance-Anforderungen, ein Geschäftsprozessmodell und IT-Komponenten und ihre Beziehungen in einem Modell modelliert werden?
- FF 2: Wie können die Auswirkungen auf die Erhaltung von Compliance identifiziert werden, die durch das Ersetzen oder Entfernen von Compliance-Anforderungen, Geschäftsaktivitäten oder IT-Komponenten entstehen können?
- FF 3: Wie können Geschäftsprozessmodelle zur Entwurfszeit Compliance-konform adaptiert werden?

1.3 Methode und Ergebnisse

Die Dissertation folgt dem Forschungsparadigma des Design Science Research (DSR). Die Ziele von DSR sind das Lösen wichtiger, ungelöster Probleme oder das effizientere Lösen bereits gelöster Probleme durch den Entwurf und die Entwicklung neuer Artefakte²¹. Die entwickelten Artefakte und ihre Demonstration in einem Softwareprototyp passen bestehende Modelle, Konstrukte, Methoden und Softwarebibliotheken zur Lösung des oben beschriebenen und bis jetzt ungelösten Problems an. Letztendlich leistet diese Arbeit einen Wissensbeitrag des Typs „Exaptation“²² durch folgende Ergebnisse:

1. Es wird die Methode MIA (Modellieren, Identifizieren, Adaptieren) zur Erreichung von Compliance in flexiblen und IT-gestützten Geschäftsprozessen präsentiert. Sie ermöglicht das Modellieren der genannten Modelle und ihrer Beziehungen in einem gemeinsamen Modell. Zur Erreichung von Compliance können sowohl Compliance-Anforderungen als auch Compliance-Verletzungen identifiziert werden. Beim Ersetzen von Geschäftsaktivitäten oder IT-Komponenten müssen Compliance-Anforderungen beachtet werden. Beim Entfernen von Elementen wiederum können Compliance-Verletzungen auftreten. Im Fall einer Compliance-Verletzung werden Vorschläge für einen Compliance-konformen Ablauf des Geschäftsprozesses unterbreitet.
2. Die Umsetzbarkeit von MIA wurde in dem Softwareprototypen BCIT demonstriert.
3. Die wahrgenommene Nützlichkeit von BCIT und der darunter liegenden Methode MIA wurde von Domänenexpert:innen in mehreren Fallstudien positiv evaluiert.

1.4 Aufbau der Arbeit

Der Aufbau der Arbeit orientiert sich an dem Vorschlag von Gregor und Hevner (2013) zur Strukturierung von DSR-Projekten.²³ Die Problemdefinition erfolgte in der Einleitung. In Kapitel 2 werden die grundlegenden Konzepte erläutert. Darauf aufbauend werden in Kapitel 3 der Stand der

²¹ Vgl. Hevner et al. 2004, S. 85; March und Smith 1995, S. 256.

²² Vgl. Gregor und Hevner 2013, S. 345.

²³ Vgl. Gregor und Hevner 2013, S. 350.

Forschung präsentiert und die Forschungslücke abgeleitet. Anschließend wird in Kapitel 4 das Forschungsdesign zur Entwicklung von MIA vorgestellt. Die entwickelten Kernartefakte der Dissertation werden zueinander in Beziehung gestellt und ihren Publikationen zugeordnet. In Kapitel 5 werden der Entwurf und die Entwicklung der Kernartefakte beschrieben. Die Evaluation der Kernartefakte erfolgte teilweise bereits während ihrer Entwicklung. Daher werden in Kapitel 6 zunächst die formativen Evaluationsepisoden in das Framework zur Evaluation von Design Science Research-Projekten nach Venable et al. (2016)²⁴ eingeordnet und kurz vorgestellt. Im Anschluss werden der Fallstudienaufbau und die -ergebnisse der abschließenden summativen Evaluation vorgestellt. In Kapitel 7 erfolgen die Diskussion der Limitationen von MIA sowie ihrer Implikationen für Wissenschaft und Praxis. Die Arbeit endet mit der Schlussbetrachtung in Kapitel 8.

²⁴ Venable et al. 2016, S. 77 ff.

2 Wechselwirkungen zwischen Compliance, Geschäftsprozessen und IT

In diesem Kapitel werden zunächst der Zusammenhang zwischen Compliance und Geschäftsprozessen sowie Strategien zur Überprüfung und Sicherstellung von Compliance in Geschäftsprozessen erläutert. Danach werden kurz der Zusammenhang zwischen Compliance und IT beschrieben bevor im Anschluss Veränderungsmuster vorgestellt werden. Das Kapitel endet mit einem Ausgangsszenario, das die Wechselwirkungen zwischen Compliance, Geschäftsprozesse und IT anhand eines internen Bestellprozesses zeigt.

2.1 Compliance

Compliance bezeichnet die Einhaltung von Compliance-Anforderungen, die aus Gesetzen, Regularien, Verträgen, etc. resultieren.²⁵ Compliance-Anforderungen haben ihren Ursprung in Compliance-Quellen und können durch weitere Compliance-Anforderungen spezialisiert werden.²⁶ Gesetze können so bspw. durch Regularien oder Bekanntmachungen spezialisiert werden.²⁷ Sollten verschiedene Compliance-Anforderungen im Kern die gleiche Bedingung stellen, können sie durch eine interne Compliance-Anweisung spezialisiert werden. Sowohl die Datenschutzgrundverordnung²⁸ (DSGVO) als auch das Institut der Wirtschaftsprüfer²⁹ stellen u.a. Bedingungen bezüglich einer Datensicherung. Sollten in einem Geschäftsprozess sowohl personenbezogene als auch rechnungslegungsrelevante Daten verarbeitet werden, können diese Compliance-Anforderungen in einer internen Compliance-Anforderung spezialisiert werden. Darüber hinaus können auch Verweise innerhalb eines Gesetzes auftreten, indem Paragraphen eines Gesetzes auf andere Paragraphen des gleichen Gesetzes verweisen³⁰.

2.1.1 Business Process Compliance

Business Process Compliance (BPC) bezeichnet die Einhaltung von Compliance-Anforderungen in Geschäftsprozessen.³¹ Ein Geschäftsprozess ist eine Menge von Geschäftsaktivitäten, die zur Erreichung eines unternehmerischen Ziels einen Input in einen Output wandeln.³² Compliance-Anforderungen können Bedingungen an Elemente eines Geschäftsprozesses stellen, die verschiedenen Sichten, wie dem Kontrollfluss, der Daten- und Organisationssicht oder die Zeit, zugeordnet werden.³³

Compliance in Geschäftsprozessen kann grundsätzlich zu verschiedenen Zeitpunkten überprüft werden. Compliance kann zur Entwurfszeit des Prozessschemas, zur Laufzeit der Prozessinstanz oder nach der Ausführung der Prozessinstanz überprüft werden.³⁴ Jedoch ist es nicht

²⁵ Vgl. u.a. Elgammal et al. 2012, S. 32; Turetken et al. 2011, S. 3; Lu et al. 2008, S. 120.

²⁶ Vgl. u.a. Schultz 2013b, S. 143; Turetken et al. 2011, S. 7; Schumm et al. 2010c, S. 327.

²⁷ Vgl. Institut der Wirtschaftsprüfer (IDW) (Hg) 2002, S. 1169.

²⁸ Artikel 32, 1c DSGVO.

²⁹ IDW PS 330, Tz. 59.

³⁰ Vgl. u.a. Sillaber und Brey 2012, S. 1313.

³¹ Vgl. Governatori und Sadiq 2009, S. 427.

³² Vgl. Hammer und Champy 1993, S. 39.

³³ Vgl. u.a. Knuplesch et al. 2013a, S. 110; Sadiq et al. 2007, S. 150 f.

³⁴ Vgl. Governatori und Sadiq 2009, S. 429; El Kharbili et al. 2008, S. 108 ff.

möglich, jede Art von Compliance-Anforderung zu allen Zeitpunkten zu überprüfen.³⁵ Die Überprüfung zur Entwurfszeit ermöglicht das Verhindern von Compliance-Verstößen durch eine Adaption des Prozessschemas vor der Prozessausführung.³⁶ Die Überprüfung zur Laufzeit ermöglicht es mehr Informationen zu berücksichtigen, als zum Entwurfszeitpunkt zur Verfügung stehen.³⁷ Die Überprüfung nach der Ausführung kann auf Basis von Logdateien ausgeführter Prozessinstanzen erfolgen.³⁸ Wie bereits in der Einleitung erwähnt, erfolgt in dieser Arbeit die Überprüfung zum Zeitpunkt des Modellentwurfs, weil dadurch die Auswirkungen auf die Erhaltung von Compliance in unterschiedlichen Szenarien bestimmt werden können.

Zur Prüfung von Compliance-Anforderungen gegen Geschäftsprozessmodelle müssen die Anforderungen in Compliance-Regeln formalisiert sein.³⁹ Mit dem Model Checking, das auf Basis deontischer oder temporaler Logik ausgeführt werden kann, und dem Model Querying, auf Basis einer Graphensuche, existieren dafür zwei Verfahrensklassen.⁴⁰ Beim Model Checking werden Geschäftsprozesse in einem endlichen Zustandsautomaten überführt, der wiederum gegen Regeln geprüft wird. Unterschiedliche Regelsprachen, wie Linear Temporal Logic (LTL), Past-LTL (PLTL) oder Formal Contract Language (FCL), können nur bestimmte Sichten eines Geschäftsprozesses abbilden.⁴¹ Im Gegensatz dazu werden beim Model Querying Compliance-Regeln in Teilgraphen überführt, die gegen den Graphen des Geschäftsprozessmodells geprüft werden.⁴² Einerseits wird damit die Einschränkung der Abbildungsfähigkeit von Regelsprachen gelöst und andererseits können die Ursachen der Compliance-Verletzung ermittelt werden. Eine Compliance-Verletzung liegt vor, wenn der Geschäftsprozess oder dessen Ausführung nicht den Compliance-Anforderungen entspricht, die Bedingungen an ihn stellen⁴³. Dementsprechend wird das Model Querying als konzeptuelle Basis für die Bearbeitung von FF 2 genutzt.

In einem Geschäftsprozess werden Compliance-Anforderungen durch Compliance-konforme Prozessfragmente operationalisiert. In der Literatur werden Compliance-konforme Prozessfragmente auch (Internal) Controls, Kontrollen, Kontrollprozesse oder Compliance-Prozesse bezeichnet, wobei sie im weiteren Verlauf der Arbeit als Compliance-Prozesse bezeichnet werden.⁴⁴ Ein Compliance-Prozess besteht aus mindestens einer Compliance-Aktivität zur Sicherstellung von Compliance-Anforderungen.⁴⁵

³⁵ Vgl. u.a. Pretschner et al. 2006, S. 41 f.

³⁶ Vgl. Reichert und Weber 2012, S. 46; Governatori und Sadiq 2009, S. 429.

³⁷ Vgl. u.a. Kittel 2013, S. 974; van der Aalst, W. M. P. et al. 2009, S. 102.

³⁸ Vgl. van Aalst 2011, S. 191 ff.

³⁹ Vgl. u.a. van der Aalst, W. M. P. et al. 2009, S. 102 ff.; Governatori und Sadiq 2009, S. 448 ff.

⁴⁰ Vgl. u.a. Elgammal et al. 2016, S. 121 ff.; Elgammal et al. 2012, S. 32; Governatori und Sadiq 2009, S. 447.

⁴¹ Vgl. u.a. Elgammal et al. 2016, S. 121 ff.; Liu et al. 2007, S. 345 ff.

⁴² Vgl. u.a. Elgammal et al. 2016, S. 121 ff.; Breuker et al. 2015, S. 73.

⁴³ Vgl. u.a. Hashmi et al. 2016, S. 430; Governatori und Sadiq 2009, S. 427; Hilty et al. 2005, S. 110.

⁴⁴ Vgl. Seyffarth et al. 2017a, S. 72; Schultz 2013b, S. 139; Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2012, S. 1; Kittel und Sackmann 2012, S. 1679; Schumm et al. 2010c S. 327.

⁴⁵ Vgl. Seyffarth et al. 2017a, S. 72.

Im Falle einer festgestellten Compliance-Verletzung müssen Geschäftsprozesse hin zu einem Compliance-konformen Ablauf adaptiert werden.⁴⁶ Einerseits können dazu die Position der Compliance-Prozesse innerhalb eines Geschäftsprozessmodells sowie dessen Geschäftsaktivitäten geändert oder Compliance-Prozesse und Geschäftsaktivitäten entfernt werden.⁴⁷ Andererseits können das Geschäfts- und Compliancemanagement teilweise voneinander entkoppelt werden.⁴⁸ Das ermöglicht u.a. eine getrennte Modellierung von Compliance- und Geschäftsprozessmodellen. Passende Compliance-Prozesse können dann zur Entwurfs- oder Laufzeit des Geschäftsprozessmodells in das Geschäftsprozessmodell integriert werden.⁴⁹

Im Vergleich zur Modellierung Compliance-konformer Geschäftsprozessmodelle ohne Unterscheidung zwischen Geschäfts- und Compliance-Prozessen bietet die Integration getrennt modellierter Compliance-Prozesse einige Vorteile. Zum einen können die Varianten verschiedener Compliance-Prozesse einfacher verwaltet werden. Zum anderen können Compliance-Prozesse in anderen Geschäftsprozessen wiederverwendet werden⁵⁰. Darüber hinaus kann eine Compliance-Sicht auf Geschäftsprozesse definiert werden, was zu übersichtlicheren Geschäftsprozessmodellen führen kann.⁵¹ Daher dient die Integration separater Compliance-Prozesse als konzeptionelle Basis für die Bearbeitung von FF 3. Jedoch kann es vorkommen, dass Geschäfts- und Compliance-Ziele sich überlappen. Aus diesem Grund wird die getrennte Modellierung der beiden Sichten auf Anwendungsfälle beschränkt, bei denen das nicht der Fall ist.⁵²

2.1.2 IT-Compliance

Neben Bedingungen an Geschäftsprozesse können Compliance-Anforderungen auch Bedingungen an IT-Komponenten stellen.⁵³ Der Zustand, in dem alle Komponenten einer IT-Architektur alle relevanten Compliance-Anforderungen einhalten, wird als IT-Compliance bezeichnet.⁵⁴ Da es aus Compliance-Sicht keine Unterscheidung zwischen verschiedenen Typen von IT-Komponenten⁵⁵, wie Hardware-, Software-, oder Netzwerkkomponenten gibt, wird im weiteren Verlauf der Arbeit ausschließlich von IT-Komponenten gesprochen.

Zur Sicherstellung von IT-Compliance-Anforderungen werden ebenfalls Compliance-Prozesse verwendet.⁵⁶ Sie werden in der Literatur auch als IT General Controls oder IT-Kontrollen bezeichnet und werden teilweise unabhängig von einem Geschäftsprozess ausgeführt.⁵⁷ Im weiteren

⁴⁶ Vgl. Sadiq und Governatori 2010, S. 265.

⁴⁷ Vgl. u.a. Awad et al. 2009, S. 10 ff.

⁴⁸ Vgl. u.a. Ramezani et al. 2012b, S. 460; Turetken et al. 2011, S. 4 ff.

⁴⁹ Vgl. Kittel et al. 2013b, S. 155 f.; Schumm et al. 2010c, S. 332 ff.

⁵⁰ Vgl. Dijkman et al. 2012, S. 92; Schumm et al. 2010c, S. 327.

⁵¹ Vgl. Schumm et al. 2010b, S. 136.

⁵² Vgl. Seyffarth et al. 2019, S. 229.

⁵³ Vgl. ISACA (Hg) 2012, S. 51; Institut der Wirtschaftsprüfer (IDW) (Hg) 2002, S. 1169.

⁵⁴ Vgl. Klotz 2007, S. 14.

⁵⁵ Vgl. Winter und Fischer 2006, S. 33 f.

⁵⁶ Vgl. Seyffarth et al. 2017a, S. 80 f.

⁵⁷ Vgl. ISACA (Hg) 2012, S. 51 ff.; Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2012, S. 98 ff.; Riesner und Pernul 2010, S. 4; Institut der Wirtschaftsprüfer (IDW) (Hg) 2002, S. 1175 ff.

Verlauf der Arbeit werden nur Compliance-Prozesse betrachtet, die in den Geschäftsprozess integriert werden.

2.1.3 Fazit

Zur Erhaltung von Compliance in IT-gestützten Geschäftsprozessen müssen die Themengebiete Business Process Compliance und IT-Compliance berücksichtigt werden, da Compliance-Anforderungen sowohl Bedingungen an Geschäftsprozessen als auch IT-Komponenten stellen können. An dieser Stelle setzt die Methode MIA an, die beide Themengebiete sowie die Doppelrolle der IT berücksichtigt. Einerseits werden die Auswirkungen auf die Erhaltung von Compliance durch das Ersetzen und Entfernen von Compliance-Anforderungen, Aktivitäten und IT-Komponenten identifiziert. Zu diesen Auswirkungen gehören auch IT-Compliance-Anforderungen, die beim Ersetzen von IT-Komponenten berücksichtigt werden müssen. Andererseits werden mögliche Compliance-Verletzungen des Geschäftsprozesses durch das Entfernen von IT-Komponenten identifiziert. Sollte eine Compliance-Verletzung festgestellt werden, wird sofern möglich, der Geschäftsprozess unter Berücksichtigung von IT-Komponenten zu einem Compliance-konformen Ablauf adaptiert.

2.2 Veränderungsmuster

In (Fdhila et al. 2012) werden strukturelle Muster zur Veränderung des Kontrollflusses von Geschäftsprozessen in die Kategorien „Element einfügen“, „Element entfernen“ und „Element ersetzen“ eingeteilt. Das Muster „Element einfügen“ ergänzt das Modell um ein neues Element. Das Muster „Element ersetzen“ entfernt ein bestehendes Element und fügt an dessen Stelle ein neues Element ein. Das Muster „Element entfernen“ hingegen löscht ein Element. Neben diesen strukturellen Mustern wird außerdem das semantische Muster „Element updaten“ vorgeschlagen, das Eigenschaften von bestehenden Elementen verändert.⁵⁸

Im weiteren Verlauf werden die Auswirkungen der Veränderungsmuster auf die Erhaltung von Compliance beschränkt, da die Identifikation der Auswirkungen auf die Ausführbarkeit von Geschäftsaktivitäten durch eine Veränderung von Geschäftsaktivitäten und IT-Komponenten bereits durch Arbeiten der Business Impact Analyse diskutiert wurden.⁵⁹ Außerdem beschränken sich die weiteren Ausführungen auf die Muster „Element ersetzen“ und „Element entfernen“. Die Auswirkungen auf die Erhaltung von Compliance durch die Muster „Element einfügen“ und „Element updaten“ können dennoch implizit bestimmt werden. Das Muster „Element einfügen“ kann durch das zweimalige Anwenden der Muster „Element ersetzen“ und „Element entfernen“ umgesetzt werden. Die Voraussetzung dafür ist die Modellierung der notwendigen Beziehungen zwischen dem neuen Element und den bestehenden Elementen in dem gemeinsamen Compliance-Modell. Die Anwendung der Muster „Element ersetzen“ und „Element einfügen“ erfolgt in dem Compliance-Modell sowohl vor als auch nach dem Einfügen des neuen Elements. Aus der Differenz der Analyseergebnisse kann die Auswirkung auf die Erreichung von Compliance durch

⁵⁸ Vgl. Fdhila et al. 2012, S. 455.

⁵⁹ Vgl. u.a. Radeschütz et al. 2015, S.; BSI (Hg) 2008, S. 28 ff.

das Einfügen des neuen Elements bestimmt werden. Ähnlich verhält es sich mit dem Muster „Element updaten“. Sollte eine Veränderung von Eigenschaften an einem Element zu strukturellen Änderungen im gemeinsamen Compliance-Modell führen, müssen diese modelliert werden. Anschließend können die Auswirkungen auf die Erhaltung von Compliance analog der Anwendung des Musters „Element einfügen“ bestimmt werden.

2.3 Ausgangsszenario

Abbildung 1 zeigt einen stark vereinfachten internen Bestellprozess, dessen Komplexität jedoch zur Erläuterung von MIA ausreichend ist.⁶⁰ Die Geschäftsaktivitäten des Bestellprozesses werden durch IT-Komponenten unterstützt, die wiederum Abhängigkeiten untereinander haben. Außerdem stellen verschiedene Compliance-Anforderungen Bedingungen an Geschäftsaktivitäten und IT-Komponenten. Der Prozess ist als Business Process Model and Notation (BPMN)-Modell abgebildet. Die IT-Komponenten sind durch Dreiecke visualisiert, da BPMN keine Modellierung von Beziehungen zwischen IT-Komponenten erlaubt⁶¹. Außerdem sind Compliance-Anforderungen als Rechtecke visualisiert, weil BPMN keine Modellierung von Beziehungen zwischen einzelnen Dokumenten erlaubt.⁶²

Eine Unternehmensarchitektur und ein Geschäftsprozess bestehen selbstverständlich aus mehr Ebenen respektive Sichten als aus einer IT-Architektur, einer Kontrollflusssicht auf Prozesse und einer Compliance-Sicht.⁶³ Die Fokussierung von MIA auf diese drei Sichten erfolgt jedoch aus zwei Gründen. Erstens können IT-Komponenten sowohl für die Ausführung von Aktivitäten eines Geschäftsprozesses als auch für die Ausführung von Compliance-Prozesse notwendig sein. Zweitens können Compliance-Anforderungen Bedingungen sowohl an Geschäftsaktivitäten als auch IT-Komponenten stellen.⁶⁴

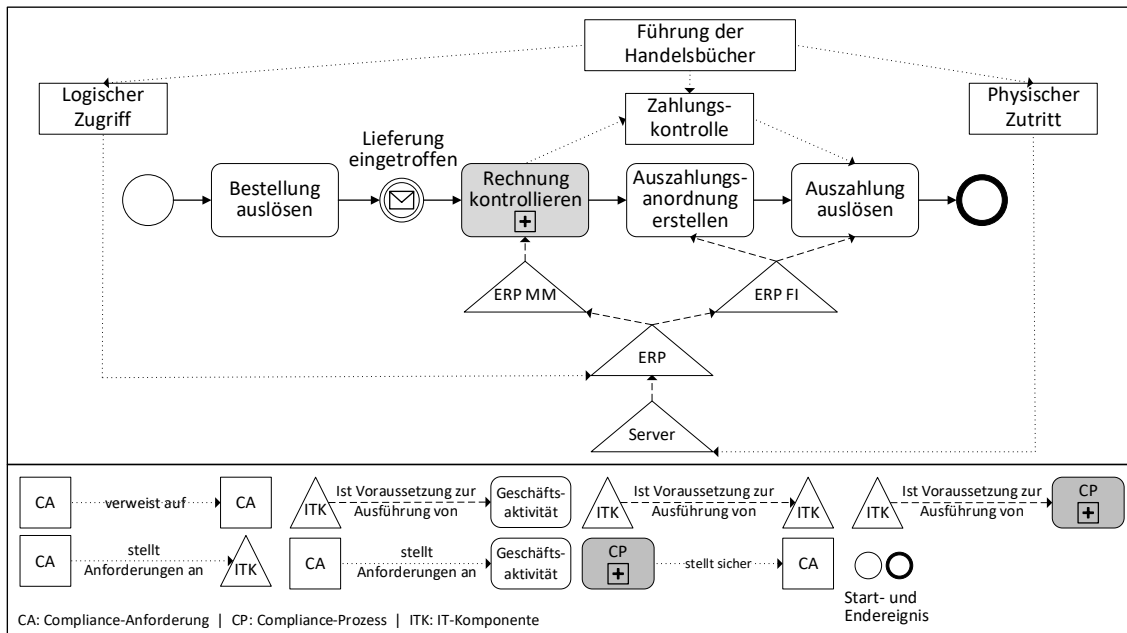
⁶⁰ Vgl. Seyffarth und Kühnel 2020, S. 4.

⁶¹ Vgl. OMG (Hg) 2011, S. 209.

⁶² Vgl. OMG (Hg) 2011, S. 205.

⁶³ Vgl. Winter und Fischer 2006, S. 33 f.; Scheer 1992, S. 18 f.

⁶⁴ Vgl. u.a. Weske 2019, S. 52; Governatori und Sadiq 2009, S. 427; Institut der Wirtschaftsprüfer (IDW) (Hg) 2002, S. 1169.

Abbildung 1. Interner Bestellprozess⁶⁵

Die Compliance-Anforderung „Führung der Handelsbücher“⁶⁶ stellt Bedingungen an die Führung der Handelsbücher. Sie wird durch die Compliance-Anforderungen „Logischer Zugriff“ und „Physischer Zutritt“ spezialisiert. Der „Logische Zugriff“⁶⁷ und „Physische Zutritt“⁶⁸ beschreiben Anforderungen an den Zugriffsschutz von Applikationen und die Zutrittsbeschränkung von Hardware im Fall einer IT-gestützten Führung der Handelsbücher. Die „Zahlungskontrolle“ stellt Bedingungen an die Geschäftsaktivität „Auszahlung auslösen“ und wird durch den Compliance-Prozess „Rechnung kontrollieren“ sichergestellt. Zur Ausführung des Compliance-Prozesses wird die IT-Komponente Materialmanagement-Modul eines Enterprise Resource Planning-Systems (ERP MM) benötigt, die wiederum die IT-Komponente „ERP“ für ihre Ausführung benötigt. Die IT-Komponente „ERP“ wird auf der IT-Komponente „Server“ ausgeführt. Außerdem werden weitere Geschäftsaktivitäten durch das Finanzmodul eines ERP-Systems (ERP FI) unterstützt.

Das Ausgangsszenario zeigt die Doppelrolle der IT. Auf der einen Seite sind die IT-Komponenten Server und ERP Träger der Compliance-Anforderungen „Führung der Handelsbücher“, „Logischer Zugriff“ und „Physischer Zutritt“. Auf der anderen Seite werden die IT-Komponenten zur Sicherstellung der Compliance-Anforderungen „Zahlungskontrolle“ und „Führung der Handelsbücher“ benötigt. Die Sicherstellung von Compliance-Anforderungen durch IT-Komponenten geschieht dabei immer durch die Unterstützung eines Compliance-Prozesses. Einerseits können IT-Komponenten Personen bei der Ausführung ihrer Aktivitäten, bspw. durch den Abgleich der

⁶⁵ In Anlehnung an Seyffarth und Kühnel 2020, S. 5.

⁶⁶ §§ 238, 239 HGB.

⁶⁷ IDW PS 330, Tz. 57.

⁶⁸ IDW PS 330, Tz. 54.

Rechnungsdaten mit den Bestelldaten in ERP MM, unterstützen. Andererseits können IT-Komponenten auch Prozesse in Form von Skripten ausführen, bei denen jeder Befehl als eigene Aktivität angesehen werden kann⁶⁹.

Viele Ereignisse, wie Outsourcing-Entscheidungen, Prozessverbesserungen oder der Ausfall einer IT-Komponente, können zum Ersetzen oder Entfernen von Elementen des Ausgangsszenarios führen. Ein Element ist entweder eine Compliance-Anforderung, eine Geschäftsaktivität, ein Compliance-Prozess oder eine IT-Komponente. Tabelle 1 beinhaltet exemplarisch einige betriebswirtschaftliche Fragen, die durch diese Veränderungen gestellt werden können. MIA hilft bei der Beantwortung dieser Fragen.

Tabelle 1. Fragen, die durch MIA beantwortet werden können

	Ersetzen	Entfernen
Compliance-Anforderung	Welchen nationalen und internationalen Compliance-Anforderungen müssen bei dem Ersetzen der Zahlungskontrolle durch eine neue interne Compliance-Anforderung beachtet werden?	Welche Compliance-Prozesse und Compliance-Anforderungen werden obsolet, wenn die Führung der Handelsbücher durch eine Verlagerung des Firmenstandortes in das Ausland nicht mehr beachtet werden muss?
Geschäftsaktivität	Welche Compliance-Anforderungen und Compliance-Prozesse müssen beachtet werden, wenn die Geschäftsaktivität „Auszahlung auslösen“ im Rahmen einer Prozessverbesserung ersetzt wird?	Welche Compliance-Anforderungen werden obsolet, wenn die Geschäftsaktivität „Bestellung auslösen“ in einem anderen Geschäftsprozess ausgeführt wird?
In Geschäftsprozess integrierter Compliance-Prozess	Welche Compliance-Anforderungen müssen explizit und implizit beachtet werden, wenn der Compliance-Prozess „Rechnung kontrollieren“ durch einen manuell ausgeführten Compliance-Prozess ersetzt wird?	Welche Compliance-Verletzungen treten auf, wenn der Compliance-Prozess „Rechnung kontrollieren“ durch einen Ausfall der IT-Komponente „ERP MM“ nicht mehr ausgeführt werden kann?
IT-Komponente	Welchen Compliance-Anforderungen müssen beachtet werden, wenn die IT-Komponente „ERP MM“ im Rahmen eines Outsourcings ersetzt wird?	Welche Compliance-Verletzungen treten auf, wenn die IT-Komponente „ERP MM“ durch ein fehlgeschlagenes Update nicht mehr zur Verfügung steht und das Zahlungsziel der Rechnung weiterhin eingehalten werden soll?

⁶⁹ Vgl. u.a. Gadatsch 2017, S. 81; OMG (Hg) 2011, S. 164.

3 Stand der Forschung

In diesem Kapitel wird zunächst die Methode zur Ermittlung des Forschungsstands erläutert. Anschließend wird der Stand der Forschung beschrieben, in Folge dessen die Forschungslücke abgeleitet wird.

3.1 Ermittlung des Forschungsstands

Der Forschungsstand wurde durch zwei strukturierte Literatursuchen nach vom Brocke et al.⁷⁰ ermittelt. In der ersten Literatursuche wurde der Fokus auf BPC unter Beachtung von IT gelegt. In der zweiten Literatursuche wurde der Fokus geweitet, indem keine Berücksichtigung von IT mehr stattfand⁷¹. Das Vorgehen zur Relevanzklassifikation ist in beiden Suchen ähnlich. Nach dem Entfernen der Dubletten erfolgte die erste Relevanzklassifikation anhand des Titels und des Abstracts. Die zweite Relevanzklassifikation erfolgte durch das vollständige Lesen der Beiträge. Tabelle 2 und Tabelle 3 zeigen die verwendeten Suchbegriffe und Datenbanken mit den entsprechenden Treffern.

Nach dem Entfernen von Dubletten der relevanten Treffer aus den beiden Literatursuchen und einer Rückwärtssuche, die zu weiteren 4 relevanten Beiträgen führte, sind 35 Beiträge relevant. Im Folgenden werden zunächst Methoden zur Identifikation von Zusammenhängen zwischen Compliance-Anforderungen, einem Geschäftsprozessmodell und IT-Komponenten diskutiert. Anschließend werden Methoden zur automatischen Geschäftsprozessadaption durch separat modellierte Compliance-Prozesse vorgestellt. Aus den vorgestellten Arbeiten wird am Ende des Kapitels die Forschungslücke abgeleitet.

Tabelle 2. Ergebnisse der ersten Literatursuche

Suchbegriff	Datenbank	Anzahl
<<("business process compliance" OR BPC) AND ("information technology" OR flexibility OR query OR change)>>	AIS Electronic Library	62
	EBSCOHost, Academic Search Premier	67
	EBSCOHost, Business Source Premier	45
	EBSCOHost, Information Science and Technology	3
	IEEEXplore	136
	Springer Link	257
Treffer		570
Unique Treffer		552
Relevante Treffer anhand Titel und Abstract		80
Relevante Treffer nach Lesen des Beitrags		28

⁷⁰ Vom Brocke et al. 2009.

⁷¹ Vgl. Sackmann et al. 2018, S. 411 ff.

Tabelle 3. Ergebnisse der zweiten Literatursuche⁷²

Suchbegriff	Datenbank	Anzahl
<<compliance AND "business process">>	ACM Digital Library	54
	AIS Electronic Library	44
	EBSCOHost, Academic Search Premier	91
	EBSCOHost, Business Source Premier	7
	EBSCOHost Information Science and Technology	27
"business process compliance"	Springer Link	29
Treffer		252
Unique Treffer		232
Relevante Treffer anhand Titel und Abstract		27
Relevante Treffer nach Lesen des Beitrags		3

3.2 Methoden zur Modellierung und Identifikation

3.2.1 Mustersuche in Prozessmodellen

Viele Beiträge befassen sich mit der Identifikation von Mustern in Prozessmodellen.⁷³ Die Mustersuche bezieht sich sowohl auf den Kontrollfluss des Prozessmodells⁷⁴ als auch auf weitere Prozesssichten, wie der Daten- oder Organisationssicht.⁷⁵ Da diese Ansätze jedoch nicht den Einfluss des Ersetzen und Entfernen eines Elements auf die Erreichung von Compliance berücksichtigen, werden sie nicht weiter diskutiert.

3.2.2 Modellieren und Identifizieren von Abhängigkeiten zwischen Compliance-Anforderungen

Einige Arbeiten befassen sich mit der Modellierung und Identifikation von Abhängigkeiten zwischen Compliance-Anforderungen. (El Kharbili und Stolarski 2009) präsentieren eine Ontologie zur Modellierung und Abfrage der Beziehungen zwischen Compliance-Anforderungen.⁷⁶ In (Ghanavati et al. 2014) wird die Legal-goal oriented Requirement Language, eine Sprache zur Modellierung der Zusammenhänge in Paragraphen von Gesetzes, vorgestellt die verschiedene Compliance-Anforderungen miteinander verbinden kann.⁷⁷ In (Barboza et al. 2016) wird eine Methode vorgeschlagen, bestehende Compliance-Anforderungen manuell miteinander zu verbinden. Die resultierenden Zusammenhänge werden in einer eXtensible Markup Language (XML)-Struktur gespeichert und können mit XQuery abgefragt werden.⁷⁸ Außerdem gibt es Arbeiten, die Zusammenhänge in Compliance-Regeln modellieren und identifizieren. (Elgammal et al. 2010) schla-

⁷² In Anlehnung an Sackmann et al. 2018, S. 414.

⁷³ Eine Übersicht von Beiträgen ist bspw. in Breuker et al. 2015, S. 79 enthalten.

⁷⁴ Vgl. u.a. Fellmann et al. 2011, S 65 ff.; Gacitua-Decar und Pahl 2009, S. 112 f.; Awad et al. 2008, S. 332 f.; Awad 2007, S. 118 ff.

⁷⁵ Vgl. u.a. Riehle et al. 2017a; Delfmann et al. 2015a, S. 480 ff.; Delfmann et al. 2015b, S. 135 ff.; Bräuer et al. 2013, S. 1249 ff.

⁷⁶ Vgl. El Kharbili und Stolarski 2009, S. 270 ff.

⁷⁷ Vgl. Ghanavati et al. 2014, S. 2ff.

⁷⁸ Vgl. Barboza et al. 2016, S. 233 ff.

gen eine Methode zur Identifikation der Ursache von Compliance-Verletzungen in zusammengesetzten LTL-Regeln vor⁷⁹. (Halle 2011) präsentieren ein ähnliches Verfahren für LTL-First-Order-Regeln.⁸⁰ Beide Arbeiten werden trotz ihrer Betrachtung von Compliance-Regeln berücksichtigt, da sie Methoden präsentieren, die Verweise zwischen Compliance-Regeln abbilden und abfragen können.

3.2.3 Modellieren und Identifizieren von Abhängigkeiten zwischen Compliance-Anforderungen und Geschäftsprozessen

Compliance-Anforderungen können in zwei Arten mit dem Geschäftsprozessmodell verbunden werden. Auf der einen Seite können die Beziehungen zwischen dem Geschäftsprozessmodell und Compliance-Anforderungen explizit über einen Link zwischen den Elementen modelliert werden. Auf der anderen Seite können Abhängigkeiten implizit über eine Compliance-Regel abgebildet werden.⁸¹ Bei der Modellierung von Compliance-Anforderungen gegenüber dem Geschäftsprozessmodell werden nur Arbeiten berücksichtigt, die Beziehung zwischen Compliance-Anforderungen und Geschäftsprozessmodellen explizit abbilden. Das Abbilden der Beziehung über Regeln und Model Checking ist eine implizite Abbildung und wird nicht berücksichtigt, da die Ursache der Regelverletzung nicht festgestellt werden kann.⁸²

Einige Beiträge schlagen die Modellierung von Risiken auf Geschäftsprozessen vor. Sie werden berücksichtigt, da das Risiko neben der Compliance-Quelle ebenfalls der Ursprung einer Compliance-Anforderung sein kann⁸³. (Zur Muehlen und Rosemann 2005) und (Jakoubi et al. 2010) integrieren jeweils Risiken in Geschäftsprozessmodelle auf konzeptioneller Ebene.⁸⁴ (Weiß und Winkelmann 2011) erweitern eine Semantic Business Process Modeling Language um eine Risikoperspektive.⁸⁵ (Pittl et al. 2017) annotieren über eine Ontologie Geschäftsprozessmodelle mit Informationen einer Risikodatenbank und können damit die Beziehungen zwischen Geschäftsaktivitäten und Risiken abfragen.⁸⁶

(Riehle et al. 2017b) schlagen eine Methode zur automatischen Annotation von Geschäftsprozessmodellen mit Domänenontologien vor, welche den Autoren zufolge auch Compliance-Anforderungen beinhalten kann.⁸⁷ In (Pham und Le Thanh 2016) werden Geschäftsprozessmodelle und Compliance-Regeln jeweils in eine Ontologie transformiert. Die beiden Ontologien werden anschließend verbunden, wodurch die Zusammenhänge zwischen Geschäftsprozess und Compliance-Regeln abgefragt werden können.⁸⁸ Einen ähnlichen Ansatz verfolgen (Corea und Delf-

⁷⁹ Vgl. Elgammal et al. 2010, S. 21 ff.

⁸⁰ Vgl. Halle 2011, S. 174 ff.

⁸¹ Vgl. Gaidukovs und Kirikova 2015, S. 347.

⁸² Vgl. u.a. Riehle 2018, S. 412; Gaidukovs und Kirikova 2015, S. 347.

⁸³ Vgl. u.a. Schumm et al. 2010c, S. 328; Namiri und Stojanovic 2007a, S. 63.

⁸⁴ Vgl. Zur Muehlen und Rosemann 2005, S. 7f; Jakoubi et al. 2010, S. 119 ff.

⁸⁵ Vgl. Weiß und Winkelmann 2011, S. 3 f.

⁸⁶ Vgl. Pittl et al. 2017, S. 329 ff.

⁸⁷ Vgl. Riehle et al. 2017b, S. 179 ff.

⁸⁸ Vgl. Pham und Le Thanh 2016, S. 13 ff.

mann 2017), die Compliance-Regeln über eine Ontologie auf dem Geschäftsprozessmodell verbinden. Die Compliance-Regel bleibt bei ihrem Ansatz erhalten und kann weiterhin per Model Checking gegen den Geschäftsprozess geprüft werden.⁸⁹

In (Ghanavati et al. 2010) schlagen die Autoren ein Framework zur Verbindung von Compliance-Anforderungen und Geschäftsprozessen vor.⁹⁰ In (Ghanavati et al. 2009) präsentieren sie dieses Framework mit einer Methode, welche die Zusammenhänge zueinander in Beziehung stehender Compliance-Anforderungen und der verlinkten Geschäftsprozesse auf Aktivitätsebene abfragen kann.⁹¹

(Rudzajs und Buksa 2011) bilden Compliance-Anforderungen in einem Versionsverwaltungssystem ab und können so Änderungen gegenüber neuen Anforderungen feststellen. In diesem Fall werden die betroffenen Geschäftsaktivitäten automatisch ermittelt, da sie mit den Compliance-Anforderungen verbunden sind.⁹²

In (Marino et al. 2009) werden Compliance-Anforderungen in Teilanforderungen zerlegt und Compliance-Prozessen zugeordnet, welche die Anforderungen sicherstellen können. Über eine Graphensuche werden die Compliance-Prozesse identifiziert, die entsprechende Teilanforderungen und Compliance-Anforderungen sicherstellen.⁹³

(Knuplesch et al. 2013b) motivieren die Herausforderung der Identifikation von Auswirkungen auf Compliance der Veränderung von Compliance-Anforderungen und Geschäftsprozessen in überbetrieblichen Geschäftsprozessen.⁹⁴ In (Knuplesch et al. 2015) wird ein Methode zur Identifikation betroffener Compliance-Anforderungen beim Entfernen von Geschäftsaktivitäten in überbetrieblichen Geschäftsprozessen vorgeschlagen.⁹⁵ Eine Erweiterung des Ansatzes um die Identifikation betroffener Geschäftsaktivitäten bei Änderung an Compliance-Anforderungen wird in (Fdhila et al. 2015b) vorgestellt.⁹⁶ In (Comuzzi 2014) werden die Zusammenhänge zwischen Compliance-Anforderungen und Geschäftsaktivitäten im Kontext des Outsourcings betrachtet. Sollten Compliance-Anforderungen Bedingungen an ausgelagerte Geschäftsaktivitäten stellen, werden diese als zu überwachende Compliance-Anforderungen hervorgehoben.⁹⁷

⁸⁹ Vgl. Corea und Delfmann 2017, S. 230 ff.

⁹⁰ Vgl. Ghanavati et al. 2010, S. 331 ff.

⁹¹ Vgl. Ghanavati et al. 2009, S. 139.

⁹² Vgl. Rudzajs und Buksa 2011, S. 100 ff.

⁹³ Vgl. Marino et al. 2009, S. 535 ff.

⁹⁴ Vgl. Knuplesch et al. 2013b, S. 658.

⁹⁵ Vgl. Knuplesch et al. 2015, S. 100 ff.

⁹⁶ Vgl. Fdhila et al. 2015b, S. 166 ff.

⁹⁷ Vgl. Comuzzi 2014, S. 172 ff.

3.2.4 Modellieren und Identifizieren von Abhängigkeiten zwischen Compliance-Anforderungen und IT-Komponenten

Best Practise, wie COBIT⁹⁸, COSO⁹⁹ oder ITIL¹⁰⁰ nennen generische Compliance-Anforderungen gegenüber IT-Komponenten und beschreiben auf qualitativer Ebene Prozesse zur Operationalisierung der Compliance-Anforderungen. In der Literatur werden ebenfalls Ansätze diskutiert, die Beziehungen zwischen Compliance-Anforderungen und IT-Komponenten sowohl konzeptionell als auch maschinenlesbar abbilden und abfragen.

In (Knackstedt et al. 2013) werden die wechselseitigen Beziehungen zwischen IT-Komponenten und Compliance-Anforderungen diskutiert.¹⁰¹ (Strecker et al. 2011) schlagen ein Metamodell zur Modellierung von Risiken an IT-Komponenten vor. Sie berücksichtigen in dem Metamodell mögliche Abhängigkeiten zwischen den Risiken.¹⁰² (Becker et al. 2014) schlagen ein Metadesign zur Integration gesetzlicher Anforderungen in Informationssysteme vor und demonstrieren sie in einem Softwareprototypen.¹⁰³ (Goeken und Looso 2006) nutzen ein semantisches Netz zur Integration von IT-Komponenten und Compliance-Anforderungen und demonstrieren dies mit Hilfe einer Graphdatenbank.¹⁰⁴ (Sillaber und Breu 2012) nutzen ebenfalls einen gerichteten Graphen zur Modellierung der Beziehung zwischen Compliance-Anforderungen und IT-Komponenten. Außerdem können sie Beziehungen zwischen einzelnen Paragraphen eines Gesetzestextes abbilden.¹⁰⁵

3.2.5 Modellieren und Identifizieren von Abhängigkeiten zwischen Compliance-Anforderungen, Geschäftsprozessen und IT-Komponenten

In (Koetter et al. 2013) wird die Idee des sogenannten Generic Compliance Descriptor beschrieben. Der Generic Compliance Descriptor verbindet Geschäftsprozesse mit IT-Komponenten und beinhaltet sowohl Compliance-Anforderungen gegenüber IT-Komponenten als auch gegenüber Geschäftsprozessen.¹⁰⁶ In (Koetter et al. 2014) wird das beschriebene Konzept des Generic Compliance Descriptors umgesetzt. In einem XML-Dokument werden natürlich-sprachliche Compliance-Anforderungen mit Compliance-Regeln verbunden. Jedoch existiert keine Möglichkeit Compliance-Anforderungen aufeinander verweisen zu können. Die Compliance-Anforderungen gegenüber dem Geschäftsprozess werden als LTL-Ausdruck, die Anforderungen gegenüber IT-Komponenten werden als Topology and Orchestration Specification for Cloud Applications (TOSCA)-Regel abgebildet. Anschließend kann per Model Checking geprüft werden, ob der Geschäftsprozess und die IT-Komponenten Compliance-konform sind.¹⁰⁷ In (Koetter et al. 2016) wird eine grafische Modellierungssprache für den Generic Compliance Descriptor vorgestellt.

⁹⁸ ISACA (Hg) 2012.

⁹⁹ Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2012.

¹⁰⁰ AXELOS 2019.

¹⁰¹ Vgl. Knackstedt et al. 2013, S. 7 ff.

¹⁰² Vgl. Strecker et al. 2011, S. 601 f.

¹⁰³ Vgl. Becker et al. 2014, S. 4 ff.

¹⁰⁴ Vgl. Goeken und Looso 2006, S. 858 ff.

¹⁰⁵ Vgl. Sillaber und Breu 2012, S. 1309 ff.

¹⁰⁶ Vgl. Koetter et al. 2013, S. 216 ff.

¹⁰⁷ Vgl. Koetter et al. 2014, S. 221 ff.

Sie erlaubt eine Verknüpfung von Compliance-Anforderungen zu Geschäftsaktivitäten und IT-Komponenten und wird in einem Softwareprototyp demonstriert und durch Experten evaluiert.¹⁰⁸

3.3 Methoden zur Geschäftsprozessadaption

Die Adaption des Geschäftsprozessmodells erfolgt durch die Integration separat modellierter und Compliance-konformer Prozessfragmente. Geschäftsprozesse können sowohl zur Entwurfszeit als auch zur Laufzeit automatisch Compliance-konform adaptiert werden. In (Schumm et al. 2010a) werden separate und Compliance-konforme Prozessfragmente zur Sicherstellung von Compliance-Anforderungen definiert¹⁰⁹. In (Schumm et al. 2010c) wird dieser Ansatz um die Möglichkeit der Integration separater Prozessfragmente in den Geschäftsprozess zu dessen Entwurfszeit erweitert.¹¹⁰ (Schultz 2013a) extrahiert Compliance-Prozesse aus ERP-Systemen und reichert damit bestehende Geschäftsprozessmodelle zur Entwurfszeit an.¹¹¹

(Hummer et al. 2011) integrieren logische Zugriffskontrollen als Compliance-Prozesse zur Laufzeit in überbetriebliche Geschäftsprozesse, die als Web Services Business Process Execution Language (WS-BPEL) modelliert sind.¹¹² In (Kittel et al. 2013a) wird die getrennte Modellierung und Integration von Compliance-Prozessen in der Domäne des Katastrophenmanagements vorgeschlagen. Außerdem wird anhand der Kontrolle der Trinkwasserqualität erläutert, dass diese Kontrolle durch verschiedene Compliance-Prozesse durchgeführt werden kann.¹¹³ In (Kittel 2013) wird die Methode zur Integration von Compliance-Prozesse zur Laufzeit und unter Berücksichtigung des Kontrollflusses des Geschäftsprozesses präsentiert.¹¹⁴ In (Kittel et al. 2013b) wird diese Methode in dem Softwareprototypen KitCom demonstriert.¹¹⁵

3.4 Ableiten der Forschungslücke

Für eine Methode zur Erreichung von Compliance in flexiblen und IT-gestützten Geschäftsprozessen fehlt es an drei Dingen. Erstens fehlt es an einer Methode, die Abhängigkeiten zwischen verschiedenen Compliance-Anforderungen, dem Geschäftsprozessmodell und IT-Komponenten in einem Modell abbildet. Zweitens fehlt es an einer Methode, die zwischen den Veränderungsmustern „Element ersetzen“ und „Element entfernen“ unterscheidet. Drittens fehlt es an einer Methode, die bei der Adaption des Geschäftsprozesses notwendige IT-Komponenten berücksichtigt. Tabelle 4 zeigt die autorenzentrierte Konzeptmatrix¹¹⁶ der relevanten Literatur, wobei MIA alle Aspekte der Modellierung und Adaption adressiert.

¹⁰⁸ Vgl. Koetter et al. 2016, S. 215 ff.

¹⁰⁹ Vgl. Schumm et al. 2010a, S. 5 ff.

¹¹⁰ Vgl. Schumm et al. 2010c, S. 329 ff.

¹¹¹ Vgl. Schultz 2013a, S. 128 ff.

¹¹² Vgl. Hummer et al. 2011, S. 23 ff.

¹¹³ Vgl. Kittel et al. 2013a, S. 4688 ff.

¹¹⁴ Vgl. Kittel 2013, S. 971 ff.

¹¹⁵ Vgl. Kittel et al. 2013b, S. 155 ff.

¹¹⁶ Vgl. Webster und Watson 2002, S. xvii.

Tabelle 4. Autorenzentrierte Konzeptmatrix

Quelle	CA-CA	CA-GP	CA-ITK	GP-ITK	Adaptieren
(Barboza et al. 2016)	X				
(El Kharbili und Stolarski 2009)	X				
(Ghanavati et al. 2014)	X				
(Elgammal et al. 2010)	X	X			
(Ghanavati et al. 2009)	X	X			
(Ghanavati et al. 2010)	X	X			
(Halle 2011)	X	X			
(Marino et al. 2009)	X	X			
(Riehle et al. 2017b)	X	X			
(Comuzzi 2014)		X			
(Corea und Delfmann 2017)		X			
(Fdhila et al. 2015b)		X			
(Jakoubi et al. 2010)		K			
(Knuplesch et al. 2013b)		X			
(Knuplesch et al. 2015)		X			
(Pham und Le Thanh 2016)		X			
(Pittl et al. 2017)		X			
(Rudzajs und Buksa 2011)		X			
(Weiß und Winkelmann 2011)		X			
(Zur Muehlen und Rosemann 2005)		K			
(Becker et al. 2014)			X		
(Goeken und Looso 2006)			X		
(Knackstedt et al. 2013)			K		
(Sillaber und Breu 2012)	X		X		
(Strecker et al. 2011)	X		X		
(Koetter et al. 2013)		X	X	X	
(Koetter et al. 2014)		X	X	X	
(Koetter et al. 2016)		X	X	X	
(Hummer et al. 2011)		R			X
(Kittel 2013)		R			X
(Kittel et al. 2013a)		R			X
(Kittel et al. 2013b)		R			X
(Schumm et al. 2010b)		R			X
(Schumm et al. 2010c)		R			X
(Schultz 2013a)		R			X
MIA	X	X	X	X	X
CA: Compliance-Anforderung GP: Geschäftsprozess ITK: IT-Komponente X: vorhanden K: konzeptuell beschrieben R: über Regel abgebildet					

Eine Erweiterung der Ansätze von (Riehle et al. 2017b), (Pham und Le Thanh 2016) oder (Corea und Delfmann 2017), die Ontologien zur Modellierung von Beziehungen zwischen Compliance-Anforderungen und Geschäftsprozessen nutzen, erschien nicht praktikabel, da bei der Transformation von Compliance-Anforderungen und Geschäftsprozessmodellen in eine Ontologie ebenfalls semantische Beziehungen zwischen den einzelnen Elementen modelliert werden müs-

sen.¹¹⁷ Bei der Modellierung einer Graphstruktur handelt es sich hingegen um einen leichtgewichtigeren Ansatz zur Modellierung der Modelle und Identifikation der Abhängigkeiten. So nutzen verschiedene Ansätze, wie (Goeken und Looso 2006) und (Sillaber und Breu 2012) eine Graphstruktur zur Modellierung und Identifikation von Abhängigkeiten zwischen Compliance-Anforderungen und IT-Komponenten sowie zwischen einzelnen Compliance-Anforderungen.¹¹⁸ Dabei handelt es sich um einen erweiterbaren Ansatz für weitere Sichten. (Marino et al. 2009) nutzt u.a. ebenfalls einen Graphen zur Modellierung von Compliance-Anforderungen gegenüber Compliance-Prozessen.¹¹⁹

Der Ansatz, welcher in der Lage ist Compliance-Anforderungen, Geschäftsprozess und IT-Komponenten abzubilden, ist der Generic Compliance Descriptor von (Koetter et al. 2014) und (Koetter et al. 2016).¹²⁰ Die Verknüpfung der IT-Komponenten mit den entsprechenden Geschäftsaktivitäten erfolgt ausschließlich über den Generic Compliance Descriptor¹²¹. Dadurch können keine Auswirkungen durch das Entfernen von IT-Komponenten auf die Ausführbarkeit der Geschäftsaktivitäten betrachtet werden, womit der Ansatz nicht die Doppelrolle der IT zur Erhaltung von Compliance abbilden kann. Außerdem ermöglicht der Generic Compliance Descriptor keine Verknüpfung von Compliance-Anforderungen untereinander¹²². Durch die unterschiedliche Verknüpfung der Modelle miteinander erschien es praktischer ein integriertes Modell auf Basis der Graphmodellierung umzusetzen, als den bestehenden Ansatz des Generic Compliance Descriptor weiter auszubauen.

Die identifizierten Ansätze zur getrennten Modellierung von geschäfts- und Compliance-Prozessen adaptieren das Geschäftsprozessmodell lediglich unter Beachtung des Kontrollflusses¹²³. Aufgrund der Doppelrolle der IT ist es jedoch notwendig, das Geschäftsprozessmodell ebenfalls unter Berücksichtigung von unterstützenden IT-Komponenten zu adaptieren.¹²⁴ Eine explizite Weiterentwicklung einer dieser Ansätze erschien jedoch aufgrund des Fehlens der IT-Infrastruktur nicht zielführend. Außerdem hätte die Regelsprache, die zur Überprüfung der Compliance-Anforderungen gegenüber dem Geschäftsprozess notwendig ist, um die Abbildungsfähigkeit von IT-Komponenten erweitert werden müssen.

¹¹⁷ Vgl. Riehle et al. 2017b, S. 179 ff.; Pham und Le Thanh 2016, S. 13 ff.; Corea und Delfmann 2017, S. 230 ff.

¹¹⁸ Vgl. Sillaber und Breu 2012, S. 1309 ff.; Goeken und Looso 2006, S. 858 ff.

¹¹⁹ Vgl. Marino et al. 2009, S. 535 ff.

¹²⁰ Vgl. Koetter et al. 2016, S. 215 ff.; Koetter et al. 2014, S. 221 ff.

¹²¹ Vgl. Koetter et al. 2016, S. 162; Fehling et al. 2014, S. 18.

¹²² Vgl. Koetter et al. 2016, S. 165.

¹²³ Vgl. u.a. Schumm et al. 2010c, S. 329 ff.; Kittel et al. 2013b, S. 155 ff.

¹²⁴ Vgl. Seyffarth und Raschke 2020, S. 109 ff.; Seyffarth et al. 2019, S. 231 ff.; Seyffarth et al. 2018, S. 181 ff.

4 Forschungsdesign

Wie der Forschungsstand gezeigt hat, fehlt es an einer Methode zur Erreichung von Compliance in flexiblen und IT-gestützten Geschäftsprozessen. Diese Lücke soll mit der Methode MIA adressiert werden. Zur Entwicklung von MIA wird das DSR-Forschungsparadigma angewendet, dessen Ziel die Entwicklung von Artefakten zur Lösung bisher ungelöster Probleme oder zur besseren Lösung bereits gelöster Probleme ist¹²⁵. Modelle, Konstrukte und Methoden sind dabei mögliche Artefakte eines DSR-Projekts.¹²⁶

Die Methode MIA besteht aus einer Menge von Modellen, Konstrukten und Methoden, die sich zu den Kernartefakten aus Abbildung 2 zusammenfassen lassen. Die Basis von MIA bildet ein konzeptuelles Domänenmodell. Die Schritte von MIA umfassen (1) das Modellieren des integrierten Compliance-Modells, (2) das Identifizieren von Auswirkungen auf Compliance beim Ersetzen und Entfernen und (3) das Compliance-konforme Adaptieren des Geschäftsprozessmodells.¹²⁷ Jeder Schritt adressiert dabei jeweils die entsprechende Forschungsfrage.

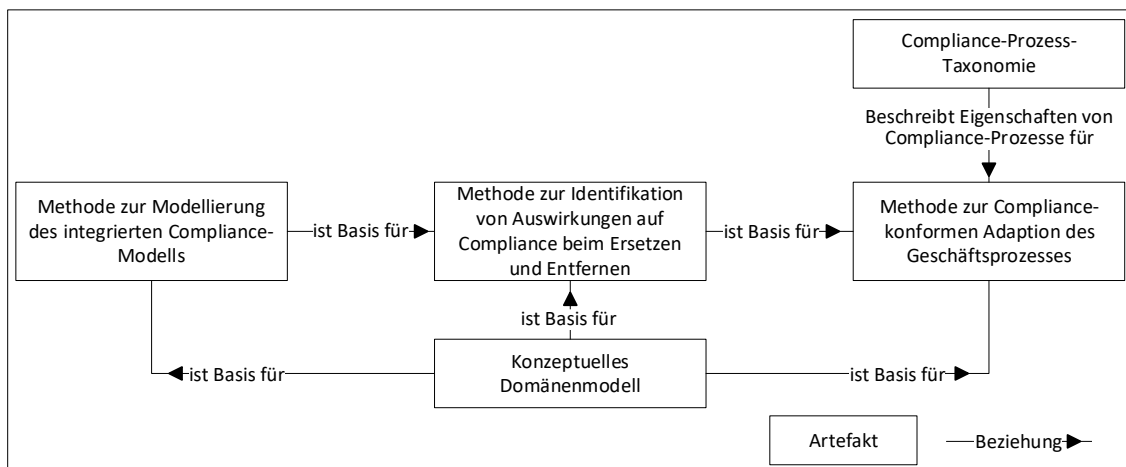


Abbildung 2. Kernartefakte von MIA

Es gibt viele Vorgehensmodelle zur Strukturierung eines DSR-Projekts,¹²⁸ die im Kern alle die DSR-Richtlinien nach Hevner et al.¹²⁹ umsetzen. Zur Strukturierung der erarbeiteten Beiträge und Artefakte wird das Vorgehensmodell nach Peffers et al.¹³⁰ in sequentieller Form verwendet, dem meist zitierten Vorgehensmodell für DSR-Projekte.¹³¹ Neben dem Entwurf und der Entwicklung von Artefakten fordert das Vorgehensmodell eine vorhergehende Problemidentifikation und eine nachgelagerte Demonstration und Evaluation. Alle Erkenntnisse sollen ebenfalls kommuniziert werden, was bspw. in Form von Publikationen erfolgen kann.¹³²

¹²⁵ Vgl. Hevner et al. 2004, S. 81; March und Smith 1995, S. 253f.

¹²⁶ Vgl. March und Smith 1995, S. 253.

¹²⁷ Vgl. Seyffarth et al. 2019; Seyffarth et al. 2018; Seyffarth et al. 2017a; Seyffarth et al. 2016.

¹²⁸ Vaishanvi et al. 2017, S. 8; Gregor und Hevner 2013, S. 349 ff.; March und Storey 2008, S. 726; Peffers et al. 2006, S. 83 ff; March und Smith 1995, S. 255.

¹²⁹ Hevner et al. 2004, S. 82 ff.

¹³⁰ Peffers et al. 2006, S. 83 ff.

¹³¹ Vgl. Vom Brocke et al. 2020, S. 3.

¹³² Vgl. Peffers et al. 2006, S. 93.

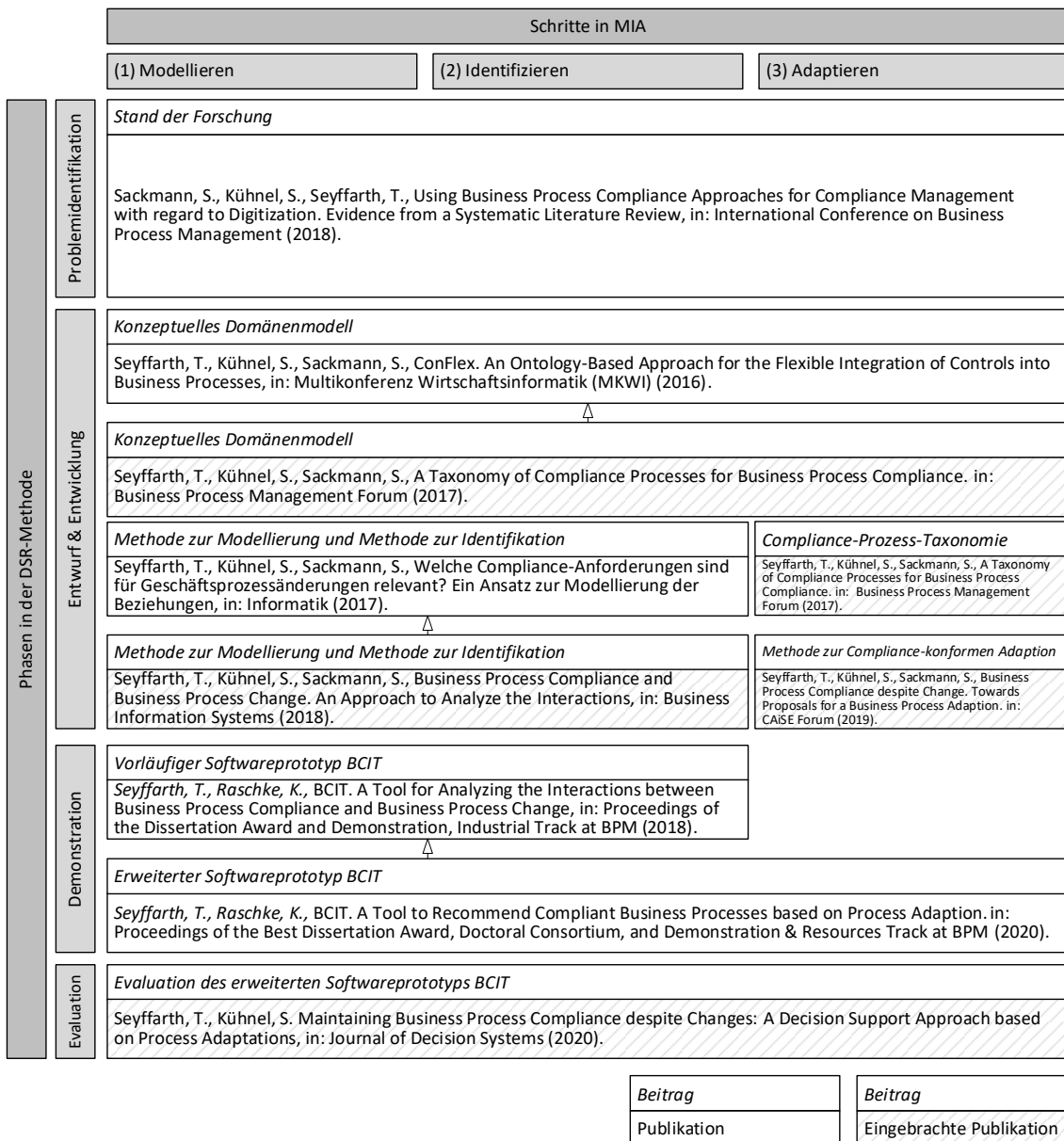


Abbildung 3. Einordnung der Publikationen

In Abbildung 3 sind die Beiträge dieser Arbeit den Schritten von MIA und den Phasen der DSR-Methode nach (Peppers et al. 2006) zugeordnet. Einige Beiträge und ihre Publikationen bauen aufeinander auf, was durch Pfeile zwischen den Beiträgen visualisiert ist. Außerdem sind alle eingebrachten Publikationen in den Anlagen zu finden.

Im Rahmen der Problemidentifikation (Kapitel 2.3) wurde der Stand der Forschung (Kapitel 3) mit Literaturrecherchen aufgearbeitet teilweise als Überblick über verwandte Arbeiten in (Sackmann et al. 2018) kommuniziert. Die Basis für den Entwurf und die Entwicklung der Artefakte bildet ein konzeptuelles Domänenmodell, das in (Seyffarth et al. 2016) vorgestellt und in (Seyffarth et al. 2017a) erweitert wurde.¹³³ Das konzeptuelle Domänenmodell wird in Kapitel 5.1 kurz vorgestellt. Die eingebrachte Publikation (Seyffarth et al. 2017a) ist in Anlage B zu finden.

133

Vgl. Seyffarth et al. 2016, S. 1344; Seyffarth et al. 2017a, S. 73.

Die Methode zur Modellierung des integrierten Compliance-Modells (FF 1 und Schritt 1 von MIA) und die Methode zur Identifikation der Auswirkungen auf die Erhaltung von Compliance beim Ersetzen einer IT-Komponente wurde zunächst in (Seyffarth et al. 2017b) kommuniziert.¹³⁴ Eine Erweiterung um Geschäftsaktivitäten, Compliance-Prozesse und Compliance-Anforderungen als änderbare Elemente und dem Veränderungsmuster „Element entfernen“ (FF 2 und Schritt 2 von MIA) erfolgte in der eingebrachten Publikation (Seyffarth et al. 2018).¹³⁵ Die Methoden werden in Kapitel 5.2 und Kapitel 5.3 vorgestellt. Die Publikation (Seyffarth et al. 2018) ist in Anlage C zu finden.

Die Compliance-konforme Adaption des Geschäftsprozesses erfolgt durch die Integration alternativer Compliance-Prozesse (FF 3 und Schritt 3 von MIA). Wie in (Seyffarth et al. 2019) beschrieben, können alternative Compliance-Prozesse auf Basis ihrer Eigenschaften modelliert und in den Geschäftsprozess integriert werden.¹³⁶ In (Seyffarth et al. 2017a) wurde eine Taxonomie vorgestellt, die Eigenschaften von Compliance-Prozessen zusammenfasst.¹³⁷ Sie kann als Basis zur Modellierung alternativer Compliance-Prozesse herangezogen werden. Die Methode zur Compliance-konformen Adaption des Geschäftsprozessmodells unter Berücksichtigung der Eigenschaften von Compliance-Prozessen wird in Kapitel 5.4 vorgestellt. Die eingebrachten Publikationen (Seyffarth et al. 2017a) und (Seyffarth et al. 2019) sind in Anlage B und Anlage D zu finden.

Die Anwendbarkeit der entwickelten Artefakte wurde in mehreren Softwareprototypen demonstriert. Der erste auf JavaScript-basierter Softwareprototyp BCIT demonstriert die Modellierung eines integrierten Compliance-Graphs und die Identifikation der Auswirkungen von Änderungen auf Compliance und wurde in (Seyffarth und Raschke 2018) kommuniziert.¹³⁸ BCIT wurde abschließend um die Funktion zur Compliance-konformen Adaption des Geschäftsprozesses erweitert und in (Seyffarth und Raschke 2020) kommuniziert.¹³⁹ Der erweiterte Softwareprototyp BCIT wird kurz in Kapitel 6.2 vorgestellt.

Die Demonstration der Anwendbarkeit von Artefakten in einem Softwareprototyp stellt eine mögliche Art der Evaluation in DSR-Projekten dar.¹⁴⁰ Nichtsdestotrotz ist für jedes DSR-Projekt essentiell, die Nützlichkeit der Artefakte zur Problemlösung zu evaluieren.¹⁴¹ Daher wurde die wahrgenommene Nützlichkeit von MIA anhand des Softwareprototypens BCIT in einer Fallstudie mit Domänenexpert:innen evaluiert und in (Seyffarth und Kühnel 2020) kommuniziert.¹⁴² Die Evaluation zur wahrgenommenen Nützlichkeit wird in Kapitel 6.3 vorgestellt. Die eingebrachte Publikation (Seyffarth und Kühnel 2020) ist in Anlage E zu finden.

¹³⁴ Vgl. Seyffarth et al. 2017b, S. 1643 f.

¹³⁵ Vgl. Seyffarth et al. 2018, S. 183 f.

¹³⁶ Vgl. Seyffarth et al. 2019, S. 231 ff.

¹³⁷ Vgl. Seyffarth et al. 2017a, S. 77 ff.

¹³⁸ Vgl. Seyffarth und Raschke 2018, S. 83 ff.

¹³⁹ Vgl. Seyffarth und Raschke 2020, S. 109 ff.

¹⁴⁰ Vgl. Hevner et al. 2004, S. 93.

¹⁴¹ Vgl. Hevner et al. 2004, S. 82.

¹⁴² Vgl. Seyffarth und Kühnel 2020, S. 19 ff.

5 Entwurf und Entwicklung der Artefakte

In diesem Kapitel werden die entwickelten Artefakte von MIA vorgestellt. Zunächst wird das konzeptuelle Domänenmodell vorgestellt, das die Basis aller Schritte von MIA bildet. Anschließend werden die Schritte Modellieren, Identifizieren und Adaptieren vorgestellt. Zu Beginn eines jeden Schritts wird jeweils ein kleines Beispiel gezeigt, das mit Hilfe des Schritts umgesetzt werden kann.

5.1 Konzeptuelles Domänenmodell

Das Ziel der Konzeptualisierung des Problembereichs ist die Definition notwendiger Terme und deren Beziehungen zueinander.¹⁴³ Eine Möglichkeit der Konzeptualisierung des Problembereichs ist seine Abbildung in Modellen, die u.a. eine verkürzte Betrachtung der Realität ermöglichen.¹⁴⁴ In (Seyffarth et al. 2016)¹⁴⁵ und der eingebrachten Publikation (Seyffarth et al. 2017a)¹⁴⁶ wurde zur Beschreibung des Problembereichs dieser Arbeit ein konzeptuelles Domänenmodell in Form eines Unified Modeling Language (UML)-Klassendiagramms¹⁴⁷ entwickelt. Die Elemente und Beziehungen dieses Domänenmodells wurden aus der Literatur abgeleitet und sind in Abbildung 4 dargestellt.

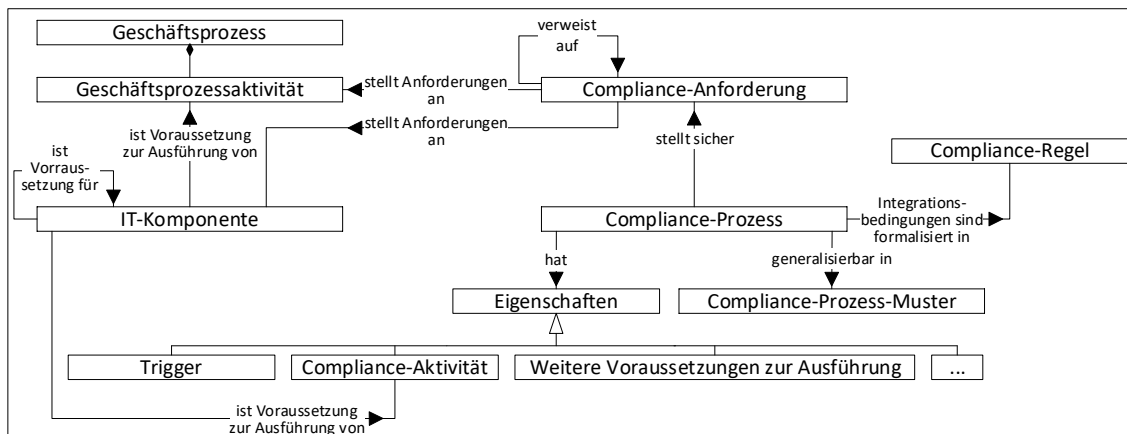


Abbildung 4. Konzeptuelles Domänenmodell¹⁴⁸

Wie bereits erwähnt, stellen Compliance-Prozesse Compliance-Anforderungen sicher, die wiederum Anforderungen an Geschäftsaktivitäten und IT-Komponenten stellen können. Compliance-Anforderungen können außerdem auf andere Compliance-Anforderungen verweisen. Dadurch können Spezialisierungsbeziehungen zwischen Compliance-Anforderungen oder Referenzen zwischen Paragraphen eines Gesetzes abgebildet werden. Ein Compliance-Prozess kann durch seine Eigenschaften, wie Trigger, Compliance-Aktivitäten oder weitere Voraussetzungen zur Ausführung, charakterisiert werden. Eine Voraussetzung zur Ausführung einer Compliance-

¹⁴³ Vgl. Hevner et al. 2004, S. 85; March und Smith 1995, S. 256.

¹⁴⁴ Vgl. Stachowiak 1973, S. 131 ff.

¹⁴⁵ Seyffarth et al. 2016, S. 1341 ff.

¹⁴⁶ Seyffarth et al. 2017a, S. 71 ff.

¹⁴⁷ OMG (Hg) 2017, S. 195 ff.

¹⁴⁸ In Anlehnung an Seyffarth et al. 2017a, S. 73; Seyffarth et al. 2016, S. 1344.

Aktivität können IT-Komponenten sein, was wieder die Doppelrolle der IT verdeutlicht. Darüber hinaus können Compliance-Prozesse in sogenannten Compliance-Prozess-Mustern generalisiert werden. Zur Überprüfung an welcher Stelle des Geschäftsprozesses ein Compliance-Prozess integriert werden kann, werden die Integrationsbedingungen des Compliance-Prozesses in einer Compliance-Regel formalisiert.

5.2 Modellieren eines integrierten Compliance-Modells

Die Methode zur Modellierung eines integrierten Compliance-Modells ist der erste Schritt von MIA und beantwortet FF 1. Die Methode wurde in (Seyffarth et al. 2017b)¹⁴⁹ und (Seyffarth et al. 2018)¹⁵⁰ vorgestellt. Das integrierte Compliance-Modell umfasst Compliance-Anforderungen, ein Geschäftsprozessmodell mit integrierten Compliance-Prozessen und IT-Komponenten.

Zur Modellierung der Beziehungen zwischen Elementen eignen sich Graphen.¹⁵¹ Sie werden in der Literatur bereits zur Modellierung von Geschäftsprozessen¹⁵², zur Modellierung von IT-Architekturen¹⁵³ oder zur Modellierung der Zusammenhänge zwischen Compliance-Anforderungen¹⁵⁴ genutzt. Daher werden die Elemente und Beziehungen des Compliance-Modells mit einem sogenannten integrierten Compliance-Graphen abgebildet¹⁵⁵.

Das Erzeugen des integrierten Compliance-Graphs ist notwendig, da in Organisationen und Unternehmen verschiedene Modelle vorliegen, die jedoch nicht vollständig miteinander integriert sind. Zum Erzeugen des integrierten Compliance-Graphs müssen die Modelle des Geschäftsprozesses, der IT-Architektur und der Compliance-Anforderungen in maschinenlesbarer Form vorliegen.¹⁵⁶ Geschäftsprozessmodelle können dafür in BPMN 2.0¹⁵⁷, IT-Architekturen in Open Group ArchiMate Model Exchange File Format¹⁵⁸ und Compliance-Anforderungen in XML-basierten Gesetzestexten¹⁵⁹ modelliert sein. Das Erzeugen des integrierten Compliance-Graphen besteht aus zwei Schritten. Zunächst werden die Elemente der Modelle (Aktivitäten, Gateways, IT-Komponenten, usw.) in entsprechende Knoten transformiert. Die Kanten zwischen den Knoten eines Modells werden ebenfalls automatisch erzeugt. Danach müssen die Kanten zwischen den jeweiligen Modellen manuell definiert werden, da die Beziehungen bislang in keiner formalen Sprache vollständig definiert sind.¹⁶⁰ Im Folgenden werden die Elemente und Eigenschaften der genannten Modelle formal definiert.

¹⁴⁹ Vgl. Seyffarth et al. 2017b, S. 1643 ff.

¹⁵⁰ Vgl. Seyffarth et al. 2018, S. 183 ff.

¹⁵¹ Vgl. Heckel und Taentzer 2020, S. 5; Knebl 2019, S. 213 f.; Mattfeld und Vahrenkamp 2014, S. 5.

¹⁵² Vgl. u.a. Weske 2019, S. 89.

¹⁵³ Vgl. u.a. Dreyfus und Iyer 2006, S. 4; Sowa und Zachman 1992, S. 606.

¹⁵⁴ Vgl. u.a. Sillaber und Breu 2012, S. 1310 f.

¹⁵⁵ Vgl. Seyffarth et al. 2018, S. 182.

¹⁵⁶ Vgl. Seyffarth et al. 2018, S. 181.

¹⁵⁷ Vgl. OMG (Hg) 2011, S 54 ff.

¹⁵⁸ Vgl. The Open Group (hg) 2019.

¹⁵⁹ Bundesministeriums der Justiz und für Verbraucherschutz (Hg) 2020.

¹⁶⁰ Vgl. Seyffarth et al. 2018, S. 182 f.

Definition 1 (Compliance-Anforderungen-Graph). Ein Graph der Compliance-Anforderungen ist ein gerichteter Graph $CAG = (N^{CAG}, E^{CAG})$, wobei N^{CAG} eine nicht leere und endliche Menge an Knoten ist, die Compliance-Anforderungen repräsentieren und $E^{CAG} \subseteq N^{CAG} \times N^{CAG}$ eine Menge an gerichteten Kanten zwischen den Knoten ist. Eine gerichtete Kante $e_{i,j}^{CAG}$ verbindet die Knoten n_i^{CAG} und n_j^{CAG} .¹⁶¹

Definition 2 (Geschäftsprozess-Graph). Ein Geschäftsprozess-Graph PG ist ein Tupel $PG = (N^{PG}, E^{PG}, c_type)$, wobei $N^{PG} = GA \cup CA \cup C$ eine Menge von Knoten in PG ist, die bestimmten Semantiken der Ausführung folgen. GA ist dabei eine Menge von Geschäftsaktivitäten und CA eine Menge von Compliance-Aktivitäten, wobei gilt $GA \cap CA = \emptyset$. C ist eine Menge koordinierender Knoten und $E^{PG} \subseteq N^{PG} \times N^{PG}$ ist eine Menge von gerichteten Kanten zwischen Knoten und repräsentieren den Kontrollfluss, sodass (N^{PG}, E^{PG}) ein vollständig verbundener Prozessgraph ist. Eine Kante $e_{i,j}^{PG}$ verbindet die Knoten n_i^{PG} und n_j^{PG} . Die Funktion $c_type: C \rightarrow \{start, end, intermediate, split, synchronize, choice, merge\}$ weist jedem koordinierenden Knoten von PG einen Koordinationstyp zu.¹⁶²

Definition 3 (Compliance-Prozess-Graph). Ein Compliance-Prozess-Graph ist ein Subgraph von PG und ein 3-Tupel $CP = (N^{CP}, E^{CP}, c_type)$, wenn gilt, dass $N^{CP} \subseteq CA \cup C$ und $E^{CP} \subseteq E^{PG}$ sind.¹⁶³

Definition 4 (IT-Architektur-Graph). Ein IT-Architektur-Graph ist ein gerichteter Graph $ITG = (N^{ITG}, E^{ITG})$, wobei N^{ITG} eine nicht leere und endliche Menge an Knoten ist, die IT-Komponenten repräsentieren. $E^{ITG} \subseteq N^{ITG} \times N^{ITG}$ ist eine Menge an gerichteten Kanten zwischen den Knoten. Eine Kante $e_{i,j}^{ITG}$ ist gerichtet zwischen den Knoten n_i^{ITG} und n_j^{ITG} .¹⁶⁴

Definition 5 (Integrierter Compliance-Graph). Zur Integration des Compliance-Anforderungen-Graphs, des Geschäftsprozess-Graphs und des IT-Architektur-Graphs wird ein integrierter Compliance-Graph definiert. Die Verbindung zwischen den Knoten der verschiedenen Graphen erfolgt mit einer Menge an gerichteten Kanten E^{con} . Eine Kante $e_{i,j}^{con}$ kann zwischen den Knotenpaaren n_i^{CAG} und n_j^{PG} , n_i^{PG} und n_j^{CAG} , n_i^{ITG} und n_j^{PG} oder n_i^{CAG} und n_j^{ITG} auftreten. Dementsprechend ist der integrierte Compliance-Graph ein vier-Tupel $G = (N^G, E^G, n_{identify}, n_{type})$, wobei $N^G = N^{CAG} \cup N^{PG} \cup N^{ITG}$ eine nicht leere und endliche Menge an Knoten und $E^G = E^{CAG} \cup E^{PG} \cup E^{ITG} \cup E^{con}$ eine Menge an gerichteten Kanten zwischen den Knoten mit $E^G \subseteq N^G \times N^G$ ist. Die Funktion $n_{identify}(n_i^G)$ weist jedem Knoten n_i^G eine eindeutige Identifikation zu. Der Knotentyp von n_i^G ist definiert über die Funktion $n_{type}(n_i^G) = \{ComplianceAnforderung: n_i^G \in CAG; Geschäftsaktivität: n_i^G \in GA; Complianceaktivität: n_i^G \in CA; Coordinating Node: n_i^G \in C; IT Komponente: n_i^G \in ITG\}$.¹⁶⁵

¹⁶¹ Vgl. Seyffarth und Kühnel 2020, S. 6; Seyffarth et al. 2018, S. 182.

¹⁶² Vgl. Seyffarth et al. 2019, S. 229.

¹⁶³ Vgl. Seyffarth et al. 2019, S. 229.

¹⁶⁴ Vgl. Seyffarth und Kühnel 2020, S. 6.

¹⁶⁵ Vgl. Seyffarth und Kühnel 2020, S. 6.

5.3 Identifizieren von Auswirkungen auf Compliance

5.3.1 Anwendung auf das Ausgangsszenario

Die Methode zur Identifikation der Auswirkungen auf die Erhaltung von Compliance beim Ersetzen oder Entfernen eines Elements ist der zweite Schritt von MIA und beantwortet FF 2. Die Methode wurde in (Seyffarth et al. 2017b) exemplarisch mit dem Veränderungsmuster „Element ersetzen“ anhand von IT-Komponenten vorgestellt. In der eingebrachten Publikation (Seyffarth et al. 2018) wurde die Methode um das Veränderungsmuster „Element entfernen“ und der Anwendung auf Geschäftsaktivitäten, Compliance-Prozesse und Compliance-Anforderungen erweitert. Anhand des Ausgangsszenarios aus Kapitel 2.3 werden im Folgenden die Auswirkungen dieser Veränderungsmuster auf die Erhaltung von Compliance erläutert, die beispielhaft in Abbildung 5 dargestellt sind.¹⁶⁶

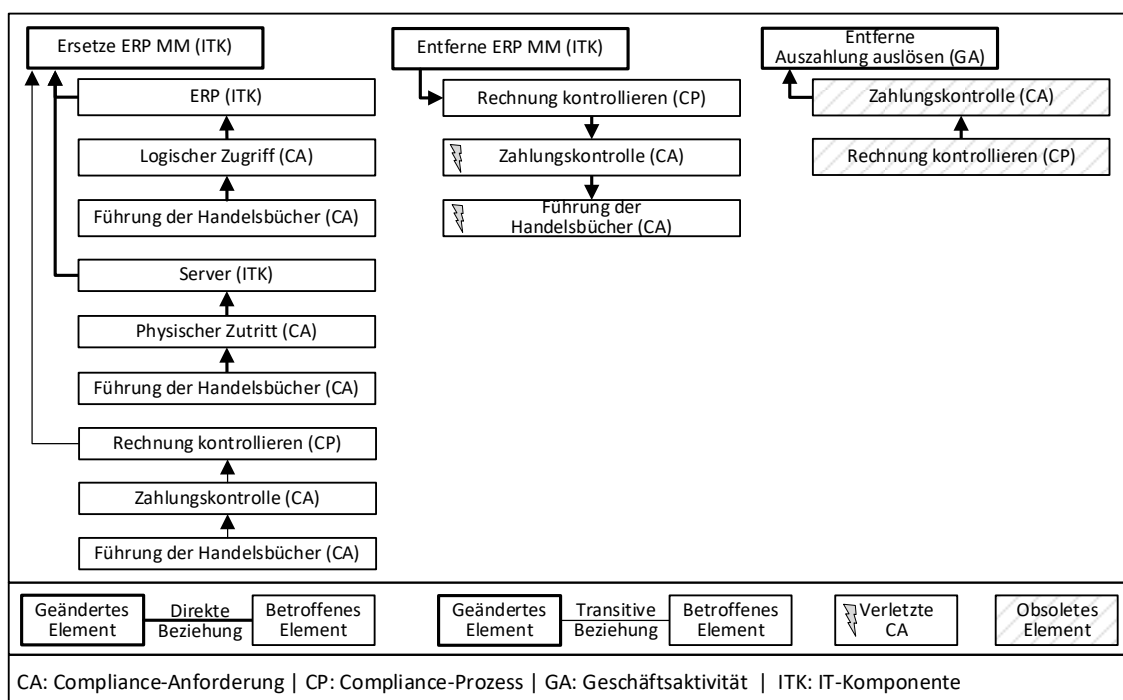


Abbildung 5. Auswirkungen auf Compliance durch das Ersetzen und Entfernen¹⁶⁷

5.3.2 Ersetzen eines Elements

Das Outsourcing einer IT-Komponente zu einem Dienstleister kann ein Grund für das Ersetzen einer IT-Komponente sein. Jedoch ist in diesem Fall der Auftraggeber weiterhin für die Einhaltung der Compliance-Anforderungen gegenüber der auszulagernden IT-Komponente verantwortlich¹⁶⁸. Demzufolge müssen beim Ersetzen eines Elements alle Compliance-Anforderungen bestimmt werden, die in direkter und transativer Beziehung zum ersetzenden Element stehen.¹⁶⁹

¹⁶⁶ Alle weiteren Suchalgorithmen sind unter <https://github.com/tobiasseyffarth/bcit/tree/master/resources/4-pseudocode> in Form von Pseudocode beschrieben.

¹⁶⁷ In Anlehnung an Seyffarth et al. 2018, S. 180.

¹⁶⁸ Vgl. §25b, Absatz 2 KWG.

¹⁶⁹ Vgl. Seyffarth et al. 2018, S. 183 f.

Das betrifft auch die Compliance-Anforderungen der IT-Komponenten, welche für die Ausführung der zu ersetzenden IT-Komponente notwendig sind, da sie ebenfalls durch den Outsourcing-Dienstleister erfüllt werden müssen. So muss die IT-Komponente, die „ERP MM“ ersetzen soll, verschiedenen Compliance-Anforderungen entsprechen. Einerseits müssen aufgrund von „ERP“ die Compliance-Anforderungen „Logischer Zugriffsschutz“ und demzufolge auch die Compliance-Anforderung „Führung der Handelsbücher“ beachtet werden. Aufgrund des Servers, auf dem „ERP“ ausgeführt wird, muss die ersetzende IT-Komponente ebenfalls die Compliance-Anforderung „Physischer Zutritt“ erfüllen.

Eine IT-Komponente kann ebenfalls zur Ausführung von Compliance-Prozessen und Geschäftsaktivitäten notwendig sein, die Compliance-Anforderungen sicherstellen bzw. von Compliance-Anforderungen betroffen sind. In diesem Fall liegen transitive Beziehungen zwischen der zu ersetzenden IT-Komponente und Compliance-Prozessen sowie Compliance-Anforderungen vor. In Abbildung 5 ist das bei dem Compliance-Prozess „Rechnung kontrollieren“ sowie den Compliance-Anforderungen „Zahlungskontrolle“ und „Führung der Handelsbücher“ der Fall.

Das Bestimmen der direkten und transitiven Abhängigkeiten erfolgt durch eine Suche in dem integrierten Compliance-Graph G nach Vorgängern und Nachfolgern des zu ersetzenden Elements, wobei es sich bei Methoden zur Suche in Graphen um bekannte und evaluierte Verfahren handelt.¹⁷⁰ Bei der Suche nach direkten und transitiven Abhängigkeiten werden die zuvor definierten Knotentypen berücksichtigt. Die konkrete Suchstrategie unterscheidet sich je nach Typ des zu ändernden Elements.¹⁷¹

<pre> Input: Graph g, zu ersetzendes Element $\{n \in g \mid n_type(n) = \text{IT component}\}$ 1 // bestimme alle direkten Compliance-Anforderungen und Compliance-Prozesse zu n 2 $preds_n = \text{get_all_predecessor}(n, \text{type}(pred_n)=\text{compliance requirement OR compliance process})$ 3 Foreach i in $(preds_n)$ do 4 mark i as direct AND add i including all vertices between i und n to $result$ 5 // bestimme alle transitiven Compliance-Anforderungen und Compliance-Prozesse zu n 6 Foreach it in $(\text{get_all_leafs}(n, \text{type}(leaf_n)=\text{IT Component}))$ do 7 Foreach $activity$ in $(\text{get_all_direct_successor}(it, \text{type}(suc_it)=\text{business activity}))$ do 8 Foreach cr in $(\text{get_all_direct_predecessor}(activity, \text{type}(pred_activity)=\text{compliance requirement}))$ do 9 $i = \text{get_all_predecessor}(cr)$ 10 mark $it, activity, cr$ and i as transitiv AND add to $result$ 11 Foreach $complianceprocess$ in $(\text{get_all_direct_successor}(it, \text{type}(dir_suc)=\text{compliance process}))$ do 12 Foreach cr in $(\text{get_all_direct_successor}(complianceprocess, \text{type}(cp)=\text{compliance requirement}))$ do 13 $i = \text{get_all_predecessor}(cr)$ 14 mark $it, complianceprocess, cr$ and i as transitiv AND add to $result$ 15 generiere $result_graph$ basierend auf g und $result$ Output: Graph $result_graph$ </pre>

Abbildung 6. Pseudocode zur Auswirkungsidentifikation beim Ersetzen einer IT-Komponente¹⁷²

Der Algorithmus zur Identifikation der Auswirkungen auf die Erhaltung von Compliance beim Ersetzen einer IT-Komponente aus Abbildung 6 kann folgendermaßen beschrieben werden. In Schritt 1 werden alle Compliance-Anforderungen bestimmt, die unmittelbar an der zu ersetzenden IT-Komponente hängen. Das umfasst auch alle Compliance-Anforderungen, die auf die unmittelbare Compliance-Anforderung referenzieren. Außerdem werden alle IT-Komponenten bestimmt, die für die Ausführung der zu ersetzenden IT-Komponente notwendig sind. In Schritt 2

¹⁷⁰ Vgl. u.a. Aleliunas et al. 1979, S. 219; Rosenkrantz et al. 1977, S. 564 f.

¹⁷¹ Vgl. Seyffarth et al. 2018, S. 183.

¹⁷² In Anlehnung an Seyffarth et al. 2018, S. 183.

werden ebenfalls alle Compliance-Anforderungen und deren verweisende Anforderungen bestimmt, die unmittelbar an den aus Schritt 1 bestimmten IT-Komponenten hängen. In Schritt 3 werden alle transitiven Compliance-Anforderungen bestimmt. Dazu werden alle Geschäftsaktivitäten und Compliance-Prozesse bestimmt, die unmittelbar oder mittelbar durch die zu ersetzende IT-Komponente ausgeführt werden. Anschließend werden die Compliance-Anforderungen dieser Geschäftsaktivitäten und Compliance-Prozesse bestimmt.¹⁷³

5.3.3 Entfernen eines Elements

Das Entfernen eines Elements führt entweder zur Verletzung von Compliance-Anforderungen oder zu obsoleten Compliance-Anforderungen, Compliance-Prozesse oder IT-Komponenten. Grundsätzlich werden Compliance-Anforderungen verletzt, wenn ihre sicherstellenden Compliance-Prozesse entfernt werden oder Compliance-Prozesse durch das Entfernen benötigter IT-Komponenten nicht mehr ausgeführt werden können. Die Compliance-Verletzung bezieht sich ebenfalls auf Anforderungen, die Bedingungen an die verletzte Compliance-Anforderung stellen.¹⁷⁴ In Abbildung 5 wird die IT-Komponente „ERP MM“ entfernt. Das führt zu einer nicht Ausführbarkeit des Compliance-Prozesses „Rechnung kontrollieren“, wodurch die Compliance-Anforderung „Zahlungskontrolle“ verletzt wird. Die Verletzung der Zahlungskontrolle führt ebenfalls zu einer Verletzung der „Führung der Handelsbücher“, welche ihrerseits Bedingungen an die Zahlungskontrolle stellt.

Unabhängig von der IT-Komponente „ERP MM“ wird in Abbildung 5 die Geschäftsaktivität „Auszahlung auslösen“ entfernt, wodurch die Compliance-Anforderung „Zahlungskontrolle“ und ihr zugeordneter Compliance-Prozess „Rechnung kontrollieren“ obsolet werden. Eine Compliance-Anforderung wird obsolet, wenn das einzige Element, an das sie Bedingungen stellt oder durch das sie spezialisiert wird, entfernt oder ebenfalls obsolet wird. Compliance-Prozesse und IT-Komponenten können ebenfalls durch das Entfernen von Compliance-Anforderungen obsolet werden. Compliance-Prozesse werden obsolet, wenn die einzige Compliance-Anforderung entfernt wird, die sie operationalisieren. Sollte der obsolete Compliance-Prozess von IT-Komponenten unterstützt werden, die nur für die Ausführung des obsoleten Compliance-Prozesses benötigt werden, sind diese IT-Komponenten ebenfalls obsolet. Gleiches gilt für ihre notwendigen exklusiv vorausgesetzten IT-Komponenten.¹⁷⁵

¹⁷³ Vgl. Seyffarth und Kühnel 2020, S. 12 f.

¹⁷⁴ Vgl. Seyffarth et al. 2018, S. 184.

¹⁷⁵ Vgl. Seyffarth und Kühnel 2020, S. 13 f.; Seyffarth et al. 2018, S. 184.

<pre> Input: Graph <i>g</i>, zu entfernendes Element {<i>n</i> ∈ <i>g</i> <i>n</i>_type(<i>n</i>) = IT component} 1 // bestimme alle verletzten Compliance-Anforderungen 2 Foreach <i>it</i> in (get_all_leafs(<i>n</i>, type(leaf(<i>n</i>))=IT component) do 3 Foreach <i>cp</i> in (get_all_direct_successor(<i>it</i>, type(suc(<i>it</i>))=compliance process) do 4 Foreach <i>cr</i> in (get_all_direct_successor(<i>cp</i>, type(suc(<i>cp</i>))=compliance requirement) do 5 <i>i</i> = get_all_predecessor(<i>cr</i>) 6 mark <i>cr</i> and <i>i</i> as violated AND add to <i>result</i> 7 // bestimme alle obsoleten Compliance-Anforderungen 8 add <i>n</i> to <i>list_it</i> 9 Foreach <i>it</i> in (get_all_successor(<i>n</i>, type(suc(<i>n</i>))=IT component) do 10 If (<i>it</i> only requires <i>n</i>) 11 add <i>it</i> to <i>list_it</i> 12 Foreach <i>it</i> in (<i>list_it</i>) do 13 Foreach <i>cr</i> in (get_all_direct_predecessor(<i>it</i>, type(pred(<i>it</i>))=compliance requirement) do 14 If (get_all_direct_successor(<i>cr</i>)==<i>it</i>) 15 mark <i>cr</i> as obsolete AND add to <i>result</i> 16 Foreach <i>cr2</i> in (get_all_predecessor(<i>cr</i>, type(pred(<i>cr</i>))=compliance requirement) do 17 If (<i>cr2</i> hasn't other direct successor than get_all_predecessor(<i>cr</i>, type(<i>cr</i>)=comp.req.) 18 mark <i>cr2</i> as obsolete AND add to <i>result</i> 19 generiere <i>result_graph</i> basierend auf <i>g</i> und <i>result</i> Output: Graph <i>result_graph</i> </pre>

Abbildung 7. Pseudocode zur Auswirkungsidentifikation beim Entfernen einer IT-Komponente¹⁷⁶

Der Pseudocode aus Abbildung 7 kann folgendermaßen beschrieben werden. In Schritt 1 werden alle Compliance-Verletzungen bestimmt, wenn eine IT-Komponente entfernt wird. Dazu werden alle Compliance-Prozesse bestimmt, die implizit oder explizit von der IT-Komponente unterstützt werden. In Schritt 2 werden alle Compliance-Anforderungen bestimmt, die durch die Compliance-Prozesse operationalisiert werden. In Schritt 3 werden alle obsoleten Compliance-Anforderungen bestimmt. Dazu werden zunächst alle nachfolgenden IT-Komponenten der entfernten IT-Komponente bestimmt. Anschließend werden alle vorhergehenden IT-Komponenten bestimmt, die ausschließlich für die Ausführung der zu ersetzenden IT-Komponente notwendig sind. Zuletzt werden die Compliance-Anforderungen von allen ermittelten IT-Komponenten ermittelt. Wenn die Compliance-Anforderungen ausschließlich Bedingungen an die IT-Komponenten stellen, werden sie als obsolet markiert.¹⁷⁷

5.4 Adaptieren des Geschäftsprozessmodells

Die Methode zur Compliance-konformen Adaption des Geschäftsprozessmodells ist der dritte Schritt von MIA und beantwortet FF 3. Die Methode wurde in der eingebrachten Publikation (Seyffarth et al. 2019)¹⁷⁸ kommuniziert und nutzt zur Beschreibung der Eigenschaften von Compliance-Prozessen die Compliance-Prozess-Taxonomie aus der eingebrachten Publikation (Seyffarth et al. 2017a)¹⁷⁹. Zunächst werden Vorschläge alternativer und Compliance-konformer Geschäftsprozessmodelle auf Basis des Ausgangsszenarios gezeigt bevor anschließend Eigenschaften von Compliance-Prozessen zur Definition alternativer Compliance-Prozesse vorgestellt werden. Danach werden die Struktur eines alternativen Compliance-Prozess-Graphen und die Methode zur Suche nach alternativen Compliance-Prozessen in diesem Graphen beschrieben.

¹⁷⁶ In Anlehnung an In Anlehnung an Seyffarth et al. 2018, S. 184.

¹⁷⁷ Vgl. Seyffarth und Kühnel 2020, S. 13 f.

¹⁷⁸ Vgl. Seyffarth et al. 2019, S. 233 ff.

¹⁷⁹ Vgl. Seyffarth et al. 2017a, S. 78.

5.4.1 Anwendung auf das Ausgangsszenario

Compliance-Anforderungen können jeweils durch verschiedene, alternative Compliance-Prozesse sichergestellt werden.¹⁸⁰ So kann bspw. die Kontrolle der Qualität von Trinkwasser u.a. an der Quelle, bei der Flaschenabfüllung oder vor dem Verzehr selbst stattfinden.¹⁸¹ Wenn diese Idee auf das Ausgangsszenario angewandt wird, kann die Compliance-Anforderung „Zahlungskontrolle“ durch die Compliance-Prozesse „Rechnung kontrollieren“, „Rechnung manuell kontrollieren“ oder „Zahlungsanordnung kontrollieren“ sichergestellt werden.¹⁸² Abbildung 8 zeigt einen alternativen Compliance-Prozess-Graph und die draus abgeleiteten Compliance-konformen Varianten des internen Bestellprozesses. Als Eigenschaften des Compliance-Prozesses werden der Trigger und weitere Voraussetzungen für die Ausführung des Compliance-Prozesses betrachtet.¹⁸³ Durch unterschiedliche Trigger werden sie an verschiedenen Stellen im Geschäftsprozess integriert. Weitere Voraussetzungen zur Ausführung beschränken sich auf das Vorhandensein einer IT-Komponente.¹⁸⁴

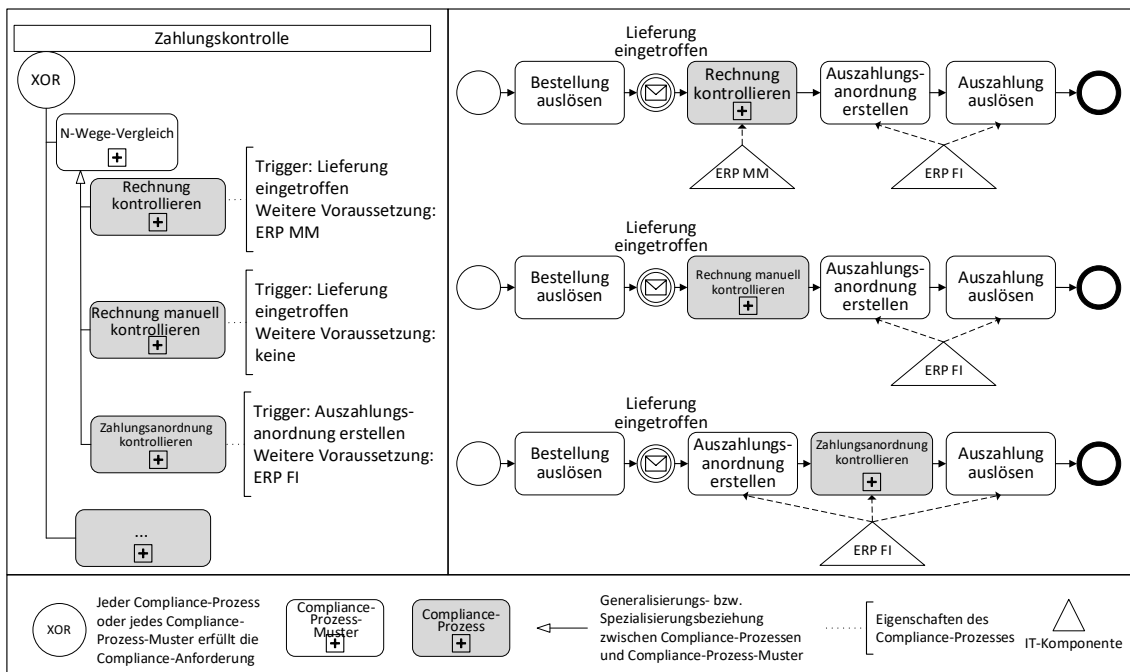


Abbildung 8. Compliance-konforme Varianten des Internen Bestellprozesses¹⁸⁵

¹⁸⁰ Vgl. Kittel et al. 2013a, S. 4693; Marino et al. 2009, S. 540.

¹⁸¹ Vgl. Kittel et al. 2013a, S. 4693.

¹⁸² Vgl. Seyffarth et al. 2019, S. 233.

¹⁸³ Vgl. Seyffarth et al. 2017a, S. 77 ff.

¹⁸⁴ Vgl. Seyffarth et al. 2019, S. 235.

¹⁸⁵ In Anlehnung an Seyffarth und Kühnel 2020, S. 15; Seyffarth et al. 2019, S. 233.

5.4.2 Eigenschaften von Compliance-Prozessen

Die Definition alternativer Compliance-Prozesse basiert auf der Idee der getrennten Modellierung von Geschäfts- und Compliance-Prozessen und deren automatische Integration zur Entwurfszeit in den Geschäftsprozess, die um zwei weitere Aspekte erweitert wird:¹⁸⁶

- Sogenannte Compliance-Prozess-Muster können Compliance-Prozesse generalisieren.
- Alternative Compliance-Prozesse werden anhand ihrer Eigenschaften unterschieden.

Grundsätzlich können Compliance-Prozess-Muster zur Generalisierung von Compliance-Prozessen dienen. Das Compliance-Prozess-Muster weist keine weiteren Voraussetzungen zur Ausführung auf und ist generisch benannt. Wenn kein alternativer Compliance-Prozess gefunden wird, kann es als Platzhalter an der Stelle eingesetzt werden, an der sich der nicht mehr ausführbare Compliance-Prozess befindet. Eine Auswahl von Mustern sind in (Namiri und Stojanovic 2007b) und (Schultz 2013a) enthalten. Neben dem N-Wege-Vergleich umfassen sie das Vier-Augen-Prinzip, die Funktionstrennung oder die logische Zugriffskontrolle¹⁸⁷. In dem Szenario aus Abbildung 8 generalisiert das Compliance-Prozess-Muster N-Wege-Vergleich die Compliance-Prozesse „Rechnung kontrollieren“, „Rechnung manuell kontrollieren“ und „Zahlungsanordnung kontrollieren“.¹⁸⁸ Die Generalisierung des Compliance-Prozesses ist jedoch nicht zwingend notwendig. Verschiedene Compliance-Prozesse können auch direkt mit der Compliance-Anforderung verbunden werden, die sie sicherstellen.

Da Compliance-Prozesse mehr Eigenschaften als einen Trigger oder die Voraussetzung zur Ausführung haben,¹⁸⁹ wurde in (Seyffarth et al. 2017a) eine Taxonomie entwickelt, die Compliance-Prozesse anhand von 9 Dimensionen und 37 Charakteristika beschreibt.¹⁹⁰ Grundsätzlich eignen sich Taxonomien zur Klassifikation von Objekten und Elementen komplexer Domänen. Die Klassifizierung hilft bei dem Verständnis der Charakteristika facettenreicher und komplexer Objekte, wodurch die Entscheidungsfindung erleichtert wird.¹⁹¹ Die Charakteristika der Compliance-Prozess-Taxonomie dienen als Orientierungshilfe bei der Definition alternativer Compliance-Prozesse.¹⁹² Nichtsdestotrotz ist die konkrete Modellierung von Compliance-Prozessen weiterhin eine individuelle Aufgabe von Unternehmen und Organisationen. Sie haben die Kenntnis über die individuellen Abläufe der eigenen Geschäftsprozesse, den Umfang und Aufbau der eigenen IT-Infrastruktur und Compliance-Anforderungen.¹⁹³

Abbildung 9 zeigt die Compliance-Prozess-Taxonomie, deren Charakteristika für das weitere Verständnis der Arbeit im Folgenden kurz vorgestellt werden. Eine vollständige Diskussion aller

¹⁸⁶ Vgl. Seyffarth et al. 2019, S. 232; Sackmann und Kittel 2015, S. 250 ff.; Kittel et al. 2013b, S. 155 ff; Schumm et al. 2010a, S. 7 ff.

¹⁸⁷ Vgl. Schultz 2013a, S. 130 ff.; Namiri und Stojanovic 2007b, S. 185.

¹⁸⁸ Vgl. Seyffarth et al. 2019, S. 234; Namiri und Stojanovic 2007b, S. 185.

¹⁸⁹ Vgl. Schultz und Radloff 2014, S. 194; S. Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2012 90 ff.; Gehrke 2010, S. 1.

¹⁹⁰ Vgl. Seyffarth et al. 2017a, S. 77 ff.

¹⁹¹ Vgl. u.a. Mwilu et al. 2015, S. 1; Nickerson et al. 2013, S. 336.

¹⁹² Vgl. Seyffarth et al. 2019, S. 232.

¹⁹³ Vgl. Seyffarth und Kühnel 2020, S. 25.

Dimensionen und Charakteristika ist in (Seyffarth et al. 2017a) enthalten¹⁹⁴. Die Meta-Charakteristik „Integrationsbedingungen“ fasst Charakteristika zusammen, die für die Ausführung eines Compliance-Prozesses notwendig sind.¹⁹⁵ Verschiedene Charakteristika können die Notwendigkeit zur Ausführung eines Compliance-Prozesses triggern (D1) sowie Gegenstand der Compliance-Aktivität (D2) sein.¹⁹⁶ Der Trigger und der Gegenstand der Compliance-Aktivität müssen aus der Compliance-Anforderung abgeleitet werden.¹⁹⁷ Der Trigger kann durch die Anwesenheit einer Geschäftsaktivität oder eines Dokuments in Form von Daten vorliegen. Manchmal gibt es weitere Voraussetzung, die für die Ausführung eines Compliance-Prozesses gegeben sein müssen (D3)¹⁹⁸. In dem Szenario aus Abbildung 8 wird der Compliance-Prozess „Rechnung kontrollieren“ durch das Ereignis „Lieferung eingetroffen“ ausgelöst und benötigt als Ressource zur Ausführung eine IT-Komponente.¹⁹⁹

	Dimension	Charakteristika						
Integrationsbedingungen	D 1: Trigger	D 1.1: Geschäftsaktivität / -ereignis	D 1.2: Daten	D 1.3: Organisationseinheit	D 1.4: Ort	D 1.5: Ressource	D 1.6: Zeit	D 1.7: Frequenz d. Geschäftsprozessinstanz
	D 2: Gegenstand der Compliance-Aktivität	D 2.1: Geschäftsaktivität	D 2.2: Daten	D 2.3: Organisationseinheit	D 2.4: Ort	D 2.5: Ressource	D 2.6: Zeit	
	D 3: Weitere Voraussetzungen zur Ausführung	D 3.1: Daten	D 3.2: Organisationseinheit	D 3.3: Ort	D 3.4: Ressource	D 3.5: Zeit	D 3.6: Keine Voraussetzungen	
Modellierung	D 4: Compliance-Aktivität	D 4.1: N-Wege-Vergleich	D 4.2: Andere					
	D 5: Abweichungshandlung	D 5.1: Abweichungsanalyse	D 5.2: Umgang mit Abweichungen	D 5.3: Keine Abweichungshandlung				
	D 6: Integration in Geschäftsprozess	D 6.1: Sequentiell	D 6.2: Parallel	D 6.3: Starterereignis	D 6.4: Endereignis	D 6.5: Unabhängig		
Eigenschaften	D 7: Zeitpunkt	D 7.1: Preventiv	D 7.2: Detektiv					
	D 8: Typ	D 8.1: Anwendungskontrolle	D 8.2: Generelle IT-Kontrolle	D 8.3: Geschäftskontrolle				Gegenseitig ausschließende Charakteristika
	D 9: Ausführung	D 9.1: Automatisch	D 9.2: Manuell	D 9.3: Halbautomatisch				Kombinierbare Charakteristika

Abbildung 9. Compliance-Prozess-Taxonomie²⁰⁰

Die Meta-Charakteristik „Modellierung“ adressiert Möglichkeiten zur Modellierung eines Compliance-Prozesses auf Ebene des Prozessmodells. Compliance-Aktivitäten (D4) umfassen alle Aktivitäten, die für die Einhaltung von Compliance-Anforderungen notwendig sind.²⁰¹ Für eine Generalisierung notwendiger Compliance-Aktivitäten bietet sich die Verwendung passender Muster an. Muster sind domainspezifische Vorlagen mit einer hohen Abstraktionsebene, die zur Darstellung von Eigenschaften und Einschränkungen verwendet werden.²⁰² Folglich ist ein Compliance-Prozess-Muster eine Prozessvorlage, die Elemente (Aktivitäten, Gateways, Konnektoren)

¹⁹⁴ Vgl. Seyffarth et al. 2017a, S. 77 ff.

¹⁹⁵ Vgl. Seyffarth et al. 2017a, S. 77 f.

¹⁹⁶ Vgl. u.a. Ramezani et al. 2012a, S. 266; Gehrke 2010, S. 2; Namiri und Stojanovic 2007a, S. 65.

¹⁹⁷ Vgl. u.a. Ramezani et al. 2012a, S. 266; Namiri und Stojanovic 2007a, S. 65.

¹⁹⁸ Vgl. Seyffarth et al. 2017a, S. 79.

¹⁹⁹ Vgl. Seyffarth et al. 2019, S. 233.

²⁰⁰ In Anlehnung an Seyffarth et al. 2017a, S. 78.

²⁰¹ Vgl. Seyffarth et al. 2017a, S. 72.

²⁰² Vgl. Turetken et al. 2011, S. 8.

für die Sicherstellung mindestens einer Compliance-Anforderung beinhaltet.²⁰³ Ein Beispiel für ein Compliance-Prozess-Muster ist ein N-Wege-Vergleich, bei dem Soll-Ist-Vergleiche zwischen zwei oder mehreren Daten vorgenommen werden.²⁰⁴

Neben Compliance-Aktivitäten umfassen Compliance-Prozesse ggf. Abweichungshandlungen (D5). Eine Abweichungshandlung kann die Analyse der Abweichung und verschiedene Formen im Umgang mit der Abweichung umfassen. Denkbare Möglichkeiten zu dem Umgang mit festgestellten Abweichungen sind die Eskalation oder das Abbrechen der betroffenen Geschäftsprozessinstanz.²⁰⁵ Der Compliance-Prozess kann außerdem in unterschiedlichen Varianten in den Geschäftsprozess integriert werden oder unabhängig von diesem ausgeführt werden (D6). Unabhängig vom Geschäftsprozess können in der Regel die Compliance-Prozesse des Typs Generelle IT-Kontrollen ausgeführt werden.²⁰⁶ Weiterhin können Compliance-Prozesse durch den Ausführungszeitpunkt, Typen und Umfang der IT-Unterstützung charakterisiert werden, die sich aus den vorherigen Eigenschaften ableiten lassen. Der Ausführungszeitpunkt (D7) unterscheidet zwischen präventiven und detektiven Compliance-Prozessen.²⁰⁷ Weiterhin werden verschiedene Typen (D8) unterschieden, die sich ebenfalls in der IT-Unterstützung ihrer Ausführung (D9) unterscheiden.²⁰⁸

Da in dieser Arbeit lediglich die Sichten Compliance-Anforderungen, Kontrollflussicht und IT-Komponenten auf Geschäftsprozesse betrachtet werden, lösen Geschäftsaktivitäten und -ereignisse den Trigger (D1.1) aus. Der Gegenstand der Compliance-Handlung bestimmt den frühestens Integrationspunkt in den Geschäftsprozess. Aufgrund der betrachteten Sichten wird der Gegenstand der Compliance-Handlung mit dem Trigger gleichgesetzt. Als weitere Voraussetzung für die Ausführung dienen IT-Komponenten (D3.4). Der Aufbau des Compliance-Prozesses spielt für die vorgeschlagene Methode der Suche und Integration alternativer Compliance-Prozesse keine Rolle, von daher werden Compliance-Prozesse lediglich als Subprozesse modelliert. Die Integration in den Geschäftsprozess erfolgt sequentiell (D6.1).

5.4.3 Struktur eines alternativen Compliance-Prozess-Graphs

Die weiteren Erläuterungen basieren auf der Struktur des alternativen Compliance-Prozess-Graphs. Er bildet Compliance-Anforderungen mit dazugehörigen Compliance-Prozess-Mustern und Compliance-Prozessen ab.²⁰⁹

Definition 6 (Alternativer Compliance-Prozess-Graph): Ein alternativer Compliance-Prozess-Graph ist ein gerichteter Graph $AG = (N^{AG}, E^{AG}, n_{identify}^{AG}, n_{type}^{AG}, n_{rule}^{AG})$, wobei N^{AG} eine nicht

²⁰³ Vgl. Seyffarth et al. 2019, S. 233.

²⁰⁴ Vgl. Seyffarth et al. 2017a, S. 79; Namiri und Stojanovic 2007b, S. 185.

²⁰⁵ Vgl. Namiri und Stojanovic 2007a, S. 64.

²⁰⁶ Vgl. u.a. ISACA (Hg) 2012, S. 53; Institut der Wirtschaftsprüfer (IDW) (Hg) 2002, S. 17 ff.

²⁰⁷ Vgl. u.a. Schultz und Radloff 2014, S. 194; Gehrke 2010, S. 2; IT Governance Institute (ITGI) 2006, S. 36.

²⁰⁸ Vgl. u.a. The Institute of Internal Auditors (IIA) 2012, S. 17; Bellino et al. 2007, S. 12; IT Governance Institute (ITGI) 2006, S. 13.

²⁰⁹ Vgl. Seyffarth und Kühnel 2020, S. 16; Seyffarth et al. 2019, S. 235.

leere und endliche Menge an Knoten ist und $E^{AG} \subseteq N^{AG} \times N^{AG}$ eine Menge an gerichteten Kanten zwischen den Knoten ist. Eine gerichtete Kante $e_{i,j}^{AG}$ verbindet die Knoten n_i^{AG} und n_j^{AG} . Der Knotentyp von n_i^{AG} wird durch die Funktion $n_{type}^{AG}(n_i^{AG}) = \{Complianceanforderung: n_i^{AG} \in CAG; Complianceprozess: n_i^{AG} \in CP; Complianceprozessmuster\}$ definiert.²¹⁰

Die Knoten des alternativen Compliance-Graphs können entweder vom Typ Compliance-Anforderung, Compliance-Prozess oder Compliance-Prozess-Muster sein. Zur Sicherstellung der Struktur von AG werden die zugelassenen Kanten nur zwischen Knoten eines bestimmten Knotentyps definiert. Dementsprechend können Kanten nur zwischen Knoten des Typs Compliance-Anforderung und Compliance-Prozessmuster, Compliance-Anforderung und Compliance-Prozess, Compliance-Prozess und Compliance-Prozess-Muster sowie zwischen Compliance-Prozess-Mustern definiert werden.²¹¹

Die Funktionen $n_{identify}^{AG}(n_i^{AG})$ und $n_{rule}^{AG}(n_i^{AG})$ weisen dem Knoten n_i^{AG} eine eindeutige ID und eine Compliance-Regel zu. Jede Compliance-Regel besteht aus einem Trigger, einem spätesten Integrationspunkt und notwendigen IT-Komponenten zur Ausführung des Compliance-Prozesses. Der Trigger zeigt an, an welcher Stelle der Compliance-Prozess frühestens in den Kontrollfluss des Geschäftsprozessmodells zu integrieren ist. Der späteste Integrationspunkt definiert bis vor welcher Geschäftsaktivität der Compliance-Prozess ausgeführt werden muss, damit die Compliance-Anforderung eingehalten wird.²¹²

Jeder Bestandteil der Regel muss nach der entsprechenden Aktivität oder dem entsprechenden Ereignisses des Geschäftsprozesses bzw. der notwendigen IT-Komponente benannt werden. Das kann zu Herausforderungen in der Eindeutigkeit der Benennung führen²¹³. Eine erste, einfache Lösung für diese Herausforderung ist eine angemessene Werkzeugunterstützung zur der Modellierung der Compliance-Regeln. Für die Regeldefinition sollten nur Elemente vorgeschlagen werden, die in den importierten Geschäftsprozess- und IT-Architekturmodellen vorhanden sind.²¹⁴

5.4.4 Suchen und integrieren alternativer Compliance-Prozesse

Die Suche nach alternativen Compliance-Prozessen in AG kann zu drei möglichen Ergebnissen führen. Erstens: es gibt nur einen alternativen ausführbaren Compliance-Prozess. In diesem Fall wird der resultierende Compliance-konforme Geschäftsprozess vorgeschlagen. Zweitens: es gibt mehrere alternative Compliance-Prozesse, die ausgeführt werden können. In diesem Fall werden alle daraus resultierenden Varianten Compliance-konformer Geschäftsprozesse vorgeschlagen. Drittens: es gibt keinen ausführbaren alternativen Compliance-Prozess. In dem Fall wird das Compliance-Prozess-Muster des nicht mehr ausführbaren Compliance-Prozesses n_i^{AG} ermittelt. Das geschieht durch die Suche nach Vorgängern von n_i^{AG} des Typs Compliance-Prozess-Muster

²¹⁰ Vgl. Seyffarth und Kühnel 2020, S. 16 f.; Seyffarth et al. 2019, S. 235.

²¹¹ Vgl. Seyffarth et al. 2019, S. 235.

²¹² Vgl. Seyffarth und Kühnel 2020, S. 16 f.

²¹³ Vgl. u.a. Klinkmüller und Weber 2017, S. 9 ff.; Leopold et al. 2015, S. 404 ff.

²¹⁴ Vgl. Seyffarth und Raschke 2020, S. 109 f.

in AG . Das gefundene Compliance-Prozess-Muster wird an der Stelle von n_i^{AG} in den Geschäftsprozess integriert.²¹⁵ Sollte kein Compliance-Prozess-Muster gefunden werden, kann der Geschäftsprozess nicht Compliance-konform adaptiert werden.

Der Algorithmus zum Vorschlagen Compliance-konformer Geschäftsprozessmodelle aus Abbildung 10 kann wie folgt beschrieben werden. Die Suche nach alternativen Compliance-Prozessen startet bei n_i^{AG} , dem nicht mehr ausführbaren Compliance-Prozess in rg . Der Ergebnisgraph rg ist das Resultat der Auswirkungsidentifikation durch das Entfernen eines Elements (siehe Kapitel 5.3.3). Anschließend werden in AG alle Geschwisterknoten des Typs „Compliance-Prozess“ von n_i^{AG} gesucht. Danach wird für jeden gefundenen Compliance-Prozess dessen Compliance-Regel geprüft. Die Compliance-Regel umfasst die Präsenz von Geschäftsaktivitäten oder Ereignissen im Geschäftsprozessmodell und, sofern notwendig, die Anwesenheit von IT-Komponenten. Die An- und Abwesenheit dieser Elemente wird anhand des Ergebnisgraphen rg geprüft. Sollte in rg mindestens ein Element vorhanden sein, das ebenfalls in der Compliance-Regel enthalten ist, kann der Compliance-Prozess nicht integriert werden. Würde in dem Ausgangsszenario aus Kapitel 2.3 bspw. der Server entfernt werden, können die IT-Komponenten „ERP FI“ und „ERP MM“ nicht mehr ausgeführt werden. In diesem Fall würde der Compliance-Prozess „Zahlungsanordnung kontrollieren“ aus Abbildung 8 nicht als alternativer Compliance-Prozess identifiziert werden, da er zur Ausführung die IT-Komponente „ERP FI“ benötigt wird.

<pre> Input: alternative graph ag, result graph rg, process graph pg 1 // get all violated compliance processes 2 Foreach cp in (get all violated compliance processes in rg) do 3 // get all alternative compliance processes 4 Foreach sibling_cp in (get sibling compliance processes of cp) do 5 // check the executability of alternative compliance process 6 req_it = sibling_cp.getRequiredIT 7 trigger = sibling_cp.getTrigger 8 If (req_it OR req_it.predecessor not in rg) AND (trigger not in rg) 9 add sibling_cp to alternatives 10 // search for compliance process patterns 11 If (alternatives is empty) 12 add get_all_successor(cp, type(suc_cp)=compliance process pattern) to alternatives 13 // integrate alternative cp into the business process graph pg 14 Foreach element in alternatives do 15 bp = pg 16 removeViolatedComplianceProcess from bp 17 integrate element in bp 18 add bp to compliantBusinessProcesses Output: list process_graph compliantBusinessProcesses </pre>

Abbildung 10. Pseudocode für das Adaptieren Compliance-konformer Geschäftsprozesse²¹⁶

²¹⁵ Vgl. Seyffarth et al. 2019, S. 235.

²¹⁶ In Anlehnung an Seyffarth und Kühnel 2020, S. 17.

6 Demonstration und Evaluation der Artefakte

In diesem Kapitel werden zunächst die Evaluationsepisoden der Dissertation in das Framework zur Evaluation von Design Science Research-Projekten (FEDS)²¹⁷ eingeordnet. Anschließend werden der Aufbau und die Ergebnisse der Fallstudie zur Evaluation der wahrgenommenen Nützlichkeit von MIA vorgestellt. Die Evaluation ist in der eingebrachten Publikation (Seyffarth und Kühnel 2020) kommuniziert.

6.1 Einordnung der Evaluationsepisoden

FEDS besteht aus drei Dimensionen: dem funktionalen Zweck der Evaluation, dem Paradigma der Evaluation und der Evaluationsstrategie.²¹⁸ Für den Fall, dass eine Evaluation mit realen Benutzern, Systemen und weiteren realen Randbedingungen nur mit sehr hohem Aufwand möglich ist, empfehlen Venable et al. die Evaluationsstrategie „Technical Risk and Efficacy“, der in dieser Arbeit gefolgt wurde. Diese Evaluationsstrategie reduziert das technische Risiko der Umsetzung durch die Durchführung formativer und künstlicher Evaluationen bereits zu Beginn des DSR-Projekts.²¹⁹ Eine formative Evaluation hilft bei der Verbesserung von Artefakten während ihrer Konstruktion.²²⁰ Im Gegensatz zur formativen Evaluation ist der Zweck einer summativen Evaluation festzustellen, inwieweit ein Artefakt die Erwartungen erfüllt.²²¹ Eine künstliche Evaluation kann u.a. in Form eines Softwareprototypens erfolgen, wohingegen eine natürliche Evaluation durch den Einsatz des Artefakts in einem realen Szenario erfolgt.²²²

Tabelle 5 gibt einen Überblick über die vier Evaluationsepisoden von MIA. In Evaluationsepisode 1 wurden sowohl das konzeptuelle Domänenmodell als auch die Compliance-Prozess-Taxonomie durch strukturierte Literatursuchen ex ante evaluiert²²³. Die Umsetzbarkeit von Artefakten kann mit einem Softwareprototyp demonstriert²²⁴ bzw. evaluiert²²⁵ werden. Daher wurden in Evaluationsepisode 2 die grundsätzliche Umsetzbarkeit der ersten beiden Schritte in einem Java-basierten Softwareprototyp demonstriert²²⁶. Die daraus abgeleiteten Erkenntnisse bildeten die Basis für den vorläufigen Softwareprototypen BCIT (Business Process, Compliance and IT), der in (Seyffarth und Raschke 2018) kommuniziert wurde.²²⁷ BCIT steht mit seinem Quellcode, einem Tutorial und einem Demoprojekt bereit zur freien Verwendung unter <https://github.com/tobiasseyffarth/BCIT-electron>.

²¹⁷ Venable et al. 2016, S. 77 ff.

²¹⁸ Vgl. Venable et al. 2016, S. 80.

²¹⁹ Vgl. Venable et al. 2016, S. 82.

²²⁰ Vgl. Venable et al. 2016, S. 80.

²²¹ Vgl. Venable et al. 2016, S. 80; Hevner et al. 2004, S. 83.

²²² Vgl. Venable et al. 2016, S. 80 f.

²²³ Vgl. Sonnenberg und Vom Brocke 2012, S. 77.; Sein et al. 2011, S. 42 f.; Pries-Heje et al. 2008, S. 2 f.

²²⁴ Vgl. Sonnenberg und Vom Brocke 2012 S. 78; Peffers et al. 2006, S. 90.

²²⁵ Vgl. Peffers et al. 2012, S. 400; Hevner et al. 2004, S. 338.

²²⁶ Vgl. Seyffarth et al. 2018, S. 181 ff.

²²⁷ Vgl. Seyffarth und Raschke 2018, S. 83 ff.

Tabelle 5. Evaluationsepisoden von MIA²²⁸

Episode	Zweck	Paradigma	Fokus	Evaluationsmethode	Evaluationsergebnis
1	Formativ	Künstlich	Konzeptuelles Domänenmodell, Compliance-Prozess-Taxonomie	Ex ante Evaluation durch eine strukturierte Literatursuche	Evaluiertes konzeptuelles Domänenmodell und Compliance-Prozess-Taxonomie
2	Formativ	Künstlich	Schritt 1 und Schritt 2 von MIA	Prototyping und Diskussion mit Fachpublikum	Vorläufiger Softwareprototyp BCIT
3	Formativ	Künstlich	Schritt 3 von MIA	Prototyping und Diskussion mit Fachpublikum	Erweiterter Softwareprototyp BCIT
4	Summativ	Lebensnah, realistisch	Erweiterter Softwareprototyp BCIT	Fallstudie mit Domänenexpert:innen	Wahrgenommene Nützlichkeit von BCIT

6.2 Erweiterter Softwareprototyp BCIT

In Evaluationsepisode 3 wurde BCIT um die Funktion der Compliance-konforme Adaption des Geschäftsprozesses (Schritt 3 von MIA) erweitert.²²⁹ Der Softwareprototyp ist mit Quellecode, Tutorial, Demoprojekten und einem Screencast zur freien Verwendung unter <https://github.com/tobiasseyffarth/BCIT> verfügbar.

Abbildung 11 zeigt den Technologie-Stack von BCIT, einer Webapp auf Basis von Node.js²³⁰. Das Frontend basiert auf dem Single-Page-Application-Framework React.js²³¹, dessen Benutzeroberfläche mit Komponenten von PrimeReact²³² umgesetzt wurde. Zum Parsen und Visualisieren von BPMN-Modellen wurde camunda-bpmn.js²³³ verwendet. Die Modellierung des integrierten Compliance-Graphen und die Visualisierungen des integrierten Compliance-Graphen und des IT-Architektur-Modells wurden mit Cytoscape.js²³⁴ umgesetzt.

²²⁸ In Anlehnung an Seyffarth und Kühnel 2020, S. 20.

²²⁹ Seyffarth und Raschke 2020.

²³⁰ OpenJS Foundation 2020.

²³¹ Facebook Inc. (Hg) 2020.

²³² Primefaces (Hg) 2020.

²³³ Camunda (Hg) 2020.

²³⁴ Franz et al. 2016.

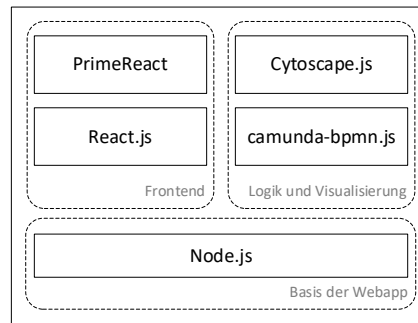


Abbildung 11. Technologie-Stack von BCIT

Abbildung 12 zeigt die in BCIT implementierten Schritte. Im ersten Schritt müssen das Modell des Geschäftsprozesses, der IT-Architektur und Compliance-Anforderungen importiert werden. Der Import des Geschäftsprozesses wurde exemplarisch anhand von BPMN-Modellen²³⁵ demonstriert. Der Import von IT-Architekturen wurde exemplarisch anhand des Open Group ArchiMate Model Exchange File Format²³⁶ demonstriert. Compliance-Anforderungen können in Form von XML-basierte Gesetzestexte²³⁷ importiert werden.

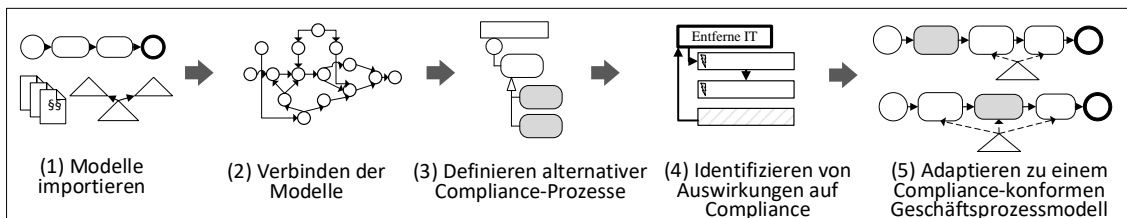


Abbildung 12. Schritte in BCIT

Während des Modellimports werden alle Modelle in einen Graphen transformiert. Anschließend müssen notwendige Verbindungen zwischen den importierten Modellen im zweiten Schritt händisch definiert werden. Beim Verbinden von Compliance-Anforderungen, Aktivitäten und IT-Komponenten erzeugt BCIT automatisch die entsprechenden Kanten zwischen den entsprechenden Knoten des Graphen. Abbildung 13 zeigt exemplarisch die Oberfläche zum Verbinden von IT-Komponenten mit Geschäftsaktivitäten. Daneben ist ein Beispiel des integrierten Compliance-Graphs abgebildet.

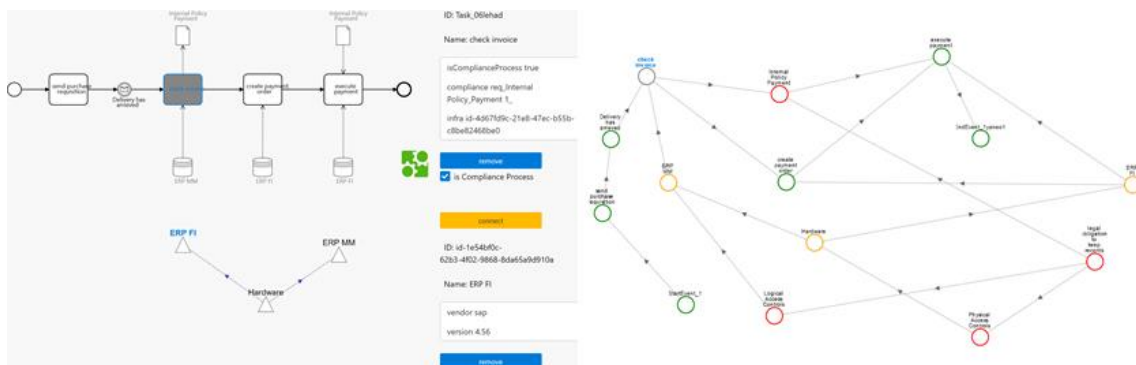


Abbildung 13. Verbinden von Elementen und integrierter Compliance-Graph

²³⁵ Vgl. OMG (Hg) 2011, S 54 ff.

²³⁶ Vgl. The Open Group (hg) 2019.

²³⁷ <https://www.gesetze-im-internet.de/gii-toc.xml>

Im dritten Schritt müssen zu Compliance-Anforderungen alternative Compliance-Prozesse definiert werden. An dieser Stelle ist ebenfalls eine Generalisierung der Compliance-Prozesse durch Compliance-Prozess-Muster möglich. Im vierten Schritt werden automatisch die Auswirkungen auf die Erhaltung von Compliance identifiziert. Jedes Element der importierten Modelle kann dabei als zu entfernendes oder zu ersetzendes Element markiert werden. Abbildung 14 zeigt exemplarisch die Auswirkungen auf die Erhaltung von Compliance beim Entfernen der IT-Komponente „ERP MM“. Im Fall einer festgestellten Verletzung von Compliance-Anforderungen des Geschäftsprozesses, schlägt BCIT in Schritt fünf automatisch Compliance-konforme Geschäftsprozessmodelle vor. Abbildung 15 zeigt einen adaptierten, Compliance-konformen Geschäftsprozess.

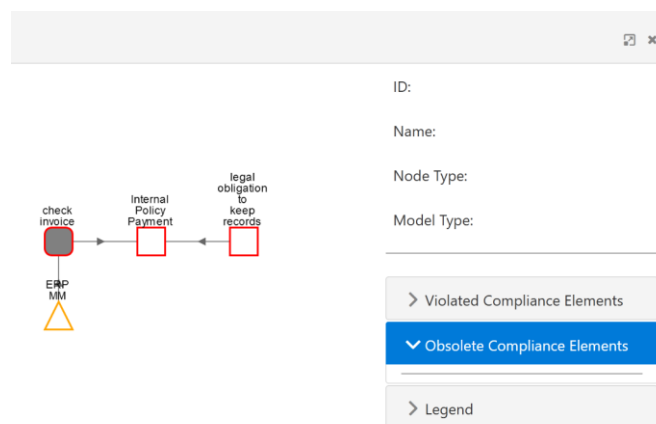


Abbildung 14. Auswirkungen auf Compliance beim Entfernen von „ERP MM“

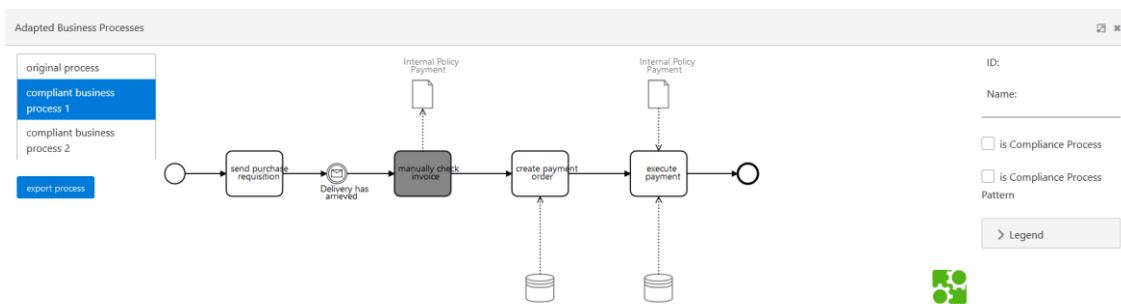


Abbildung 15. Adaptierter Compliance-konformer Geschäftsprozess in BCIT²³⁸

6.3 Evaluation der wahrgenommenen Nützlichkeit

Das Ziel von DSR ist das Lösen identifizierter organisationaler Probleme, wobei die Nützlichkeit der Lösung durch Evaluationen bestimmt werden soll.²³⁹ Dementsprechend wurde in Evaluationsepisode 4 die wahrgenommene Nützlichkeit von BCIT in Fallstudien durch Domänenexperten:innen bewertet. BCIT demonstriert die Umsetzung der Algorithmen aus Kapitel 5 demonstriert und zeigt alle notwendigen Voraussetzungen zur Umsetzung von MIA in der Praxis. Für den praktischen Einsatz von BCIT müssen u.a. Compliance-Anforderungen, Geschäftsprozessmodelle und IT-Architekturmodellen vorliegen und alternative Compliance-Prozesse modelliert werden.

²³⁸ Seyffarth und Kühnel 2020, S. 21.

²³⁹ Vgl. Hevner et al. 2004, S. 82; March und Smith 1995, S. 224.

6.3.1 Fallstudienaufbau

Der Aufbau der Fallstudie orientiert sich an dem Vorschlag von Robson (2009) und besteht aus vier Teilen.²⁴⁰ Als erstes wurde den Teilnehmer:innen das Ziel der Fallstudie vorgestellt, bevor anschließend die Problemstellung und die grundlegenden Konzepte zur Problemlösung präsentiert wurden. Die Lösung der Problemstellung wurde danach in dem erweiterten Softwareprototypen BCIT demonstriert. Die abschließende Datenerhebung zur wahrgenommenen Nützlichkeit von BCIT erfolgte mit Fragebögen²⁴¹.

Der Fragebogen basiert auf Aussagen des Technology Acceptance Models (TAM).²⁴² TAM ist ein weit verbreitetes Modell zur Beschreibung und Vorhersage der Nützlichkeit von Informationssystemen auf Basis der wahrgenommenen Nützlichkeit und Benutzerfreundlichkeit.²⁴³ Trotz dass die Reliabilität und Validität von TAM in vorherigen Studien bestätigt wurde, ist TAM nicht frei von Kritik.²⁴⁴ Einerseits werden die Methoden zur Evaluation von TAM, insbesondere die Teilnahme von Studierenden und die Nutzung selbsterhobenen Daten anstelle realer Daten kritisiert.²⁴⁵ Weitere Kritik bezieht sich auf die Abhängigkeiten der Elemente von TAM und ihr Einfluss auf die tatsächliche Systemnutzung²⁴⁶. Darüber hinaus wird die wenig fundierte theoretische Begründung der Beziehungen zwischen den Konstrukten von TAM kritisiert.²⁴⁷ Im Fragebogen wurden nur Aussagen zur wahrgenommenen Nützlichkeit verwendet, wodurch die Einflüsse zwischen weiteren Konstrukten von TAM für die Fallstudiedurchführung zu vernachlässigen sind. Darüber hinaus haben nur Domänenexpert:innen an der Fallstudie teilgenommen.

Alle Aussagen zur wahrgenommenen Nützlichkeit wurden durch die Teilnehmer:innen auf einer Likert-Skala bewertet. Die 7-stufige Intervall-skalierte Likert-Skala reichte von „Stimme überhaupt nicht zu“ (-3) bis „Stimme voll zu“ (+3). Jede Aussage konnte außerdem kommentiert oder mit „keine Antwort“ beantwortet werden. In der Auswertung wurden die Aussagen den Kategorien (A) „Arbeitseffizienz“, (B) „Produktivität und Zeitersparnis“, (C) „Bedeutung des Systems für die Arbeit der Benutzer:in“, (D) „Kontrolle über die Arbeit“ und (E) „Gesamtbeurteilung“ zugeordnet²⁴⁸. Die Fallstudie wurde acht Mal mit insgesamt 41 verschiedenen Domänenexpert:innen durchgeführt. Der Fragebogen war auf freiwilliger Basis auszufüllen, was zu 24 Rückläufern führte und einer Rücklaufquote von 58% entspricht. Die Mehrheit der Teilnehmer:innen sind in großen Unternehmen und in den Branchen Finanzen oder IT-Dienstleistung tätig. Weitere sind in einer großen deutschen Forschungseinrichtung oder in kleinen Beratungsunternehmen beschäftigt. Die Teilnehmer:innen arbeiten in den Bereichen Compliance-Management (bspw. Leitung der Internen Revision, Chief Compliance Officer, IT-Risikomanager, Auditor), Geschäftspro-

²⁴⁰ Vgl. Robson 2009.

²⁴¹ Vgl. Kriglstein et al. 2016, S. 400; Runeson und Höst 2009, S. 142.

²⁴² Vgl. Davis 1989, S. 320.

²⁴³ Vgl. Lee et al. 2003, S. 756; Moody 2003, S. 3; Davis 1989, S. 320.

²⁴⁴ Vgl. Moody 2003, S. 4; Venkatesh 1999, S. 247 ff.; Davis 1989, S. 327 ff.

²⁴⁵ Vgl. u.a. Yousafzai et al. 2007; Lee et al. 2003.

²⁴⁶ Vgl. u.a. Brown et al. 2017.

²⁴⁷ Vgl. Bagozzi 2007, S. 245 ff.

²⁴⁸ Vgl. Seeliger et al. 2019, S. 228.

zessmanagement (bspw. Leitung des Prozessmanagements, Prozessmanager) oder IT-Architekturmanagement (bspw. IT-Architekt, IT-Projektmanager). Die Berufserfahrungen liegen zwischen 4 und 32 Jahren.

6.3.2 Diskussion der Testgütekriterien

Die Validität einer Studie beschreibt, zu welchem Grad die Ergebnisse der Studie wahr sind und sie nicht durch Einflüsse der Initiatoren der Studie beeinflusst wurden.²⁴⁹ Im Software Engineering können die Testgütekriterien der Konstruktvalidität, Interne Validität, Externe Validität und Reliabilität unterschieden werden.²⁵⁰ Im Folgenden wird jeweils kurz beschrieben, wie diese Testgütekriterien bei dem Entwurf und der Durchführung der Fallstudie berücksichtigt wurden.

Die Konstruktvalidität gibt an, inwieweit die richtigen Dinge gemessen wurden.²⁵¹ Diesem Testgütekriterium wurde genüge getan, indem standardisierter Fragen nach TAM zur wahrgenommenen Nützlichkeit eines Informationssystems verwendet wurden.²⁵² Die interne Validität ist zu beachten, wenn kausale Zusammenhänge betrachtet werden.²⁵³ Da in der Fallstudie keine kausalen Zusammenhänge betrachtet wurden, ist die interne Validität von geringer Bedeutung. Dennoch ist das Risiko vorhanden, dass eine untersuchte Variable von anderen Faktoren abhängt. Zur Verringerung dieses Risikos waren alle Iterationen der Fallstudie identisch aufgebaut. Außerdem kann die Berufspraxis jeder Teilnehmer:innen für das Verständnis der Fallstudie als angemessen angesehen werden.²⁵⁴ Die externe Validität beschreibt die Verallgemeinerbarkeit der Evaluationsergebnisse.²⁵⁵ Die teilnehmenden Personen der Umfrage sind in unterschiedlichen Rollen und in Unternehmen verschiedener Branchen tätig. Die Verallgemeinerbarkeit der Ergebnisse kann durch eine größere Anzahl an teilnehmenden Personen aus weiteren Branchen weiter erhöht werden.²⁵⁶ Die Reliabilität beschreibt die Forscherunabhängigkeit zwischen dem Aufbau der Fallstudie und den Evaluationsergebnissen.²⁵⁷ Durch einen identischen Ablauf der Fallstudien und die Verwendung von Standardfragen in den Fragebögen wurde versucht, diesem Testgütekriterium zu entsprechen.²⁵⁸

²⁴⁹ Vgl. Wohlin et al. 2012, S. 68; Friedrichs 1990, S. 100.

²⁵⁰ Vgl. Wohlin et al. 2012, S. 68.

²⁵¹ Vgl. Wohlin et al. 2012, S. 68.

²⁵² Vgl. Seyffarth und Kühnel 2020, S. 23.

²⁵³ Vgl. Wohlin et al. 2012, S. 68; Wrona 2006, S. 204 ff.

²⁵⁴ Vgl. Seyffarth und Kühnel 2020, S. 24.

²⁵⁵ Vgl. Wohlin et al. 2012, S. 68 f.; Wrona 2006, S. 206 f.

²⁵⁶ Vgl. Seyffarth und Kühnel 2020, S. 24.

²⁵⁷ Vgl. Wohlin et al. 2012, S. 69; Wrona 2006, S. 207.

²⁵⁸ Vgl. Seyffarth und Kühnel 2020, S. 24 f.

6.3.3 Fallstudienenergebnisse und Diskussion der Ergebnisse

Tabelle 6 fasst die Fallstudienenergebnisse zur wahrgenommenen Nützlichkeit zusammen. Der Fragebogen und die Antworten aller Rückläufer sind unter <https://github.com/tobiasseyffarth/bcit/tree/master/resources/3-evaluation> verfügbar.

Tabelle 6. Wahrgenommene Nützlichkeit von BCIT²⁵⁹

Kategorie	Aussage	Mittelwert	Standardabweichung	Median	Anzahl
A	A1: Ich kann mir vorstellen, dass die Verwendung von BCIT die Qualität meiner Arbeit verbessert.	1,043	1,574	2	23
A	A6: Ich kann mir vorstellen, dass die Verwendung von BCIT meine Arbeitsleistung verbessert.	0,455	1,437	1	22
A	A8: Ich kann mir vorstellen, dass die Verwendung von BCIT meine Effektivität am Arbeitsplatz erhöht.	0,409	1,586	1	22
B	A3: Ich kann mir vorstellen, dass die Verwendung von BCIT es mir ermöglicht, meine Arbeit schneller zu erledigen.	0,727	1,420	1	22
B	A5: Ich kann mir vorstellen, dass die Verwendung von BCIT meine Produktivität steigert.	0,429	1,466	0	21
B	A7: Ich kann mir vorstellen, dass die Verwendung von BCIT es mir ermöglicht mehr Aufgaben zu erledigen, als es sonst möglich wäre.	0,609	1,635	1	23
C	A4: Ich kann mir vorstellen, dass die Verwendung von BCIT kritische Aspekte meiner Arbeit unterstützt.	1,318	1,394	2	22
C	A9: Ich kann mir vorstellen, dass die Verwendung von BCIT es mir leichter macht, meinen Job zu machen.	0,522	1,559	1	23
D	A2: Ich kann mir vorstellen, dass die Verwendung von BCIT mir eine größere Kontrolle über die Arbeit gibt, die ich tue.	1,000	1,826	2	24
E	A10. Insgesamt kann ich mir vorstellen, dass BCIT nützlich für meinen Job ist.	1,083	1,441	1,5	24
A: Arbeitseffizienz, B: Produktivität und Zeitersparnis, C: Bedeutung des Systems für die Arbeit der Benutzer:in, D: Kontrolle über die Arbeit, E: Gesamtbeurteilung					

Abbildung 16 zeigt den Boxplot der Evaluationsergebnisse. Wie Aussage 10 zeigt, wird der erweiterte Softwareprototyp BCIT von einer Mehrheit der Domänenexpert:innen als nützlich be-

²⁵⁹ In Anlehnung an Seyffarth und Kühnel 2020, S. 23.

wertet. Der Mehrheit der teilnehmenden Personen gefällt außerdem die Idee, Compliance-Anforderungen, Geschäftsprozesse und IT-Komponenten in einem Modell abzubilden. Weiterhin kommentierten einige Teilnehmer:innen, dass IT- und Compliance-Abhängigkeiten mit Hilfe des Modells abgebildet werden können, wodurch Aussagen über Ursache-Wirkungszusammenhänge getroffen werden können, die zu Wettbewerbsvorteilen führen können. Diese Kommentare erklären die Bewertungen zu Aussage 1 (Qualität der Arbeit), Aussage 4 (Unterstützung kritischer Aspekte) und Aussage 2 (größere Kontrolle über die Arbeit).

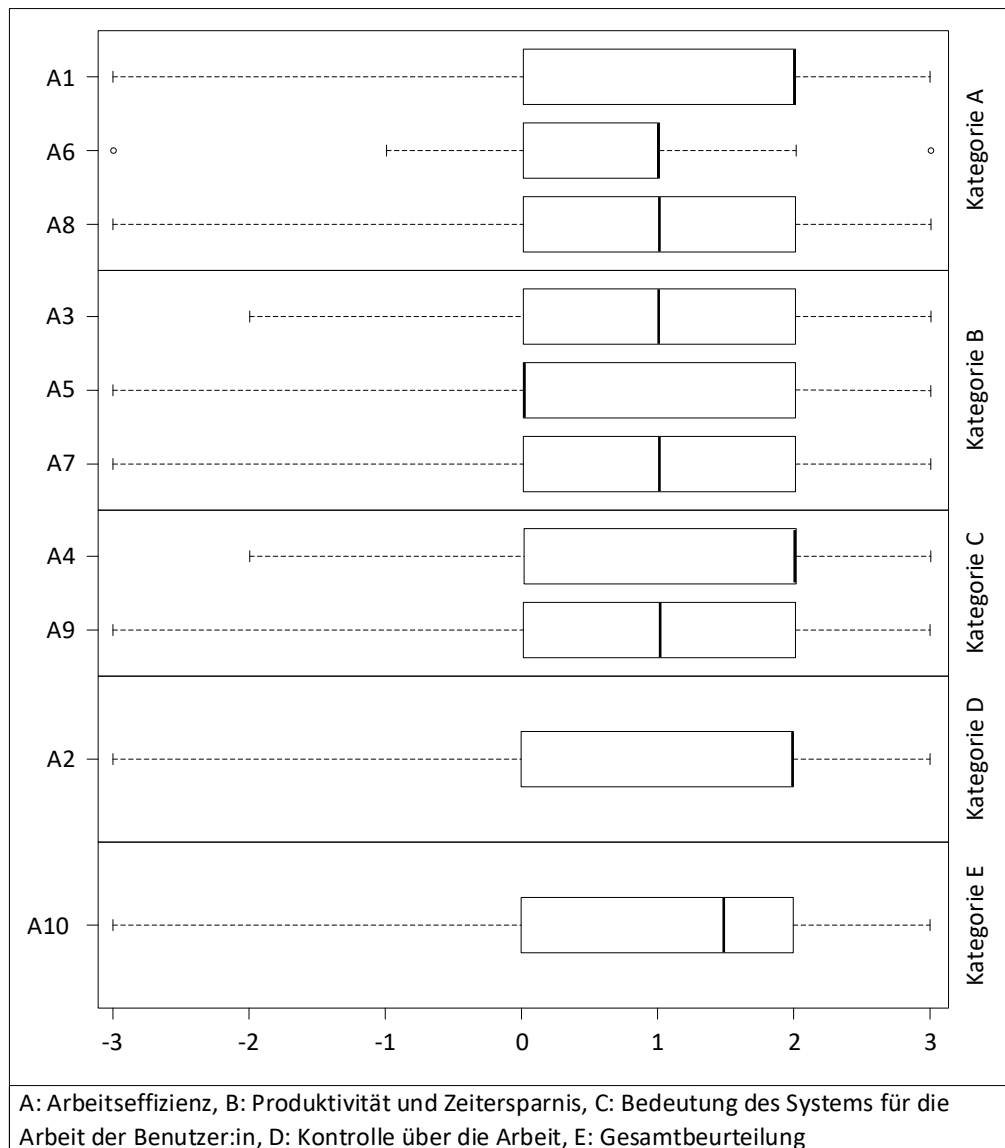


Abbildung 16. Boxplot der Evaluationsergebnisse²⁶⁰

Einige Aussagen des Fragebogens werden von den Domänenexpert:innen auch kritisch bewertet. Vaishnavi et al. (2017) folgend, werden daher im Folgenden die Abweichungen der Evaluation zu den erwarteten Ergebnissen beschrieben²⁶¹. Aussage 6 (Verbesserung der Arbeitsleistung),

²⁶⁰ In Anlehnung an Seyffarth und Kühnel 2020, S. 24.

²⁶¹ Vgl. Vaishnavi et al. 2017, S. 9.

Aussage 8 (Steigerung der Effektivität) und Aussage 5 (Steigerung der Produktivität) sind im Vergleich zu den anderen Aussagen schlechter bewertet. Den Kommentaren der teilnehmenden Personen zufolge, können Bedenken für den generellen Modellierungsaufwand von Geschäftsprozessen und IT-Architekturen ein Grund für die schlechtere Bewertung dieser Aussagen sein. Darüber hinaus wird von vier Umfrageteilnehmern der Aufwand zur Modellierung und Pflege alternativer Compliance-Prozesse als zu hoch im Vergleich zum erwarteten Nutzen angesehen.

7 Diskussion

Wie von Gregor und Hevner gefordert, werden in diesem Kapitel sowohl die Limitationen von MIA als auch ihre Implikationen für Wissenschaft und Praxis diskutiert.²⁶²

7.1 Limitationen

Bei der Identifikation der Auswirkungen von Veränderungen auf die Erhaltung von Compliance wurden die Muster „Element ersetzen“ und „Element entfernen“ betrachtet. Nichtsdestotrotz kann das Muster „Element einfügen“ umgesetzt werden, wenn neue Elemente manuell in den integrierten Compliance-Graph eingefügt und die Beziehungen zu den bestehenden Knoten modelliert werden. Durch die Identifikation der Auswirkungen auf die Erhaltung von Compliance vor- und nach dem Einfügen eines neuen Elements kann die Auswirkungen auf die Erhaltung von Compliance durch das Einfügen eines neuen Elements identifiziert werden. Analog verhält es sich mit dem Muster „Element updaten“. Sollten sich durch das Verändern von Eigenschaften eines Elements neue Beziehungen zu bestehenden Knoten ergeben, können die Auswirkungen dann durch das Anwenden des Musters „Element einfügen“ bestimmt werden.

Außerdem kann MIA keine Auswirkungen neuer Richtlinien, Verträge oder Gesetze ohne explizite Modellierung auf bestehende Compliance-Anforderungen, Geschäftsprozesse oder IT-Komponenten identifizieren.²⁶³ Dazu müssen neue Gesetze semantisch interpretiert werden. In der Interpretation können Ähnlichkeiten zu bestehenden Gesetzen gesucht werden, wodurch die Auswirkungen des neuen Gesetzes den Auswirkungen des alten Gesetzes entsprechen könnten.

Darüber hinaus liegt eine weitere Limitation von MIA in den berücksichtigten Sichten auf Geschäftsprozesse. Trotz verschiedener Sichten auf Geschäftsprozesse wurden lediglich eine Kontrollfluss-, Compliance-, und IT-Sicht auf den Geschäftsprozess berücksichtigt.²⁶⁴ Zur Berücksichtigung weiterer Sichten, wie der Daten- oder Ressourcensicht²⁶⁵, müssen diese als weiterer Knoten eines neuen Typs im integrierten Compliance-Graph modelliert werden. Folgerichtig müssen die Algorithmen zur Identifikation der Auswirkungen auf die Erhaltung von Compliance durch die Suche nach anderen Vorgänger- und Nachfolgerknoten beim Auftreten der neuen Knotentypen angepasst werden.

MIA berücksichtigt aktuell lediglich Geschäftsprozessintegrierte Compliance-Prozesse. Geschäftsprozessunabhängige Compliance-Prozesse, wie die Datensicherung oder Benutzerverwaltung, werden nicht betrachtet.²⁶⁶ Eine Erweiterung auf prozessunabhängige Compliance-Prozesse ist jedoch möglich, da MIA bereits alle notwendigen Schritte enthält. In einer Erweiterung um die Integration prozessunabhängiger Compliance-Prozesse muss lediglich während der

²⁶² Vgl. Gregor und Hevner 2013, S. 339 ff.

²⁶³ Vgl. Seyffarth et al. 2018, S. 179.

²⁶⁴ Vgl. Seyffarth et al. 2018, S. 178.

²⁶⁵ Vgl. Knuplesch et al. 2013a, S. 110; Winter und Fischer 2006, S. 33 f.; Scheer 1992, S. 18 f.

²⁶⁶ Vgl. Seyffarth et al. 2019, S. 229; Seyffarth et al. 2017a, S. 77 ff.

Adaption das Überprüfen der Integrierbarkeit des Compliance-Prozesses in den Geschäftsprozess nicht mehr vorgenommen werden.

Die Basis der vorgeschlagenen Compliance-konformen Geschäftsprozesse bilden alternative Compliance-Prozesse, die zuvor modelliert und den entsprechenden Compliance-Anforderungen und optionalen Compliance-Prozess-Mustern zugeordnet werden müssen.²⁶⁷ Die Idee der Modellierung, Speicherung und Identifikation alternativer Compliance-Prozessen kann in verschiedene Richtungen weiterentwickelt werden. Einerseits können mehr Charakteristika der Compliance-Prozess-Taxonomie berücksichtigt werden. Eine denkbare Erweiterung ist der Gegenstand der Compliance-Aktivität. Zur Berücksichtigung dieser Charakteristika muss Schritt 3 von MIA erweitert werden. Die Erweiterung erfolgt analog zur Berücksichtigung des Kontrollflusses und der IT-Komponenten. Andererseits können alternative Compliance-Prozessen durch quantitative Attributen beschrieben werden. Ein Beispiel sind die Kosten oder die Effektivität der Ausführung eines einzelnen Compliance-Prozesses.²⁶⁸ Außerdem können ebenfalls einmalige Implementierungskosten des alternativen Compliance-Prozesses in den Geschäftsprozess in den Kosten enthalten sein.²⁶⁹

Im Fall mehrerer Vorschläge für Compliance-konforme Geschäftsprozesse erfolgt bis jetzt keine Bewertung der Vorschläge. Eine Bewertung nach Effektivität oder Effizienz der alternativen Compliance-Prozesse muss durch die entscheidende Organisationseinheit weiterhin selbstständig durchgeführt werden²⁷⁰. Daher kann eine quantitative Bewertung von Compliance-Prozessen eine Grundlage für eine automatische Auswahlentscheidung verschiedener alternativer Compliance-Prozesse bilden.

Weiterer Forschungsbedarf besteht hinsichtlich der Identifikation, Modellierung und Integration alternativer Compliance-Prozesse. Die Identifikation möglicher Compliance-Prozesse kann sowohl auf Basis von Prozessmodellen als auch auf Logdateien ausgeführter Prozessinstanzen erfolgen. In Prozessmodellen können Verfahren der Mustererkennung²⁷¹ angepasst werden, um Compliance-konforme Prozessfragmente zu identifizieren. In der Literatur werden bereits Logdateien zur Erkennung von Anomalien in ausgeführten Prozessen genutzt.²⁷² Dementsprechend können sie eine denkbare Datengrundlage zur Identifikation neuer Muster und Eigenschaften von real ausgeführten Compliance-Prozessen darstellen. Bei der Integration von Compliance-Prozessen in Geschäftsprozesse besteht ebenfalls weiterer Forschungsbedarf. Ansätze zur Vorhersage von Prozessverläufen²⁷³ können bspw. adaptiert werden, um bereits während der Erstellung des Geschäftsprozessmodells Hinweise und Vorschläge für mögliche Compliance-Prozesse zu geben.

²⁶⁷ Vgl. Seyffarth et al. 2019, S. 234.

²⁶⁸ Vgl. Kuehnel und Zasada 2018, S. 230 ff.

²⁶⁹ Vgl. Seyffarth und Kühnel 2020, S. 26.

²⁷⁰ Vgl. Kuehnel und Zasada 2018, S. 231 ff.

²⁷¹ Vgl. u.a. Riehle et al. 2017a; Delfmann et al. 2015a, S. 480 ff.

²⁷² Vgl. Schultz und Tropmann-Frick 2020, S. 5424 ff.

²⁷³ Vgl. Metzger et al. 2019, S. 551 ff.

Die Methode MIA adaptiert Geschäftsprozessmodelle zu einem Compliance-konformen Ablauf. Die Idee der Prozessadaption durch alternative Compliance-Prozesse kann ebenfalls auf die IT-Infrastruktur übertragen werden. Ein Unterscheidungsmerkmal zwischen alternativen IT-Komponenten kann die Differenzierung zwischen einem On-Premise-Betrieb und einem Betrieb in der Cloud sein. Cloud-basierte IT-Komponenten lassen sich wiederum anhand verschiedener Provider oder Service-Modelle unterscheiden²⁷⁴. Außerdem ist es denkbar, die Adaption der IT-Infrastruktur ebenfalls um eine Kostenperspektive für den Adaptionprozess und den Betrieb zu erweitern.

7.2 Implikationen für Wissenschaft und Praxis

Die vorgeschlagene Methode MIA, das Domänenmodell und die Compliance-Prozess-Taxonomie erweitern die präskriptive Wissensbasis.²⁷⁵ Gregor und Hevner folgend lassen sich alle Artefakte außerdem dem Wissensbeitrag der Exaptation zuordnen, dessen Ziel die Anwendung bestehender Methoden auf neue Probleme ist.²⁷⁶ Einerseits basieren die Methoden zur Modellierung des integrierten Compliance-Graphs und des alternativen Compliance-Prozess-Graphs auf der Idee der Abbildung von Abhängigkeiten zwischen Elementen in einem gerichteten Graph. Andererseits nutzen die Methoden zur Identifikation von Compliance-Verletzungen und Suche nach alternativen Compliance-Prozessen eine Vorwärts- und Rückwärtssuche im Graphen.²⁷⁷ Darüber hinaus bedient sich die Methode zur Adaption von Geschäftsprozessen bei der Integration alternativer und Compliance-konformer Compliance-Prozessen wiederum der grundsätzlichen Idee der Prozessveränderung durch das Entfernen und Hinzufügen von Elementen.²⁷⁸

Wie von dem Forschungsparadigma des DSR gefordert, kann MIA auch in anderen Domänen eingesetzt werden.²⁷⁹ Die Auswirkungsidentifikation kann unter anderem in der Domäne der IT-Sicherheit auf die Schutzbedarfsanalyse adaptiert werden.²⁸⁰ Die Analyse kann aus zwei Perspektiven erfolgen. Ausgehend von den verarbeitenden Daten der Geschäftsaktivitäten, kann einerseits der Schutzbedarf betroffener IT-Komponenten bestimmt werden. Andererseits kann die Einhaltung der Schutzbedarfe über die Identifikation der zu berücksichtigten IT-Komponenten ebenfalls kontrolliert werden.

Außerdem kann die Berücksichtigung von Alternativen zum Erreichen eines bestimmten Ziels ebenfalls auf IT-Komponenten übertragen werden. Zum einen können alternative IT-Komponenten im Sinne alternativer Produkte modelliert werden. Zum anderen können alternative IT-Komponenten auch in Form eines (alternativen) Cloud-Service-Providers auftreten²⁸¹. Weiterhin ist

²⁷⁴ Vgl. Seifert und Kühnel 2020, S. 10.

²⁷⁵ Vgl. Gregor und Hevner 2013, S. 343.

²⁷⁶ Vgl. Gregor und Hevner 2013, S. 345.

²⁷⁷ Vgl. Seyffarth et al. 2019, S. 235; Seyffarth et al. 2018, S. 182 ff.; Seyffarth et al. 2017b, S. 1643 ff.

²⁷⁸ Vgl. u.a. Kittel 2013, S. 971; Kittel et al. 2013b, S. 154 ff.; Kopp et al. 2011, S. 59 ff.; Schumm et al. 2010a, S. 5 ff.; Awad et al. 2009, S. 13 ff.

²⁷⁹ Vgl. March und Storey 2008, S. 726.

²⁸⁰ Vgl. BSI (Hg) 2017, S. 78 ff.

²⁸¹ Vgl. Seyffarth und Kühnel 2020, S. 26; Seifert und Kühnel 2020, S. 10.

es denkbar die automatische Adaption von Geschäftsprozessen auch auf Geschäftsprozesse anzuwenden, die nicht als explizites Prozessmodell vorliegen. Ein möglicher Anwendungsfall ist die Implementierung von Geschäftsprozessen in Skriptsprachen, wie es bspw. bei Smart Contracts der Fall ist.²⁸²

Die entwickelte Methode MIA und ihre Demonstration in dem Softwareprototypen BCIT ermöglichen die Auswirkungen auf die Erhaltung von Compliance schneller zu identifizieren, als es durch eine manuelle Tätigkeit der Fall ist. Außerdem kann die automatische Identifikation der Auswirkungen auf die Erhaltung von Compliance und das Adaptieren zu Compliance-konformen Geschäftsprozessen zum Testen verschiedener Szenarien, wie Restrukturierungs- oder Outsourcingprojekte verwendet werden, wodurch Wettbewerbsvorteile erzielt werden können. Zusätzlich ermöglicht die zentrale Modellierung, Verlinkung und Speicherung alternativer Compliance-Prozesse die Wiederverwendung von Compliance-Prozessen in Unternehmen und Institutionen, wodurch ein Beitrag zum Wissensmanagement und Wissensaustausch durch ein zentrales Compliance-Prozess-Repository²⁸³ denkbar ist.

Die vorgeschlagene Methode ist zudem nur für Fälle anwendbar, in denen Compliance-Prozesse und Geschäftsprozesse disjunkt sind.²⁸⁴ Die notwendige Unterscheidung zwischen Geschäftsaktivitäten und Compliance-Prozessen kann jedoch ebenfalls einen Beitrag zum Wissensmanagement leisten, da der Grund für die Durchführung eines Compliance-Prozesses explizit im Prozessmodell abgebildet werden kann. Compliance-Anforderungen können neben Compliance-Quellen ihren Ursprung auch in Compliance-Risiken haben²⁸⁵. Dementsprechend kann die Bonitätsprüfung in einer Bank, dessen Ziel die Minimierung des Zahlungsfallrisikos durch den Kunden ist, ebenfalls als Compliance-Prozess betrachtet werden. Der Wertbeitrag des Compliance-Prozesses liegt demzufolge nicht in der Schaffung eines Wertes für den Kunden sondern in der Verringerung der Höhe eines möglichen Schadens für die Bank²⁸⁶.

²⁸² Vgl. Meironke et al. 2019, S. 1894 ff.

²⁸³ Vgl. Schumm et al. 2011, S. 8.

²⁸⁴ Vgl. Seyffarth et al. 2019, S. 230.

²⁸⁵ Vgl. u.a. Schumm et al. 2010c, S. 328; Namiri und Stojanovic 2007a, S. 63.

²⁸⁶ Vgl. Sonnenreich et al. 2006, S. 46.

8 Schlussbetrachtung

Compliance-Anforderungen können sowohl Bedingungen an Aktivitäten eines Geschäftsprozesses als auch an IT-Komponenten stellen.²⁸⁷ IT-Komponenten können wiederum sowohl Aktivitäten eines Geschäftsprozesses unterstützen als auch durch die Unterstützung von Compliance-Prozessen die Sicherstellung von Compliance-Anforderungen ermöglichen.²⁸⁸ Daraus ergeben sich wechselseitige Beziehungen zwischen Compliance-Anforderungen, Aktivitäten eines Geschäftsprozesses und IT-Komponenten.²⁸⁹

Viele Faktoren, wie Prozessverbesserungen, neue Technologien oder Outsourcing-Entscheidungen können zum Ersetzen oder Entfernen von Aktivitäten eines Geschäftsprozesses, IT-Komponenten oder Compliance-Anforderungen führen.²⁹⁰ Dennoch ist weiterhin die Einhaltung betroffener Compliance-Anforderungen notwendig.²⁹¹ Insofern müssen Auswirkungen auf die Erhaltung von Compliance durch Änderungen an den genannten Elementen bereits im Vorfeld erkannt und die Konsequenzen zur Entwurfszeit der entsprechenden Modelle berücksichtigt werden.²⁹² Folglich ist das Ziel eine Methode zur Erhaltung von Compliance in flexiblen und IT-gestützten Geschäftsprozessen. Zur Konkretisierung des Ziels wurden drei Forschungsfragen als Teilziele abgeleitet:

- FF 1: Wie können Compliance-Anforderungen, ein Geschäftsprozessmodell und IT-Komponenten und ihre Beziehungen in einem Modell modelliert werden?
- FF 2: Wie können die Auswirkungen auf die Erhaltung von Compliance identifiziert werden, die durch das Ersetzen oder Entfernen von Compliance-Anforderungen, Geschäftsaktivitäten oder IT-Komponenten entstehen können?
- FF 3: Wie können Geschäftsprozessmodelle zur Entwurfszeit Compliance-konform adaptiert werden?

Zur Zielerreichung wurden Modelle, Konstrukte und Methoden entsprechend des DSR-Forschungsparadigmas entwickelt und durch Konferenz- und Journalbeiträge kommuniziert.²⁹³ Die Artefakte lassen sich zur Methode MIA orchestrieren, die drei Schritte umfasst:

- Schritt 1: Das Modellieren von Compliance-Anforderungen, Geschäftsprozessen und IT-Komponenten in einem Modell.²⁹⁴
- Schritt 2: Die Identifikation von Auswirkungen auf die Erhaltung von Compliance.²⁹⁵

²⁸⁷ Vgl. Vgl. u.a. Klotz 2007, S. 14; Governatori und Sadiq 2009, S. 427. Institut der Wirtschaftsprüfer (IDW) (Hg) 2002, S. 1169.

²⁸⁸ Vgl. u.a. Klotz 2007, S. 14; Governatori und Sadiq 2009, S. 427; Institut der Wirtschaftsprüfer (IDW) (Hg) 2002, S. 1169.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2012, S. 1.

²⁸⁹ Vgl. Seyffarth und Kühnel 2020, S. 1; Seyffarth et al. 2018, S. 178.

²⁹⁰ Vgl. Fdhila et al. 2015a, S. 2; Rudzajs und Buksa 2011, S. 96; Rinderle et al. 2004, S. 9.

²⁹¹ Vgl. Rudzajs und Buksa 2011, S. 97; Governatori und Sadiq 2009, S. 429.

²⁹² Vgl. Sadiq und Governatori 2010 S. 267.

²⁹³ Vgl. Peffers et al. 2006, S. 91 ff.; Hevner et al. 2004, S. 82 ff; March und Smith 1995, S. 256 ff.

²⁹⁴ Vgl. Seyffarth et al. 2017a, S. 71 ff.; Seyffarth et al. 2016, S. 1341 ff.

²⁹⁵ Vgl. Seyffarth et al. 2018, S. 176 ff.; Seyffarth et al. 2017b, S. 1641 ff.

- Schritt 3: Das Compliance-konforme Adaptieren des Geschäftsprozesses auf Basis zuvor modellierter alternativer Compliance-Prozesse.²⁹⁶

Tabelle 7. Eingebachte Publikationen

Eingebachte Publikation 1	Seyffarth, Tobias; Kühnel, Stephan; Sackmann, Stefan (2017): A Taxonomy of Compliance Processes for Business Process Compliance. In: 15th International Conference on Business Process Management, Business Process Management Forum. In: Lecture Notes in Business Information Processing (LNBIP), S. 71–87.
Eingebachte Publikation 2	Seyffarth, Tobias; Kühnel, Stephan; Sackmann, Stefan (2018): Business Process Compliance and Business Process Change. An Approach to Analyze the Interactions. In: Business Information Systems. BIS 2018. Lecture Notes in Business Information Processing (320), S. 176–189.
Eingebachte Publikation 3	Seyffarth, Tobias; Kühnel, Stephan; Sackmann, Stefan (2019): Business Process Compliance despite Change. Towards Proposals for a Business Process Adaption. In: Information Systems Engineering in Responsible Information Systems. CAiSE 2019. Lecture Notes in Business Information Processing, vol. 350, S. 227–239.
Eingebachte Publikation 4	Seyffarth, Tobias; Kühnel, Stephan (2020): Maintaining Business Process Compliance despite Changes. A Decision Support Approach based on Process Adaptations. In: Journal of Decision Systems.

Alle vier eingebrachten Publikationen dieser Arbeit, die in Tabelle 7 aufgeführt sind, leisten einen Kernbeitrag zu MIA. Die Kernbeiträge der Publikationen zu MIA werden im Folgenden noch einmal kurz zusammengefasst. Alle Schritte von MIA basieren auf dem konzeptuellen Domänenmodell, das in (Seyffarth et al. 2016) initial vorgeschlagen und in der eingebrachten Publikation 1²⁹⁷ finalisiert wurde. Das Modell wurde auf Basis der Literatur erarbeitet und zeigt im Wesentlichen die Beziehungen zwischen Compliance-Anforderungen, Geschäftsprozessen, Compliance-Prozessen und IT-Komponenten.

Die Methoden zur Modellierung eines gemeinsamen Modells aus Compliance-Anforderungen, dem Geschäftsprozessmodell und IT-Komponenten (Schritt 1) und zur Identifikation der Auswirkungen auf die Erhaltung von Compliance beim Entfernen und Ersetzen von Elementen (Schritt 2) beantworten FF 1 und FF 2. Beide Methoden wurden in der eingebrachten Publikation 2²⁹⁸ kommuniziert. Das gemeinsame Modell wird durch einen gerichteten Graph abgebildet, dessen Knoten eine Compliance-Anforderung, ein Element des Geschäftsprozessmodells oder eine IT-Komponente repräsentieren. Die unterschiedlichen Modelltypen werden durch verschiedene Knotentypen abgebildet. Die Beziehungen zwischen den Elementen der Modelle werden über gerichtete Kanten zwischen den entsprechenden Knoten abgebildet. Zur Identifikation der Auswirkungen auf die Erhaltung von Compliance wurden verschiedene Suchstrategien auf dem Graphen vorgestellt, die auf einer Vorwärts- und Rückwärtssuche beruhen.

²⁹⁶ Vgl. Seyffarth et al. 2019, S. 227 ff.

²⁹⁷ Seyffarth et al. 2017a.

²⁹⁸ Seyffarth et al. 2018.

Die Methode zur Compliance-konformen Adaption des Geschäftsprozesses (Schritt 3) beantwortet FF 3 und wurde in der eingebrachten Publikation 3²⁹⁹ kommuniziert. Die Adaption von Geschäftsprozessen basiert auf der Idee, dass verschiedene Compliance-Prozesse eine Compliance-Anforderung sicherstellen können. Außerdem können Compliance-Prozesse in Compliance-Prozess-Mustern generalisiert werden. In der Publikation 3 wurde ein alternativer Compliance-Graph und eine Suchmethode vorgestellt, um passende Compliance-Prozesse zu identifizieren und sie automatisch in den Geschäftsprozess zu integrieren. Zur Charakterisierung der Compliance-Prozesse und Compliance-Prozess-Muster wurde in der eingebrachten Publikation 1³⁰⁰ eine Taxonomie auf Basis relevanter Literatur zu Eigenschaften von Compliance-Prozessen entwickelt. Sie ermöglicht die Beschreibung von Compliance-Prozessen durch 37 Charakteristika, die in 9 Dimensionen gruppiert sind.

Die finale Umsetzbarkeit von MIA wurde in dem erweiterten Softwareprototypen BCIT demonstriert.³⁰¹ Abschließend wurde in der eingebrachten Publikation 4³⁰² die wahrgenommene Nützlichkeit von MIA in mehreren Fallstudien von Domänenexpert:innen anhand des erweiterten Softwareprototypen BCIT positiv evaluiert.

²⁹⁹ Seyffarth et al. 2019.

³⁰⁰ Seyffarth et al. 2017a.

³⁰¹ Vgl. Seyffarth und Raschke 2020, S. 109 ff.; Seyffarth und Raschke 2018, S. 81 ff.

³⁰² Seyffarth und Kühnel 2020.

9 Literaturverzeichnis

- Aleliunas, Romas; Karp, Richard M.; Lipton, Richard J.; Lovasz, Laszlo; Rackoff, Charles (1979): Random walks, universal traversal sequences, and the complexity of maze problems. In: *20th Annual Symposium on Foundations of Computer Science (sfcs 1979)*, S. 218–223.
- Awad, Ahmed (2007): BPMN-Q. A Language to Query Business Processes. In: *Proceedings of EMISA'07*, S. 115–128.
- Awad, Ahmed; Decker, Gero; Weske, Mathias (2008): Efficient Compliance Checking Using BPMN-Q and Temporal Logic. In: Marlon Dumas, Manfred Reichert und Ming-Chien Shan (Hg.): *Business Process Management*, Bd. 5240. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 326–341.
- Awad, Ahmed; Smirnov, Sergey; Weske, Mathias (2009): Resolution of Compliance Violation in Business Process Models. A Planning-Based Approach. In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (Hg.): *On the Move to Meaningful Internet Systems: OTM 2009*, Bd. 5870. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 6–23.
- AXELOS (2019): ITIL Foundation ITIL 4 edition. ITIL 4. London: The Stationery Office Ltd.
- Bagozzi, Richard (2007): The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. In: *JAIS* 8 (4), S. 244–254.
- Barboza, L. d. S.; Filho, G. A. d. A. C.; Souza, R. A. C. d. (2016): Towards Legal Compliance in IT Procurement Planning in Brazil's Federal Public Administration. In: *IEEE 24th International Requirements Engineering Conference Workshops (REW)*, S. 229–238.
- Becker, Jörg; Heddier, Marcel; Braeuer, Sebastian; Knackstedt, Ralf (2014): Integrating Regulatory Requirements into Information Systems Design and Implementation. In: *ICIS 2014 Proceedings*.
- Bellino, Christine; Wells, Jefferson; Hunt, Steve (2007): Auditing application controls. Altamonte Springs, Fla.: IIA (Global technology audit guide, 8).
- Bräuer, Sebastian; Delfmann, Patrick; Dietrich, Hanns-Alexander; Steinhorst, Matthias (2013): Using a Generic Model Query Approach to Allow for Process Model Compliance Checking. An Algorithmic Perspective. In: *Internationale Tagung Wirtschaftsinformatik*.
- Breuker, Dominic; Delfmann, Patrick; Dietrich, Hanns-Alexander; Steinhorst, Matthias (2015): Graph theory and model collection management. Conceptual framework and runtime analysis of selected graph algorithms. In: *Inf Syst E-Bus Manage* 13 (1), S. 69–106.
- Brown, S. A.; Massey, A. P.; Montoya-weiss, M. M.; Burkman, J. R. (2017): Do I really have to? User acceptance of mandated technology. In: *Eur J Inf Syst* 11 (4), S. 283–295.

- BSI (Hg) (2008): BSI-Standard 100-4. Notfallmanagement. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2, zuletzt geprüft am 06.09.2020.
- BSI (Hg) (2017): BSI-Standard 200-2. IT-Grundschutz-Methodik. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=7.
- Bundesministeriums der Justiz und für Verbraucherschutz (Hg) (2020): Gesetze im Internet. Online verfügbar unter <https://www.gesetze-im-internet.de/gii-toc.xml>, zuletzt geprüft am 02.11.2020.
- Camunda (Hg) (2020): bpmn-js. BPMN 2.0 for the web. Online verfügbar unter <https://github.com/bpmn-io/bpmn-js>, zuletzt geprüft am 18.09.2020.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2012): Internal Control - Integrated Framework. Framework and Appendices.
- Comuzzi, Marco (2014): Aligning Monitoring and Compliance Requirements in Evolving Business Networks. In: *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems 8841*, S. 166–183.
- Corea, Carl; Delfmann, Patrick (2017): Detecting Compliance with Business Rules in Ontology-Based Process Modeling. In: *Internationale Tagung Wirtschaftsinformatik*, S. 226–240.
- Davis, Fred D. (1989): Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. In: *MIS Quarterly* 13 (3), S. 319.
- Delfmann, Patrick; Breuker, Dominic, Matzner, Martin; Becker, Jörg (2015a): Supporting information systems analysis through conceptual model query. The diagrammed model query language (DMQL). In: *Communications of the Association for Information Systems* 37, S. 473–509.
- Delfmann, Patrick; Steinhorst, Matthias; Dietrich, Hanns-Alexander; Becker, Jörg (2015b): The generic model query language GMQL – Conceptual specification, implementation, and runtime evaluation. In: *Information Systems* 47, S. 129–177.
- Dijkman, Remco; La Rosa, Marcello; Reijers, Hajo A. (2012): Managing large collections of business process models—Current techniques and challenges. In: *Computers in Industry* 63 (2), S. 91–97.
- Dreyfus, D.; Iyer, B. (2006): Enterprise Architecture. A Social Network Perspective. In: *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, 178a-178a.

- El Kharbili, M.; Medeiros, A.K.A.d.; Stein, S.; van der Aalst, W.M.P. (2008): Business Process Compliance Checking. Current State and Future Challenges. In: *Modellierung betrieblicher Informationssysteme (MobIS 2008)*, S. 107–113.
- El Kharbili, Marwane; Stolarski, Piotr (2009): Building-Up a Reference Generic Regulation Ontology. A Bottom-Up Approach. In: *Business Information Systems Workshops*, S. 268–279.
- Elgammal, Amal; Turetken, Oktay; van den Heuvel, Willem-Jan (2012): Using Patterns for the Analysis and Resolution of Compliance Violations. In: *Int. J. Coop. Info. Syst.* 21 (01), S. 31–54.
- Elgammal, Amal; Turetken, Oktay; van den Heuvel, Willem-Jan; Papazoglou, Mike (2010): Root-Cause Analysis of Design-Time Compliance Violations on the Basis of Property Patterns. In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (Hg.): *Service-Oriented Computing*, Bd. 6470. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 17–31.
- Elgammal, Amal; Turetken, Oktay; van den Heuvel, Willem-Jan; Papazoglou, Mike (2016): Formalizing and applying compliance patterns for business process compliance. In: *Softw Syst Model* 2016 (15), S. 119–146.
- Facebook Inc. (Hg) (2020): React. A JavaScript library for building user interfaces. Online verfügbar unter <https://reactjs.org/>, zuletzt geprüft am 18.09.2020.
- Fdhila, Walid; Indiono, Conrad; Rinderle-Ma, Stefanie; Reichert, Manfred (2015a): Dealing with change in process choreographies. Design and implementation of propagation algorithms. In: *Information Systems* 49, S. 1–24.
- Fdhila, Walid; Rinderle-Ma, Stefanie; Knuplesch, David; Reichert, Manfred (2015b): Change and Compliance in Collaborative Processes. In: *12th IEEE International Conference on Services Computing (SCC 2015)*, S. 162–169.
- Fdhila, Walid; Rinderle-Ma, Stefanie; Reichert, Manfred (2012): Change propagation in collaborative processes scenarios. In: *8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*.
- Fehling, Christoph; Koetter, Falko; Leymann, Frank (2014): Compliance Modeling. Formal Descriptors and Tools. Online verfügbar unter <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.701.5220&rep=rep1&type=pdf>, zuletzt aktualisiert am 28.03.2014, zuletzt geprüft am 18.09.2020.
- Fellmann, Michael; Thomas, Oliver; Busch, Bastian (2011): A Query-Driven Approach for Checking the Semantic Correctness of Ontology-Based Process Representations. In: Witold Abramowicz (Hg.): *Business Information Systems. 14th International Conference, BIS 2011, Poznań, Poland, June 15-17, 2011. Proceedings*. Berlin, Heidelberg: Springer-Verlag GmbH Berlin Heidelberg (Lecture Notes in Business Information Processing, 87), S. 62–73.

- Frank, Ulrich (2002): Multi-perspective enterprise modeling (MEMO) conceptual framework and modeling languages. In: *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, S. 1258–1267.
- Franz, Max; Lopes, Christian T.; Huck, Gerardo; Dong, Yue; Sumer, Onur; Bader, Gary D. (2016): Cytoscape.js. A graph theory library for visualisation and analysis. In: *Bioinformatics (Oxford, England)* 32 (2), S. 309–311.
- Friedrichs, Jürgen (1990): Methoden empirischer Sozialforschung. Wiesbaden: VS Verlag für Sozialwissenschaften.
- Gacitua-Decar, Veronica; Pahl, Claus (2009): Automatic Business Process Pattern Matching for Enterprise Services Design. In: *2009 World Conference on Services - II*, S. 111–118.
- Gadatsch, Andreas (2017): Grundkurs Geschäftsprozess-Management. Wiesbaden: Springer Fachmedien Wiesbaden.
- Gaidukovs, Andrejs; Kirikova, Marite (2015): Types of Linkages between Business Processes and Regulations. In: *New Contributions in Information Systems and Technologies* 353, S. 343–349.
- Gehrke, Nick (2010): The ERP Auditlab. A Prototypical Framework for Evaluating Enterprise Resource Planning System Assurance. In: *43rd Hawaii International Conference on System Sciences (HICSS)*, S. 1–9.
- Ghanavati, S.; Amyot, D.; Siena, A.; Susi, A.; Perini, A. (2010): Towards a Framework for Business Process Compliance. In: *2010 14th IEEE International Enterprise Distributed Object Computing Conference Workshops*.
- Ghanavati, Sepideh; Amyot, Daniel; Peyton, Liam (2009): Compliance Analysis Based on a Goal-oriented Requirement Language Evaluation Methodology. In: *17th IEEE International Requirements Engineering Conference*, S. 133–142.
- Ghanavati, Sepideh; Amyot, Daniel; Rifaut, André (2014): Legal goal-oriented requirement language (legal GRL) for modeling regulations. In: *International Conference on Software Engineering*, S. 1–6.
- Goeken, Matthias; Looso, Stefanie (2006): Anwendung von referenzmodellen der IT-Governance. konzeptionelle Grundlage und Anwendungsszenarien. In: *Informatik 2006*, S. 855–868.
- Governatori, Guido; Sadiq, Shazia (2009): The Journey to Business Process Compliance. In: *Handbook of research on business process modeling*, S. 426–454.
- Gregor, Shirley; Hevner, Alan R. (2013): Positioning and Presenting Design Science Research for Maximum Impact. In: *MIS Quarterly* 37 (2).

- Halle, Sylvain (2011): Causality in Message-Based Contract Violations. A Temporal Logic "Whodunit". 2011 IEEE 15th International Enterprise Distributed Object Computing Conference.
- Hammer, Michael; Champy, James (1993): Reengineering the corporation. a manifesto for business revolution. New York: HarperBusiness.
- Hashmi, Mustafa; Governatori, Guido; Wynn, Moe Thandar (2016): Normative requirements for regulatory compliance. An abstract formal framework. In: *Inf Syst Front* 18 (3), S. 429–455.
- Heckel, Reiko; Taentzer, Gabriele (2020): Graph Transformation for Software Engineers. With Applications to Model-Based Development and Domain-Specific Language Engineering. 1st ed. 2020. Cham, Cham: Springer International Publishing; Imprint Springer (Springer eBook Collection).
- Hevner, Alan R.; March, Salvatore T.; Park, Jinsoo; Ram, Sudha (2004): Design Science in Information Systems Research. In: *MIS Quarterly* 28 (1), S. 75–105.
- Hilty, Manuel; Basin, David; Pretschner, Alexander (2005): On Obligations. In: De Capitani di Vimercati, Sabrina und Paul Syverson (Hg.): Computer security - ESORICS 2005. 10th European Symposium on Research in Computer Security, Milan, Italy, September 12 - 14, 2005 ; proceedings, Bd. 3679. Berlin: Springer (Lecture Notes in Computer Science, 3679), S. 98–117.
- Hummer, Waldemar; Gaubatz, Patrick; Strembeck, Mark; Zdun, Uwe; Dustdar, Schahram (2011): An integrated approach for identity and access management in a SOA context. In: *Proceedings of the 16th ACM symposium on Access control models and technologies - SACMAT '11*, S. 21–31.
- Institut der Wirtschaftsprüfer (IDW) (Hg) (2002): IDW PS 330. Abschlußprüfung bei Einsatz von Informationstechnologie. In: *WPg* 21, S. 1167–1197.
- ISACA (Hg) (2012): COBIT 5. A business framework for the governance and management of enterprise IT. Rolling Meadows, Ill.: ISACA.
- IT Governance Institute (ITGI) (2006): IT Control Objectives for Sarbanes-Oxley. 2nd Edition.
- Jakoubi, Stefan; Tjoa, Simon; Goluch, Sigrun; Kitzler, Gerhard (2010): Risk-Aware Business Process Management. Establishing the Link Between Business and Security. In: *Complex Intelligent Systems and Their Applications* 41, S. 109–135.
- Kittel, Kai (2013): Agilität von Geschäftsprozessen trotz Compliance. In: *Tagungsband der 11. Internationale Tagung Wirtschaftsinformatik*, S. 967–981.
- Kittel, Kai; Sackmann, Stefan (2012): Flexible Controls for Compliance in Catastrophe Management Processes. In: *Tagungsband der Multikonferenz Wirtschaftsinformatik (MKWI'12)*, S. 1675–1687.

- Kittel, Kai; Sackmann, Stefan; Betke, Hans; Hofmann, Marlen (2013a): Achieving Flexible and Compliant Processes in Disaster Management. In: *46. Hawaii Internat. Conference on System Sciences (HICSS'13)*, S. 4687–4696.
- Kittel, Kai; Sackmann, Stefan; Göser, Kevin (2013b): Flexibility and Compliance in Workflow Systems. The KitCom Prototype. In: *Proceedings of the CAiSE'13 Forum at the 25th International Conference on Advanced Information Systems Engineering (CAiSE)*, S. 154–160.
- Klinkmüller, Christopher; Weber, Ingo (2017): Analyzing control flow information to improve the effectiveness of process model matching techniques. In: *Decision Support Systems* 100, S. 6–14.
- Klotz, Michael (2007): IT-Compliance. auf den Kern reduziert. In: *IT-Governance* 1, S. 14–18.
- Knackstedt, Ralf; Eggert, Mathias; Heddier, Marcel; Chasin, Friedrich; Becker, Jörg (2013): The Relationship Of Is And Law - The Perspective Of And Implications For IS Research. In: *ECIS 2013 Completed Research*. Online verfügbar unter http://aisel.aisnet.org/ecis2013_cr/18.
- Knebl, Helmut (2019): Algorithmen und Datenstrukturen. Grundlagen und probabilistische Methoden für den Entwurf und die Analyse.
- Knuplesch, David; Fdhila, Walid; Reichert, Manfred; Rinderle-Ma, Stefanie (2015): Detecting the Effects of Changes on the Compliance of Cross-Organizational Business Processes. In: *Conceptual Modeling. Lecture Notes in Computer Science*, S. 94–107.
- Knuplesch, David; Reichert, Manfred; Ly, Linh Thao; Kumar, Akhil; Rinderle-Ma, Stefanie (2013a): Visual Modeling of Business Process Compliance Rules with the Support of Multiple Perspectives. In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (Hg.): *Conceptual Modeling*, Bd. 8217. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 106–120.
- Knuplesch, David; Reichert, Manfred; Mangler, Jürgen; Rinderle-Ma, Stefanie; Fdhila, Walid (2013b): Towards Compliance of Cross-Organizational Processes and Their Changes. In: Wil van der Aalst, John Mylopoulos, Michael Rosemann, Michael J. Shaw, Clemens Szyperski, Marcello La Rosa und Pnina Soffer (Hg.): *Business Process Management Workshops*, Bd. 132. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Business Information Processing), S. 649–661.
- Koetter, F.; Kochanowski, M.; Weisbecker, A.; Fehling, C.; Leymann, F. (2014): Integrating Compliance Requirements across Business and IT. 2014 IEEE 18th International Enterprise Distributed Object Computing Conference.

- Koetter, Falko; Kintz, Maximilien; Kochanowski, Monika; Wiriyarattanakul, Thatchanok; Fehling, Christoph; Gildein, Philipp et al. (2016): An Universal Approach for Compliance Management Using Compliance Descriptors. In: Markus Helfert, Donald Ferguson, Victor Méndez Muñoz und Jorge Cardoso (Hg.): *Cloud Computing and Services Science. 6th International Conference, CLOSER 2016, Rome, Italy, April 23-25, 2016, Revised Selected Papers*. Cham, s.l.: Springer International Publishing (Communications in Computer and Information Science, 740), S. 209–231.
- Koetter, Falko; Kochanowski, Monika; Renner, Thomas; Fehling, Christoph; Leymann, Frank (2013): Unifying Compliance Management in Adaptive Environments through Variability Descriptors (Short Paper). In: *2013 IEEE 6th International Conference on Service-Oriented Computing and Applications (SOCA)*, S. 214–219.
- Kopp, Oliver; Leymann, Frank; Schumm, David; Unger, Tobias (2011): On BPMN process fragment auto-completion. In: *3rd Central-European Workshop on Services and their Composition*, S. 58–64.
- Kriglstein, Simone; Leitner, Maria; Kabicher-Fuchs, Sonja; Rinderle-Ma, Stefanie (2016): Evaluation Methods in Process-Aware Information Systems Research with a Perspective on Human Orientation. In: *Bus Inf Syst Eng* 58 (6), S. 397–414.
- Kuehnel, Stephan; Zasada, Andrea (2018): An Approach Toward the Economic Assessment of Business Process Compliance. In: *Advances in Conceptual Modeling. ER. In: Lecture Notes in Computer Science (LNCS) 1928*, 228-238.
- Lee, Younghwa; Kozar, Kenneth A.; Larsen, Kai R.T. (2003): The Technology Acceptance Model. Past, Present, and Future. In: *Communications of the Association for Information Systems* 12.
- Leopold, Henrik; Meilicke, Christian; Fellmann, Michael; Pittke, Fabian; Stuckenschmidt, Heiner; Mendling, Jan (2015): Towards the Automated Annotation of Process Models. In: *International Conference on Advanced Information Systems Engineering*, S. 401–416.
- Liu, Y.; Muller, S.; Xu, K. (2007): A static compliance-checking framework for business process models. In: *IBM Syst. J.* 46 (2), S. 335–361.
- Lu, Ruopeng; Sadiq, Shazia; Governatori, Guido (2008): Compliance Aware Business Process Design. In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (Hg.): *Business Process Management Workshops*, Bd. 4928. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 120–131.
- March, Salvatore T.; Smith, Gerald F. (1995): Design and natural science research on information technology. In: *Decision Support Systems* 15 (4), S. 251–266.

- March, Salvatore T.; Storey, Veda C. (2008): Design Science in the Information Systems Discipline. An Introduction to the Special Issue on Design Science Research. In: *MIS Quarterly* 32 (4), S. 725–730.
- Marino, Daniela; Massacci, Fabio; Micheletti, Andrea; Rassadko, Nataliya; Neuhaus, Stephan (2009): Satisfaction of Control Objectives by Control Processes. In: *International Conference on Service-Oriented Computing*, S. 531–545.
- Mattfeld, Dirk; Vahrenkamp, Richard (2014): Logistiknetzwerke. Wiesbaden: Springer Fachmedien Wiesbaden.
- Meironke, Anja; Seyffarth, Tobias; Damarowsky, Johannes (2019): Business Process Compliance and Blockchain. How Does the Ethereum Blockchain Address Challenges of Business Process Compliance? In: *Wirtschaftsinformatik Proceedings 2019*, S. 1894–1905.
- Metzger, Andreas; Neubauer, Adrian; Bohn, Philipp; Pohl, Klaus (2019): Proactive Process Adaptation Using Deep Learning Ensembles. In: *International Conference on Advanced Information Systems Engineering*, S. 547–562.
- Moody, Daniel L. (2003): The method evaluation model. A theoretical model for validating information systems design methods. In: *Proceedings of the 11th European Conference on Information Systems, ECIS 2003*.
- Mwilu, Odette Sangupamba; Prat, Nicolas; Comyn-Wattiau, Isabelle (2015): Taxonomy Development for Complex Emerging Technologies. The Case of Business Intelligence and Analytics on the Cloud. In: *19th Pacific Asia Conference on Information Systems (PACIS 2015)*, S. 1–16.
- Namiri, Kioumars; Stojanovic, Nenad (2007a): Pattern-Based Design and Validation of Business Process Compliance. In: Robert Meersman und Zahir Tari (Hg.): *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS*, Bd. 4803. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 59–76.
- Namiri, Kioumars; Stojanovic, Nenad (2007b): Using Control Patterns in Business Processes Compliance. In: *WISE 2007 Workshops*, S. 178–190.
- Nickerson, Robert C.; Varshney, Upkar; Muntermann, Jan (2013): A method for taxonomy development and its productservice in information systems. In: *European Journal of Information Systems* 22, S. 336–359.
- OMG (Hg) (2011): Business Process Model and Notation (BPMN). Online verfügbar unter <http://www.omg.org/spec/BPMN/2.0/PDF/>, zuletzt geprüft am 29.09.2020.
- OMG (Hg) (2017): Unified Modeling Language. Online verfügbar unter <https://www.omg.org/spec/UML/2.5.1/PDF>, zuletzt geprüft am 25.03.2020.
- OpenJS Foundation (2020): Node.js. Online verfügbar unter <https://nodejs.org/en/>, zuletzt geprüft am 18.09.2020.

- Peffers, Ken; Rothenberger, Marcus; Tuunanen, Tuure; Vaezi, Reza (2012): Design Science Research Evaluation. In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (Hg.): Design Science Research in Information Systems. Advances in Theory and Practice, Bd. 7286. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 398–410.
- Peffers, Ken; Tuunanen, Tuure; Gengler, Charles; Rossi, Matti; Hui, Wendy; Virtanen, Ville; Bragge, Johanna (2006): The Design Science Research Process. A Model for Producing and Presenting Information Systems Research. In: *1st International Conference on Design Science in Information Systems and Technology (DESRIST)*, S. 83–106.
- Pham, Tuan Anh; Le Thanh, Nhan (2016): Checking the Compliance of Business Processes and Business Rules Using OWL 2 Ontology and SWRL. In: *Proceedings of the Second International Afro-European Conference for Industrial Advancement AECIA 2015*, S. 11–20.
- Pittl, Benedikt; Fill, Hans-Georg; Honegger, Gerald (2017): Enabling Risk-Aware Enterprise Modeling using Semantic Annotations and Visual Rules. In: *ECIS 2017 Proceedings*.
- Pretschner, Alexander; Hilty, Manuel; Basin, David (2006): Distributed usage control. In: *Commun. ACM* 49 (9), S. 39.
- Pries-Heje, Jan; Baskerville, Richard; Venable, John R. (2008): Strategies for Design Science Research Evaluation. In: *ECIS 2008 Proceedings*.
- Primefaces (Hg) (2020): PrimeReact. Build Better Apps with React. Online verfügbar unter <https://www.primefaces.org/primereact/>, zuletzt geprüft am 18.09.2020.
- Radeschütz, Sylvia; Schwarz, Holger; Niedermann, Florian (2015): Business impact analysis—a framework for a comprehensive analysis and optimization of business processes. In: *Comp. Sci. Res. Dev.* 30 (1), S. 69–86.
- Ramezani, Elham; Fahland, Dirk; van der Aalst, Wil M. P. (2012a): Where Did I Misbehave? Diagnostic Information in Compliance Checking. In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (Hg.): Business Process Management, Bd. 7481. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 262–278.
- Ramezani, Elham; Fahland, Dirk; van der Werf, Jan Martijn; Mattheis, Peter (2012b): Separating Compliance Management and Business Process Management. In: Wil van der Aalst, John Mylopoulos, Michael Rosemann, Michael J. Shaw, Clemens Szyperski, Florian Daniel et al. (Hg.): Business Process Management Workshops, Bd. 100. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Business Information Processing), S. 459–464.
- Reichert, Manfred; Weber, Barbara (2012): Enabling Flexibility in Process-Aware Information Systems. Berlin, Heidelberg: Springer Berlin Heidelberg.

- Riehle, Dennis (2018): Checking Business Process Models for Compliance. Comparing Graph Matching and Temporal Logic. In: *Business Process Management Workshops*, S. 403–415.
- Riehle, Dennis; Höhenberger, Steffen; Cording, Rainer; Delfmann, Patrick (2017a): Live Query. Visualized Process Analysis. In: *Wirtschaftsinformatik 2017 Proceedings*.
- Riehle, Dennis; Jannaber, Sven; Delfmann, Patrick; Thomas, Oliver; Becker, Jörg (2017b): Automatically Annotating Business Process Models with Ontology Concepts at Design-Time. In: *International Conference on Conceptual Modeling*, S. 177–186.
- Riesner, Moritz; Pernul, Günther (2010): Supporting Compliance through Enhancing Internal Control Systems by Conceptual Business Process Security Modeling. In: *ACIS 2010 Proceedings*.
- Rinderle, Stefanie; Reichert, Manfred; Dadam, Peter (2004): Correctness criteria for dynamic changes in workflow systems. a survey. In: *Data & Knowledge Engineering* 50 (1), S. 9–34.
- Robson, Colin (2009): Real world research. A resource for social scientists and practitioner-researchers. 2. ed., [Nachdr.]. Malden, MA: Blackwell.
- Rosenkrantz, Daniel J.; Stearns, Richard E.; Lewis, I. Philip M.I (1977): An Analysis of Several Heuristics for the Traveling Salesman Problem. In: *SIAM J. Comput.* 6 (3), S. 563–581.
- Rudzajs, Peteris; Buksa, Ilze (2011): Business Process and Regulations. Approach to Linkage and Change Management. In: Janis Grabis und Marite Kirikova (Hg.): *Perspectives in Business Informatics Research*, Bd. 90. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Business Information Processing), S. 96–109.
- Runeson, Per; Höst, Martin (2009): Guidelines for conducting and reporting case study research in software engineering. In: *Empir Software Eng* 14 (2), S. 131–164.
- Sackmann, Stefan; Kittel, Kai (2015): Flexible Workflows and Compliance: A Solvable Contradiction?! In: Jan Vom Brocke und Theresa Schmiedel (Hg.): *BPM - Driving Innovation in a Digital World*. Cham: Springer International Publishing (Management for Professionals), S. 247–258.
- Sackmann, Stefan; Kuehnel, Stephan; Seyffarth, Tobias (2018): Correction to. Using Business Process Compliance Approaches for Compliance Management with Regard to Digitization: Evidence from a Systematic Literature Review. In: Mathias Weske, Marco Montali, Ingo Weber und Jan Vom Brocke (Hg.): *Business Process Management. 16th International Conference, BPM 2018, Sydney, NSW, Australia, September 9-14, 2018, Proceedings*, Bd. 11080. Cham: Springer International Publishing (Information Systems and Applications, incl. Internet/Web, and HCI, 11080), C1-C1.
- Sadiq, Shazia; Governatori, Guido (2010): Managing Regulatory Compliance in Business Processes. In: *Handbook on Business Process Management 2*, S. 159–175.

- Sadiq, Shazia; Governatori, Guido; Namiri, Kioumars (2007): Modeling Control Objectives for Business Process Compliance. In: Gustavo Alonso, Peter Dadam und Michael Rosemann (Hg.): Business Process Management, Bd. 4714. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 149–164.
- Scheer, August-Wilhelm (1992): Architektur integrierter Informationssysteme. Berlin, Heidelberg: Springer Berlin Heidelberg.
- Schultz, Martin (2013a): Enriching Process Models for Business Process Compliance Checking in ERP Environments. In: *Design Science at the Intersection of Physical and Virtual Design* 7939, S. 120–135.
- Schultz, Martin (2013b): Towards an Empirically Grounded Conceptual Model for Business Process Compliance. In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (Hg.): Conceptual Modeling, Bd. 8217. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 138–145.
- Schultz, Martin; Radloff, Michael (2014): Modeling Concepts for Internal Controls in Business Processes – An Empirically Grounded Extension of BPMN. In: Shazia Sadiq, Prina Soffer und Hagen Völzer (Hg.): Business Process Management, Bd. 8659. Cham: Springer International Publishing (Lecture Notes in Computer Science), S. 184–199.
- Schultz, Martin; Tropmann-Frick, Marina (2020): Autoencoder Neural Networks versus External Auditors. Detecting Unusual Journal Entries in Financial Statement Audits. In: *Proceedings of the Annual Hawaii International Conference on System Sciences*.
- Schumm, David; Karastoyanova, Dimka; Leymann, Frank; Strauch, Steve (2011): Fragmento. Advanced Process Fragment Library. In: *Information Systems Development*.
- Schumm, David; Leymann, Frank; Ma, Zhilei.; Scheibler, Thorsten.; Strauch, Steve (2010a): Integrating Compliance into Business Processes. Process Fragments as Reusable Compliance Controls. In: *Proc. of the MKWI'10*.
- Schumm, David; Leymann, Frank; Streule, Alexander (2010b): Process Views to Support Compliance Management in Business Processes. In: Will van der Aalst, John Mylopoulos, Norman M. Sadeh, Michael J. Shaw, Clemens Szyperski, Francesco Buccafurri und Giovanni Semeraro (Hg.): E-Commerce and Web Technologies, Bd. 61. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Business Information Processing), S. 131–142.
- Schumm, David; Turetken, Oktay; Kokash, Natallia; Elgammal, Amal; Leymann, Frank; van den Heuvel, Willem-Jan (2010c): Business Process Compliance through Reusable Units of Compliant Processes. In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (Hg.): Current Trends in Web Engineering, Bd. 6385. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 325–337.

- Seeliger, Alexander; Guinea, Alejandro Sánchez; Mühlhäuser, Max (2019): ProcessExplorer. Intelligent Process Mining Guidance. In: *Business Process Management. BPM 2019.*, S. 216–231.
- Seifert, Michael; Kühnel, Stephan (2020): HySLAC. A Conceptual Model for Service Level Agreement Compliance in Hybrid Cloud Architectures. In: *Informatik*.
- Sein, Maung K.; Henfridsson, Ola; Purao, Sandeep; Rossi, Matti; Lindgren, Rikard (2011): Action Design Research. In: *MIS Quarterly* 35 (1), S. 37–56.
- Seyffarth, Tobias; Kühnel, Stephan (2020): Maintaining business process compliance despite changes. a decision support approach based on process adaptations. In: *Journal of Decision Systems*.
- Seyffarth, Tobias; Kühnel, Stephan; Sackmann, Stefan (2016): ConFlex. An Ontology-Based Approach for the Flexible Integration of Controls into Business Processes. In: *Multikonferenz Wirtschaftsinformatik (MKWI) 2016*, S. 1341–1352.
- Seyffarth, Tobias; Kühnel, Stephan; Sackmann, Stefan (2017a): A Taxonomy of Compliance Processes for Business Process Compliance. In: *15th International Conference on Business Process Management, Business Process Management Forum*. In: *Lecture Notes in Business Information Processing (LNBIP)*, S. 71–87.
- Seyffarth, Tobias; Kühnel, Stephan; Sackmann, Stefan (2017b): Welche Compliance-Anforderungen sind für Geschäftsprozessänderungen relevant? Ein Ansatz zur Modellierung der Beziehungen. In: *Proceedings of the Informatik 2017, Lecture Notes in Informatics (LNI)*, S. 1641–1646.
- Seyffarth, Tobias; Kühnel, Stephan; Sackmann, Stefan (2018): Business Process Compliance and Business Process Change. An Approach to Analyze the Interactions. In: *Business Information Systems. BIS 2018. Lecture Notes in Business Information Processing (320)*, S. 176–189.
- Seyffarth, Tobias; Kühnel, Stephan; Sackmann, Stefan (2019): Business Process Compliance despite Change. Towards Proposals for a Business Process Adaption. In: *Information Systems Engineering in Responsible Information Systems. CAiSE 2019. Lecture Notes in Business Information Processing, vol 350.*, S. 227–239.
- Seyffarth, Tobias; Raschke, Kai (2018): BCIT. A Tool for Analyzing the Interactions between Business Process Compliance and Business Process Change. In: *Proceedings of the Dissertation Award and Demonstration, Industrial Track at BPM 2018*, S. 81–85.
- Seyffarth, Tobias; Raschke, Kai (2020): BCIT. A Tool to Recommend Compliant Business Processes based on Process Adaption. In: *Proceedings of the Best Dissertation Award, Doctoral Consortium, and Demonstration & Resources Track at BPM 2020 co-located with the 18th International Conference on Business Process Management (BPM 2020)*, S. 107–111.

- Sillaber, Christian; Brey, Ruth (2012): Managing legal compliance through security requirements across service provider chains. A case study on the German Federal Data Protection Act. In: *GI-Jahrestagung*, 1306--1318.
- Sonnenberg, Christian; Vom Brocke, Jan (2012): Evaluation Patterns for Design Science Research Artefacts. In: Markus Helfert und Brian Donnellan (Hg.): *Practical Aspects of Design Science*, Bd. 286. Berlin, Heidelberg: Springer Berlin Heidelberg (Communications in Computer and Information Science), S. 71--83.
- Sonnenreich, Wes; Albanese, Jason; Stout, Bruce (2006): Return on security investment (ROSI). A practical quantitative model. In: *Journal of Research and Practice in Information Technology* 38 (1), S. 45--56.
- Sowa, J. F.; Zachman, J. A. (1992): Extending and formalizing the framework for information systems architecture. In: *IBM Syst. J.* 31 (3), S. 590--616.
- Stachowiak, Herbert (1973): *Allgemeine Modelltheorie*. Wien: Springer.
- Strecker, Stefan; Heise, David; Frank, Ulrich (2011): RiskM: A multi-perspective modeling method for IT risk assessment. In: *Inf Syst Front* 13 (4), S. 595--611.
- The Institute of Internal Auditors (IIA) (2012): *Global Technology Audit Guide (GTAG) 1. Information Technology Risk and Controls*. Online verfügbar unter http://www.theiia.org/bookstore/downloads/freetomembers/0_1006.dl_gtag1%20nded.pdf, zuletzt geprüft am 11.05.2016.
- The Open Group (hg) (2019): *ArchiMate Model Exchange File Format for the ArchiMate 3.1 Modeling Language*. Online verfügbar unter <https://www.opengroup.org/xsd/archimate/>, zuletzt geprüft am 20.09.2020.
- Turetken, Oktay; Elgammal, Amal; van den Heuvel, Willem-Jan; Papazoglou, Mike (2011): Enforcing compliance on business processes through the use of patterns. In: *ECIS 2011*.
- Vaishanvi, Vijay; Kuechler, Bill; Petter, Stacie (2017): *Design Science Research in Information Systems*. Online verfügbar unter <http://desrist.org/desrist/content/design-science-research-in-information-systems.pdf>.
- van Aalst, Wil M. P. der (2011): *Process Mining. Discovery, Conformance and Enhancement of Business Processes*. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg.
- van der Aalst, W. M. P.; Pesic, M.; Schonenberg, H. (2009): Declarative workflows. Balancing between flexibility and support. In: *Comp. Sci. Res. Dev.* 23 (2), S. 99--113.
- Venable, John; Pries-Heje, Jan; Baskerville, Richard (2016): FEDS. A Framework for Evaluation in Design Science Research. In: *European Journal of Information Systems* 25 (1), S. 77--89.
- Venkatesh, Viswanath (1999): Creation of Favorable User Perceptions. Exploring the Role of Intrinsic Motivation. In: *MIS Quarterly* 23 (2), S. 239--260.

- Vom Brocke, Jan; Hevner, Alan; Maedche, Alexander (2020): Design Science Research. Cases. Cham: Springer International Publishing.
- Vom Brocke, Jan; Simons, Alexander; Niehaves, Björn; Riemer, Kai; Plattfaut, Ralf; Cleven, Anne (2009): Reconstructing the giant. On the importance of rigour in documenting the literature search process. In: *17th European Conference on Information Systems*, S. 2206–2217.
- Webster, Jane; Watson, Richard T. (2002): Analyzing the past to prepare for the future. writing a literature review. In: *MIS Quarterly* 26 (2), S. xiii–xxiii.
- Weiß, Burkhard; Winkelmann, Axel (2011): Developing a Process-Oriented Notation for Modeling Operational Risks. A Conceptual Metamodel Approach to Operational Risk Management in Knowledge Intensive Business Processes within the Financial Industry. 44th Hawaii International Conference on System Sciences, S. 1–10.
- Weske, Mathias (2019): Business Process Management. Concepts, Languages, Architectures. 3rd ed. 2019.
- Winter, Robert; Fischer, Ronny (2006): Essential Layers, Artifacts, and Dependencies of Enterprise Architecture. In: *2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06)*, S. 30–37.
- Wohlin, Claes; Runeson, Per; Höst, Martin; Ohlsson, Magnus C.; Regnell, Björn; Wesslén, Anders (2012): Experimentation in Software Engineering. Berlin, Heidelberg: Springer Berlin Heidelberg.
- Wrona, Thomas (2006): Fortschritts- und Gütekriterien im Rahmen qualitativer Sozialforschung. In: *Fortschritt in den Wirtschaftswissenschaften: Wissenschaftstheoretische Grundlagen und exemplarische Anwendungen*, S. 189–216.
- Yousafzai, Shumaila Y.; Foxall, Gordon R.; Pallister, John G. (2007): Technology acceptance. A meta-analysis of the TAM: Part 1. In: *Jnl of Modelling in Management* 2 (3), S. 251–280.
- Zur Muehlen, Michael; Rosemann, Michael (2005): Integrating Risks in Business Process Models. In: *15th Australasian Conference on Information Systems (ACIS 2005)*.

Anlage A: Autorenerklärung über die Arbeitsanteile der Artikel

Der Artikel „*A Taxonomy of Compliance Processes for Business Process Compliance*“ wurde in Ko-Autorenschaft mit Stephan Kühnel (KS) und Stefan Sackmann (SaS) verfasst. Die nachfolgende Tabelle gibt einen Überblick über die Arbeitsanteile der Autoren am Artikel.

Aspekt	Autor/en
Problemstellung und Zielsetzung	ST
Forschungskonzept	ST
Literaturrecherche	ST
Konzeptualisierung des Themas	ST
Entwicklung der Taxonomie	ST unter Mitwirkung von KS
Entwicklung des Beispielszenarios	ST
Erstellung des Manuskripts	ST unter Mitwirkung von KS
Überprüfung und Überarbeitung vor der Einreichung	ST, KS, SaS
Überarbeitung nach der Begutachtung	ST, KS

Der Artikel „*Business Process Compliance and Business Process Change. An Approach to Analyze the Interactions*“ wurde in Ko-Autorenschaft mit Stephan Kühnel (KS) und Stefan Sackmann (SaS) verfasst. Die nachfolgende Tabelle gibt einen Überblick über die Arbeitsanteile der Autoren am Artikel.

Aspekt	Autor/en
Problemstellung und Zielsetzung	ST
Forschungskonzept	ST
Literaturrecherche	ST
Konzeptualisierung des Themas	ST
Entwicklung der Methode	ST
Entwicklung des Beispielszenarios	ST
Entwicklung des Softwareprototypens	ST
Erstellung des Manuskripts	ST
Überprüfung und Überarbeitung vor der Einreichung	ST, KS, SaS
Überarbeitung nach der Begutachtung	ST

Der Artikel „*Business Process Compliance despite Change. Towards Proposals for a Business Process Adaption*“ wurde in Ko-Autorenschaft mit Stephan Kühnel (KS) und Stefan Sackmann (SaS) verfasst. Die nachfolgende Tabelle gibt einen Überblick über die Arbeitsanteile der Autoren am Artikel.

Aspekt	Autor/en
Problemstellung und Zielsetzung	ST
Forschungskonzept	ST
Literaturrecherche	ST
Konzeptualisierung des Themas	ST unter Mitwirkung von KS
Entwicklung der Methode	ST
Entwicklung des Beispielszenarios	ST
Erstellung des Manuskripts	ST
Überprüfung und Überarbeitung vor der Einreichung	ST, KS, SaS
Überarbeitung nach der Begutachtung	ST

Der Artikel „*Maintaining Business Process Compliance despite Changes. A Decision Support Approach based on Process Adaptations*“ wurde in Ko-Autorenschaft mit Stephan Kühnel (KS) verfasst. Die nachfolgende Tabelle gibt einen Überblick über die Arbeitsanteile der Autoren am Artikel.

Aspekt	Autor/en
Problemstellung und Zielsetzung	ST
Forschungskonzept	ST
Literaturrecherche	ST
Konzeptualisierung des Themas	ST
Definition der Evaluationsstrategie	ST
Entwicklung des Softwareprototypens	ST
Entwicklung und Durchführung der Fallstudien	ST
Auswertung und Interpretation der Fallstudienenergebnisse	ST
Diskussion der Implikationen	ST
Erstellung des Manuskripts	ST
Überprüfung und Überarbeitung vor der Einreichung	ST, KS
Überarbeitung nach der Begutachtung	ST, KS

Anlage B: Publikation „A Taxonomy of Compliance Processes for Business Process Compliance“

Seyffarth, Tobias; Kühnel, Stephan; Sackmann, Stefan (2017): A Taxonomy of Compliance Processes for Business Process Compliance. In: 15th International Conference on Business Process Management, Business Process Management Forum. In: Lecture Notes in Business Information Processing (LNBIP), S. 71–87. DOI: 10.1007/978-3-319-65015-9_5.

A Taxonomy of Compliance Processes for Business Process Compliance

Tobias Seyffarth^(✉), Stephan Kühnel, and Stefan Sackmann

Martin Luther University Halle-Wittenberg, 06108 Halle (Saale), Germany
{tobias.seyffarth, stephan.kuhnel,
stefan.sackmann}@wiwi.uni-halle.de

Abstract. Dynamic markets and new technology developments lead to an increasing number of compliance requirements. Thus, affected business processes must be flexible and adaptable. Ensuring business processes compliance (BPC) is traditionally operationalized by means of controls, which can be described as simple target-performance comparisons. Since such controls are not always suitable for achieving BPC, the view is extended by so-called compliance processes. However, the definition and design of appropriate compliance processes for effective BPC depend on a multitude of process characteristics. To address this issue on a general level, we developed a taxonomy for compliance processes consisting of 9 dimensions and 37 characteristics. As a result, the taxonomy allows researchers and practitioners to classify compliance processes according to the state of the art in a formal way. Furthermore, it provides a systematic fundament for greater flexibility, i.e. an ad hoc integration of compliance processes into ongoing business processes to ensure BPC during runtime.

Keywords: Business Process Compliance · Classification · Compliance Process · Taxonomy

1 Introduction

Dynamic markets, competitive constraints, and technological developments require flexible business responsiveness as well as the flexible adaptation of affected business processes [1]. This includes adherence to prescribed and/or agreed-upon norms, which is known as compliance [2, 3]. Such norms can originate from various compliance sources, like laws, regulations or standards, which have to be interpreted and translated into numerous (organization-specific) compliance requirements [2, 4, 5]. Not only business scandals but also modern technological developments such as digitalization, big data, and cloud computing lead to new and changing norms, which define a constantly increasing number of compliance requirements [6, 7].

Usually, controls are used to ensure business process compliance (BPC) [8, 9]. In [10], a control activity is defined as a single target-performance comparison. This is a narrow definition, since not all compliance requirements can be operationalized accordingly (e.g. obligatory duties) [11]. Other authors describe controls as restraining or direct influence to enforce, observe, or verify compliance requirements [12]. In this context, methods for business process modeling can also be used for control modeling

[13–15]. Therefore, BPC approaches depict controls as reusable [4] and autonomous control processes [14, 15], i.e. combinations of one or more control activities. Thus, and due to the inconsistent understanding of the term “control”, we rely on the term “compliance process” in this paper. We define a compliance process as an independent process (part) consisting of at least one compliance-related activity that ensures BPC.

Compared to backward compliance checking, which is subsequently analyzing log files, runtime compliance checking allows to instantly avoid or react to possible compliance violations during the business process execution [12, 16, 17]. Ensuring BPC by runtime compliance checking becomes a challenging task when taking process flexibility into account [4, 14, 15], and it becomes more challenging when process flexibility is understood as “flexibility by change” [18], i.e. a business process can be adjusted on a per-instance basis during its runtime [4, 14, 15]. The separate modeling of reusable compliance processes [4] and its ad hoc integration in ongoing business process instances is a promising approach for ensuring BPC during runtime [14, 15]. However, a major challenge is the determination of appropriate compliance processes, as they depend on a large number of different characteristics (c.f. [9, 13, 19–21]). The characteristics of a compliance process can determine its execution in a business process [22] or its efficiency and effectiveness (c.f. [9, 23]).

Meanwhile, a substantial body of research has discussed the characteristics of compliance processes. For example, Riesner and Pernul [21] classify compliance processes according to their security semantics, such as integrity or availability. Panko [24] distinguishes between detective, preventive, and corrective compliance processes. Gehrke [19] as well as Schultz and Radloff [13] make a distinction according to their timing, frequency, or nature. Nevertheless, none of the authors addresses process flexibility or the ad hoc integration of compliance processes into business processes. Furthermore, none describes the proposed classification in a comprehensible way. Thus, we address the following research question: what characteristics address an ad hoc integration of compliance processes, what are general characteristics of compliance processes and how can they be classified? To answer this question, we developed a comprehensive compliance process taxonomy according to the well-established approach of Nickerson et al. [25]. Within the taxonomy development, we conducted a structured literature review according to vom Brocke et al. [26] and Webster and Watson [27] to conceptualize the characteristics of compliance processes. The resulting compliance process taxonomy enhances the descriptive knowledge in the field of BPC with two main contributions [28]. First, it extends existing classifications [13, 19, 21, 24] according to characteristics that are relevant for the ad hoc integration of compliance processes in ongoing business processes to ensure BPC during runtime [22]. Second, it combines additional general characteristics of compliance processes (e.g. [9, 20, 29, 30]) in a traceable way.

The contribution is structured as follows: in Sect. 2, a compliance model is presented that provides the formal basis for an ad hoc integration of compliance processes in ongoing business processes. In Sect. 3, according to the approach of Nickerson et al. [25], the development of our taxonomy is described and made comprehensible. In Sect. 4, the resulting taxonomy is discussed in greater detail, and in Sect. 5, the taxonomy is evaluated, and an exemplary application is presented. Finally, a brief conclusion and research outlook are provided in Sect. 6.

2 Connecting Business Processes with Compliance Processes

To describe relevant elements and their interrelations in the field of BPC, compliance models are often used. Many compliance models display the connection between compliance requirements, business processes, and controls or control processes [2, 4, 5, 12, 22]. For an ad hoc integration of compliance processes in ongoing business processes, a compliance model must depict at least three major requirements: (a) a separate modelling of business processes and compliance processes [15]; (b) a detailed description of the connection between compliance requirements, business processes, and further compliance processes; and (c) a separated view of process scheme and process instance. To develop an adequate compliance model, we refer to prior research [22]¹. In Sect. 3, the compliance model is used to derive necessary characteristics of compliance processes. They are used within the taxonomy for the ad hoc integration of compliance processes in ongoing business processes.

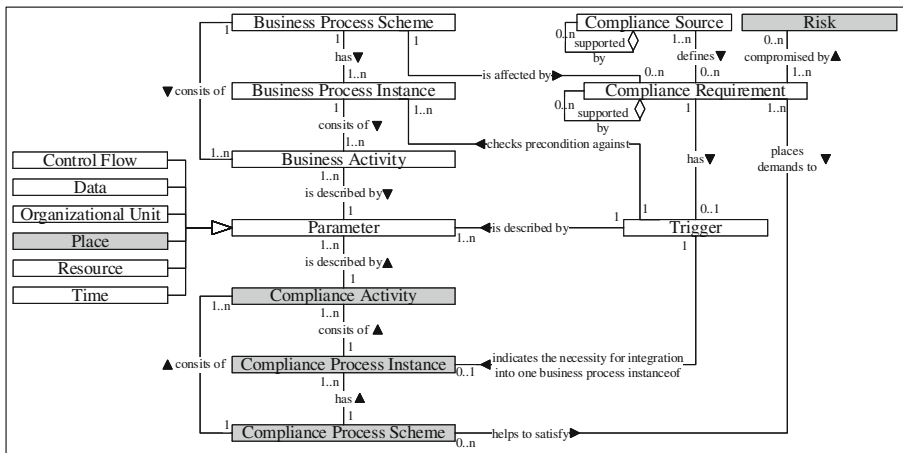


Fig. 1. Adjusted compliance model (based on [22])

At its core, the compliance model in [22] indicates the necessity for creation and integration of a compliance process instance into an ongoing business process instance. For example, a business process scheme called “Authorizing a Customer Loan Request” might be affected by a compliance requirement whenever a loan request exceeds a certain amount. Here, not every instance of the business process scheme is affected by the compliance requirement. Since the business and compliance processes are modelled separately, the compliance model in [22] aims at integration. Therefore, the connection between business activities (i.e. activities of the actual business process) and compliance process instances is formalized by parameters describing the properties

¹ Due to space limitations, we refer to [22] for a detailed explanation of the model.

of business activities and integration constraints of compliance process instances. A parameter consists of different parameter types, such as data, or organizational unit. Thus, the compliance model in [22] provides a method for determining all valid points within a business process at activity level for integrating compliance processes if required.

Although the view of the compliance model in [22] is already detailed, several adjustments are proposed. The resulting adjusted compliance model is visualized in Fig. 1 (adjusted and enhanced entities are highlighted in grey) and discussed in the following. The adjustments are grouped into three clusters, according to their characteristics, as follows: The original entities “control process scheme” and “control process instance” are redefined as “compliance process scheme” and “compliance process instance”. As previously noted, a control activity is a single target-performance comparison [10] that is not capable of operationalizing all types of compliance requirements accordingly. Following our argument, a compliance process is the combination of one or more compliance activities that are capable of meeting an underlying compliance requirement. Thus, the entity “control activity” is also redefined as “compliance activity”, representing an atomic work item (partly) ensuring that business processes are in accordance with a specified set of compliance requirements.

The compliance model is extended by an entity “risk” [4, 5]. Failures to meet compliance requirements increase the likelihood of risks materializing. For instance, a risk could occur as a result of an error in IT use. Usually, an error has an impact on the accuracy of financial reporting hence a compliance requirement could be compromised by a risk [9, 20, 29, 30]. This extension is required since the selection of a concrete compliance process from a set of possible alternatives is necessary in the context of flexible integration and economic risk is seen as a valid parameter for decision-making in the context of business processes [15].

The compliance model is extended by the parameter type “place” [31]. This is necessary, since the location of the execution of a business activity affects the integration of compliance processes in at least two ways: (a) depending on the place of processing different compliance requirements can affect a business process instance; and (b) the place might present integration constraints for compliance processes. For example, the German Federal Data Protection Act defines various compliance requirements for processing personal data [32] that are related to place, namely, place-related jurisdiction, which only affects business activities processed in Germany. An integration constraint occurs whenever a business or compliance process is constrained by its place of execution.

Based on this extended compliance model, it is still unclear how to categorize compliance processes (or their schemes and instances) in an appropriate way. Nevertheless, a classification is necessary for their appropriate selection and integration in ongoing business process instances. A taxonomy can be used to classify objects, thereby bringing order to the complex area of compliance processes [25, 33].

3 Taxonomy Development in Information Systems Research

Following the design science research (DSR) paradigm, our taxonomy is subsumed under the most fundamental artifact type “construct”. Constructs define conceptual vocabulary providing the basis for the representation of problem domains or the construction of models [34]. According to Gregor and Mwilu et al. [28, 35], a taxonomy classifies objects or phenomena of interest, according to the dimensions that are relevant for characterizing and discriminating between these objects. As defined in Nickerson et al. [25], a taxonomy is used for the description and classification of existing or future objects in a specific domain. In addition, they define a taxonomy as a set of n dimensions each consisting of $k \geq 2$ mutually exclusive and collectively exhaustive characteristics. Mutually exclusive means that no object can have two different or even more than one characteristic in every dimension. Collectively exhaustive means that an object must have one characteristic in each dimension.

In the following, we refer to the definition of a taxonomy provided by Gregor and Mwilu et al. [28, 35] and apply the well-established methodological approach proposed by Nickerson et al. [25], which is variously used in the field of information systems [33, 35, 36]. According to Gregor and Mwilu et al., an object to be classified by the taxonomy can have different characteristics in one dimension. We will refer to this statement in the discussion of our taxonomy in Sect. 4.

The goal is to develop a “useful” taxonomy [25] for compliance processes and not a “correct” or the “best” one, since searching for the best solution is often intractable for information systems problems in DSR [34]. Figure 2 illustrates the applied approach for taxonomy development that is explained in greater detail in [25].

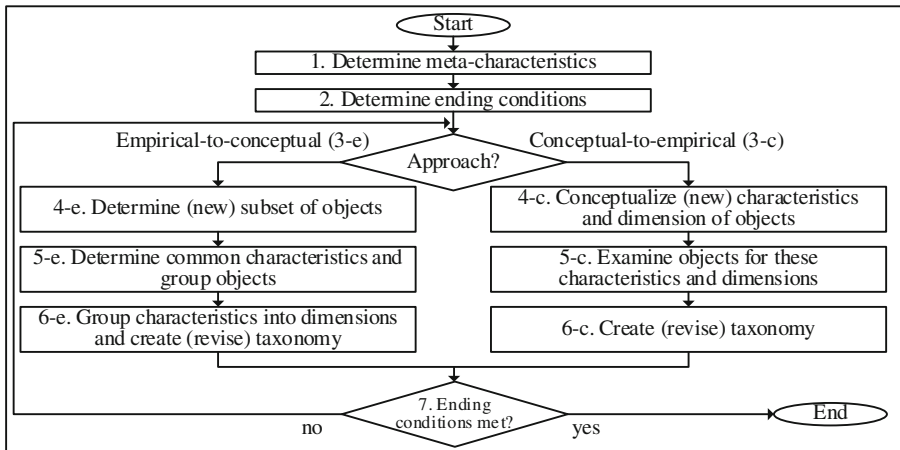


Fig. 2. Taxonomy development method [25]

Since comprehensibility is required in a scientific procedure, the first three steps of our taxonomy development are explained in detail. The last steps are explained by our application of the taxonomy development process.

Step 1. To begin with, meta-characteristics must be defined according to the purpose of the taxonomy [25]. The meta-characteristic is the most comprehensive characteristic that serves as the basis for choosing dimensions and characteristics. Since the aim is the specification of compliance processes that can be flexibly integrated in ongoing business processes, the following meta-characteristics are defined: (1) based on the compliance model as introduced in Sect. 2, the meta-characteristic “integration constraint” specifies integration constraints for a compliance process; (2) “modelling” specifies opportunities to model a compliance process at its compliance activity level, as well as opportunities for its integration in business processes; and (3) “property” specifies the properties of a compliance process for its processing.

Step 2. Defining a taxonomy involves an iterative approach; thus, ending conditions have to be defined [25]. Our development process stops if the number of dimensions allows the taxonomy to be meaningful (concise), and the dimensions as well as the characteristics provide differentiation among objects (robust). Furthermore, all dimensions of interest shall be identified (comprehensive) and new dimensions or characteristics shall be added easily (extendible). Finally, the development process ends if the taxonomy can explain the classified objects (explanatory).

Step 3. The actual taxonomy development begins with either an empirical-to-conceptual approach (step 3-e) or a conceptual-to-empirical approach (step 3-c). The decision regarding which approach shall be used depends on the availability of data. Step 3-e shall be used if significant data regarding the domain are available; step 3-c shall be used if the researcher has significant knowledge about the domain.

Because the field of BPC entails a large body of literature, the first iteration was done using the empirical-to-conceptual approach (step 3-e). Therefore, we conducted a structured literature review according to vom Brocke et al. [26]. As proper sources, we used the following databases: AIS Electronic Library (AISeL), EBSCOhost, IEEE Xplore Digital Library, the Journals of the American Accounting Association (AAA), and SpringerLink. Following Hevner et al. [34], the search was restricted to academic articles published within the last decade. We searched for contributions with full-text availability by using the search terms «application control», «(“compliance process” OR “control process” OR “internal control”) AND (category OR taxonomy)». As noted in [26], the resulting hits were selected by title, abstract, and full-text evaluation. Finally, [7, 13, 19, 21, 24] were identified as proper sources. According to Webster and Watson [27], a backward search was also conducted leading to [10, 37]. Furthermore, with respect to the domain, relevant international as well as German (available in English) standards and best practices in accounting, such as standards from the Institute of Public Auditors in Germany or COBIT and COSO [8, 9, 20, 29, 30, 38–41] were taken into consideration. A total of 16 highly relevant contributions were identified, providing the basis for our taxonomy development. Based on this body of literature, we defined the dimensions “controlled entity” and “assertion” within the meta-characteristic “integration constraints”. Both dimensions set conditions according to the integration of a compliance process in a business process. Within the meta-characteristic “property”, we defined the

dimensions “timing”, “type”, and “execution”. However, at this point, the taxonomy was not entirely concise according to the model proposed in Sect. 2.

Hence, the second iteration was conducted using the conceptual-to-empirical approach (step 3-c): the dimension “trigger” was added to the meta-characteristic “condition” and the dimensions “integration” and “compliance activity pattern” were added to the meta-characteristic “modelling”. The dimension “integration” was identified due to extensive internal discussions. According to [22], a trigger is required in order to indicate the necessity to integrate a compliance process in an ongoing business process instance. According to [10], a control consists of a target-performance comparison and a deviation analysis. Each target-performance comparison should be supported by a recovery action to avoid compliance violations by handling negative results of the business process [37]. Therefore, we added the characteristics “target-performance comparison”, “deviation analysis”, and “recovery action” to the dimension “compliance activity pattern”. By checking the ending conditions in step 7, the taxonomy was still not robust because the dimension “compliance activity pattern” does not provide a useful differentiation of compliance processes.

Therefore, the third iteration was conducted according to the conceptual-to-empirical approach. In practice, a compliance process does not exclusively consist of a deviation analysis or a recovery action. A compliance activity is always necessary for triggering a deviation analysis or a recovery action. Therefore, we divided the previously added dimension “compliance activity pattern” into the two dimensions “compliance requirement pattern” and “resolution pattern”. In case of a negative target-performance comparison, the resolution pattern detects the results of a negative target-performance comparison and the recovery actions aim to avoid compliance violations.

The fourth iteration was conducted using the empirical-to-conceptual approach. We searched the International Standards on Accounting No. 315 [42] in order to build a more explanatory taxonomy. Including the results from the literature review of the first iteration, 15 different characteristics within the dimension “assertion” were identified. There are too many characteristics within one dimension for the application and comprehension of the taxonomy [25]. Therefore, the dimension was removed to provide a robust taxonomy according to [25]. In the next section, the resulting compliance process taxonomy and its characteristics are presented in detail.

4 A Compliance Process Taxonomy

Figure 3 shows the resulting compliance process taxonomy that finally allows for the categorization of compliance processes for ensuring BPC in an ongoing business process instance. The taxonomy consists of the three meta-characteristics “integration constraint” (dimension D 1 to D 3), “modelling” (D 4 to D 6) and “property” (D 7 to D 9).

D 1 – Trigger: As described in the compliance model, triggers are required for a flexible integration of compliance processes in ongoing business process instances [22]. A trigger is defined as a production rule that performs a certain action whenever a trigger condition is evaluated as true [43]. Following our understanding, a trigger

	Dimension	Characteristics						
Integration Constraint	D 1: Trigger	D 1.1: Business Activity	D 1.2: Data	D 1.3: Organizational Unit	D 1.4: Place	D 1.5: Resource	D 1.6: Time	D 1.7: Frequency of Business Process Instance
	D 2: Controlled Entity	D 2.1: Business Activity	D 2.2: Data	D 2.3: Organizational Unit	D 2.4: Place	D 2.5: Resource	D 2.6: Time	
	D 3: Further Requirements for Execution	D 3.1: Data	D 3.2: Organizational Unit	D 3.3: Place	D 3.4: Resource	D 3.5: Time	D 3.6: No Further Requirements	
Modelling	D 4: Compliance Requirement Pattern	D 4.1: Target Performance Comparison	D 4.2: Other Compliance Activity					
	D 5: Resolution Pattern	D 5.1: Deviation Analysis	D 5.2: Recovery Action	D 5.3: No Resolution Pattern				
	D 6: Integration	D 6.1: Sequential	D 6.2: Parallel	D 6.3: Start Event	D 6.4: End Event	D 6.5: Independent		
Property	D 7: Timing	D 7.1: Preventive	D 7.2: Detective					
	D 8: Type	D 8.1: Application Control	D 8.2: IT General Control	D 8.3: Business Control				Mutually exclusive characteristic
	D 9: Execution	D 9.1: Automated	D 9.2: Manual	D 9.3: IT-dependent manual				Non-mutually exclusive characteristic

Fig. 3. Compliance process taxonomy

indicates the need to integrate a compliance process in a business process. The trigger condition is checked against each business activity and/or its properties.

In principle, the execution of a compliance process can be triggered based on an event or frequency [19, 37, 44]. For example, an event can be specified by the occurrence or absence of a business activity. Following the process flexibility type “flexibility by change” [18], the occurrence or absence of a business activity within a business process instance remains unclear at starting time. Therefore, the characteristic “business activity” (D 1.1) was added. Besides that, the relationships between further characteristics in D 1 are obvious [37]. A business activity may produce or consume “data” (D 1.2). An “organizational unit” (D 1.3) performs a business activity at a certain “place” (D 1.4) and may require several “resources” (D 1.5) to carry out the business activity. Finally the business activity has a processing time and starts and ends at a specific “time” (D 1.6). In the case of executing compliance processes for a random check of controlled entities, we added the characteristic “frequency of business process instance” (D 1.7). The characteristics in D 1 are defined as non-mutually exclusive [28, 35]. Therefore, a combination of them is possible to build the trigger.

D 2 – Controlled Entity: A controlled entity specifies the entity that is the subject of a compliance requirement. It arises from the entity parameter as discussed in the compliance model in Sect. 2. To integrate a compliance process in an ongoing business process, the controlled entity must be available. Therefore, the characteristic “business activity” (D 2.1) and its related elements “data” (D 2.2), “organizational unit” (D 2.3), “place” (D 2.4), “resource” (D 2.5), and “time” (D 2.6) were added. Like the characteristics in D 1, the characteristics in D 2 are defined as non-mutually exclusive [28, 35]. For instance, a compliance process, “Verify backup creation”, is necessary to validate the occurrence of a required business activity, “Create data backup”, at a certain place, “Data Center”. Here, the compliance process has two characteristics

within one dimension: the characteristic business activity is necessary to check the occurrence of the business activity “Create data backup”, and the characteristic place is required to check the place of execution.

D 3 – Further Requirements for Execution: Sometimes, a compliance requirement induces further demands for the execution of a compliance process. Imagine that, a compliance requirement demands the authorization of a purchase request by an employee of the role manager. In this case, an organizational unit of the specified role must be available to execute the corresponding compliance process. For the description of these further requirements, again the characteristics “data” (D 3.1), “organizational unit” (D 3.2), “place” (D 3.3), “resource” (D 3.4), “time” (D 3.5), or even “no further requirement” (D 3.6) were added.

D 4 – Compliance Requirement Pattern: A pattern is an abstract process building that may contain various process elements [45]. Following this, a compliance requirement pattern is a pattern that contains various compliance process elements to ensure adherence to a compliance requirement [11].

A compliance process consists of at least one compliance activity directly enforcing compliance as well as optional activities resolving the results of former compliance activities or avoiding compliance violations. As stated in [14, 15], a control activity is simply a single “target-performance comparison” (D 4.1) returning a true/false statement. A target-performance comparison can be realized by various patterns, for example, by N-way match and plausibility or completeness checks [8, 9, 30, 37, 46]. Following COSO [8], a target-performance comparison can be used in so-called supervisory compliance activities to verify the correctness of other compliance processes or to validate compliance.

In some cases, satisfying compliance requirements does not need target-performance comparisons but rather non-comparative measures of the type “other compliance activity” (D 4.2). In the case of Section 14 of the German Banking Act, an approved loan amount greater than one million Euros requires the notification of the German Federal Financial Supervisory Authority [47]. The required notification by the credit institute can be realized by a compliance process consisting of patterns of the type “other compliance activity”. Besides that, a compliance process sometimes consists of both types, which is why the characteristics are highlighted as non-mutually exclusive.

D 5 – Resolution Pattern: A resolution pattern comprises activities that analyze and react on the negative results of compliance requirement patterns. As noted, a target-performance comparison detects only deviations and finally returns only a true/false statement. Nevertheless, the identified deviation can be either positive or negative. In order to check this, the pattern “deviation analysis” (D 5.1) was added [10]. If the target-performance comparison returns as “false”, the deviation analysis detects reasons for that result. Depending on the result of the deviation analysis and/or the degree of deviation, the handling of an affected business process instance can be determined. A “recovery action” (D 5.2) handles any further processing of affected business process instances to avoid compliance violations [8, 29, 37]. Recovery actions can also be interpreted as corrective control activities [8, 24, 41]. In [37], various recovery actions, such as “redo the affected business activity”; “in case of deviation,

notify a responsible employee”; or “cancel the affected business process instance” are discussed. Besides that, sometimes a compliance process consists of neither a deviation analysis nor a recovery action [47]. Therefore, we also added the characteristic “no resolution pattern” (D 5.3).

D 6 – Integration: Based on the compliance model as proposed in Sect. 2, a compliance process has to be integrated in affected business process instances. In this context, the integration can occur as “sequential” (D 6.1) or “parallel” (D 6.2). As a result of the integration, the compliance process directly influences the business process instance and, e.g., its performance.

In addition, a compliance process is sometimes integrated in a business process only by its “start event” (D 6.3). As discussed above, the notification of the German Federal Financial Supervisory Authority does not require a confirmation of receipt. In this case, the result of the compliance process does not influence the business process instance. Both the business process instance and the integrated compliance process instance are completed separately. Moreover, only the “end event” (D 6.4) of a compliance process can be integrated into a business process instance. Finally, a compliance process can occur as completely “independent” (D 6.5) of a business process instance [9, 19]; for example the IT Governance Institute [9, 20] or ISACA [38] can demand a strategy for the cyclical backup of data and programs. A compliance process that satisfies this compliance requirement is performed independently of a special business process.

D 7 – Timing: As discussed in Sect. 2, our taxonomy considers compliance processes to realize BPC during runtime. In general, compliance processes are either “preventive” (D 7.1) or “detective” (D 7.2). A preventive compliance process attempts to keep deviations from occurring. In contrast, a detective compliance process attempts to uncover compliance violations in a business process instance after the time of their occurrence [8, 9, 12, 24, 39, 41]. The detection takes place before the ultimate objective of the business process instance has concluded [8]. In both cases, the critical part is the recovery action, which is used to correct or avoid an unintended event or result [8, 12, 17, 19, 24, 39]. Therefore, a detective compliance process may still (at least partly) enforce compliance [11].

D 8 – Type: Compliance processes are also categorized according to their type. There is a distinction between an “application control”, an “IT general control”, and a “business control” [20, 40, 46]. An application control (D 8.1) enforces, verifies, or observes compliance requirements within its embedded application. Furthermore, it observes the input, processing, and output of data processing [9, 29, 40, 46]. For instance, the identification and authentication of a user can be realized through a logical access control by checking a unique user ID and password [7, 29]. IT general controls (ITGC) (D 8.2) support the proper and continued operation of IT including application controls. ITGCs include compliance processes over program development, program changes, access to programs, or data and computer operations [7, 9, 20, 21, 40, 41]. They are either embedded or independent of business processes [9, 21]. A compliance process satisfying the illustrative compliance requirement “Implement a cyclical backup of data and programs” is categorized as an ITGC [9, 20, 29]. Finally, a business

control (D 8.3) is a (manual) compliance process that is integrated in a business process or is independent from a business process [9, 40, 46].

D 9 – Execution: A compliance process is either processed “automated”, “manual”, or “IT-dependent manual”. Within an automated (D 9.1) execution, all compliance activities of a compliance process are performed without human interaction. In contrast, a manual (D 9.2) compliance process is performed entirely without the use of any technology [8, 9, 12, 20, 29, 39, 41]. Hence, a compliance process of the type application control can also be processed manually [8, 29]. The design, implementation, and update of logical access controls are examples of a manual application control. If a compliance process consists of automatic and manual compliance activities, its execution is called IT-dependent manual (D 9.3) [9, 39]. In the next section, the evaluation of the developed compliance process taxonomy is discussed. Furthermore, the application is demonstrated by an example.

5 Compliance Process Taxonomy: Evaluation and Application

In DSR, artifacts are evaluated in two successive ways: *ex ante* or *ex post* [48, 49]. An *ex-ante* evaluation occurs prior to the artifact construction and focusses on artifact refinement during the design phase. An *ex-post* evaluation validates artifacts in use. Since the definition of a taxonomy is difficult to be evaluated *ex post* [25, 50], it was evaluated *ex ante* by conducting the following two steps: first, an extensive literature review based on a well-established methodology for literature review [26, 27] was conducted. Most of the taxonomy’s dimensions and characteristics are derived from state-of-the-art literature. Second, our taxonomy was refined during the development phase [25].

After four iterations of the taxonomy development process, the (subjective) ending conditions were met. As required by [25], the resulting compliance process taxonomy is concise, robust, comprehensive, extendible, and explanatory. Consisting of nine dimensions, the taxonomy is concise. It is also robust with a maximum of seven characteristics in the dimension “trigger”. By defining the meta-characteristics “integration constraint”, “modelling”, and “property” as well as the identification of dimensions and characteristics through the literature review, the taxonomy is also comprehensive. Furthermore, the taxonomy can easily be extended, e.g., by adding further characteristics to the dimensions “Compliance Requirement Pattern” or “Resolution Pattern”. In addition, the taxonomy is explanatory, which is demonstrated by its application.

Figure 4 shows a simplified and adapted Purchase-to-Pay business process [51] that is modelled in BPMN 2.0 [52]. We call this process model an adapted process model because it contains business activities and integrated compliance processes. The business activities are modelled by the BPMN element “activity” (white); the integrated compliance processes are modelled by the BPMN element “collapsed sub-process” (grey). In the event of a negative result of the target-performance comparison the recovery action within each compliance process will terminate the adapted process

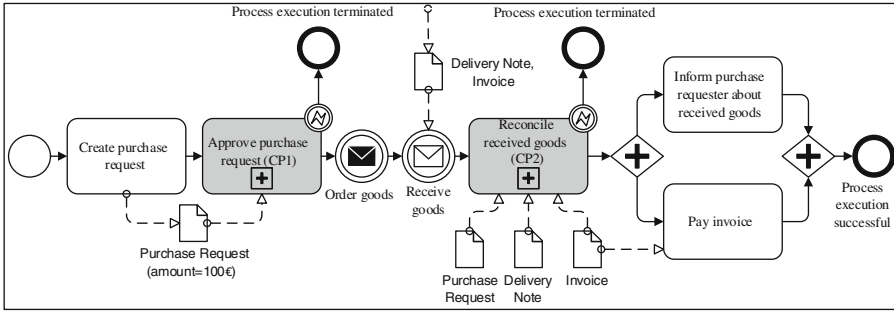


Fig. 4. Adapted purchase-to-pay business process model (based on [51])

instance. All required documents are also modelled by the corresponding BPMN element “data object”.

The following two compliance requirements are assumed to affect the adapted purchase process discussed above:

- Compliance Requirement CR1: “Purchase requests with an order amount greater than 50€ must be approved according to existing order conditions by an employee of the role manager.”
- Compliance Requirement CR2: “50% of all received goods must be reconciled to the purchase request.”

Following the corresponding associations of the compliance model proposed in Sect. 2, we assume that the compliance process “Approve purchase request” (CP1) satisfies CR1. Equivalently, the compliance process “Reconcile received goods” (CP2) satisfies CR2. Figure 5 shows the compliance process taxonomy application by classifying both compliance processes.

	Dimension	Applicable characteristics of CP1	Applicable characteristics of CP2
Integration Constraint	D 1: Trigger	D 1.2: Data (amount of purchase request)	D 1.7: Frequency of Business Process Instance
	D 2: Controlled Entity	D 2.2: Data (purchase request)	D 2.2: Data (purchase request, delivery note, invoice)
	D 3: Further Requirements for Execution	D 3.2: Organizational Unit (employee of the role manager)	D 3.6: No further Requirements
Modelling	D 4: Compliance Requirement Pattern	D 4.1: Target -Performance Comparison	D 4.1: Target -Performance Comparison
	D 5: Resolution Pattern	D 5.2: Recovery Action	D 5.1: Deviation Analysis
			D 5.2: Recovery Action
Property	D 6: Integration	D 6.1: Sequential	D 6.1: Sequential
	D 7: Timing	D 7.1: Preventive	D 7.2: Detective
	D 8: Type	D 8.1: Application Control	D 8.3: Business Control
	D 9: Execution	D 9.3: IT dependent manual	D 9.2: Manual

Fig. 5. Applied compliance process taxonomy

Based on CR1, CP1 is triggered by data because the amount of the purchase request is 100€, which is clearly above the 50€ stated in CR1. The controlled entity of CP1 is the purchase request. Therefore, the controlled entity is subsumed under the characteristic data. A further requirement for executing the compliance process is an organizational unit, since an employee of the role manager must approve the purchase request. CP1 consists of a target performance comparison. We assume that the purchase request is compared to requirements of internal guidelines. CP1 also contains a recovery action, which terminates the adapted process instance in the event of a negative target-performance comparison. CP1 is integrated sequentially in the business process and has preventive timing because the purchase request is checked before goods are ordered. Furthermore, CP1 is an application control that is performed as “IT-dependent manual” since the approval by an employee of the role manager still requires human interaction.

We assume that the purchase process instance occurs within the sample scope of the second compliance requirement. Furthermore, the compliance process is triggered by frequency of the business process instance. The compliance process CP2 compares the purchase request with the delivery note and invoice which means that it consists of a target-performance comparison. Thus, the controlled entity is of the type data. Besides that, there are no further requirements for the execution of CP2. We assume that CP2 performs a deviation analysis in case of a negative result of its target-performance comparison, before the recovery action takes place. The recovery action also terminates the adapted purchase process instance. Like the first compliance process, CP2 is integrated sequentially in the business process instance. In contrast to CP1, CP2 is a detective compliance process. The detection takes place after a possible violation (e.g. purchase request and delivery note do not match) but before the ultimate objective of the business process instance has occurred (i.e. informing the purchase requester about received goods). In addition, CP2 is a manually executed business control.

6 Conclusion and Outlook

Recent scandals and modern technological developments lead to new and changing norms, defining a constantly increasing number of compliance requirements [6, 7]. To comply with these requirements, the aim of business process compliance (BPC) is a comprehensive and comprehensible definition of compliance processes and their integration in business processes. For maintaining process flexibility in the context of BPC [18], a separate modelling of compliance and business processes as well as their ad hoc integration during runtime is discussed [4, 14, 15]. The determination of appropriate compliance processes for BPC becomes a major challenge, since they depend on a multitude of characteristics (c.f. [9, 13, 19, 20]). A major shortcoming of existing classifications for controls is the missing discussion of comprehensive compliance processes that are more than “simple” controls and their flexible integration in business processes. This research gap is addressed in the present contribution by the novel compliance process taxonomy which extends the descriptive DSR knowledge base. The taxonomy allows a classification of compliance processes based on 9

dimensions and 37 characteristics. Specifically, the first meta-characteristic “integration constraint” focuses on necessary characteristics to integrate compliance processes in ongoing business processes. The methodical development of the resulting compliance process taxonomy is considered to be comprehensive, concise, robust, extendible, and explanatory.

A well-known shortcoming of any literature review and taxonomy development is the fact that it is not possible to determine whether each and every relevant work, dimension, and characteristic has been found. However, by documenting the search for literature according to vom Brocke et al. [26] and Webster and Watson [27], as well as the use of the established methodology for taxonomy development by Nickerson et al. [25], comprehensibility in the development is provided in a scientific manner. Future research results, such as additional compliance requirement patterns might, thus, be incorporated relatively easily in the presented taxonomy.

The application of the developed compliance process taxonomy was demonstrated by a simplified business example. It shows that the taxonomy is an easy to-use tool for practitioners and academics. The taxonomy can also be used to focus further research or to provide a starting point for further investigations, e.g. by adding economic values for efficiency and effectiveness to several characteristics and, thus, to choose an optimal compliance process instance [23]. Furthermore, the taxonomy might be a sound basis for constructive discussions of or selections between alternative compliance processes by considering different process or execution types that satisfy the same compliance requirements. Another scenario could be the definition of different recovery actions depending on controlled entities or results of deviation analyses to enforce runtime compliance (at least partly).

References

1. Fdhila, W., Rinderle-Ma, S., Knuplesch, D., Reichert, M.: Change and compliance in collaborative processes. In: 12th IEEE International Conference on Services Computing (SCC 2015), pp. 162–169 (2015)
2. Sadiq, S., Governatori, G., Namiri, K.: Modeling control objectives for business process compliance. In: Alonso, G., Dadam, P., Rosemann, M. (eds.) BPM 2007. LNCS, vol. 4714, pp. 149–164. Springer, Heidelberg (2007). doi:[10.1007/978-3-540-75183-0_12](https://doi.org/10.1007/978-3-540-75183-0_12)
3. Teubner, A., Feller, T.: Informationstechnologie, governance und compliance. *Wirtsch. Inform.* **50**, 400–407 (2008)
4. Schumm, D., Turetken, O., Kokash, N., Elgammal, A., Leymann, F., Heuvel, W.-J.: Business process compliance through reusable units of compliant processes. In: Daniel, F., Facca, F.M. (eds.) ICWE 2010. LNCS, vol. 6385, pp. 325–337. Springer, Heidelberg (2010). doi:[10.1007/978-3-642-16985-4_29](https://doi.org/10.1007/978-3-642-16985-4_29)
5. Turetken, O., Elgammal, A., van den Heuvel, W.-J., Papazoglou, M.: Enforcing compliance on business processes through the use of patterns. In: 19th ECIS 2011 (2011)
6. Bagban, K., Nebot, R.: Governance und compliance im cloud computing. *HMD* **51**, 267–283 (2014)
7. Wallace, L., Lin, H., Cefaratti, M.A.: Information security and sarbanes-oxley compliance: an exploratory study. *J. Inf. Syst.* **25**, 185–211 (2011)

8. Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control - Integrated Framework. Framework and Appendices (2012)
9. IT Governance Institute (ITGI): IT Control Objectives for Sarbanes-Oxley, 2nd Edn. (2006)
10. Beeck, V., Wischermann, B.: Kontrolle. <http://wirtschaftslexikon.gabler.de/Definition/kontrolle.html>
11. Pretschner, A., Massacci, F., Hilty, M.: Usage control in service-oriented architectures. In: Lambrinouidakis, C., Pernul, G., Tjoa, A.M. (eds.) TrustBus 2007. LNCS, vol. 4657, pp. 83–93. Springer, Heidelberg (2007). doi:[10.1007/978-3-540-74409-2_11](https://doi.org/10.1007/978-3-540-74409-2_11)
12. Turetken, O., Elgammal, A., van den Heuvel, W.-J., Papazoglou, M.P.: Capturing compliance requirements: a pattern-based approach. *IEEE Softw.* **29**, 28–36 (2012)
13. Schultz, M., Radloff, M.: Modeling concepts for internal controls in business processes – an empirically grounded extension of BPMN. In: Sadiq, S., Soffer, P., Völzer, H. (eds.) BPM 2014. LNCS, vol. 8659, pp. 184–199. Springer, Cham (2014). doi:[10.1007/978-3-319-10172-9_12](https://doi.org/10.1007/978-3-319-10172-9_12)
14. Kittel, K., Sackmann, S., Göser, K.: Flexibility and compliance in workflow systems: the KitCom prototype. In: CAiSE Forum - 25th International Conference on Advanced Information Systems Engineering, pp. 154–160 (2013)
15. Sackmann, S., Kittel, K.: Flexible workflows and compliance: a solvable contradiction?! In: vom Brocke, J., Schmiedel, T. (eds.) BPM - Driving Innovation in a Digital World. MP, pp. 247–258. Springer, Cham (2015). doi:[10.1007/978-3-319-14430-6_16](https://doi.org/10.1007/978-3-319-14430-6_16)
16. Kharbili, M., Medeiros, A., Stein, S., van der Aalst, W.M.P.: Business process compliance checking: current state and future challenges. In: MobIS (2008)
17. van der Aalst, W., van Hee, K., van der Werf, J.M., Kumar, A., Verdonk, M.: Conceptual model for online auditing. *Decis. Supp. Syst.* **50**, 636–647 (2011)
18. Schonenberg, M.H., Mans, R.S., Russell, N., Mulyar, N., van der Aalst, W.M.P.: Towards a taxonomy of process flexibility (extended version). BPM reports (2007)
19. Gehrke, N.: The ERP auditlab: a prototypical framework for evaluating enterprise resource planning system assurance. In: 43rd Hawaii International Conference on System Sciences (HICSS) (2010)
20. IT Governance Institute (ITGI): COBIT 4.1. Frameworks, Control Objectives, Management Guidelines, Maturity Models. Rolling Meadows (2007)
21. Riesner, M., Pernul, G.: Supporting compliance through enhancing internal control systems by conceptual business process security modeling. In: ACIS 2010 Proceedings (2010)
22. Seyffarth, T., Kühnel, S., Sackmann, S.: ConFlex: an ontology-based approach for the flexible integration of controls into business processes. In: Multikonferenz Wirtschaftsinformatik (MKWI) 2016, pp. 1341–1352 (2016)
23. Kühnel, S.: Toward a conceptual model for cost-effective business process compliance. In: Proceedings of the Informatik 2017. Lecture Notes in Informatics (LNI) (2017)
24. Panko, R.R.: Spreadsheets and Sarbanes-Oxley. Regulations, Risks, and Control Frameworks. Communications of the Association for Information Systems (2006)
25. Nickerson, R.C., Varshney, U., Muntermann, J.: A method for taxonomy development and its product service in information systems. *Eur. J. Inf. Syst.* **22**, 336–359 (2013)
26. Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A.: Reconstructing the giant: on the importance of rigour in documenting the literature search process. In: 17th European Conference on Information Systems, pp. 2206–2217 (2009)
27. Webster, J., Watson, R.T.: Analyzing the past to prepare for the future: writing a literature review. *MIS Quarterly* **26**, 12–24 (2002)
28. Gregor, S.: The nature of theory in information systems. *MIS Q.* **30**, 611–642 (2006)

29. The Institut der Wirtschaftsprüfer in Deutschland e.V. [Institute of Public Auditors in Germany, Incorporated Association] (IDW) (ed.): Principles of Proper Accounting When Using Information Technology. IDW AcP FAIT 1 (2002)
30. The Institut der Wirtschaftsprüfer in Deutschland e.V. [Institute of Public Auditors in Germany, Incorporated Association] (IDW) (ed.): The Audit of Financial Statements in an Information Technology Environment. IDW AuS 330 (2002)
31. Tilburg University (ed.): COMPAS. Compliance-driven Models, Languages, and Architectures for Services. <http://cordis.europa.eu/docs/projects/cnect/5/215175/080/deliverables/D2-1-State-of-the-art-for-compliance-languages.pdf>
32. German Federal Ministry of Justice and Consumer Protection: Federal Data Protection Act (2009)
33. Silic, M., Back, A., Silic, D.: Taxonomy of technological risks of open source software in the enterprise adoption context. *Inf. Comput. Secur.* **23**, 570–583 (2015)
34. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. *MIS Q.* **28**, 75–105 (2004)
35. Mwilu, O.S., Prat, N., Comyn-Wattiau, I.: Taxonomy development for complex emerging technologies. The case of business intelligence and analytics on the cloud. In: 19th Pacific Asia Conference on Information Systems (PACIS 2015), pp. 1–16 (2015)
36. Glaser, F., Bezenberger, L.: Beyond cryptocurrencies: a taxonomy of decentralized consensus systems. In: Proceedings of the ECIS (2015)
37. Namiri, K., Stojanovic, N.: Pattern-based design and validation of business process compliance. In: Meersman, R., Tari, Z. (eds.) OTM 2007. LNCS, vol. 4803, pp. 59–76. Springer, Heidelberg (2007). doi:[10.1007/978-3-540-76848-7_6](https://doi.org/10.1007/978-3-540-76848-7_6)
38. ISACA (ed.): COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA, Rolling Meadows (2012)
39. The Institute of Internal Auditors (IIA): SARBANES-OXLEY SECTION 404. A Guide for Management by Internal Controls Practitioners (2008)
40. The Institute of Internal Auditors (IIA): Global Technology Audit Guide (GTAG) 1. Information Technology Risk and Controls (2012)
41. The International Federation of Accountants (IFAC): ISA 315. Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment (2009)
42. Public Company Accounting Oversight Board (PCAOB): Auditing Standard No. 5. An Audit of Internal Control Over Financial Reporting That is Integrated with an Audit of Financial Statements (2007)
43. Weigand, H., van den Heuvel, W.-J., Hiel, M.: Business policy compliance in service-oriented systems. *Inf. Syst.* **36**, 791–807 (2011)
44. Ramezani, E., Fahland, D., Aalst, W.M.P.: Where did i misbehave? Diagnostic information in compliance checking. In: Barros, A., Gal, A., Kindler, E. (eds.) BPM 2012. LNCS, vol. 7481, pp. 262–278. Springer, Heidelberg (2012). doi:[10.1007/978-3-642-32885-5_21](https://doi.org/10.1007/978-3-642-32885-5_21)
45. Schäfer, T., Fettke, P., Loos, P.: Control patterns: bridging the gap between is controls and BPM. In: Proceedings of the 21st European Conference on Information Systems (ECIS), pp. 88–100 (2013)
46. Bellino, C., Wells, J., Hunt, S.: Auditing Application Controls. IIA, Altamonte Springs (2007)
47. German Federal Financial Supervisory Authority: Banking Act of the Federal Republic of Germany (Kreditwesengesetz, KWG). KWG (2016)
48. Pries-Heje, J., Baskerville, R., Venable, J.R.: Strategies for design science research evaluation. In: ECIS 2008 Proceedings (2008)

49. Sonnenberg, C., Brocke, J.: Evaluations in the science of the artificial – reconsidering the build-evaluate pattern in design science research. In: Peffers, K., Rothenberger, M., Kuechler, B. (eds.) DESRIST 2012. LNCS, vol. 7286, pp. 381–397. Springer, Heidelberg (2012). doi:[10.1007/978-3-642-29863-9_28](https://doi.org/10.1007/978-3-642-29863-9_28)
50. Tremblay, M.C., Hevner, A.R., Berndt, D.J.: Focus Groups for Artifact Refinement and Evaluation in Design Research. *Communications of the Association for Information Systems* 26 (2010)
51. Namiri, K.: *Model-Driven Management of Internal Controls for Business Process Compliance*. Karlsruhe (2008)
52. OMG (ed.): *Business Process Model and Notation (BPMN)*. <http://www.omg.org/spec/BPMN/2.0/PDF/>

Anlage C: Publikation „Business Process Compliance and Business Process Change“

Seyffarth, Tobias; Kühnel, Stephan; Sackmann, Stefan (2018): Business Process Compliance and Business Process Change. An Approach to Analyze the Interactions. In: Business Information Systems. BIS 2018. Lecture Notes in Business Information Processing (320), S. 176–189. DOI: 10.1007/978-3-319-93931-5_13.



Business Process Compliance and Business Process Change: An Approach to Analyze the Interactions

Tobias Seyffarth^(✉), Stephan Kuehnel, and Stefan Sackmann

Martin Luther University Halle-Wittenberg, 06108 Halle (Saale), Germany
{tobias.seyffarth, stephan.kuehnel,
stefan.sackmann}@wiwi.uni-halle.de

Abstract. The adherence of business process compliance (BPC) is crucial for many companies. In addition, business processes may be supported by IT components, which can also be affected by compliance requirements. Due to business process change and the avoidance of compliance violations, companies must analyze, among other things, the interactions between business process change and BPC. Following the design science research paradigm, we developed and prototypically implemented a method that is able to analyze interactions between BPC and business process change considering supporting IT components and compliance processes. The method takes the business process change patterns “replace” and “delete” into account.

Keywords: Business process compliance · Business process change
Compliance process · Information technology

1 Introduction

The adherence of compliance requirements resulting from the interpretation of laws, standards, or business contracts is crucial for many companies [1, 2]. The execution of business processes in accordance with their applicable compliance requirements is called business process compliance (BPC) [3]. Nevertheless, compliance requirements can affect both business processes and their supporting information technology (IT) [4–7]. However, many factors, such as new technologies, improvement of business processes, and outsourcing decisions can lead to business process changes, including changed IT components or compliance requirements [8, 9]. In dynamic markets, the fast detection of compliance violations and the adherence to the demands of compliance requirements to changed business processes and supporting IT components are necessary [10].

So far, an approach to determine the interactions between BPC and business process change considering supporting IT components automatically is lacking. Existing approaches only solve a small part of the problem. For example, in [11], a language to query business process models is presented. The presented software artifact in [8] automatically detects effects on business activities due to changed compliance requirements. In [12] an approach to model compliance requirements, business processes, and their

supporting IT components together is proposed. Consequently, we address the following research questions (RQ):

- RQ 1: *What are the interactions between BPC and business process change considering supporting IT components?*
- RQ 2: *How can these interactions be determined automatically?*

We address this research questions by developing two different artifacts. In this paper, we focus on their design and development according to the design science research paradigm by Hevner et al. [13]. The artifacts are each an exaptation that extends known solutions to new problems. Following the problem statement, the developed artifacts address a relevant problem and the required scientific rigor is fulfilled by the usage of existing methodologies. With the utilization of methodologies in the field of graph modeling and graph search (e.g. [14]) in addition to already existing software libraries for the development of our software prototype [15, 16], we present the following contributions:

- We propose a method that can analyze the interactions between BPC and business process change considering supporting IT components and compliance processes.
- We propose a prototypical implementation of our method. It uses models based on common standards such as the Business Process Model and Notation (process models), ArchiMate (IT architecture models), and laws that are provided as XML files by the German Federal Ministry of Justice (compliance requirements) [17–19].

This contribution is structured as follows: In Sect. 2, the backgrounds of business process compliance in conjunction with enterprise architecture and business process change patterns is briefly introduced. In Sect. 3, a running scenario is presented to illustrate the problem statement. In Sect. 4, a method that analyzes the interactions between BPC, supporting IT components and business process change is shown. In addition, the prototypical implementation of the method is presented. In Sect. 5 the related work is discussed. Finally, a brief conclusion and research outlook are provided in Sect. 6.

2 Theoretical Background

2.1 Business Process Compliance

As already mentioned, business process compliance (BPC) denotes the execution of business processes in adherence to applicable compliance requirements [3]. In this case, a compliance requirement is a constraint or assertion that results from the interpretation of compliance sources, such as laws, regulations or standards (e.g., [1, 2, 20]).

Various approaches check or ensure BPC. As an example, BPC can be checked after process execution by analyzing log files (e.g., [21]) or ensured at the design time of business processes. Here, a possible solution is the separate modeling of so-called compliance processes and its integration into business processes. Whenever a business process is affected by a compliance requirement, an appropriate compliance process can be integrated in the business process [1, 22]. In this context, a compliance process is

defined as an independent process (part) consisting of at least one compliance-related activity that ensures BPC [23].

2.2 Enterprise Architecture

An architecture is defined as the fundamental organization of a system embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution [24]. Following this, an enterprise architecture is understood as the fundamental organization of a government agency or a corporation, either as a whole or together with partners, suppliers and/or customers (“extended enterprise”), or in part (e.g., a division, a department, etc.) as well as the principles governing its design and evolution [25].

In the literature, various sub-architectures of enterprise architectures have been discussed. For example, Winter and Fischer [26] divided an enterprise architecture into a business, process, integration, software, and technology architecture. The Open Group split an enterprise architecture into the business, data, application and technology architecture [27]. Within business architecture, both Winter and Fischer [26] as well as the Open Group [27] have situated business processes. Within software/application and infrastructure architecture, the application services, application components or network devices as special hardware types are situated. For reasons of simplicity, we refer to a single element within an IT architecture as an IT component. In this paper, we do not distinguish between different types of IT components. Nevertheless, in the following we will focus on three perspectives of an enterprise architecture: (1) business process (2), compliance, and (3) IT architecture. The interrelations between the single elements of these perspectives are illustrated in Fig. 1.

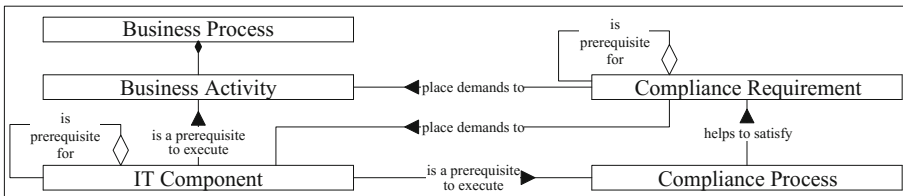


Fig. 1. Considered elements and their interrelations (based on [20, 23])

We focus on these perspectives for many reasons: The perspectives on business processes and compliance are considered because of the definition of BPC. As mentioned earlier, BPC denotes the execution of business processes in adherence to applicable compliance requirements [3]. Furthermore, we split the compliance perspective into the elements compliance requirement and the compliance process. As already mentioned, a compliance process operationalizes the compliance requirement that affects a single business activity [23]. Thus, the compliance process within a business process helps to satisfy the compliance requirement [22, 23]. We consider IT components as single elements within an IT architecture for three reasons. First, IT components are sometimes necessary to execute a business activity. Second, within an automatic

compliance process, IT components are also necessary for the proper execution of automatic compliance processes [23]. Third, both business processes and also IT components are affected by numerous compliance requirements. For example, COSO [7] and the Institute of Public Auditors in Germany [6] provide a lot of requirements for the proper operation of IT components.

2.3 Business Process Change Patterns

In addition to many sub-architectures of an enterprise architecture, various business process change patterns have been discussed, as well. For example, Weber et al. [28] distinguished 18 change patterns and split them into adaption patterns and patterns of change in predefined regions of business processes. As shown in Fig. 2, further authors have combined the proposed 18 changed patterns to four change patterns: “insert element”, “delete element”, “replace element” and “update element” [29, 30].

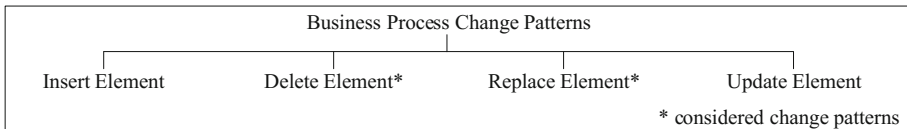


Fig. 2. Business process change patterns (based on [29, 30])

The insert change pattern inserts a new element into the business process at a defined place. The delete pattern removes an existing element. The replace pattern replaces an existing element with a new one. The update pattern modifies an attribute of an existing element [30].

These change patterns can also be applied to our perspectives on enterprise architecture. Therefore, we assume that IT components, compliance requirements, and compliance processes are additional views of a business process that are similar to for example, a data view. Due to space limitations, we will only apply the change patterns “delete element” and “replace element”. Next, we discuss a running scenario to motivate our research problem and to demonstrate the solution through our method.

3 Running Scenario

The left side of Fig. 3 shows a simplified purchase to pay process based on [31, 32], including perspectives on compliance requirements, compliance processes, and IT components. Some of the business activities are supported by IT components that are modeled as triangles.

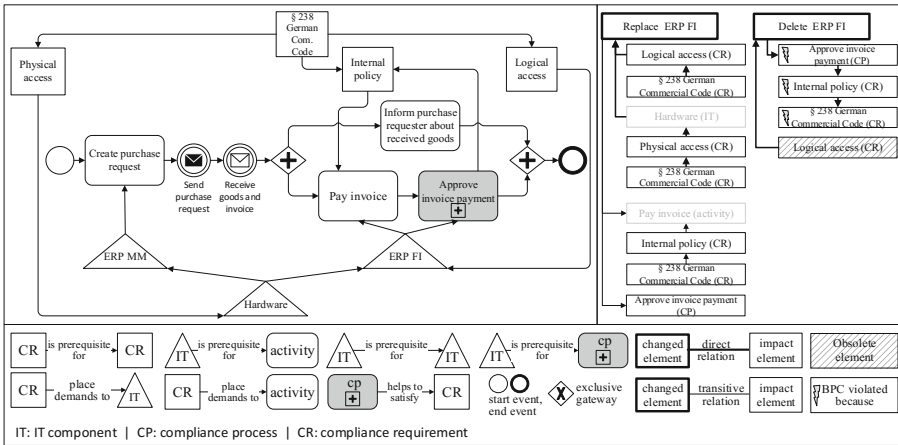


Fig. 3. Running scenario (based on [31, 32])

We assume that the material management module of an enterprise resource planning system (ERP MM) is a prerequisite to creating a purchase request. Furthermore, a financial module of an ERP system (ERP FI) is a prerequisite for both the compliance process “approve invoice payment” and the business activity “pay invoice”.

In addition to that, both business activities and IT components are sometimes affected by compliance requirements. In this example, “§ 238 of the German Commercial Code” demands the accounting obligation for merchants in Germany. It is also related to the proper operation of IT that supports the accounting activities. In this example, the compliance requirements “physical access” and “logical access” are prerequisite by “§ 238 of the German Commercial Code”. The compliance requirement “physical access” requires a regulated access to physical IT components while “logical access” requires the identification and authentication of users of an application [33]. Furthermore, the compliance requirement “internal policy” specifies additional requirements that are necessary for the payment of invoices. The compliance process “approve invoice payment” helps to satisfy the “internal policy”.

The right side of Fig. 3 shows (1) the compliance requirements that shall be taken into consideration when replacing the IT component “ERP FI” and (2) the effects on BPC by deleting “ERP FI”. The edge direction corresponds to that of the model on the left side. Our method and prototypical implementation can automatically calculate these interactions considering the business process change patterns “replace element” and “delete element”.

In the case of replacing “ERP FI”, there are two compliance requirements that place direct demands to them. In addition to the compliance requirement “logical access”, the “physical access” compliance requirement must also be taken into account. Furthermore, there is a transitive relation by “internal policy” and “§ 238 of the German Commercial Code”. The IT component “ERP FI” is a prerequisite for the business activity “pay invoice” which is affected by the “internal policy” which is, in turn, the “§ 238 of the German Commercial Code” is the prerequisite of the “internal policy”.

In the case of deleting “ERP FI” the compliance process “approve invoice payment” cannot be executed. Thus, the compliance requirements “internal policy” and “§ 238 of the German Commercial Code” are violated. Furthermore, the compliance requirement “logical access” is obsolete. In the next section, we propose a method and its prototypical implementation for analyzing the interactions between BPC and business process change considering supporting IT components and compliance processes.

4 Interaction Between BPC and Business Process Change

Figure 4 shows the three steps of our method for analyzing the interactions of BPC and business process change. First, business process, compliance process, IT architecture, and compliance requirements must be imported into the software prototype. Second, the imported models must be transformed and integrated into a single graph. Third, the interactions of BPC and business process change must be analyzed. In the following sections, we explain each step in detail with respect to the running scenario introduced in the previous section.

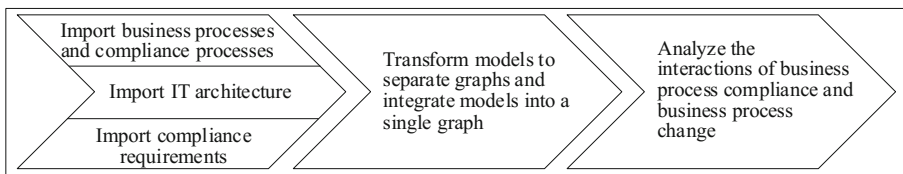


Fig. 4. Steps to analyze the interactions of BPC and business process change

4.1 Import Models

All above mentioned model types must be available as formal models for an import into our prototype. We used the process modeling language Business Process Model and Notation (BPMN) as the import format for both business and compliance process models, which offers various XML schemas for the process model description [17]. The modeling language ArchiMate [18] was used as the import format for IT architectures for two reasons. First, it provides a formal data exchange format [27]. Second, ArchiMate is a promising approach to model an enterprise architecture on the bottom of the BPMN process models [34]. Finally, we used several German laws, which were provided as XML files by the German Federal Ministry of Justice [19] as an import format for compliance requirements.

Our prototype was developed in Java. For the deserialization of the BPMN process according to the XML schemas proposed by the OMG [17], we used the Java library “Camunda BPMN model API” [15]. It allows the deserialization of each element within the process model into a single Java object. For the deserialization of the IT architecture and compliance requirements we each developed a XML wrapper.

4.2 From Separate Models to an Integrated Graph

We adapted graph search methods (e.g., [14]) to analyze the interaction of BPC and business process change considering supporting IT components and compliance processes. In order to formalize this concept, a number of auxiliary concepts must be introduced. We define a non-empty finite set of directed and labeled multigraphs $G = (V, E, F, H, I)$ with its elements $g_i \in G$. In addition, V is a nonempty finite set of vertices, $e_l \in E$ is a set of directed edges between two vertices (v_i, v_j) and $f_i \in F$ is the unique identification (id) of the vertex v_i . In addition, $h_i \in H$ is the model type of the vertex v_i with $H = \{BP, CP, IT, CR\}$, which corresponds to the imported model types business process (BP), compliance process (CP), IT architecture (IT) or compliance requirement (CR). Finally, $i_l \in I$ is the label of edge e_l .

The transformation of the previously imported models to an integrated graph consists of two major steps. First, each imported model is transformed into a graph g_i and added to the graph set G . The transformation of the imported models works as follows: Within business and compliance processes the “Camunda BPMN model API” [15] allows the extraction of the lists of all flow nodes and sequence flows of a process model. Based on the list of flow nodes it is possible to create a vertex $v_{i,n}$ for each flow node. Therefore, each vertex id $f_{i,n}$ is equal to the id of the flow nodes within the process models. The model type $h_{i,n}$ of each vertex is either a business process or compliance process. The list of sequence flows contains the predecessor and successor relations of all flow nodes. Based on this predecessor and successor relations, the appropriate edges e_l between the vertices can be created. The respective edge labels i_l are equal to the edge labels connecting different model types in the legend of Fig. 3. Similarly to business and compliance process models, the imported IT architecture also contains a list of IT components and a list of relations that describes the IT component predecessor and successor relations. Therefore, the graph of the IT architecture can be generated similarly to the graph of a process model. Finally, each compliance requirement and its corresponding compliance source are represented by two vertices that are connected by an edge.

Second, the generated graphs must be integrated into a single graph. Therefore, an empty graph is generated and all previously generated graphs within the graph collection G are added to it. Then, the required edges between the vertices of the business process model, compliance process model, IT components, and compliance requirements must be created manually. However, the edges that are connected to a process model can also be modeled automatically. Whenever a flow node of a business or compliance process is the target vertex of a compliance requirement or an IT component, additional meta-information is added to the respective flow node. This is done by using the BPMN class extension element [17]. The extension is a list of key-value-pairs. Thereby, the keys represent the referenced model types h_i and the values their respective id f_i . Thus, the edges that touch a business or compliance process can also be modelled automatically. This is always possible when the business or compliance process contains an aforementioned BPMN extension element.

Within our software prototype, we used the Java library “JGraphT” [16] to model and visualize graphs. In the next step, the integrated graph is used as a basis for analyzing the interactions between BPC and business process change.

4.3 Analyzing the Interactions Between BPC and Business Process Change

By taking the business process change patterns “replace element” and “delete element” into consideration, their semantic interpretation to the business process model considering IT components, compliance processes, and compliance requirements must be defined. When replacing an element, the replaced elements are sometimes affected by compliance requirements (see replace “ERP FI” within the running scenario). Thus, the new element must take these respective compliance requirements into consideration to ensure BPC. The removal of an element can also have an impact on BPC (see remove “ERP FI” within the running scenario). First, it can have an impact on compliance requirements and/or compliance processes that satisfy the impacted compliance requirements. Second, due to a removal of an element, the respective compliance requirements can become obsolete. In the following, we describe our algorithm to analyze the interactions between BPC and business process change. Due to space limitations, we will refer to an IT component as the replaced or deleted element.

Replacing an Element

Figure 5 shows the algorithm to analyze the relations of compliance requirements and compliance processes to the IT component that shall be replaced. To ensure BPC, the replaced element must fulfill the related compliance requirements and be able to execute a related compliance process. Thereby, we distinguish between direct and transitive relations.

<pre> Input: Graph <i>g</i>, element that shall be replaced $v \in g$ where $h(v)=it$ architecture 1 // get all direct related compliance requirements and compliance processes to <i>v</i> 2 ForEach <i>i</i> in (get all predecessor of <i>v</i> where $h=$compliance requirement or $h=$compliance process) do 3 mark <i>i</i> as direct AND add <i>i</i> including all vertices between <i>i</i> und <i>v</i> to <i>result</i> 4 // get all transitive related compliance processes and compliance requirements to <i>v</i> 5 ForEach <i>it</i> in (get all leafs of <i>v</i> where $h=it$ architecture) do 6 ForEach <i>activity</i> in (get all direct successor of <i>it</i> where $h=$business process) do 7 ForEach <i>cr</i> in (get all direct predecessor of <i>activity</i> where $h=$compliance requirement) do 8 <i>i</i> = get all predecessor of <i>cr</i> 9 mark <i>it</i>, <i>activity</i>, <i>cr</i> and <i>i</i> as transitive AND add to <i>result</i> 10 ForEach <i>complianceprocess</i> in (get all direct successor of <i>it</i> where $h=$compliance process) do 11 ForEach <i>cr</i> in (get all direct successor of <i>complianceprocess</i> where $h=$compliance requirement) do 12 <i>i</i> = get all predecessor of <i>cr</i> 13 mark <i>it</i>, <i>complianceprocess</i>, <i>cr</i> and <i>i</i> as transitive AND add to <i>result</i> 14 generate <i>result_graph</i> based on <i>g</i> and <i>result</i> Output: Graph <i>result_graph</i> </pre>
--

Fig. 5. Algorithm to analyze interactions by replacing an IT component

A direct relation between compliance requirements and a replaced IT component occurs in two different ways. First, each compliance requirement that is directly related to the replaced IT component must be considered. Within our running scenario the compliance requirement “logical access” is directly related to the replaced IT component “ERP FI”. Consequently, the compliance requirement “§ 238 of the German Commercial Code” is also directly related, because it is a prerequisite for “logical access”.

Second, all compliance requirements of the replaced element prerequisites must be taken into consideration, as well. Within the running scenario, the compliance requirement “Physical access” is direct related to the replaced element “ERP FI” because it is a prerequisite for the IT component “hardware”, which is, in turn a prerequisite for “ERP FI”.

A transitive relation between an updated IT component and a compliance requirement or a compliance process also occurs in two different cases. First, the changed IT component is a prerequisite of a business activity that is affected by at least one compliance requirement. Second, the updated IT component is a prerequisite of a compliance process that helps to satisfy at least one compliance requirement. Within the running scenario, this is the case at the business activity “pay invoice” and its prerequisite compliance requirements “internal policy” and “§ 238 of the German Commercial Code”.

Deleting an Element

Figure 6 shows the algorithm to analyze the impacts on BPC by removing an IT component. Here, we distinguish between two different impacts. First, the removal an IT component can lead to a compliance process not being executable. This concerns the compliance process “approve invoice payment”, since the IT component “ERP FI” is a prerequisite for its execution. Consequently, the compliance requirements “internal policy” and “§ 238 of the German Commercial Code” are violated.

<pre> Input: Graph g, element that shall be removed v ∈ g where h(v)=it architecture 1 // get all violated compliance requirements 2 Foreach it in (get all leaves of v where h=it architecture) do 3 Foreach complianceprocess in (get all direct successor of it where h=compliance process) do 4 Foreach cr in (get all direct successor of complianceprocess where h=compliance requirement) do 5 i = get all predecessor of cr 6 mark cr and i as violated AND add cr and i to result 7 // get all obsolete compliance requirements 8 add v to list_it 9 Foreach it in (get all successor of v where h=it architecture) do 10 If (it only requires v) 11 add it to list_it 12 Foreach it in (list_it) do 13 Foreach cr in (get all direct predecessor of it where h=compliance requirement) do 14 If (get all direct successor of cr=it) 15 mark cr as obsolete AND add cr to result 16 Foreach cr2 in (get all predecessor of cr where h=compliance requirement) do 17 If (cr2 hasn't other direct successor than get all predecessor of cr where h=comp.req.) 18 mark cr2 as obsolete AND add cr2 to result 19 generate result_graph based on g and result Output: Graph result_graph </pre>

Fig. 6. Algorithm to analyze interactions by deleting an IT component

Second, the removal of an IT component can may cause a compliance requirement to become obsolete within the respective model. This concerns the compliance requirement “logical access”. It only affects the removed IT component “ERP FI”. Nevertheless, its prerequisite compliance requirement “§ 238 of the German Commercial Code” does not become obsolete. It is already a prerequisite for the compliance requirements “physical access” and “internal policy”.

5 Related Work

We conducted a structured literature review according to vom Brocke et al. [35] to retrieve the related work. As proper databases we used AISel, IEEE, SpringerLink as well as the EbscoHost libraries “Science & Technology Abstracts”, “Business Source Premier” and “Academic Source Premier”. With respect to our research question, we defined the following abstract query: << (“business process compliance” OR BPC) AND (“information technology” OR flexibility OR query OR change)>>. Furthermore we performed a backward search according to Webster and Watson [36]. These searches identified a total of 552 unique hits. After analyzing the articles abstract, keywords and full text, if necessary, we excluded 519 articles. In total, 33 articles were read in full.

Finally, the articles can be classified into two main topics. There are articles that discuss (1) querying of business processes and (2) the linkage and (partly) the querying of the considered enterprise architecture perspectives on business processes, compliance, and IT architecture. Nevertheless, none of the proposed approaches analyzed the interaction between BPC and business process change, considering IT components or compliance processes. Due to space limitations, we will highlight the main ideas of the selected approaches.

Awad [11] proposed a visual language called BPMN-Q to query BPMN process models. Delfmann et al. [37] developed a generic model query language (GMQL). GMQL is able to express pattern queries for all graph-based modelling languages by treating the modeling language as an attributed graph. In addition to structural aspects of graph matching, Gacitua-Decar and Pahl [38] proposed an approach to identify patterns in business processes based on structural and semantic aspects. Fellmann et al. [39] transformed a business process model into an ontology and enriched the ontology instance with structural and domain representation information; they queried business processes by using SPARQL queries within the ontology.

Several authors have proposed approaches to link compliance requirements with business processes, such as Ghanavati et al. [40]. Rudzajs and Buksa [8] developed an approach to detect changes in compliance requirements by storing them into a version control system. Thus, it is able to detect the business activities affected by the changed compliance requirements. Furthermore, both Fdhila et al. [41] and Knuplesch et al. [42] analyzed the possible effects on both compliance requirements and business processes in the context of collaborative business processes.

Only a few authors have discussed the link between compliance requirements and IT components, such as Knackstedt et al. [5]. Furthermore, Knackstedt et al. [43] extended their previous work by developing a software prototype that models and shows the link between compliance requirements and IT components.

In addition, only a few authors have discussed the linkage between different compliance requirements. Independently of each other, Elgammal et al. [44] and Halle [45] presented approaches to detect root cause violations in rules that are formalized in linear temporal logic.

Furthermore, Koetter et al. [12, 46] presented an approach to link compliance requirements to both business processes and IT components. They used so-called compliance descriptors to formalize compliance requirements for business processes

and IT components. The formalized compliance requirements allow the determination of the interrelation between business processes or IT components and compliance requirements.

6 Conclusion and Outlook

New technologies, improvement of business processes, and outsourcing decisions can lead to changing business processes, IT components, or compliance requirements [8, 9]. Therefore, the fast detection of compliance violations and the adherence to demands of compliance requirements to changed business processes and IT components are necessary [10]. To solve that challenge, we proposed a method to analyze the interactions between BPC and business process change considering IT components and compliance processes. Hence, we focused on the perspectives business processes, compliance processes, compliance requirements, and IT components of an enterprise architecture. Furthermore, we took the business process change patterns “replace element” and “delete element” into consideration. On the one hand, a replaced element can be affected directly or transitive by compliance requirements. On the other hand, the removal of an element can lead to a violation or an irrelevance of compliance requirements. In addition, a prototype implementation of the method was shown. The prototype is based on well-established libraries for handling BPMN and graphs in Java [15, 16].

In the first step, we only considered the aforementioned perspectives of an enterprise architecture. Unquestionably, there are more perspectives, such as data or an organizational perspective (e.g., [26, 27]). Apart from that, there are also more preconditions than the existence of IT components, e.g., data or organizational units, to execute a compliance process [23]. Thus, we plan to extend our graph search algorithm and its demonstration to other perspectives of an enterprise architecture. In addition, the applicability of the proposed method will be evaluated. Another open research question is the adaption of a business process in case a compliance process is not executable. In this case, the integration of an alternative compliance process seems to be a promising approach to ensure BPC despite a business process change. Furthermore, we plan to extend our prototype for an automatic integration of alternative compliance processes.

References

1. Schumm, D., Turetken, O., Kokash, N., Elgammal, A., Leymann, F., van den Heuvel, W.-J.: Business process compliance through reusable units of compliant processes. In: Daniel, F., Facca, F.M. (eds.) ICWE 2010. LNCS, vol. 6385, pp. 325–337. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-16985-4_29
2. Turetken, O., Elgammal, A., van den Heuvel, W.-J., Papazoglou, M.: Enforcing compliance on business processes through the use of patterns. In: 19th ECIS 2011 (2011)
3. Schäfer, T., Fettke, P., Loos, P.: Towards an integration of GRC and BPM – requirements changes for compliance management caused by externally induced complexity drivers. In: Daniel, F., Barkaoui, K., Dustdar, S. (eds.) BPM 2011. LNBIP, vol. 100, pp. 344–355. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-28115-0_33

4. Sadiq, S., Governatori, G., Namiri, K.: Modeling control objectives for business process compliance. In: Alonso, G., Dadam, P., Rosemann, M. (eds.) BPM 2007. LNCS, vol. 4714, pp. 149–164. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-75183-0_12
5. Knackstedt, R., Eggert, M., Heddier, M., Chasin, F., Becker, J.: The relationship of is and law - the perspective of and implications for IS research. In: ECIS 2013 Completed Research (2013)
6. The Audit of Financial Statements in an Information Technology Environment. IDW AuS 330 (2002)
7. Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control - Integrated Framework. Framework and Appendices (2012)
8. Rudzajs, P., Buksa, I.: Business process and regulations: approach to linkage and change management. In: Grabis, J., Kirikova, M. (eds.) BIR 2011. LNBIP, vol. 90, pp. 96–109. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24511-4_8
9. Fdhila, W., Indiono, C., Rinderle-Ma, S., Reichert, M.: Dealing with change in process choreographies: design and implementation of propagation algorithms. *Inf. Syst.* **49**, 1–24 (2015)
10. Rinderle, S., Reichert, M., Dadam, P.: Correctness criteria for dynamic changes in workflow systems—a survey. *Data Knowl. Eng.* **50**, 9–34 (2004)
11. Awad, A.: BPMN-Q: a language to query business processes. In: Proceedings of EMISA 2007, pp. 115–128 (2007)
12. Koetter, F., Kochanowski, M., Weisbecker, A., Fehling, C., Leymann, F.: Integrating compliance requirements across business and IT. In: 2014 IEEE 18th International Enterprise Distributed Object Computing Conference (2014)
13. Hevner, A.R., Gregor, S.: Positioning and presenting design science research for maximum impact. *MIS Q.* **37** (2013)
14. Yu, P.S., Han, J., Faloutsos, C. (eds.): Link Mining: Models, Algorithms, and Applications. Springer Science + Business Media LLC, New York (2010). <https://doi.org/10.1007/978-1-4419-6515-8>
15. Camunda: Camunda BPMN model API. <https://github.com/camunda/camunda-bpmn-model>
16. Naveh, B.: JGraphT. <http://jgraph.org/>
17. OMG (Hg): Business Process Model and Notation (BPMN). <http://www.omg.org/spec/BPMN/2.0/PDF/>
18. Jonkers, H., Lankhorst, M., van Buuren, R., Hoppenbrouwers, S., Bonsangue, M., van der Torre, L.: Concepts for modeling enterprise architectures. *Int. J. Coop. Inf. Syst.* **13**, 257–287 (2004)
19. Juris (ed.): Gesetze im Internet. <http://www.gesetze-im-internet.de>
20. Seyffarth, T., Kühnel, S., Sackmann, S.: ConFlex: an ontology-based approach for the flexible integration of controls into business processes. *Multikonferenz Wirtschaftsinformatik (MKWI) 2016*, 1341–1352 (2016)
21. Kharbili, M., Medeiros, A.K.A.d., Stein, S., van der Aalst, W.M.P.: Business process compliance checking: current state and future challenges. *MobIS* **141**, 107–113 (2008)
22. Sackmann, S., Kittel, K.: Flexible workflows and compliance: a solvable contradiction?! In: Vom Brocke, J., Schmiedel, T. (eds.) BPM - Driving Innovation in a Digital World, pp. 247–258. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-14430-6_16
23. Seyffarth, T., Kühnel, S., Sackmann, S.: A taxonomy of compliance processes for business process compliance. In: Carmona, J., Engels, G., Kumar, A. (eds.) BPM 2017. LNBIP, vol. 297, pp. 71–87. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-65015-9_5
24. IEEE: IEEE Recommended Practice for Architectural Description of Software Intensive Systems, (IEEE Std 1 1471–2000). IEEE Computer Society, New York (2000)

25. TOGAF (ed.): Content Metamodel. Content Metamodel Vision and Concepts. <http://pubs.opengroup.org/architecture/togaf9-doc/arch/>
26. Winter, R., Fischer, R.: Essential layers, artifacts, and dependencies of enterprise architecture. In: 2006 10th IEEE International Enterprise Distributed Computing Conference Workshops (EDOCW 2006), p. 30 (2006)
27. The Open Group (ed.): TOGAF 9.1. Content Meta Model. <http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap34.html>
28. Weber, B., Reichert, M., Rinderle-Ma, S.: Change patterns and change support features – enhancing flexibility in process-aware information systems. *Data Knowl. Eng.* **66**, 438–466 (2008)
29. Rinderle-Ma, S., Reichert, M., Weber, B.: On the formal semantics of change patterns in process-aware information systems. In: Li, Q., Spaccapietra, S., Yu, E., Olivé, A. (eds.) ER 2008. LNCS, vol. 5231, pp. 279–293. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-87877-3_21
30. Fdhila, W., Rinderle-Ma, S., Reichert, M.: Change propagation in collaborative processes scenarios. In: 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom) (2012)
31. Namiri, K.: Model-Driven Management of Internal Controls for Business Process Compliance. Karlsruhe (2008)
32. Frank, U., Heise, D., Ulrich, Kattenstroth, H., Ferguson, D.F., Hadar, E., Waschke, M.G.: ITML: a domain-specific modeling language for supporting business driven IT management. In: Proceedings of the 9th OOPSLA Workshop on Domain-Specific Modeling (2009)
33. Principles of Proper Accounting When Using Information Technology. IDW AcP FAIT 1 (2002)
34. Kirikova, M., Penicina, L., Gaidukovs, A.: Ontology based linkage between enterprise architecture, processes, and time. *Commun. Comput. Inf. Sci.* **539**, 382–391 (2015)
35. Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A.: Reconstructing the giant: on the importance of rigour in documenting the literature search process. In: 17th European Conference on Information Systems, pp. 2206–2217 (2009)
36. Webster, J., Watson, R.T.: Analyzing the past to prepare for the future: writing a literature review. *MIS Q.* **26**, xiii–xxiii (2002)
37. Delfmann, P., Steinhorst, M., Dietrich, H.-A., Becker, J.: The generic model query language GMQL – conceptual specification, implementation, and runtime evaluation. *Inf. Syst.* **47**, 129–177 (2015)
38. Gacitua-Decar, V., Pahl, C.: Automatic business process pattern matching for enterprise services design. In: 2009 World Conference on Services - II (2009)
39. Fellmann, M., Thomas, O., Busch, B.: A query-driven approach for checking the semantic correctness of ontology-based process representations. In: Abramowicz, W. (ed.) BIS 2011. LNBIP, vol. 87, pp. 62–73. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21863-7_6
40. Ghanavati, S., Amyot, D., Peyton, L.: Compliance analysis based on a goal-oriented requirement language evaluation methodology. In: 2009 17th IEEE International Requirements Engineering Conference (2009)
41. Fdhila, W., Rinderle-Ma, S., Knuplesch, D., Reichert, M.: Change and compliance in collaborative processes. In: 2015 IEEE International Conference on Services Computing (2015)

42. Knuplesch, D., Fdhila, W., Reichert, M., Rinderle-Ma, S.: Detecting the effects of changes on the compliance of cross-organizational business processes. In: Johannesson, P., Lee, M.L., Liddle, Stephen W., Opdahl, Andreas L., López, Ó.P. (eds.) ER 2015. LNCS, vol. 9381, pp. 94–107. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-25264-3_7
43. Knackstedt, R., Braeuer, S., Heddier, M., Becker, J.: Integrating regulatory requirements into information systems design and implementation. In: ICIS 2014 Proceedings (2014)
44. 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, Paul P., Weske, M., Yang, J., Fantinato, M. (eds.) ICISOC 2010. LNCS, vol. 6470, pp. 17–31. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17358-5_2
45. Halle, S.: Causality in message-based contract violations. a temporal logic “Whodunit”. In: 2011 IEEE 15th International Enterprise Distributed Object Computing Conference (2011)
46. Koetter, F., et al.: An universal approach for compliance management using compliance descriptors. In: Helfert, M., Ferguson, D., Méndez Muñoz, V., Cardoso, J. (eds.) CLOSER 2016. CCIS, vol. 740, pp. 209–231. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-62594-2_11

Anlage D: Publikation „Business Process Compliance despite Change“

Seyffarth, Tobias; Kühnel, Stephan; Sackmann, Stefan (2019): Business Process Compliance despite Change. Towards Proposals for a Business Process Adaption. In: Information Systems Engineering in Responsible Information Systems. CAiSE 2019. Lecture Notes in Business Information Processing, vol 350., S. 227–239. DOI: 10.1007/978-3-030-21297-1_20.



Business Process Compliance Despite Change: Towards Proposals for a Business Process Adaptation

Tobias Seyffarth^(✉), Stephan Kuehnel, and Stefan Sackmann

Martin Luther University Halle-Wittenberg, 06108 Halle (Saale), Germany
{tobias.seyffarth, stephan.kuehnel,
stefan.sackmann}@wiwi.uni-halle.de

Abstract. Business Process Compliance (BPC) denotes the execution of business processes in accordance with applicable compliance requirements. BPC can be satisfied through compliance processes that are integrated into the business process. In addition, compliance requirements place demands against IT components that are sometimes necessary to execute business or compliance processes. Various factors, such as outsourcing or business process reengineering can lead to a change of processes or IT components and thus to a violation of BPC. Consequently, our goal is to provide proposals for a business process adaptation to further ensure BPC. Following the design science research methodology, we developed two artifacts to reach our goal. First, we developed a meta-model that represents the interrelations between alternative compliance process patterns and compliance processes that satisfy the same compliance requirement. Second, we developed a method to automatically put forward proposals for a business process adaptation through the integration of alternative compliance processes to further ensure BPC.

Keywords: Adaptation · Business process compliance · Change · Compliance process · IT component

1 Introduction

Business Process Compliance (BPC) denotes the execution of business processes in accordance with applicable compliance requirements [1]. A compliance requirement is a constraint or assertion that prescribes a desired result or purpose to be achieved by factoring actions or control procedures into processes [2]. In addition to business processes, compliance requirements place demands to components of an information technology (IT) architecture (e.g. software such as a ERP system or hardware such as a physical server) [3]. Further, IT components are sometimes necessary to execute activities of a business process. Thus, there are multilevel interrelations between compliance requirements, business activities, and IT components.

Many factors such as outsourcing decisions, business process reengineering, and new technologies can lead to changing compliance requirements, business activities, or IT components [4, 5]. In dynamic markets the fast adaptation to changing environments is key [6]. Consequently, the fast detection of BPC violations through changes and the

adaptation of business processes to avoid BPC violations are both important tasks [7]. However, this might be a challenging and time consuming manual task due to many compliance requirements, business process models, and large IT architectures [8].

In the literature various approaches exist to identify impacts on BPC through the respective changes in business processes [4, 5], IT components [3, 9] and even a common change of business processes and IT components [10]. Additionally, there are approaches for an adaptation of business processes to satisfy compliance requirements regarding the control flow of the business process and thus ensuring BPC [11, 12]. Nevertheless, these approaches do not consider IT components for the execution of business activities. So far, there is a lack of an approach to ensure BPC during the design time of business processes despite changes to business processes and IT components. Additionally, to the best of our knowledge, there is no decision support system for the adaptation of business processes to avoid violations of BPC. Thus, we address the following research question: *How can proposals be provided for an adaptation of the business process to further ensure BPC?*

We address this research question by designing and developing two artifacts according to the design science paradigm by Hevner et al. [13]. In this paper we focus on their design and development. The artifacts are each an exaptation that extends known solutions to new problems. Following the problem statement, the developed artifacts address a relevant problem and the required scientific rigor is fulfilled by the usage of existing methodologies of graph search techniques. Finally, we present the following contributions:

- First, we present a meta-model to model alternative compliance processes and their interrelation.
- Second, we present a method to automatically put forward proposals for a business process adaptation through the integration of alternative compliance processes to further ensure BPC.

The remainder of this contribution is structured as follows: In Sect. 2, the preliminaries background of BPC in combination with relevant views on an enterprise architecture, and a motivation scenario are discussed. In Sect. 3, we present a method to put forward proposals for a business process adaptation. In Sect. 4, the related work is discussed and finally, Sect. 5 concludes the contribution.

2 Preliminaries and Motivation Scenario

2.1 Business Process Compliance

As already mentioned, business process compliance (BPC) denotes the execution of business processes in adherence to applicable compliance requirements [1]. In this case, a compliance requirement is a constraint or assertion that results from the interpretation of compliance sources, such as laws, regulations, and standards (e.g. [2]). Various approaches check or ensure BPC. As an example, BPC can be checked after process execution by analyzing log files, or it can be ensured at the time the business processes are designed (e.g., [14]).

In a narrow sense, a business process is simply a sequence of work items (also referred to as business activities). These processes transform one or more kinds of input into output and are aimed at generating value [15]. However, ensuring compliance requires activities that are not merely geared toward pure value generation, but to also meet compliance requirements. The so-called compliance activities are appended to the business process, e.g. at design time or as part of a process redesign [16]. The simple combination of both business and compliance activities increases process complexity and reduces process transparency [17]. For example, with an increasing number of activities in a process model, it becomes increasingly difficult to differentiate between those activities that serve to generate value and thus serve the core business and those that ensure compliance. A promising way to address this difficulty is to separate the view of business and compliance activities or activity sequences [17]. Similar to modular software design, a process graph can thus be built modularly so that it can be separated into exchangeable, functional components [18], i.e., process fragments that serve business goals and those that serve compliance goals (e.g. [19]). Accordingly, we provide the following formal definition of a process graph.

Definition 1 (Process Graph). A process graph G is a 3-tuple $G = (N, E, \text{type})$ [20], where: $N = BA \cup CA \cup C$ is a set of nodes in G , that follow common execution semantics. BA is a set of business activities and CA is a set of compliance activities, where: $BA \cup CA = \emptyset$. C is a set of coordinating nodes and $E \subseteq N \times N$ is a set of edges between nodes representing a control flow such that (N, E) is a connected process graph. The function $\text{type} : C \rightarrow \{\text{start, end, split, synchronize, choice, merge}\}$ assigns a coordinator type to each coordinating node of G .

A major advantage of a modular process structure is the potential for reusing compliance processes or compliant process fragments to meet compliance requirements in other business processes [12]. In addition, adherence to compliance requirements can be automated and made more flexible through the tool-supported integration of compliance processes into workflows at runtime as shown in [16, 21]. Thus, we define a compliance process as an independent process (part) consisting of compliance-related activities that ensure BPC [22].

Definition 2 (Compliance Process). A compliance process is a subgraph of G and a 3-tuple $CP = (N', E', \text{type}')$ if $N' \subseteq CA \cup C$, $E' \subseteq E$ and $\text{type}' = \text{type}|_{N'}$. type' restricts the function type of G to the set of N' . A compliance fragment CF is a special type of CP with exactly one input and one output node, i.e. CF does not contain coordination nodes of type $\{\text{start, end}\}$. Given the business activity $BA_i \in BA$ of process graph G , $\text{Trigger}(G, BA_i)$ denotes the compliance process(es) triggered by BA_i .

Although business and compliance objectives seem to sometimes overlap in practice, they can usually be treated and modelled separately, if there is a compliance view of processes (e.g., [12, 17]). A compliance view of processes includes, among other things, the knowledge of relevant compliance requirements that place demands against these process or their single activities [10]. An example is the credit rating before granting a loan.

On the one hand, credit institutions inquire into credit ratings to protect against payment defaults; on the other hand, compliance requirements such as the German

Banking Act stipulate obligations to check creditworthiness. However, the protection against payment defaults is not used to generate value, but to maintain value. Thus, it does not belong to the core business process. A credit rating always pursues a compliance objective, either based on a statutory provision or on an internal need for protection (internal compliance requirement). The credit rating would thus have to be operationalized as a compliance process. Consequently, the idea of modularization is based on the assumption that the amount of business and compliance activities are disjoint, i.e. that an activity meets either a business or a compliance objective.

If the pursuit of a compliance goal only serves value generation, compliance and business activities are difficult to distinguish. This might be the case when complying with requirements constitutes the unique selling proposition of a product or service. However, our approach is limited to cases where modularization is possible.

2.2 Views on Enterprise Architectures

An enterprise architecture is understood as the fundamental organization of a government agency or corporation, either as a whole or together with partners, suppliers and/or customers ('extended enterprise'), or in part (e.g., a division, a department, etc.) as well as the principles governing its design and evolution [23]. In the literature, various sub-architectures of enterprise architectures have been proposed. They include, among other things, a business, process, integration, software, and technology architecture (e.g. [24]). As stated in the introduction, we will focus on three perspectives of an enterprise architecture: (1) business process (2), compliance, and (3) IT architecture. For reasons of simplicity, we refer to a single element within an IT architecture as an IT component that can be either software or hardware-based. The interrelations between the single elements of these perspectives are illustrated in Fig. 1.

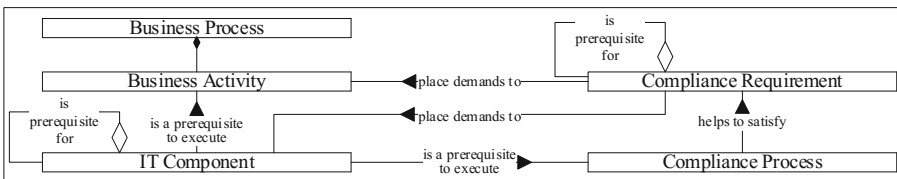


Fig. 1. Considered elements of an enterprise architecture and their interrelations [10]

2.3 Motivation Scenario

The left side of Fig. 2 shows a simplified purchase to pay process including perspectives on compliance requirements, compliance processes, and IT components. Some of the business activities are supported by IT components that are modeled as triangles. We assume that the material management module of an enterprise resource planning system (ERP MM) is a prerequisite for both the business activity 'send purchase requisition' and the compliance process 'check invoice'. Furthermore, a financial module of an ERP system (ERP FI) is a prerequisite for the business activities 'create payment order' and 'execute payment'.

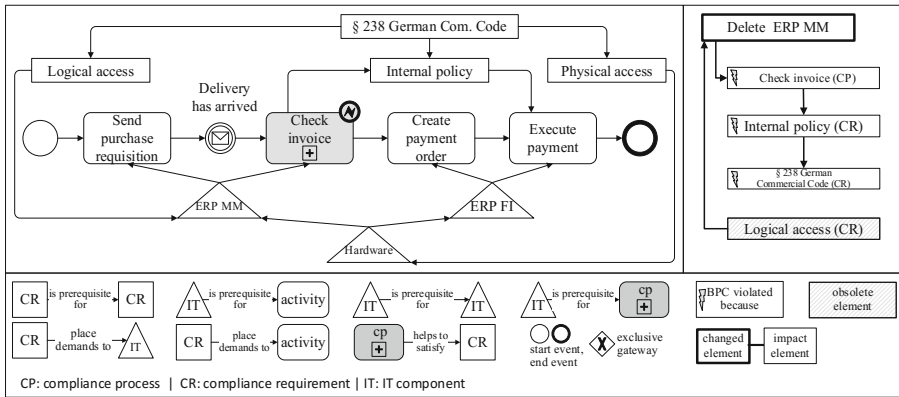


Fig. 2. Purchase-to-pay process (based on [10])

In addition, both business activities and IT components are sometimes affected by compliance requirements. In this example, ‘§ 238 of the German Commercial Code’ demands an accounting obligation for merchants in Germany. It is also related to the proper operation of IT that supports the accounting activities. In this example, the compliance requirements ‘physical access’ and ‘logical access’ are prerequisite by ‘§ 238 of the German Commercial Code’. The compliance requirement ‘physical access’ requires a regulated access to physical IT components while ‘logical access’ requires the identification and authentication of users of an application [25]. For simplification, this compliance requirement only place demands on the IT component ‘ERP MM’. Furthermore, the compliance requirement ‘internal policy’ specifies additional requirements that are necessary for the payment of invoices. Finally, the compliance process ‘check invoice’ helps to satisfy the ‘internal policy’.

As shown on the right side of Fig. 2, the compliance process ‘check invoice’ cannot be executed in the case of deleting ‘ERP MM’. Thus, the compliance requirements ‘internal policy’ and ‘§ 238 of the German Commercial Code’ are violated. Furthermore, the compliance requirement ‘logical access’ is obsolete. A method and a software prototype to determine the interactions between BPC and business process change have been provided in [10, 26]. In the upcoming section, we propose an approach to put forward proposals for an adaptation of the business process through the integration of alternative compliance processes to further ensure BPC.

3 Towards Proposals for a Business Process Adaptation

In this section we present artifacts to put forward proposals for a business process adaptation to further ensure BPC. First of all, we present the main ideas of our method and show it in a running scenario. Second, we present a meta-model to represent the relations between alternative compliance process and compliance process patterns. Third, we present our method in detail.

3.1 Main Ideas

The elaboration of proposals for business process adaptation is based on three main ideas:

- The separate modelling of business processes and so-called compliance processes and its automatic integration into the business process during design time (e.g. [12, 27, 28]) as mentioned in the previous section;
- The definition of alternative compliance processes that satisfy the same compliance requirement [11]; and
- The differentiation of alternative compliance processes based on their properties.

Alternative Compliance Processes. The compliance process that is integrated into the business process helps satisfy at least one compliance requirement [22]. In addition, a compliance requirement can be satisfied by more than one compliance process, i.e. alternative compliance processes. An example of an alternative compliance processes is the control of the number of bacteria in drinking water. The number of bacteria can be controlled by alternative compliance processes and at different points in the supply process e.g., by analyzing the water sources, the water depots, the hand-over to the consumer, or the consumer him or herself [11].

In case of detecting a violation of BPC due to a changed compliance requirement, business activity, or IT component the business process must be adapted to further ensure BPC. Thus, proposals for the integration of alternative compliance processes into the business process need to be put forward. The bases for these proposals are alternative compliance processes that are separately modelled and stored from the business process.

Properties of a Compliance Process. Each compliance process may have different properties, such as the type of integration into the business process or the type of execution. In [22] we proposed a taxonomy that categorizes properties of compliance processes. In the end, our compliance process taxonomy contains 37 characteristics in 9 dimensions and 3 meta-characteristics.

The meta-characteristic ‘Integration Constraint’ contains requirements for the integration of a compliance process into a business process. One dimension within these meta-characteristic is the dimension ‘Trigger’ that indicates the need for the integration of a compliance process into a business process to satisfy a compliance requirement. Another dimension contains further requirements that are necessary for the execution of a compliance process, e.g. the existence of an IT component. The meta-characteristic ‘Modeling’ includes, in addition to other features, patterns for modelling compliance processes. The meta-characteristic ‘Property’ contains further properties of a compliance process. These properties may depend on other characteristics of the compliance process taxonomy, such as the type of execution which can either be automatic, IT dependent manual or manual.

3.2 Running Scenario

As explained, the change of a business process or IT component sometimes leads to a violation of BPC. In the motivation example, the removal of the IT component ‘ERP MM’ leads to the violation of the compliance requirements ‘internal policy’ and ‘§ 238 of the German Commercial Code’ and thus also leads to a violation of BPC. The reason is the unfeasibility of the compliance process ‘check invoice’. In order to avoid this violation, there must be a proposal for a business process adaptation through the integration of an alternative compliance process.

The left side of Fig. 3 shows the interrelation of alternative compliance process patterns and compliance processes that satisfy the compliance requirement ‘internal policy’. The right side of Fig. 3 shows the integration of the two alternative compliance processes into the business process. For reasons of simplicity, we do not model the IT components in Fig. 3. As an alternative to checking the invoice, the payment order can also be checked. The annotations at the compliance processes contain their properties derived from the compliance process taxonomy.

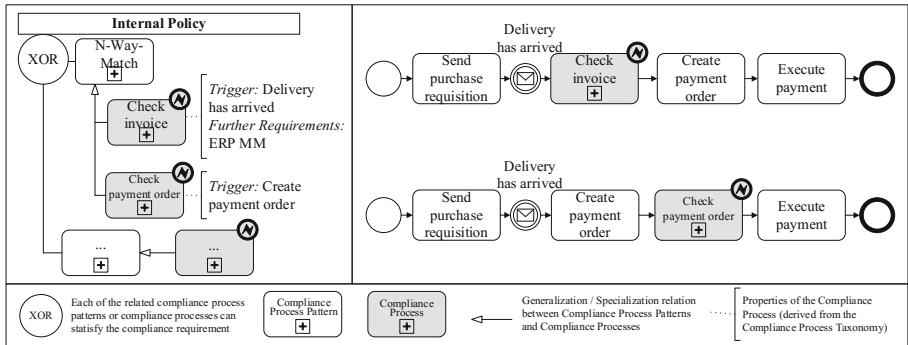


Fig. 3. Model alternative compliance processes and propose an adapted business process

3.3 Meta-model and Method to Put Forward Proposals

In order to understand the following steps of our method, Fig. 4 shows the interrelations between necessary elements. In the following, we briefly define two new elements: the compliance process pattern and the compliance rule.

In general, patterns are high-level domain-specific templates used to represent desired properties and constraints [2]. Following this, we define a compliance process pattern as a process template that contains process elements (e.g. activities, gateways, and connectors) that are necessary to satisfy at least one compliance requirement. Consequently, a compliance process is still necessary to satisfy at least one compliance requirement. Thus, a compliance process is the specialization of the compliance pattern; its properties are derived from the compliance process taxonomy [22]. Further, the compliance requirement and the integration constraint of the compliance process are formalized in a machine readable compliance rule.

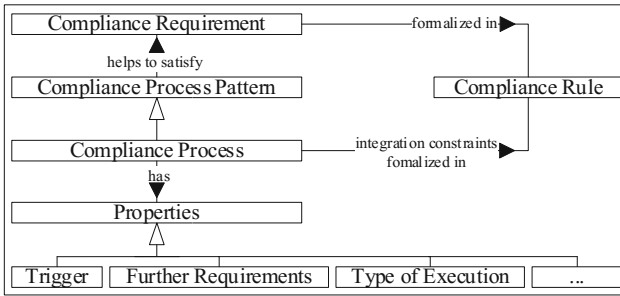


Fig. 4. Modelling alternative compliance processes

Next, we propose a three-step method, in order to put forward proposals for a business process adaptation through the integration of alternative compliance processes:

- First, define alternative compliance processes which are based on a compliance process pattern to satisfy the same compliance requirement [11, 22].
- Second, transform compliance requirements into machine readable compliance rules.
- Third, automatically select an alternative compliance process and integrate it into the business process.

Define Alternative Compliance Processes. As a basis for modelling alternative compliance processes we use compliance process patterns proposed by Namiri [29] and Schultz [30]. These patterns can be assigned to the corresponding dimension of our compliance process taxonomy [22]. A compliance requirement pattern includes, among other patterns, a second set of eyes pattern, a separation of duties pattern and document patterns such as an N-way-match that compares different text values.

In our running scenario, the compliance requirement ‘internal policy’ can be satisfied by a compliance process pattern ‘N-way-match’ on a general level. Further, we specialize its level of detail by modelling two alternative compliance processes. One possible specialization is the compliance process ‘check invoice’. The trigger to execute this compliance process is the existence of the event ‘delivery has arrived’. Further, the compliance process needs the IT component ‘ERP MM’ to be executed. As already mentioned, the payment order can also be checked as an alternative to the invoice. The trigger for the integration of the corresponding compliance process ‘check payment order’ is the existence of the business activity ‘create payment order’. In contrast to the compliance process ‘check invoice’, there is no further requirement for the execution of this compliance process.

Transform Compliance Requirements into Compliance Rules. For the automatic selection of an appropriate compliance process, the possibility of its integration into the business process must be examined. Accordingly, a prerequisite for this is the transformation of the compliance requirement into a machine readable compliance rule. Additionally, the compliance rule must be modelled individually for each compliance process. In our case the rule must be able to represent the presence or absence of both

business activities and IT components. Thus, the compliance rule must include the control flow and resource perspective of a process. A suitable compliance rule language for this purpose is Linear Temporal Logic (LTL) [31].

Select and Integrate an Alternative Compliance Process. Alternative compliance processes must be selected and integrated to put forward proposals for a business process adaptation. For further explanations, we define the conceptual modelling of compliance requirements and their associated compliance processes, etc., as a directed graph $G = (N, E, F, H, K)$ with its elements $g_i \in G$. In addition, N is a nonempty finite set of nodes, and $e_1 \in E$ is a set of directed edges between two nodes $(n_{(i)}, n_{(j)})$. In addition, $f_i \in F$ is the unique identification (id) of the node n_i ; $h_i \in H$ is the model type of the node $n_{(i)}$ with $H = \{\text{Compliance Requirement (CR)}, \text{Compliance Process Pattern (CPP)}, \text{Compliance Process (CP)}\}$; and $k_i \in K$ is the machine readable compliance rule of node n_i . Further we limit the allowed edges between the defined node types: $E_r = \{((n_i|h_i = \text{CPP}), (n_j|h_j = \text{CR})); ((n_k|h_k = \text{CP}), (n_l|h_l = \text{CR})); ((n_m|h_m = \text{CPP}), (n_n|h_n = \text{CPP})); ((n_o|h_o = \text{CP}), (n_p|h_p = \text{CPP}))\}$ with $n_i..n_p \in N$; $h_i..h_p \in H$; and $E_r \subseteq E$.

Basically, the search for alternative compliance processes starts at n_i , which represents the compliance process that is no longer executable. First, we search for sibling nodes of n_i and their existing specializations. The specializations can be found by searching the predecessors of each sibling node of n_i . To check whether these compliance processes can be executed within the business process, each of their compliance rules must be checked against the business process by using graph searching methods (e.g. [32]). If there is no appropriate compliance process, we perform a second search for an appropriate compliance process pattern. Accordingly, we search for successors of n_i that are of the type ‘compliance process pattern’.

The search for alternative compliance processes can lead to three results. First, there is one alternative compliance process, which is already the case in the running scenario. Second, there is more than one alternative compliance process. Third, there is no alternative compliance process. We propose a solution for each case. In case of exactly one alternative compliance process the adapted business process is proposed. In case of numerous alternative compliance processes, our method proposes all alternative compliance processes. In these cases, our method will propose more than one adapted business process. In case of no alternative compliance process, our method proposes a generic compliance process pattern, if available. For a first and easy solution, the compliance process pattern is integrated at the place of the original compliance process within the business process.

4 Related Work

In [10, 14] we conducted two structured literature reviews in the field of BPC, business process change and business process adaptation. Despite manual approaches to remodel business processes, there are also methods that automatically adapt business processes to satisfy compliance requirements. The latter approaches can be classified into approaches that (1) change the order of activities, gateways and other flow

elements in a business process, and (2) integrate separate modelled compliant process fragments into a business process. However, none of the identified approaches consider IT components as a prerequisite to execute a compliance process and put forward proposals for an adaptation of business processes through (1) alternative compliance processes or (2) compliance process patterns to ensure compliance due to business process change.

Kopp et al. [33] proposed a method that transforms the business process into a well-defined process model that can be used for further automatic compliance checking techniques such as graph searching. Awad et al. [32] developed a method to reorder business activities or change the gateway types within a business process to meet compliance requirements. In addition, Höhn [34] proposed a method to automatically rewrite the business process to enforce obligations.

Schumm et al. [12] proposed a method to integrate separate stored compliant process subgraphs into a business process during their design-time. In [19] they demonstrated their method with a software prototype. Schultz [30] modelled business processes based on log files of an ERP system. Furthermore, he automatically added activities that represent application controls for the business process. Kittel and Sackmann [27, 28] proposed and demonstrated a method with a software prototype to integrate control processes in business processes during their execution.

5 Conclusion

Various factors such as business process reengineering and outsourcing decisions can lead to changing compliance requirements, business processes, compliance processes, and new IT components. Consequently, this can lead to a violation of BPC. In order to avoid such violations, the business process has to be adapted. Thus, we proposed the idea of separate modelling of alternative compliance processes whereby each compliance process has different properties (e.g., manual or automatic execution) and specializes in a specific compliance process pattern. The modelling of the relationships and the search for alternative processes is performed using a graph. In the end, our method proposes adapted business process to further ensure BPC.

Currently, our method considers the control flow and the presence and absence of IT components for the selection and integration of alternative compliance process patterns or compliance processes. Each alternative compliance process pattern and compliance process must be modelled individually. In case of more than one appropriate compliance process there is no criteria for the selection of an alternative compliance process, e.g. by an economic assessment [35].

In a next step, we will demonstrate our method through an extension of our software prototype, BCIT [26]. In addition, the software prototype will be evaluated through the presentation of different scenarios to experts in the field of IT architecture management, business process management and compliance. Additionally, the method can be extended to include, e.g. a data or an organizational perspective on a business process. Further, unsupervised machine learning techniques, such as frequent pattern

analysis (e.g., a FP-Growth algorithm) can be used to propose possible alternative compliance processes without explicit prior modelling based on existing business process models that include compliance processes.

References

1. Governatori, G., Sadiq, S.: The Journey to Business Process Compliance. Handbook of Research on Business Process Modeling, pp. 426–454 (2009)
2. Turetken, O., Elgammal, A., van den Heuvel, W.-J., Papazoglou, M.: Enforcing compliance on business processes through the use of patterns. In: 19th ECIS 2011 (2011)
3. Knackstedt, R., Eggert, M., Heddier, M., Chasin, F., Becker, J.: The Relationship of is and Law - The Perspective of and Implications For IS Research. ECIS 2013 Completed Research (2013)
4. Rudzajs, P., Buksa, I.: Business process and regulations: approach to linkage and change management. In: Grabis, J., Kirikova, M. (eds.) BIR 2011. LNBIP, vol. 90, pp. 96–109. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24511-4_8
5. Fdhila, W., Indiono, C., Rinderle-Ma, S., Reichert, M.: Dealing with change in process choreographies design and implementation of propagation algorithms. *Inf. Syst.* **49**, 1–24 (2015)
6. Rinderle, S., Reichert, M., Dadam, P.: Correctness criteria for dynamic changes in workflow systems—a survey. *Data Knowl. Eng.* **50**, 9–34 (2004)
7. Kittel, K.: Agilität von Geschäftsprozessen trotz Compliance. Tagungsband der 11. Internationale Tagung Wirtschaftsinformatik, pp. 967–981 (2013)
8. 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. *Serv. Oriented Comput.* **6470**, 17–31 (2010)
9. Becker, J., Heddier, M., Braeuer, S., Knackstedt, R.: Integrating regulatory requirements into information systems design and implementation. In: Proceedings ICIS 2014 (2014)
10. Seyffarth, T., Kühnel, S., Sackmann, S.: Business Process Compliance and Business Process Change. An Approach to Analyze the Interactions. Business Information Systems. BIS 2018, Lecture Notes in Business Information Processing, pp. 176–189 (2018)
11. Kittel, K., Sackmann, S., Betke, H., Hofmann, M.: Achieving flexible and compliant processes in disaster management. In: 46th Hawaii International Conference on System Sciences (HICSS 2013), pp. 4687–4696 (2013)
12. Schumm, D., Leymann, F., Ma, Z., Scheibler, T., Strauch, S.: Integrating compliance into business processes. process fragments as reusable compliance controls. In: Proceedings of the MKWI 2010 (2010)
13. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. *MIS Quart.* **28**, 75–105 (2004)
14. Sackmann, S., Kuehnel, S., Seyffarth, T.: Using business process compliance approaches for compliance management with regard to digitization: evidence from a systematic literature review. In: Weske, M., Montali, M., Weber, I., vom Brocke, J. (eds.) BPM 2018. LNCS, vol. 11080, pp. 409–425. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98648-7_24
15. Hammer, M., Champy, J.: Reengineering the corporation. a manifesto for business revolution. Harper Business, New York (1993)
16. Kittel, K., Sackmann, S.: Gaining Flexibility and Compliance in Rescue Processes with BPM. Workshops Resilience and IT-Risk in Social Infrastructures (RISI) im Rahmen der 6th International Conference on Availability, Reliability, and Security (2011)

17. Betke, H., Kittel, K., Sackmann, S.: Modeling Controls for Compliance. An Analysis of Business Process Modeling Languages. In: The 27th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA-2013), pp. 866–871 (2013)
18. Eberle, H., Unger, T., Leymann, F.: Process fragments. In: Meersman, R., Dillon, T., Herrero, P. (eds.) OTM 2009. LNCS, vol. 5870, pp. 398–405. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-05148-7_29
19. Schumm, D., Turetken, O., Kokash, N., Elgammal, A., Leymann, F., van den Heuvel, W.-J.: Business process compliance through reusable units of compliant processes. In: Daniel, F., Facca, F.M. (eds.) ICWE 2010. LNCS, vol. 6385, pp. 325–337. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-16985-4_29
20. Rastrepkina, M.: Managing variability in process models by structural decomposition. In: Mendling, J., Weidlich, M., Weske, M. (eds.) BPMN 2010. LNBIP, vol. 67, pp. 106–113. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-16298-5_10
21. Kittel, K., Sackmann, S., Göser, K.: Flexibility and Compliance in Workflow Systems. The KitCom Prototype. Tagungsband CAiSE Forum - 25th International Conference on Advanced Information Systems Engineering, 154–160 (2013)
22. Seyffarth, T., Kühnel, S., Sackmann, S.: A Taxonomy of Compliance Processes for Business Process Compliance. 15th International Conference on Business Process Management, Business Process Management Forum (2017)
23. TOGAF (ed.): Content Metamodel. Content Metamodel Vision and Concepts. <http://pubs.opengroup.org/architecture/togaf9-doc/arch/>
24. Winter, R., Fischer, R.: Essential Layers, Artifacts, and Dependencies of Enterprise Architecture. In: 2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW 2006), p. 30 (2006)
25. Principles of Proper Accounting When Using Information Technology. IDW AcP FAIT 1 (2002)
26. Seyffarth, T., Raschke, K.: BCIT. A tool for analyzing the interactions between business process compliance and business process change. In: Proceedings of the Dissertation Award and Demonstration, Industrial Track at BPM 2018, pp. 81–85 (2018)
27. Sackmann, S., Kittel, K.: Flexible Workflows and Compliance: A Solvable Contradiction?! In: vom Brocke, J., Schmiedel, T. (eds.) BPM - Driving Innovation in a Digital World. MP, pp. 247–258. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-14430-6_16
28. Kittel, K., Sackmann, S., Göser, K.: Flexibility and Compliance in Workflow Systems. The KitCom Prototype. Tagungsband CAiSE Forum - 25th International Conference on Advanced Information Systems Engineering, pp. 154–160 (2013)
29. Namiri, K., Stojanovic, N.: Using Control Patterns in Business Processes Compliance. WISE 2007 Workshops, pp. 178–190 (2007)
30. Schultz, M.: Enriching Process Models for Business Process Compliance Checking in ERP Environments. Design Science at the Intersection of Physical and Virtual Design 7939, pp. 120–135 (2013)
31. Elgammal, A., Turetken, O., van den Heuvel, W.-J., Papazoglou, M.: Formalizing and applying compliance patterns for business process compliance. Software System Modeling (2014)
32. Awad, A., Smirnov, S., Weske, M.: Resolution of compliance violation in business process models: a planning-based approach. In: Meersman, R., Dillon, T., Herrero, P. (eds.) OTM 2009. LNCS, vol. 5870, pp. 6–23. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-05148-7_4

33. Kopp, O., Leymann, F., Schumm, D., Unger, T.: On BPMN process fragment auto-completion. In: 3rd Central-European Workshop on Services and their Composition, pp. 58–64 (2011)
34. Höhn, S.: Model-based reasoning on the achievement of business goals. In: Proceedings of the 2009 ACM symposium on Applied Computing, pp. 1589–1593 (2009)
35. Kuehnel, S., Zasada, A.: An approach toward the economic assessment of business process compliance. In: Woo, C., Lu, J., Li, Z., Ling, T.W., Li, Guoliang, Lee, MLi (eds.) ER 2018. LNCS, vol. 11158, pp. 228–238. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01391-2_28

Anlage E: Publikation „Maintaining Business Process Compliance despite Changes“

Seyffarth, Tobias; Kühnel, Stephan (2020): Maintaining Business Process Compliance despite Changes. A Decision Support Approach based on Process Adaptations. In: Journal of Decision Systems. DOI: 10.1080/12460125.2020.1861920.

Maintaining business process compliance despite changes: a decision support approach based on process adaptations

Tobias Seyffarth and Stephan Kuehnel

Department of Management Information Systems and Operations Research, Martin Luther University Halle-Wittenberg, Chair of Information Management, Halle (Saale), Germany

ABSTRACT

The term compliance essentially refers to ensuring that business processes, operations and practices conform to an agreed set of rules. Such rules can influence both business processes and components of an information technology (IT) architecture, resulting in relationships between (1) compliance requirements, (2) process elements and (3) IT components. Whenever one element of these three classes is changed, e.g. when outsourcing decisions are made, a relationship analysis becomes necessary in order to identify demanding and violated compliance requirements. Since a manual relationship analysis is a complicated and elaborate task, the paper at hand presents methods to 1) automatically identify potential compliance violations in the context of changes and 2) automatically propose process adaptations for maintaining or re-establishing compliance. The methods are implemented as a software artefact, evaluated as useful in the context of an expert survey and contribute to the support of process adaptation decisions for maintaining compliance following changes.

ARTICLE HISTORY

Received 18 March 2020
Accepted 1 December 2020

KEYWORDS

Business process;
compliance; change;
decision support system;
decision support approach;
IT architecture

1. Introduction

Business process compliance refers to the modelling and execution of business processes in accordance with regulatory requirements (Governatori & Sadiq, 2009). In an age of increasingly digitised business activities or even completely digital business processes, a great number of companies are confronted with increasing compliance requirements originating from the IT environment, and these regulations are both laborious and costly (Becker et al., 2016; Sackmann et al., 2018). To keep the effect of compliance on business activities minimal and to avoid a negative impact on profitability, compliance violations have to be prevented, especially in digital business fields that are characterised by frequent changes (Sackmann et al., 2018). However, the prevention of such violations is only possible if the dependencies between compliance requirements, business processes and IT components are known and can be continuously analysed.

A compliance requirement is a constraint or assertion that prescribes a desired result or purpose to be achieved by incorporating actions or control procedures in processes (Turetken et al., 2011). Compliance requirements not only place demands on business

CONTACT Tobias Seyffarth  tobias.seyffarth@wiwi.uni-halle.de  Martin Luther University Halle-Wittenberg, Chair of Information Management, Halle (Saale) 06108, Germany

© 2020 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

processes, but also on components of information technology (IT) architecture, such as data protection and information security laws addressing the operation of software and/or hardware (Committee of Sponsoring Organizations of the Treadway Commission, 2012; Knackstedt et al., 2013; Sadiq et al., 2007; The Institut der Wirtschaftsprüfer in Deutschland e.V. [Institute of Public Auditors in Germany, Incorporated Association], 2002b).

Compliance requirements imposed on an IT infrastructure have at the least an indirect influence on business processes if an IT component is a prerequisite for process execution, as is the case with non-manual process activities. Consequently, there are direct and indirect dependencies between compliance requirements, IT components and process activities. Each of them require consideration as part of a comprehensive management of business process compliance. Outsourcing decisions, business process re-engineering, new technologies and many other factors can lead to changing compliance requirements, business activities, or IT components (Fdhila et al., 2015; Rudzajs & Buksa, 2011).

In dynamic markets, the rapid adaption of business activities and processes to such changes is seen as a competitive advantage (Rinderle et al., 2004). Thus, the fast detection of demanding compliance requirements (prior to a compliance breach) and violated compliance requirements (subsequent to a compliance breach) as well as the related adaption of business processes for maintaining compliance are important tasks (Sackmann & Kittel, 2015). However, due to the steadily rising level of regulation and increasingly complex business process models and IT architectures, this is becoming a challenging and time-consuming manual task (Elgammal et al., 2010; Ghanavati et al., 2009). In this context, IT support and automation open up the potential for time and cost savings.

There is already a body of literature, which provides a range of approaches that allow for querying the relationships between compliance requirements and business processes, compliance requirements and IT components as well as interrelated requirements (e.g. (Fdhila et al., 2012; Rudzajs & Buksa, 2011)). However, an analysis of these relationships is a prerequisite for the identification of demanding and violated compliance requirements. It is also necessary for process adaptations in order to maintain or re-establish business process compliance. To the best of our knowledge, so far there is no approach that allows for a comprehensive and automatic analysis of all direct and transitive relationships as well as subsequent process adaptation proposals.

Consequently, the goal of this research is a decision support approach that allows for identifying demanding and violated compliance requirements by means of design-time information, and for maintaining compliance despite changes in process activities, IT components, or regulations. In this study, we focus on the compliance change patterns 'replace' and 'delete', as their impact on compliance can be determined based on information from the underlying design-time models, i.e. previously modelled dependencies between compliance requirements, business processes, and IT components. In order to reach that goal, we raise the following research questions (RQ):

- RQ1: How to automatically determine compliance requirements and compliance violations by replacing or deleting business activities, IT components, or regulations?
- RQ2: How to automatically generate proposals for compliant business process models at design time?

To investigate the research questions, we apply the well-known design science research methodology proposed by (Peffer et al., 2006). In this study, we bring together models and methods to recommend compliant business processes based on integrating previously modelled alternative compliance processes of organisations. In addition, we demonstrate our artefacts in a proof-of-concept implementation called BCIT, which helps to eliminate potential naming ambiguities when integrating compliance processes into business processes. Finally, we evaluate our artefacts using a case study.

The paper is structured as follows: In [Section 2](#), we introduce required preliminaries and present a motivating example. In [Section 3](#), we present the related work and briefly describe the extent to which the related work is able to implement the motivation example. [Section 4](#) addressed our applied research method, and [Section 5](#), introduces a method that allows an automatic identification of demanding and violated compliance requirements triggered by changes. In [Section 6](#), we introduce a method that allows for the automatic suggestion of business process adaptations to maintain or re-establish compliance subsequent to a compliance violation. [Section 7](#) provides evaluation episodes of this research project and presents a case study based on which domain experts evaluated the perceived usefulness of our approaches. After discussing the implications of this contribution for research and practice in [Section 8](#), we conclude the paper in [Section 9](#).

2. Theoretical background

2.1. Theories

From a broader perspective, compliance is about unambiguously ensuring conformance to a set of prescribed and/or agreed upon requirements (Turetken et al., 2011). In this context, a compliance requirement is a constraint or assertion that prescribes a desired result or purpose that derives from a compliance source, such as a regulation, legislation or law (Turetken et al., 2011). As previously stated out, compliance requirements may place demands on business processes and/or information technology (IT).

The execution of business processes in adherence to applicable compliance requirements is called business process compliance (BPC) (Governatori & Sadiq, 2009). The operation of IT in adherence to applicable compliance requirements such as COSO (Committee of Sponsoring Organizations of the Treadway Commission, 2012) and COBIT (ISACA, 2013) is called IT compliance. From a business process management perspective, business process cannot be viewed separately from IT (Weske, 2019). Therefore, compliance requirements for IT must also considered. In this context, this includes BPC and IT compliance. In the following, we will only use the terms 'compliance' and 'compliance requirement' regardless of whether the core concept is BPC or IT compliance.

2.2. Interrelations between compliance, business processes and IT Components

[Figure 1](#) shows our compliance meta-model which illustrates the relations between business activities, IT components, compliance requirements and other elements to which we refer throughout the paper.

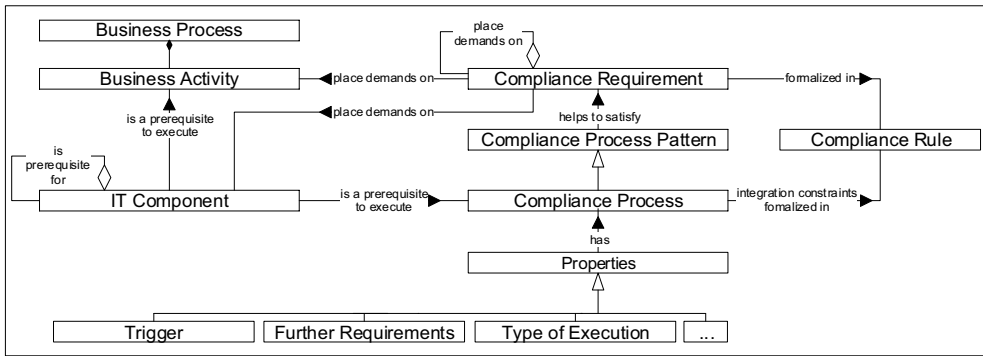


Figure 1. Compliance meta-model (based on (Seyffarth et al., 2016; 2017a)).

For reasons of simplicity, we refer to a single element within an IT architecture as an IT component and we do not distinguish between different types of IT components, which can be e.g. application services, application components or network devices such as special types of hardware (Winter & Fischer, 2006).

Various approaches check or ensure BPC. As an example, BPC can be checked after process execution by analysing log files (e.g. (El Kharbili et al., 2008)) or ensured at the design time of business processes, e.g. during modelling. A possible solution to ensure BPC at the design time of the business processes is the separate modelling of so-called compliance processes and its integration into business process models. In this context, a compliance process is defined as an independent process (part) consisting of at least one compliance-related activity that satisfies a compliance requirement (Seyffarth et al., 2017a). Whenever a business process activity is affected by a compliance requirement, a corresponding compliance process can be integrated in the business process (Sackmann & Kittel, 2015; Schumm et al., 2010a). Further, a compliance requirement can be satisfied by numerous alternative compliance processes. These can differ in a number of properties such as the kind of conditions to be verified, further necessary requirements for execution, and the type of execution (Seyffarth et al., 2017a).

The idea of separating compliance and business processes corresponds to a special kind of process modularisation which has the potential for reusing compliance processes or compliant process fragments to meet compliance requirements in various business processes (Schumm et al., 2010a). It is based on the assumption that the amount of business and compliance activities are disjointed, i.e. that an activity meets either a business or a compliance objective. If the pursuit of a compliance goal serves only value generation, it becomes difficult to distinguish between compliance and business activities. This might be the case when complying with requirements constitutes the unique selling proposition of a product or service. However, our approach focuses on cases where modularisation is possible.

2.3. Example model

Figure 2 shows a simplified purchase to pay process, which is modelled as a Business Process Model and Notation (BPMN) model, including perspectives on compliance requirements, a business process, a compliance process, and IT components. We are

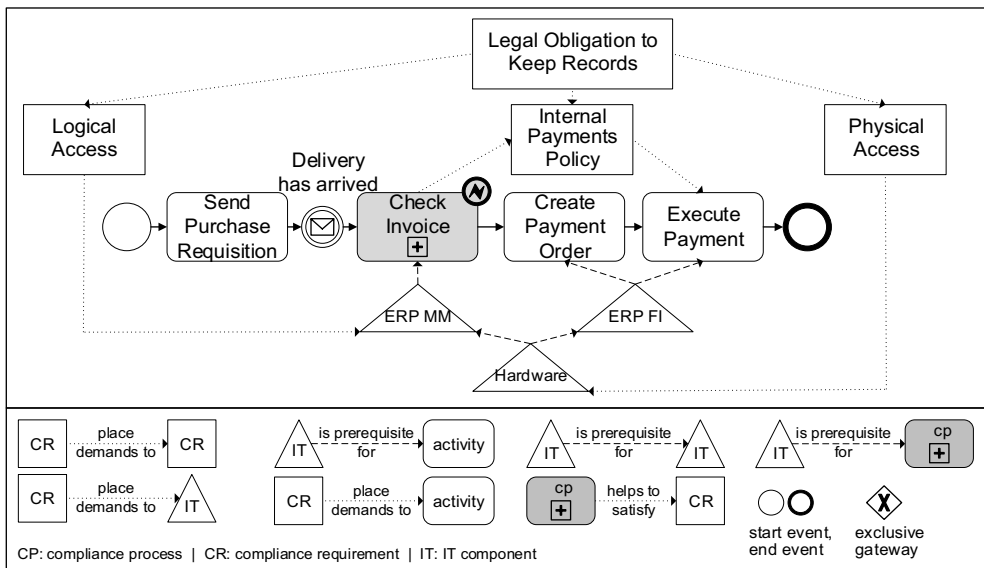


Figure 2. Simplified purchase to pay process (based on (Frank et al., 2009; Namiri & Stojanovic, 2007; Seyffarth et al., 2018; 2019)).

aware that the process might be overly simplified for any real scenario; however, the goal of the example model is to explain our methods that also works for more realistic and complex processes. Further explanations are based on this example.

In the example, some activities are supported by IT components that are modelled as triangles. On the one hand, we assume that the material management module of an enterprise resource planning system (ERP MM) is a prerequisite for the compliance process ‘check invoice’. On the other hand, a financial module of an ERP system (ERP FI) is a prerequisite for the activities ‘create payment order’ and ‘execute payment’.

In addition, some business activities and IT components are affected by compliance requirements. In the example, the requirement ‘legal obligation to keep records’ obliges German merchants to do accounting. According to IDW RS FAIT 1, this requirement is also related to the proper operation of IT that supports accounting activities (The Institut der Wirtschaftsprüfer in Deutschland e.V. [Institute of Public Auditors in Germany, Incorporated Association], 2002a). In this particular case, the compliance requirements ‘physical access’ and ‘logical access’ are prerequisites of ‘legal obligation to keep records’. The compliance requirement ‘physical access’ requires a regulated access to physical IT components while ‘logical access’ requires the identification and authentication of the users of an application (The Institut der Wirtschaftsprüfer in Deutschland e.V. [Institute of Public Auditors in Germany, Incorporated Association], 2002a). For simplification purposes, the compliance requirement ‘logical access’ only places demands to the IT component ‘ERP MM’. Furthermore, the compliance process ‘check invoice’ satisfies the requirement ‘internal payments policy’, which specifies additional requirements that are necessary for the payment of invoices.

2.4. Formal definitions

Formal graph theory is widely used to model interrelations between elements (Heckel & Taentzer, 2020). This is also applied to business process models (Weske, 2019), IT architecture models (Dreyfus & Iyer, 2006), and compliance requirements (Sillaber & Breu, 2012). Following the compliance meta-model presented in Section 2.2 and (Seyffarth et al., 2018), we introduce several definitions to formally define relationships between compliance requirements, business processes, compliance processes and IT components.

Definition 1 (Compliance Requirement Graph). A compliance requirement graph is a directed graph $CRG = (N^{CRG}, E^{CRG})$, where: N^{CRG} is a nonempty finite set of nodes representing compliance requirements and $E^{CRG} \subseteq N^{CRG} \times N^{CRG}$ is a set of directed edges between nodes. An edge e_{ij}^{CRG} is considered to be directed from n_i^{CRG} to n_j^{CRG} .

Definition 2 (Business Process Graph). A business process graph PG is a 3-tuple $PG = (N^{PG}, E^{PG}, c_type)$, where: $N^{PG} = BA \cup CA \cup C$ is a set of nodes in PG that follow common execution semantics. BA is a set of business activities and CA is a set of compliance activities, where: $BA \cap CA = \emptyset$. C is a set of coordinating nodes and $E^{PG} \subseteq N^{PG} \times N^{PG}$ is a set of directed edges between nodes representing a control flow such that (N^{PG}, E^{PG}) is a connected process graph. An edge e_{ij}^{PG} is considered to be directed from n_i^{PG} to n_j^{PG} . The function $c_type : C \rightarrow \{start, end, intermediate, split, synchronize, choice, merge\}$ assigns a coordinator type to each coordinating node of PG .

Definition 3 (Compliance Process Graph). A compliance process graph is a subgraph of PG and a 3-tuple $CP = (N^{CP}, E^{CP}, c_type)$ if $N^{CP} \subseteq CA \cup C$ and $E^{CP} \subseteq E^{PG}$.

Definition 4 (IT Architecture Graph). We define an IT architecture as a directed graph $ITG = (N^{ITG}, E^{ITG})$ where N^{ITG} is a nonempty finite set of nodes representing IT components and $E^{ITG} \subseteq N^{ITG} \times N^{ITG}$ is a set of directed edges between nodes. An edge e_{ij}^{ITG} is considered to be directed from n_i^{ITG} to n_j^{ITG} .

Definition 5 (Integrated Compliance Graph). In order to integrate the elements of the aforementioned models into one model, we define an integrated graph, which includes compliance requirements, a business process with integrated compliance processes and IT components (Seyffarth et al., 2018). The connection of elements of the different graph types is based on the set of directed edges E^{con} . An edge e_{ij}^{con} is considered to be directed from n_i^{PG} to n_j^{ITG} , n_i^{PG} to n_j^{CRG} , n_i^{ITG} to n_j^{PG} , n_i^{CRG} to n_j^{PG} , or n_i^{CRG} to n_j^{ITG} . In consequence, a directed integrated compliance graph G is a 4-tuple $G = (N^G, E^G, n_identify, n_type)$, where: $N^G = N^{CRG} \cup N^{PG} \cup N^{ITG}$ is a nonempty finite set of nodes, $E^G = E^{CRG} \cup E^{PG} \cup E^{ITG} \cup E^{con}$ is a set of directed edges between nodes with $E^G \subseteq N^G \times N^G$. The function $n_identify(n_i^G)$ assigns an unique identifier (id) to each node n_i^G . The node type of n_i^G is specified by the function

$$n_type(n_i^G) = \begin{cases} BusinessActivity : n_i^G \in BA \\ ComplianceActivity : n_i^G \in CA \\ CoordinatingNode : n_i^G \in C \\ ITComponent : n_i^G \in ITG \\ ComplianceRequirement : n_i^G \in CRG \end{cases}$$

For a practical implementation of the generation of the integrated compliance graph G , the process model, the IT architecture model and the compliance model must be available in machine-readable form (Seyffarth et al., 2018; Seyffarth & Raschke, 2018). Given that processes are available, e.g. in BPMN 2.0, IT architectures, e.g. in TOGAF Open Exchange, and compliance requirements, e.g. XML-based legal texts, the models are automatically parsed and converted into corresponding nodes and edges in a first step. To realise an instance of the integrated graph G , connections between the different model types are defined manually in a second step.

3. Related work

3.1. Method

We conducted two structured literature reviews (Sackmann et al., 2018; Seyffarth et al., 2017b) in order to analyse related work. We followed the method proposed by (Vom Brocke et al., 2009). Our first review focused on a broad search for approaches from the field of business process management dealing with compliance in order to get an overall impression of the research field. Our second review focused on an in-depth search for approaches from the field of business process compliance dealing with changes in processes, compliance requirements and IT components. In the following, we highlight the main ideas of relevant related approaches, which we categorised according to our research questions.

3.2. Analysing the interactions

There are approaches that queries the relations between compliance requirements and business processes, compliance requirements and IT components and interrelated requirements. We also consider query languages against the process, as they can, for example, also consider documents in the process model. However, none of these distinguishes different change patterns.

Many approaches query the relations within business process models based on pattern matching. (Awad, 2007) presents an approach for querying specific patterns on process graphs that are modelled using BPMN. Both (Delfmann et al., 2015) and (Gacitua-Decar & Pahl, 2009) use graph searching techniques to realise pattern matching in in business process models. In addition, the approach of (Delfmann et al., 2015) is a multi-model approach, which is able to consider different model types, such as documents, organisational units, or IT components. (Gacitua-Decar & Pahl, 2009) also consider semantical aspects. (Fellmann et al., 2011) transform business process models into ontologies and enrich them with structural and domain representation information. However, approaches that are based on pattern matching always require an a priori known pattern query (Delfmann et al., 2015). Although these approaches are in principle applicable in the given application context, they are limited to a specific set of known patterns. However, the practice is characterised by new and constantly changing compliance requirements. Therefore, it is of particular importance that approaches to ensure compliance in business processes are not exclusively limited to known patterns.

Several authors, such as (Ghanavati et al., 2009) and (Corea & Delfmann, 2017), propose approaches for linking business processes and compliance requirements in formal models. Beyond that, (Rudzajns & Buksa, 2011) developed an approach that identifies business activities which are affected by changes in compliance requirements. This approach is based on a version control system for the compliance requirements. Both (Knuplesch et al., 2015) and (Fdhila et al., 2015) discuss the impacts of changed compliance requirements on business processes in a cross-organisational context.

Moreover, a few authors discuss the interrelations between compliance requirements and IT components on a conceptual level (Becker et al., 2011; Knackstedt et al., 2013). (Becker et al., 2014) present an approach for formally modelling and querying interrelations between IT components and single compliance requirements.

Only a few authors address the link between different compliance requirements. Independently of each other, both (Elgammal et al., 2010) and (Halle, 2011) present approaches for detecting root cause violations in rules that are formalised in linear temporal logic.

(Koetter et al., 2014) propose a so called 'compliance descriptor' to model interrelations between compliance requirements, business processes and IT components; however, their approach cannot link compliance requirements. This work is extended in (Koetter et al., 2016) with a graphical modelling notation for the compliance descriptor. The approach of Koetter et al. shows a conceptual relationship to our work. However, due to the inability to map connections between interdependent requirements and the focus of modelling dependencies rather than graph search algorithms, we could not use their approach as a starting point for developing our decision support system for maintaining compliance despite changes.

3.3. Business process adaption

The literature discusses two different types of approaches for adapting business processes automatically to ensure compliance in case changes are made to process activities or process flows.

On the one hand, there are approaches aimed at ensuring compliance within business processes by removing or reordering flow elements, such as gateways or activities, e.g. (Awad et al., 2009; Elgammal et al., 2012). On the other hand, there are approaches aimed at modelling and storing compliant process fragments separately from the business process model. Each compliant process fragment serves to fulfil a compliance requirement. The fragments can be integrated into the business process either at design time or during run time (Sackmann & Kittel, 2015; Schumm et al., 2010a). The separate modelling and storage of fragments offers the possibility for reuse in different business process models. However, none of these approaches considers explicitly the modelling of alternative compliance processes in consideration of IT components.

3.4. Research gap

As depicted in [Table 1](#), we summarised the related work in an author centric concept in accordance with (Webster & Watson, 2002). On the one hand, there is a lack of a method that allows for automatically determining compliance requirements and compliance

Table 1. Author centric concept matrix.

	Determine compliance requirements and compliance violations					Generate compliant business processes	
	BP	BP-CR	CR-IT	CR-CR	BP-IT-CR	Reorder	Separate
(Awad, 2007)	X						
(Gacitua-Decar & Pahl, 2009)	X	(X)					
(Delfmann et al., 2015)	X	(X)			(X)		
(Fellmann et al., 2011)	X	(X)					
(Ghanavati et al., 2009)		X					
(Corea & Delfmann, 2017)		X					
(Rudzajs & Buksa, 2011)		X					
(Fdhila et al., 2015)		X					
(Knuplesch et al., 2015)		X					
(Becker et al., 2011)			X				
(Becker et al., 2014)			X				
(Knackstedt et al., 2013)			X				
(Elgammal et al., 2010)				X			
(Halle, 2011)				X			
(Koetter et al., 2014)					X		
(Koetter et al., 2016)					X		
(Awad et al., 2009)						X	
(Elgammal et al., 2012)						X	
(Schumm et al., 2010a)							X
(Sackmann & Kittel, 2015)							X
Our proposed method	X	X	X	X	X	(X)	X

Legend

- BP: Query within Business Process
- BP-CR: Query relations between Business Process and Compliance Requirement
- CR-IT: Query relations between compliance requirement and IT component
- CR-CR: Query relations between different compliance requirements
- BP-IT-CR: Business Process, Compliance Requirement and IT component
- Reorder: reorder process elements to ensure compliance
- Separate: separate modelling and storing of business processes and compliant business fragments
- (X): Can be done implicitly

violations when considering the change patterns of delete and replace. This is particularly true if the underlying model includes business processes, IT components, and compliance requirements, which in turn can be connected to each other. On the other hand, existing methods for a business process adaption do not make a process adjustment based on the previous analysis, and they do not consider prerequisite IT components to execute compliant process fragments.

4. Research method

We applied a design science research approach inspired by the method described in (Peppers et al., 2006) to structure our procedure and ensure scientific rigour. Accordingly, we conducted six process steps to implement our research project (Peppers et al., 2006) as shown in Figure 3: (1) identify problem and motivate; (2) define objectives of a solution; (3) design and development; (4) demonstration; (5) evaluation; and (6) communication.

We previously addressed the problem of identification and motivation (step 1) in the introduction (c.f. Section 1) and explained it using an illustrative example (cf. Section 2.3). To the best of our knowledge, there are currently no solutions available both for the automatic identification of compliance requirements and compliance violations after the

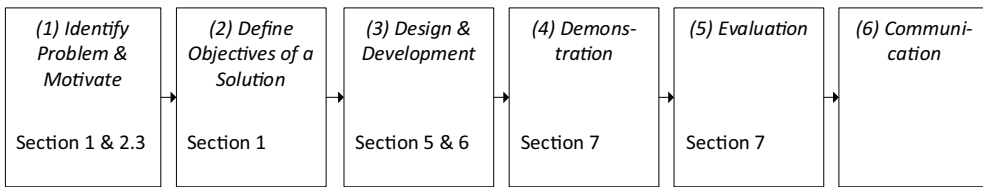


Figure 3. Our design science research approach based on (Peffer et al., 2006).

replacement or deletion of business activities, IT components, and/or compliance requirements, and for the automatic generation of proposals of compliant business processes for curing compliance violations. Therefore, as already outlined in the introduction (cf. Section 1), our research objective (step 2) is a decision-support approach to recommend compliant business processes. Consequently, we developed two artefacts for problem solving (step 3). First, we developed a method to analyse the impact of both replacements and deletions of model elements on compliance (cf. Section 5). Second, we developed a method to recommend compliant business processes in response to compliance violations resulting from replacements or deletions of model elements (cf. Section 6).

To verify the feasibility of our artefacts, we demonstrated them with the software prototype called 'BCIT' (step 4; c.f. Section 7). The demonstration of artefacts by means of a prototype is already considered as an evaluation in DSR (Hevner et al., 2004). However, an essential objective of evaluating design studies is to investigate the usability of artefacts (Hevner et al., 2004). Accordingly, we evaluated the perceived usefulness of our solution artefacts in Section 7 by means of an expert survey (step 5). Finally, the communication of our completed research project (step 6) occurs in this research paper.

5. Analyse the interactions between compliance and change

In this section, we address RQ1 by presenting a method to identify compliance requirements when replacing an element as well as compliance violations when removing an element (Seyffarth et al., 2018). In the following, any arbitrary nodes of the integrated compliance graph will be referred to as 'elements'.

5.1. Business process change patterns

Various business process change patterns have been discussed in the literature. For example, (Weber et al., 2008) distinguished 18 change patterns and split them into 'adaption patterns' and 'patterns of change in predefined regions of business processes'. Further authors have combined the patterns into four change patterns: 'insert element', 'delete element', 'replace element', and 'update element' (Fdhila et al., 2012; Rinderle-Ma et al., 2008). The 'insert pattern' inserts a new element into a business process at a defined place. The 'delete pattern' removes an existing element. The 'replace pattern' replaces an existing element with a new one. The 'update pattern' modifies an attribute of an existing

element (Fdhila et al., 2012). These change patterns can be applied to all kinds of elements in the integrated compliance graph.

As outlined in the introduction section, we focus this study on the impact of the change patterns ‘replace element’ and ‘delete element’, since their resulting influences on compliance can be derived directly from information of the integrated compliance graph *G*. Of course, the mentioned change patterns can also have an impact on business activities and/or IT components. However, we do not take these into account, as they are not part of a focused compliance investigation, but rather of a business impact analysis e.g. (Radeschütz et al., 2015).

The analyses differ depending on the change pattern applied. In the case of a replacement, existing compliance requirements have an effect on the changed element. In the case of a deletion, the change to process-/IT-elements has an effect on the relevance of existing compliance requirements. Consequently, the change patterns ‘replace’ and ‘delete’ lead to different cause and effect relationships. Figure 4 refers to

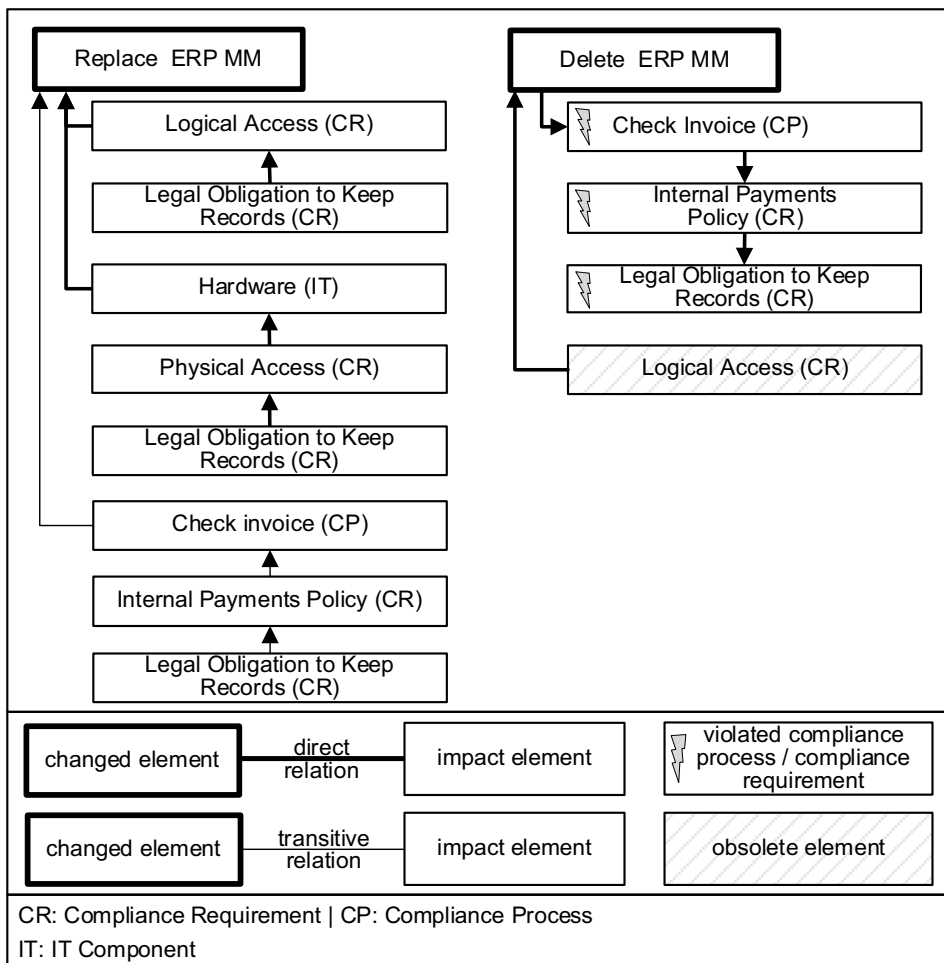


Figure 4. Compliance requirements when replacing and compliance violations when deleting ‘ERP MM’.

our example model and shows the compliance demands when replacing the IT component 'ERP MM'. Further, it shows compliance violations and obsolete compliance requirements when removing 'ERP MM'.

5.2. Replacing an element

In order to satisfy related compliance requirements, the replaced element must fulfil the related compliance requirements and if necessary be able to execute a related compliance process. In this case, compliance requirements as well as compliance processes may place conditions on elements, which in turn must be taken into consideration by the element replacing the old one. There are direct and transitive relations between a compliance requirement and the replaced element.

A direct relation between compliance requirements and replaced IT components occurs in two different ways. First, it is necessary to consider any compliance requirement that is directly related to the replaced element. Within our example, model the compliance requirement 'logical access' is directly related to the replaced IT component 'ERP MM'. Consequently, the compliance requirement 'legal obligation to keep records' is also directly related, since it is a prerequisite of 'logical access'. Second, all compliance requirements of the replaced element prerequisites must also be taken into consideration. Within the motivation scenario, the compliance requirement 'physical access' is directly related to the replaced element 'ERP MM' because it is a prerequisite for the IT component 'hardware', which is, in turn a prerequisite for 'ERP MM'.

A transitive relation between an updated IT component and a compliance requirement (or respectively a compliance process) also occurs in two different ways. First, the changed IT component can be a prerequisite of a business activity that is affected by at least one compliance requirement. Within the example model, this is the case at the compliance process 'check invoice' whose prerequisites are the compliance requirements 'internal payments policy' and 'legal obligation to keep records'. Second, the replaced IT component is a prerequisite of a compliance process that satisfies at least one compliance requirement.

Basically, the result when replacing an IT component (as shown in [Figure 4](#)) is automatically generated by a forward and backward search. The search is performed on the integrated compliance graph G and takes the different node types into account. Since we defined all possible interrelations between the different node types, the identification of demanding compliance requirements is based on fixed search strategies, which depend on the type of changed node. [Figure 5](#) shows the corresponding algorithm to determine compliance requirements when replacing an IT component.

The algorithm in [Figure 5](#) can be described as follows. First, all compliance requirements directly related to the replacement of an IT component are identified and all previous IT components are determined. Second, all compliance requirements that are directly related to the previous IT components are identified as well. Third, to identify all transitively related compliance requirements, we define all business activities and compliance processes supported by the replaced IT component. This also includes IT components that are a prerequisite for IT components that in turn directly support business activities and compliance processes.

Input: Graph g , element that shall be replaced $\{n \in g \mid n_type(n) = \text{IT component}\}$
<pre> 1 // get all direct related compliance requirements and compliance processes to n 2 preds_n = get_all_predecessor(n, type(pred_n)=compliance requirement OR compliance process) 3 Foreach i in (preds_n) do 4 L mark i as direct AND add i including all vertices between i und n to result 5 // get all transitive related compliance processes and compliance requirements to n 6 Foreach it in (get_all_leafs(n, type(leaf_n)=it component)) do 7 Foreach activity in (get_all_direct_successor(it, type(suc_it)= business process)do 8 Foreach cr in (get_all_direct_predecessor(activity, type(pred_activity)=compliance requirement) do 9 i = get_all_predecessor(cr) 10 L mark it, activity, cr and i as transitiv AND add to result 11 Foreach complianceprocess in (get_all_direct_successor(it, type(dir_suc)=compliance process) do 12 Foreach cr in (get_all_direct_successor(complianceprocess, type(cp)=compliance requirement) do 13 i = get_all_predecessor(cr) 14 L mark it, complianceprocess, cr and i as transitiv AND add to result generate result_graph based on g and result </pre>
Output: Graph $result_graph$

Figure 5. Algorithm to automatically determine compliance requirements when replacing an IT component.

5.3. Deleting an element

The removal of an element can affect compliance in two different ways. On the one hand, any deletion can impact compliance requirements and/or compliance processes that are related to the deleted element. On the other hand, the deletion of an element can result in an affected compliance requirement becoming obsolete.

In our motivating example, the removal of the IT component ‘ERP MM’ leads to the non-executability of the compliance process ‘check invoice’. Consequently, the compliance requirements ‘internal payments policy’ and ‘legal obligation to keep records’ are violated. In addition, the removal makes the compliance requirement ‘logical access’ obsolete because it only affects the d IT component ‘ERP MM’. However, the superior compliance requirement ‘legal obligation to keep records’ does not become obsolete, as it is still the prerequisite of the compliance requirements ‘physical access’ and ‘internal policy’.

As with the replacement method, the method for automatically identifying the effects of the element deletion on compliance is based on a backward and forward search in graph G . The search strategy depends on the deleted element type. Figure 6 shows the corresponding algorithm.

The algorithm in Figure 6 can be described as follows: First, to determine compliance violations when removing an IT component, we identify all compliance processes supported by the component. This includes both an implicit and explicit support. Second, we determine all compliance requirements that are satisfied by the supported compliance process. Third, to obtain all obsolete compliance requirements when an IT component is deleted, three major steps are done.

In step 1, we determine all succeeding IT components of the deleted IT component. In step 2, we determine all previous IT components of the deleted IT component until none of these predecessors support a component that is not an implicit predecessor of the deleted one. In step 3, for each IT component identified and the deleted IT component, we determine all related compliance requirements including all of their associated child elements. We check systematically whether each of the identified compliance requirements also affect an element other than the deleted IT component and the IT components identified in steps 1 and 2. If this is not the case, we mark them as obsolete.

<pre> Input: Graph g, element that shall be removed {n ∈ g n_type(n) = IT component} 1 // get all violated compliance requirements 2 Foreach it in (get_all_leafs(n, type(leaf(n))=it component) do 3 Foreach cp in (get_all_direct_successor(it, type(suc(it))=compliance process) do 4 Foreach cr in (get_all_direct_successor(cp, type(suc(cp))=compliance requirement) do 5 i = get_all_predecessor(cr) 6 mark cr and i as violated AND add to result 7 // get all obsolete compliance requirements 8 add n to list_it 9 Foreach if in (get_all_successor(n, type(suc(n))=it component) do 10 If (it only requires n) 11 add it to list_it 12 Foreach it in (get_all_predecessor(n, type(pred(n))=it component) do 13 If (it only supports n) 14 add it to list_it 15 Foreach it in (list_it) do 16 Foreach cr in (get_all_direct_predecessor(it, type(pred(it))=compliance requirement) do 17 If (get_all_direct_successor(cr)==it) 18 mark cr as obsolete AND add to result 19 Foreach cr2 in (get_all_predecessor(cr), type(pred(cr))=compliance requirement) do 20 If (cr2 hasn't other direct successor than get_all_predecessor(cr, type(cr)=comp.req.) 21 mark cr2 as obsolete AND add to result 22 generate result_graph based on g and result Output: Graph result_graph </pre>
--

Figure 6. Algorithm to automatically determine compliance violations and obsolete compliance requirements when deleting an IT component.

6. Propose compliant business process models

In this section, we present a method that recommends compliant business process models at design time in response to compliance violations (Seyffarth et al., 2019). The compliance violations are caused by replacement or deletion at design time. The method automatically generates adaptation proposals for non-compliant business processes and thus addresses RQ2. First, we present a running scenario. Second, we present a method to recommend compliant business processes and thus operationalise the running scenario.

6.1. Running scenario

As a continuation of our example model, Figure 7 shows different variants of a purchase to pay process that complies with the requirement ‘internal payments policy’. The compliance processes shown in Figure 7 are, of course, not complete, but can easily be extended if new ideas or opportunities arise. The alternative compliance processes shown on the left side lead to different compliant business processes on the right side. The compliance processes included in the purchase to pay processes differ according to their triggers and execution requirements.

6.2. Modelling alternative compliance processes

In general, the modelling of alternative compliance processes during design time of the business process model (e.g. (Kittel et al., 2013; Sackmann & Kittel, 2015; Schumm et al., 2010b)) is based on two ideas:

- The differentiation of alternative compliance processes based on their properties, and

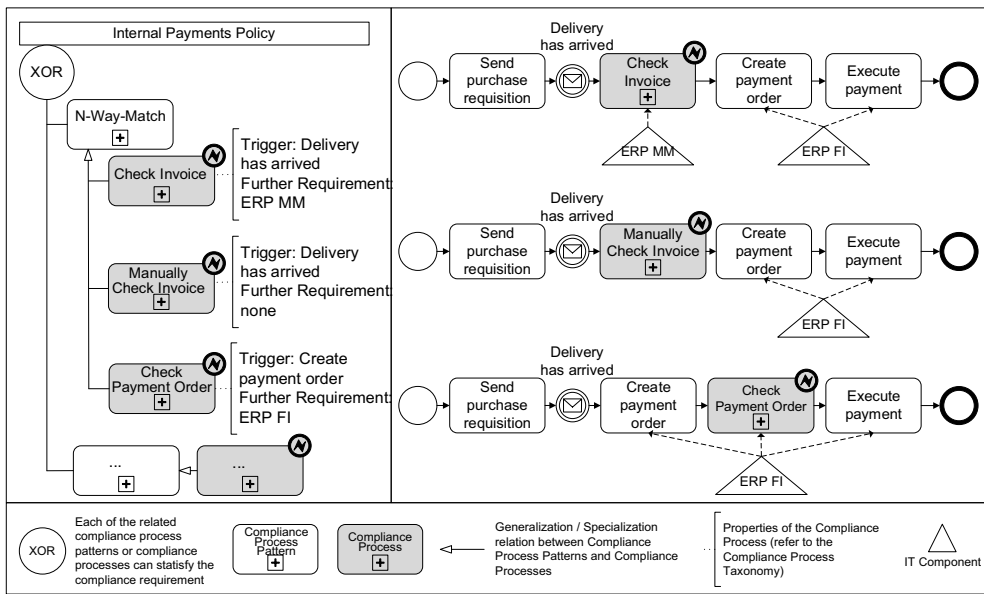


Figure 7. Alternative compliance processes and proposed compliant purchase to pay processes (based on (Seyffarth et al., 2019)).

- The generalisation of alternative compliance processes in one so-called compliance process pattern.

6.2.1. Properties of a compliance process

Each compliance process may have different properties, such as different triggers, execution requirements or execution types. In (Seyffarth et al., 2017a) we proposed a compliance process taxonomy that enables the categorisation of compliance processes based on their characteristics. Thus, it is possible to differentiate (alternative) compliance processes by means of 3 meta-characteristics and 37 sub-characteristics in 9 dimensions. Even though the taxonomy allows for a theoretical differentiation of compliance processes, their specific modelling and instantiation always depend on the conditions of the respective company. For example, the content and number of compliance requirements, or the degree of automation determine the type and number of available alternative compliance processes.

In the following, we present several characteristics and dimensions whose understanding is necessary for the further course of argumentation. A complete discussion of all characteristics and dimensions can be found in (Seyffarth et al., 2017a). The meta-characteristic ‘integration constraint’ specifies requirements for the integration of a compliance process into a business process. One dimension within these meta-characteristic is the dimension ‘trigger’. A trigger initiates the integration of a compliance process into a business process to meet a compliance requirement.

Another dimension of ‘integration constraint’ is ‘further requirements for execution’, which specifies the dependency of process execution on various characteristics, such as the existence of an IT component. Besides other features, the meta-characteristic

'modelling' includes patterns for modelling compliance processes. The meta-characteristic 'property' allows for differentiation compliance processes based on their timing, degree of automation or process type. These properties may depend on other dimensions and characteristics of the compliance process taxonomy, such as the type of execution, which can be either fully automated, fully manual or manual, but IT dependent.

6.2.2. Compliance process patterns as a generalisation of compliance processes

As a basis for modelling alternative compliance processes we use the compliance process patterns proposed in (Namiri & Stojanovic, 2007; Schultz, 2013). In general, patterns are high-level domain-specific templates used to represent desired properties and constraints (Turetken et al., 2011). Consequently, we define a compliance process pattern as a process template that contains process elements (e.g. activities, gateways and connectors) that are necessary to satisfy at least one compliance requirement. Examples of such compliance process patterns includes the 'second set of eyes' pattern, the 'separation of duties' pattern or document patterns such as an 'N-way-match' that compares different text values.

On a general level, the compliance requirement 'internal payments policy' from Figure 7 can be satisfied by a compliance process pattern of type 'N-way-match'. In our example, the level of detail of this pattern is increased by specifying three corresponding compliance processes, which differ in their characteristics. Consequently, the three alternative compliance processes 'check invoice', 'manually check invoice' and 'check payment order' in Figure 7 can each be used to ensure the requirement 'internal payments policy' and represent specialisations of the compliance process pattern 'N-way-match'.

6.3. Query compliance processes and integrate them into the business process model

For further explanations, we first define a data structure that contains compliance requirements, compliance process patterns and associated compliance processes. The data structure can be used to represent the alternative compliance processes shown in Figure 7. Second, we describe a method that (1) queries suitable compliance processes from these data structures and (2) integrates them into the business process model.

Definition 6 (Alternative Compliance Process Graph). We define a directed graph $AG = (N^{AG}, E^{AG}, n_{identify}^{AG}, n_{type}^{AG}, n_{rule}^{AG})$. In addition, N^{AG} is a nonempty finite set of nodes and an edge e_{ij}^{AG} is considered to be directed from n_i^{AG} to n_j^{AG} .

The node type of n_i^{AG} is specified by the function $n_{type}^{AG}(n_i^{AG})$ and represents the node types that can occur in the alternative compliance process graph.

$$n_{type}^{AG}(n_i^{AG}) = \begin{cases} Compliancerequirement(CR) \\ Complianceprocesspattern(CPP) \\ Complianceprocess(CP) \end{cases}$$

In accordance with Definitions 1–5, the nodes of AG can be of the type of compliance requirement (CR), compliance process pattern (CPP), or compliance process (CP). To

ensure adherence to the data structure of the AG (as shown in Figure 7), we restrict the allowed edges between the defined node types as follows

$$E^{AG} = \left\{ \left(\left(n_i^{AG} | n_{type}^{AG} (n_i^{AG}) = CPP \right), \left(n_j^{AG} | n_{type}^{AG} (n_j^{AG}) = CR \right) \right); \right. \\ \left(\left(n_k^{AG} | n_{type}^{AG} (n_k^{AG}) = CP \right), \left(n_l^{AG} | n_{type}^{AG} (n_l^{AG}) = CR \right) \right); \\ \left(\left(n_m^{AG} | n_{type}^{AG} (n_m^{AG}) = CPP \right), \left(n_n^{AG} | n_{type}^{AG} (n_n^{AG}) = CPP \right) \right); \\ \left. \left(\left(n_o^{AG} | n_{type}^{AG} (n_o^{AG}) = CP \right), \left(n_p^{AG} | n_{type}^{AG} (n_p^{AG}) = CPP \right) \right) \right\}$$

Accordingly, only edges between CR and CPP, CR and CP, CP and CPP, as well as CPP and CPP are allowed.

The function $n_{identify}^{AG}(n_i^{AG})$ assigns a unique identification (ID) to each node n_i^{AG} , the function $n_{rule}^{AG}(n_i^{AG})$ assigns a rule to each node n_i^{AG} . Each rule includes a trigger, a business activity prior to which the compliance process was executed and required IT components. Each element of the rule must be named after the name of the corresponding business activities and IT components. We are aware that this can lead to naming ambiguities. In the literature there are already approaches to tackle this challenge in business processes (e.g. (Klinkmüller & Weber, 2017; Leopold et al., 2015)). However, a first simple solution to this challenge is a tool support, which specifies the appropriate elements based on existing process models and IT architecture models.

As Figure 8 shows, the query of alternative compliance processes starts at n_i^{AG} , which represents the compliance process that is no longer executable. Within AG, we first search for alternative compliance processes. These compliance processes are modelled as sibling nodes of n_i^{AG} where $n_{type}^{AG} = CP$. Next, the rule or integration constraints of each sibling node must be checked against the business process to investigate if the sibling nodes found can be integrated into the business process PG. In our case, the integration constraints include the presence or absence of both business activities and IT components. Hence, we consider the control flow and resource perspective of a process.

The method for querying alternative compliance processes is based on three steps. In order to check the executability of each alternative compliance processes n_i^{AG} in AG, we

<pre> Input: alternative graph ag, result graph rg, process graph pg 1 // get all violated compliance processes 2 foreach cp in (get all violated compliance processes in rg) do 3 // get all alternative compliance processes 4 foreach sibling_cp in (get sibling compliance processes of cp) do 5 // check the executability of alternative compliance process 6 req_it = sibling_cp.getRequiredIT 7 trigger = sibling_cp.getTrigger 8 if (req_it OR req_it.predecessor not in rg) AND (trigger not in rg) 9 add sibling_cp to alternatives 10 // search for compliance process patterns 11 if (alternatives is empty) 12 add get_all_successor(cp, type(suc_cp)=compliance process pattern) to alternatives 13 // integrate alternative cp into the business process graph pg 14 foreach element in alternatives do 15 bp = pg 16 removeViolatedComplianceProcess from bp 17 integrate element in bp 18 add bp to compliantBusinessProcesses Output: list process_graph compliantBusinessProcesses </pre>

Figure 8. Algorithm to propose compliant business process models.

first check their integration constraints against the result graph. As discussed in [Section 5.3](#) the result graph, is calculated when an element is deleted. It contains the deleted element, the violated compliance requirements or compliance processes and obsolete compliance requirements. In the second step, a compliance process is classified as executable if the triggering business activity is not deleted. It is further executable if the required IT component is not deleted or if the required IT component is not a predecessor of the deleted IT component. To check these conditions, in the third step we look at whether the trigger or the required IT component are part of the result graph. If this is the case for at least one of the conditions, the compliance process cannot be integrated into the business process.

If there is no appropriate compliance process, we perform a second search, one for appropriate compliance process patterns. Accordingly, we search for successors of n_i^{AG} that are of the type 'compliance process pattern'. Finally, each query can lead to three possible results: one alternative compliance process, more than one alternative compliance process or no alternative compliance process.

We propose a solution for each case. In the case of one alternative compliance process, exactly one adapted business process is proposed. If there are numerous alternative compliance processes, our method queries all alternative compliance processes and thus proposes more than one adapted business process, as is the case in our example. Subsequently, the user decides which process adaptation should be made. If no suitable compliance process is available, our method proposes a generic compliance process pattern. In this case, the compliance pattern is integrated in place of the former compliance process. Subsequently, the compliance process pattern must be specified syntactically and semantically for practical use.

7. Evaluation

The goal of DSR is to solve identified organisational problems. Since the evaluation of design-oriented studies serves to assess the usefulness of solution artefacts (March & Smith, 1995), it is essential to evaluate the usefulness of our solutions (Hevner et al., 2004). Consequently, we evaluated the perceived usefulness of our decision support approach with domain experts. For such an expert evaluation, knowledge of the requirements that are placed on a method to assess the perceived usefulness is very important. We demonstrated the application of our solution artefacts with a software prototype. In addition to our algorithms introduced in [Section 6](#), the demonstration also takes into account the necessary requirements, such as the modelling of alternative compliance processes.

[Section 7](#) is divided into two logical parts. First, we apply the Framework for Evaluation in Design Science Research (FEDS) (Venable et al., 2016) to specify appropriate evaluation episodes of our DSR project. Second, we present a case study based on which domain experts evaluate the perceived usefulness of our approaches.

7.1. Evaluation strategy based on FEDS

Basically, FEDS (Venable et al., 2016) consists of three dimensions: (1) functional purpose of evaluation, (2) paradigm of the evaluation study and (3) evaluation strategies. (Venable

et al., 2016) recommend the evaluation strategy ‘technical risk and efficacy’, if an evaluation with real users and real systems in a real setting is only possible with tremendous effort. Based on this strategy, we conducted four evaluation episodes in line with our research project, with the first three episodes being artificially formative. They are also preparative for the final evaluation in episode 4, which is naturalistically summative (see Table 2). Within the artificial evaluation paradigm, we applied the evaluations methods ‘literature review’ and ‘prototyping’. Within the naturalistic evaluation we performed a case study based on a proof-of-concept implementation called ‘BCIT’.

In evaluation episode 1 we derived both the elements of the compliance meta-model and the dimensions and characteristics of the compliance process taxonomy from the literature. Thus, both artefacts were artificially evaluated ex ante (Sonnenberg & Vom Brocke, 2012) and meet the ending conditions according to (Nickerson et al., 2013).

In evaluation episode 2, we demonstrated the feasibility of an integrated graph G which includes compliance requirements, business activities, compliance activities and IT components. Further, we demonstrated the identification of compliance demands and violations through a prototypical implementation of the corresponding algorithms. (March & Storey, 2008) referred to this as prototyping suitable evaluation methods for demonstrating the feasibility of artefacts. The result of this evaluation episode is the tentative proof-of-concept implementation ‘BCIT’ (Seyffarth & Raschke, 2018), which we presented at an international conference and discussed with peers of the BPM community.

In evaluation episode 3, we extended the tentative proof-of-concept of the previous evaluation episode. We added the functionality to provide adaption proposals for business processes following the identification of compliance violations (Seyffarth & Raschke, 2020). The prototype uses the adapted graph search algorithms introduced in Section 6. In general, graph search techniques are well known in computer science and their operation is widely proven (Aleliunas et al., 1979; Rosenkrantz et al., 1977). Thus, the aim is not to evaluate the formal correctness of the established graph search methods we use, but rather their usefulness for identifying compliance violations and alternative compliance processes in the context of the given problem.

Figure 9 shows the identified compliance violations when removing an IT component from the advanced prototype ‘BCIT’. A proposed compliant business process by ‘BCIT’ is shown in Figure 10. A tutorial document, a screencast and two demo projects for ‘BCIT’ are available on the following GitHub repository: <https://github.com/tobiasseyffarth/bcit/>.

In evaluation episode 4, we performed a naturalistic summative evaluation. We used the goal question metric approach (Basili, 1992) for formulating the evaluation goal: The aim of the evaluation is to determine the perceived usefulness and relevance (purpose) of our solution artefacts by means of the advanced proof-of-concept implementation BCIT from the perspective of domain experts. In order to reach this goal, we followed the recommendations of (Hevner et al., 2004; Sonnenberg & Vom Brocke, 2012) and conducted a case study with a subsequent expert survey.

7.2. Case study design and results

In this section, we briefly present the case study structure, the test design, our questionnaire and our sample. In order to document the data collection and the analysis in a comprehensible way (Foster & Deardorff, 2017), the questionnaire and



Table 2. Evaluation episodes in the research project.

#	Functional Purpose	Paradigm of Evaluation Study	Focus of Evaluation	Applied Evaluation Method	Evaluation Result
1	Formative	Artificial	Compliance meta model, compliance process taxonomy	Ex ante evaluation (Literature review)	Meet ending conditions according to (Nickerson et al., 2013)
2	Formative	Artificial	Methods to create the analyse graph and compliance requirements/compliance violations	Prototyping and discussion with peers	Tentative proof-of-concept BCIT
3	Formative	Artificial/Naturalistic	Method to recommend compliant business processes	Prototyping and discussion with peers	Advanced proof-of-concept BCIT
4	Summative	Naturalistic	Extension of Proof-of-concept BCIT	Case study with domain experts	Perceived usefulness of BCIT

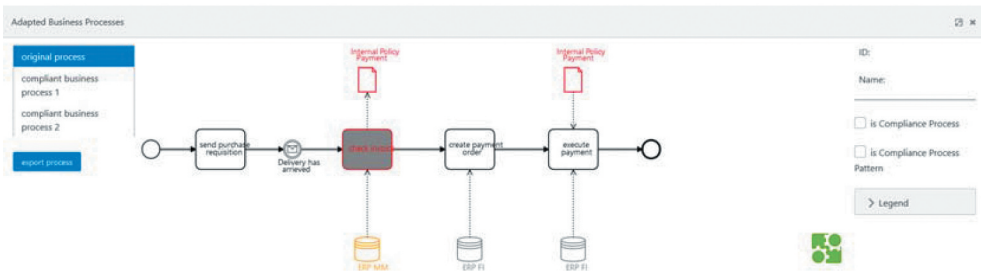


Figure 9. Violated compliance requirement when removing an IT component.

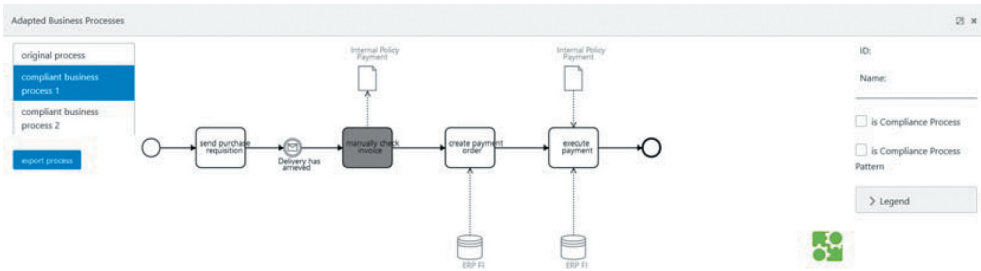


Figure 10. Compliant business process including the alternative compliance process ‘manually check invoice’.

all answers are also available on our GitHub project page: <https://github.com/tobiasseyffarth/bcit/tree/master/resources/3-evaluation>. Subsequently, we discuss the evaluation results and threats to validity. Inspired by (Runeson & Höst, 2009), we structured the case study in four parts:

- (1) *Objective of the case study.* As previously stated, the goal of our case study is to evaluate the perceived usefulness and relevance of our proof-of-concept implementation of ‘BCIT’.
- (2) *Frame the knowledge and present the cases.* Based on a case study, we explained the (research) problem to the test persons and presented our basic ideas for its solution.
- (3) *Demonstration of BCIT.* We exemplarily demonstrated BCIT’s graph search algorithms and process adaptation procedures for solving the problem presented in the case study.
- (4) *Collect data.* Following (Kriglstein et al., 2016; Runeson & Höst, 2009), we used questionnaires to obtain expert estimations of the perceived usefulness of BCIT.

7.2.1. Questionnaire and respondents

The construct of perceived usefulness is widely used for evaluating software artefacts and is part of various models, such as the Technology Acceptance Model (TAM), integrated models of TAM and the Theory of Planned Behaviour (TPB), and numerous extensions of these model types (Cheng, 2019; Hess et al., 2014). Science has already expressed strong

criticism of TAM. In the literature, e.g. the lack of contextual factors and external predictors is complained about (Marangunić & Granić, 2015), the importance of the construct Ease of Use is questioned (Yousafzai et al., 2007), and the general conception of the model is scrutinised (Cheng, 2019; Yousafzai et al., 2007). However, to the best of our knowledge and belief, the construct of perceived usefulness itself is not subject to criticism and is still frequently used for evaluating design-oriented research in general (see, e.g. (Sturm & Sunyaev, 2019), (Coenen et al., 2018; Santos & Alves, 2017)) and for decision support systems in particular (see, e.g. (Buchert et al., 2019; Kramer et al., 2017; Mican et al., 2020)). With regard to the objective of our case study, external predictors, contextual factors, and the construct Ease of Use are not relevant to our evaluation. Therefore, in accordance with our evaluation strategy according to (Venable et al., 2016) and their requirements for summative evaluations, we do not focus on TAM, TPB, or their extensions in our summative evaluation, but rather on specifically measuring the perceived usefulness of BCIT. The standard questionnaire for evaluating the perceived usefulness consists of ten statements (Davis, 1985). These statements are assigned to specific clusters which are related to the following usefulness aspects (Seeliger et al., 2019): (A) job effectiveness, (B) productivity and time savings, (C) importance of the system to the users' job, (D) control over the job and (E) overall assessment.

The statements were evaluated by experts on a Likert scale ranging from 'strongly disagree' (-3) to 'strongly agree' (3). It was also possible to comment on each statement or to reply with 'not specified' (abstention). In addition, the participants had the opportunity to make final comments on the questionnaire, the case study or BCIT in a blank comment field.

Before the actual case study took place, we pre-tested the questionnaire with four people having profound knowledge of research methods and the research field (three PhD students and one postdoctoral researcher). The pre-test gave an indication about the required time frame for the case study and the time to complete the questionnaire. Moreover, we corrected several ambiguities and minor mistakes in the questionnaire and created its final version.

We performed the case study 8 times with a total of 41 participants. The completion of the questionnaire was voluntary which led to 24 completed questionnaires (response rate: 58%). Table 3 contains the statements and the aggregated results including the arithmetic mean, standard deviation, median and the number of responses.

Additionally, we collected socio-demographic data on a voluntary basis, such as the job role or work experience. The majority of the participants worked in large companies and mainly in the financial and IT service sectors. A few worked in a large German research organisation or in small consulting companies. The participants worked in the field either of compliance (e.g. head of internal audit, chief compliance officer, IT risk manager and auditor), business process management (e.g. head of process management, process manager) or IT architecture management (e.g. IT architect, IT project manager). The working experience ranged from 4 to 32 years.

7.2.2. Discussion of the evaluation results

Figure 11 illustrates the distribution of the experts' voting results for the statements S1 to S10 using box plots. In addition, the box plots were categorised into the clusters A to E. We interpreted S10 and S6; all other box plots shown in Figure 11 are

Table 3. Statements and aggregated results of the perceived usefulness evaluation.

Statement (S)	Cluster	Mean	Standard Deviation	Median	Number of responses
S1: Using BCIT improves the quality of the work I do.	A	1.043	1.574	2	23
S6: Using BCIT improves my job performance.	A	0.455	1.437	1	22
S8: Using BCIT enhances my effectiveness on the job.	A	0.409	1.586	1	22
S3: BCIT enables me to accomplish tasks more quickly.	B	0.727	1.420	1	22
S5: Using BCIT increases my productivity.	B	0.429	1.466	0	21
S7: Using BCIT allows me to accomplish more work than would otherwise be possible.	B	0.609	1.635	1	23
S4: BCIT supports critical aspects of my job.	C	1.318	1.394	2	22
S9: Using BCIT makes it easier to do my job.	C	0.522	1.559	1	23
S2: Using BCIT gives me greater control over my work.	D	1.000	1.826	2	24
S10: Overall, I find BCIT useful in my job.	E	1.083	1.441	1.5	24

A: job effectiveness | B: productivity and time savings | C: Importance of the system to the users' job | D: control over the job | E: overall assessment

to be interpreted analogously. A look at the box plot of S10 (overall usefulness) shows that BCIT was generally evaluated positively. Even though the assessment of S10 covers the entire spectrum of possible answers, the interquartile range is still in the positive area of the Likert scale. Further, 75% of the participants agreed with statement S10. Looking at the results of S6 (job performance), outliers appear at both ends of the scale.

The majority of the participants liked the idea of modelling the relations between compliance requirements, business processes and IT components, because it provides the basis for an integrated model. They stated that the integrated model increases the transparency of their workflow as well as the associated technical and legal dependencies. This opens up new potentials for detailed root cause analyses, which can result in a competitive advantage. These comments also correspond to the results for S4 (support of critical aspects) and S2 (control over the job).

However, some participants pointed out that the effort for both modelling the business/compliance processes and the IT architecture was too high in comparison to the expected benefit. This is also a possible explanation for the poorer ratings on productivity (S5), performance (S6), and effectiveness (S8) compared to increasing quality (S1) and greater control (S2).

7.2.3. Threads to validity

Following (Runeson & Höst, 2009; Wohlin et al., 2012), we discuss several aspects of validity to acknowledge the limitations of our study. Construct validity denotes that the variables of interest are measured correctly. The construct we were interested in was the perceived usefulness. Since this construct has been used for several decades and has proven its worth in numerous studies, construct validity can be taken for granted.

The internal validity is of concern when causal relations are examined. Since we did not examine any causal relationships in our evaluation, the internal validity is of rather minor importance. Nevertheless, there is a risk that the variable being investigated may be affected by other neglected factors. To address this problem, we explained the case study in detail to all participants and made sure that there was a consistent knowledge base.

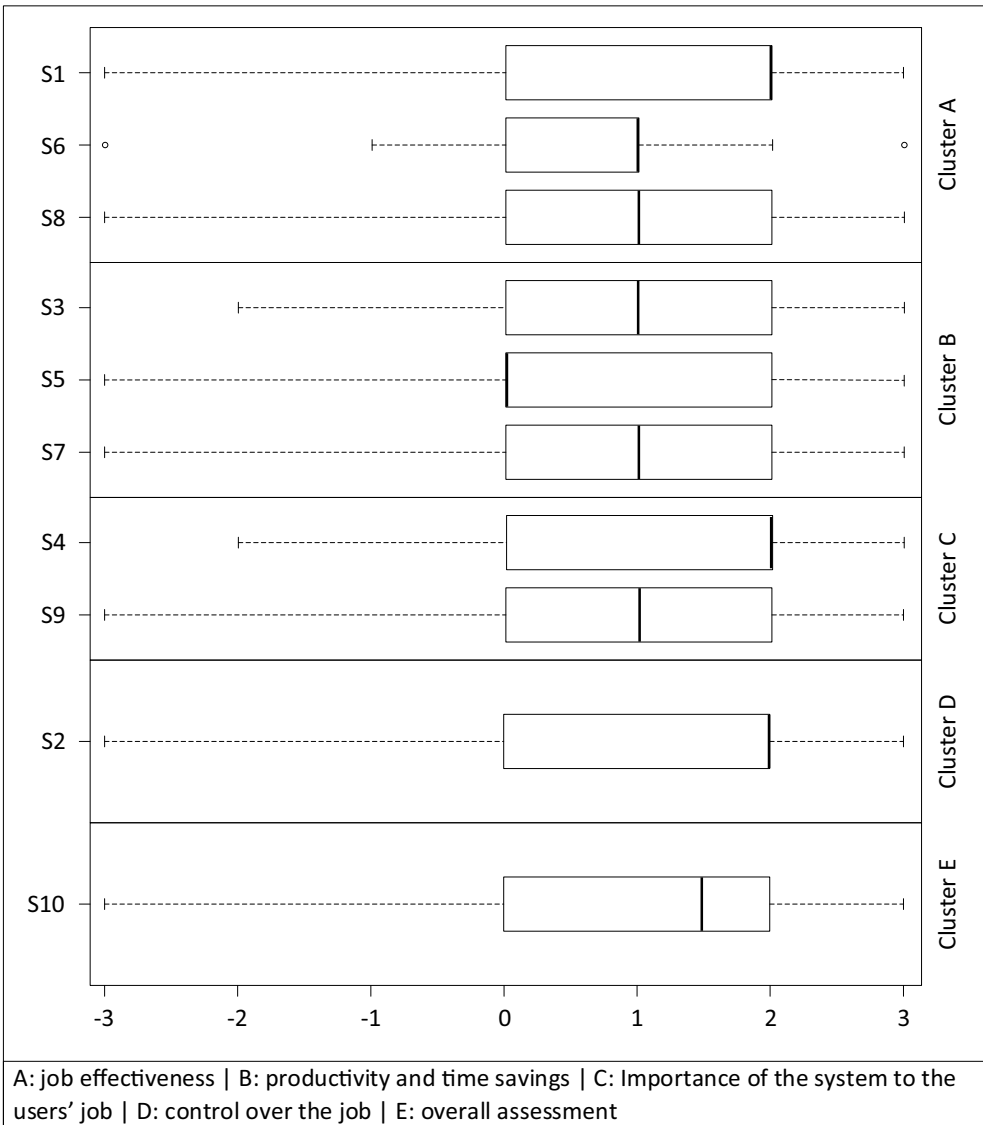


Figure 11. Overview of the perceived usefulness assessment of BCIT.

Furthermore, the skills of the participants involved in the experiments can be assumed to be appropriate due to their professional roles.

The external validity concerns the generalisability of our evaluation results. We interviewed participants with different positions and experiences from different companies and industries to address generalisability. Of course, the generalisability of the results could have been further improved by choosing a larger sample with additional participants from other companies and industries.

The conclusion validity is concerned with the relationship between the treatment and the outcome. We used the well-known questionnaire of (Davis, 1985) to measure

perceived usefulness with Likert scales in our evaluation for ensuring this relationship.

8. Implication for research and practice

In this paper, we presented methods for the identification of compliance requirements and compliance violations in case of replacing or removing an element. Further, we presented a method that recommends adaptations of business process models following compliance violations. We demonstrated the feasibility of our methods in the proof-of-concept implementation called BCIT. From these contributions, implications for research and practice can be derived.

For research, there are implications to the descriptive and prescriptive knowledge base (Gregor & Hevner, 2013). Contributions to the descriptive knowledge base are the identified research gap, and the compliance meta-model in order to conceptualise our domain. The contribution to the prescriptive knowledge base includes the methods to identify compliance violations and propose compliant business process models.

Despite the fact that compliance processes have to be modelled and instantiated individually in each organisation due to specific conditions, our solution artefacts have a general impact on practice. First, the explicit modelling of compliance requirements, business processes and IT components in an integrated model enhances the transparency of an enterprise architecture. The identified effects on compliance when changing business processes and IT components are therefore supported by factual evidence and can be used to support decisions. This support can also be further improved by allowing different scenarios to be tested quickly and cost-effectively. Second, a separate compliance view, which includes compliance processes, allows for thinking in alternatives. Just as business processes can be stored in a repository, alternative compliance processes can also be stored centrally and connected to their respective compliance requirements. Consequently, the repository can be used to identify a kind of best-practice compliance processes.

9. Conclusion

Compliance requirements can place demands on both business activities and IT components. In case of replacing and removing one of these elements, the demanding and violated compliance requirements have to be identified. If a business process violates a compliance requirement, an adaption needs to be initiated to re-establish compliance conformity. In order to solve this challenge, we presented three contributions. First, we presented methods for determining the interactions between requirements and the consequences on compliance when replacing or removing a business activity, an IT component or another compliance requirement. Second, we developed the proof-of-concept BCIT, which shows the feasibility of our methods. Third, we presented the results of a case study followed by an expert survey that confirmed the perceived usefulness of our methods and BCIT.

A prerequisite for the applicability of our method is the availability of corresponding information from existing design-time models, whose level of detail is company-specific. The availability of models, their levels of detail and the amount of information influences

how many solutions for compliance violations can be offered by our algorithm. The amount of information and, thus, the amount of available alternative compliance processes naturally increases over time. It is foreseeable that additional information will be gained through a long-term use of our approach/tool, thus extending its applicability. A central compliance process repository, similar to existing process fragment repositories, e.g. (Schumm et al., 2011), is a promising approach for the further development and joint use of compliance processes.

Further, naming ambiguities between the business process and the rule of the compliance process is currently an open topic. Currently, we bypass this challenge with the tool-support of BCIT.

We focused on the compliance change patterns ‘replace’ and ‘delete’, as their impact on compliance can be determined based on previously modelled dependencies between compliance requirements, business processes and IT components. An extension of the presented approach for further patterns is a research desideratum, as the impact of patterns such as ‘insert a (possibly prohibited) new element’ or ‘update attributes of an element’ on compliance cannot be derived exclusively by means of information from the underlying design-time models. Accordingly, further sources of information would have to be consulted to broaden our approach.

Besides considering further views on business processes, such as a data and organisational views, it is also possible to take into account additional parameters, such as effectiveness and costs, as a starting point for further research. Additional parameters allow for, e.g. the choice of alternative compliance processes regarding economic principles. This also enables making economic decisions on the migration to alternative compliant business process models. Beyond that, the idea of modelling alternative compliance processes can also be adopted to a modelling of alternative IT components, which may expand to a part of an alternative IT architecture. An alternative IT architecture can be used to react quickly to changes in the existing IT architecture.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

- Aleliunas, R., Karp, R.M., Lipton, R.J., Lovasz, L., & Rackoff, C. (1979). Random walks, universal traversal sequences, and the complexity of maze problems. In *20th Annual Symposium on Foundations of Computer Science (sfcs 1979)* (pp. 218–223), San Juan, Puerto Rico, USA. <https://doi.org/10.1109/SFCS.1979.34>
- Awad, A. (2007). BPMN-Q: A language to query business processes. In Reichert, M., Strecker, S. & Turowski, K. (Hrsg.), (Eds.), *Enterprise modelling and information systems architectures – concepts and applications* (pp. 115–128). Bonn: Gesellschaft für Informatik e. V.
- Awad, A., Smirnov, S., & Weske, M. (2009). Resolution of compliance violation in business process models: A planning-based approach. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, R. Meersman, T. Dillon, & P. Herrero (Eds.), *On*

- the Move to Meaningful Internet Systems: OTM 2009* (Vol. 5870, pp. 6–23). Springer Berlin Heidelberg.
- Basili, V. (1992). *Software modeling and measurement: The Goal/Question/Metric Paradigm*. University of Maryland, CS-TR-2956, UMIACS-TR-92-96, September 1992.
- Becker, J., Delfmann, P., Dietrich, H.-A., Steinhorst, M., & Eggert, M. (2016). Business process compliance checking – Applying and evaluating a generic pattern matching approach for conceptual models in the financial sector. *Information Systems Frontiers*, 18(2), 359–405. <https://doi.org/10.1007/s10796-014-9529-y>
- Becker, J., Eggert, M., Winkelmann, A., & Knackstedt, R. (2011). Towards a contingency theory based model of the influence of regulation on MIS. In *Americas conference on information systems*, Detroit, Michigan, USA.
- Becker, J., Heddier, M., Braeuer, S., & Knackstedt, R. (2014). Integrating regulatory requirements into information systems design and implementation. In *ICIS 2014 proceedings*, Auckland, New Zealand.
- Buchert, T., Ko, N., Graf, R., Vollmer, T., Alkhayat, M., Brandenburg, E., Stark, R., Klocke, F., Leistner, P., & Schleifenbaum, J.H. (2019). Increasing resource efficiency with an engineering decision support system for comparison of product design variants. *Journal of Cleaner Production*, 210, 1051–1062. <https://doi.org/10.1016/j.jclepro.2018.11.104>
- Cheng, E.W.L. (2019). Choosing between the theory of planned behavior (TPB) and the technology acceptance model (TAM). *Educational Technology Research and Development*, 67(1), 21–37. <https://doi.org/10.1007/s11423-018-9598-6>
- Coenen, T., Coertjens, L., Vlerick, P., Lesterhuis, M., Mortier, A.V., Donche, V., & Ballon, P. (2018). An information system design theory for the comparative judgement of competences. *European Journal of Information Systems*, 27(2), 248–261. <https://doi.org/10.1080/0960085X.2018.1445461>
- Committee of Sponsoring Organizations of the Treadway Commission. (2012). Internal control - integrated framework: framework and appendices.
- Corea, C., & Delfmann, P. (2017). Detecting Compliance with Business Rules in Ontology-Based Process Modeling, in Leimeister, J.M.; Brenner, W. (eds.): *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)*, St. Gallen, 226–240.
- Davis, F. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. MIT.
- Delfmann, P., Steinhorst, M., Dietrich, H.-A., & Becker, J. (2015). The generic model query language GMQL – Conceptual specification, implementation, and runtime evaluation. *Information Systems*, 47(1), 129–177. <https://doi.org/10.1016/j.is.2014.06.003>
- Dreyfus, D., & Iyer, B. (2006). Enterprise architecture: A social network perspective. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (pp. 178a–178a), Kauia, HI, USA. <https://doi.org/10.1109/HICSS.2006.155>
- El Kharbili, M., Medeiros, A., Stein, S., & van der Aalst, W.M.P. (2008). Business process compliance checking: Current state and future challenges. *Modellierung betrieblicher Informationssysteme (MobIS 2008)*, 107–113.
- Elgammal, A., Turetken, O., van den Heuvel, W.-J., & Papazoglou, M. (2010). Root-cause analysis of design-time compliance violations on the basis of property patterns. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, P. P. Maglio, M. Weske, J. Yang, & M. Fantinato (Eds.), *Service-oriented computing* (Vol. 6470, pp. 17–31). Springer Berlin Heidelberg.
- Elgammal, A., Turetken, O., & van den Heuvel, W.-J. (2012). Using patterns for the analysis and resolution of compliance violations. *International Journal of Cooperative Information Systems*, 21(1), 31–54. <https://doi.org/10.1142/S0218843012400023>
- Fdhila, W., Indiono, C., Rinderle-Ma, S., & Reichert, M. (2015). Dealing with change in process choreographies: Design and implementation of propagation algorithms. *Information Systems*, 49(1), 1–24. <https://doi.org/10.1016/j.is.2014.10.004>

- Fdhila, W., Rinderle-Ma, S., & Reichert, M. (2012). Change propagation in collaborative processes scenarios. In *8th international conference on collaborative computing: networking, applications and worksharing (CollaborateCom)*, Pittsburgh, PA, USA.
- Fellmann, M., Thomas, O., & Busch, B. (2011). A query-driven approach for checking the semantic correctness of ontology-based process representations. In: W. Abramowicz (ed) *Business Information Systems: 14th International Conference, BIS 2011* (pp. 62–73). Poznań, Poland, June 15–17, 2011. Proceedings. Springer-Verlag GmbH Berlin Heidelberg, Berlin, Heidelberg.
- Foster, M.E.D., & Deardorff, M.A. (2017). Open Science Framework (OSF). *Journal of the Medical Library Association (JMLA)*, 105(2). <https://doi.org/10.5195/JMLA.2017.88>
- Frank, U., Heise, D., Ulrich, K.H., Ferguson, D.F., Hadar, E., & Waschke, M.G. (2009). ITML: A domain-specific modeling language for supporting business driven IT management. In *Proceeding of the 9th OOPSLA workshop on domain-specific modeling*, Helsinki, Finland.
- Gacitua-Decar, V., & Pahl, C. (2009). Automatic business process pattern matching for enterprise services design. In *2009 world conference on services – II* (pp. 111–118), Bangalore, India . <https://doi.org/10.1109/SERVICES-2.2009.28>
- Ghanavati, S., Amyot, D., & Peyton, L. (2009). Compliance analysis based on a goal-oriented requirement language evaluation methodology. In *17th IEEE international requirements engineering conference* (pp. 133–142), Atlanta, GA, USA. <https://doi.org/10.1109/RE.2009.42>
- Governatori, G., & Sadiq, S. (2009). The journey to business process compliance. *Handbook of Research on Business Process Modeling*, 426–454. <https://doi.org/10.4018/978-1-60566-288-6.ch020>
- Gregor, S., & Hevner, A.R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 37(2), 337–355. <https://doi.org/10.25300/MISQ/2013/37.2.01>
- Halle, S. (2011). Causality in message-based contract violations: A temporal logic “Whodunit”. In *2011 IEEE 15th international enterprise distributed object computing conference, Helsinki, Finland* . <https://doi.org/10.1109/EDOC.2011.21>
- Heckel, R., & Taentzer, G. (2020). *Graph transformation for software engineers: With applications to model-based development and domain-specific language engineering* (1st ed.). Springer eBook Collection. Springer International Publishing; Imprint Springer.
- Hess, T.J., McNab, A.L., & Basoglu, K.A. (2014). Reliability generalization of perceived ease of use, perceived usefulness, and behavioral intentions. *MIS Quarterly*, 38(1), 1–28. <https://doi.org/10.25300/MISQ/2014/38.1.01>
- Hevner, A.R., March, S.T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105. <https://doi.org/10.2307/25148625>
- ISACA. (2013). *COBIT 5: Enabling information*.
- Kittel, K., Sackmann, S., & Göser, K. (2013). Flexibility and compliance in workflow systems: The KitCom prototype. In *Proceedings of the CAiSE'13 Forum at the 25th International Conference on Advanced Information Systems Engineering (CAiSE)* (pp. 154–160), Valencia, Spain.
- Klinkmüller, C., & Weber, I. (2017). Analyzing control flow information to improve the effectiveness of process model matching techniques. *Decision Support Systems*, 100(1), 6–14. <https://doi.org/10.1016/j.dss.2017.06.002>
- Knackstedt, R., Eggert, M., Heddier, M., Chasin, F., & Becker, J. (2013). The relationship of is and law - The perspective of and implications for IS research. *ECIS 2013 Completed Research*. https://aisel.aisnet.org/ecis2013_cr/18/URL
- Knuplesch, D., Fdhila, W., Reichert, M., & Rinderle-Ma, S. (2015). Detecting the effects of changes on the compliance of cross-organizational business processes. In P. Johannesson, M. Lee, S. Liddle, A. Opdahl, & Ó. Pastor López (eds) *Conceptual Modeling. Lecture Notes in Computer Science* (pp. 94–107), Springer, Cham. https://doi.org/10.1007/978-3-319-25264-3_7
- Koetter, F., Kintz, M., Kochanowski, M., Wiryarattanakul, T., Fehling, C., Gildein, P., Wagner, S., Leymann, F., & Weisbecker, A. (2016). An universal approach for compliance management using compliance descriptors. In M. Helfert, D. Ferguson, V. Méndez Muñoz, & J. Cardoso (eds) *Cloud Computing and Services Science: 6th International Conference, CLOSER 2016* (pp. 209–231). Rome, Italy, April 23–25, 2016, Springer International Publishing. Revised Selected Papers. Cham, s.l.

- Koetter, F., Kochanowski, M., Weisbecker, A., Fehling, C., & Leymann, F. (2014). Integrating compliance requirements across business and IT. In *2014 IEEE 18th international enterprise distributed object computing conference*, Ulm, Germany. <https://doi.org/10.1109/EDOC.2014.37>
- Kramer, T., Heinzl, A., & Neben, T. (2017). Cross-organizational software development: Design and evaluation of a decision support system for software component outsourcing. In *Hawaii international conference on system sciences* (pp. 343–352), Puako, Hawaii, United States. <https://doi.org/10.24251/HICSS.2017.041>
- Kriglstein, S., Leitner, M., Kabicher-Fuchs, S., & Rinderle-Ma, S. (2016). Evaluation methods in process-aware information systems research with a perspective on human orientation. *Business & Information Systems Engineering*, 58(6), 397–414. <https://doi.org/10.1007/s12599-016-0427-3>
- Leopold, H., Meilicke, C., Fellmann, M., Pittke, F., Stuckenschmidt, H., & Mendling, J. (2015). Towards the automated annotation of process models. In *International Conference on Advanced Information Systems Engineering* (pp. 401–416), Stockholm, Sweden.
- Marangunić, N., & Granić, A. (2015). Technology acceptance model: A literature review from 1986 to 2013. *Universal Access in the Information Society*, 14(1), 81–95. <https://doi.org/10.1007/s10209-014-0348-1>
- March, S.T., & Smith, G.F. (1995). Design and natural science research on information technology. *Decision Support Systems*, 15(4), 251–266. [https://doi.org/10.1016/0167-9236\(94\)00041-2](https://doi.org/10.1016/0167-9236(94)00041-2)
- March, S.T., & Storey, V.C. (2008). Design science in the information systems discipline: An introduction to the special issue on design science research. *MIS Quarterly*, 32(4), 725–730. <https://doi.org/10.2307/25148869>
- Mican, D., Sitar-Tăuta, D.-A., & Moisescu, O.-I. (2020). Perceived usefulness: A silver bullet to assure user data availability for online recommendation systems. *Decision Support Systems*, 139(1), 113420. <https://doi.org/10.1016/j.dss.2020.113420>
- Namiri, K., & Stojanovic, N. (2007). Using control patterns in business processes compliance. In *WISE 2007 Workshops* (pp. 178–190), Nancy, France.
- Nickerson, R.C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its productservice in information systems. *European Journal of Information Systems*, 22(3), 336–359. <https://doi.org/10.1057/ejis.2012.26>
- Peffer, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). The design science research process: A model for producing and presenting information systems research. In *1st International Conference on Design Science in Information Systems and Technology (DESIRIST)* (pp. 83–106), Claremont, California, USA.
- Radeschütz, S., Schwarz, H., & Niedermann, F. (2015). Business impact analysis—a framework for a comprehensive analysis and optimization of business processes. *Computer Science – Research and Development*, 30(1), 69–86. <https://doi.org/10.1007/s00450-013-0247-3>
- Rinderle, S., Reichert, M., & Dadam, P. (2004). Correctness criteria for dynamic changes in workflow systems: A survey. *Data & Knowledge Engineering*, 50(1), 9–34. <https://doi.org/10.1016/j.datak.2004.01.002>
- Rinderle-Ma, S., Reichert, M., & Weber, B. (2008). On the formal semantics of change patterns in process-aware information systems. In *Proc. 27th Int'l Conference on Conceptual Modeling (ER'08)* (pp. 279–293), Barcelona, Spain.
- Rosenkrantz, D.J., Stearns, R.E., & Lewis, I.P.M.I. (1977). An analysis of several heuristics for the traveling salesman problem. *SIAM Journal on Computing*, 6(3), 563–581. <https://doi.org/10.1137/0206041>
- Rudzaj, P., & Buksa, I. (2011). Business process and regulations: Approach to linkage and change management. In J. Grabis & M. Kirikova (Eds.), *Perspectives in business informatics research* (Vol. 90, pp. 96–109). Springer Berlin Heidelberg.
- Runeson, P., & Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering*, 14(2), 131–164. <https://doi.org/10.1007/s10664-008-9102-8>

- Sackmann, S., & Kittel, K. (2015). Flexible workflows and compliance: A solvable contradiction? In J. Vom Brocke & T. Schmiedel (Eds.), *BPM - Driving innovation in a digital world* (pp. 247–258). Springer International Publishing.
- Sackmann, S., Kühnel, S., & Seyffarth, T. (2018). Using business process compliance approaches for compliance management with regard to digitization: Evidence from a systematic literature review. In *International Conference on Business Process Management (BPM)* (pp. 409–425), Sydney, Australia.
- Sadiq, S., Governatori, G., & Namiri, K. (2007). Modeling control objectives for business process compliance. In G. Alonso, P. Dadam, & M. Rosemann (Eds.), *Business process management* (Vol. 4714, pp. 149–164). Springer Berlin Heidelberg.
- Santos, H., & Alves, C. (2017). Exploring the ambidextrous analysis of business processes: A design science research. In *International conference on enterprise information systems* (pp. 543–566), Porto, Portugal.
- Schultz, M. (2013). Enriching process models for business process compliance checking in ERP environments. *International Conference on Design Science Research in Information Systems*, 120–135, Helsinki, Finland. https://doi.org/10.1007/978-3-642-38827-9_9
- Schumm, D., Turetken, O., Kokash, N., Elgammal, A., Leymann, F., & van den Heuvel, W.-J. (2010a). Business process compliance through reusable units of compliant processes. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, F. Daniel, & F. M. Facca (Eds.), *Current trends in web engineering* (Vol. 6385, pp. 325–337). Springer Berlin Heidelberg.
- Schumm, D., Karastoyanova, D., Leymann, F., & Strauch, S. (2011). Fragmento: Advanced process fragment library. *19th International Conference on Information Systems Development*, Prague, Czech Republic.
- Schumm, D., Leymann, F., Ma, Z., Scheibler, T., & Strauch, S. (2010b). Integrating compliance into business processes: process fragments as reusable compliance controls. *Proceedings of the Multikonferenz Wirtschaftsinformatik* (pp. 10), Göttingen, Germany.
- Seeliger, A., Guinea, A.S., & Mühlhäuser, M. (2019). Process Explorer: Intelligent process mining guidance. *17th International Conference on Business Process Management (BPM), 2019*, (pp. 216–231), Vienna, Austria. https://doi.org/10.1007/978-3-030-26619-6_15
- Seyffarth, T., Kühnel, S., & Sackmann, S. (2016). ConFlex: An ontology-based approach for the flexible integration of controls into business processes. *Proceedings of the Multikonferenz Wirtschaftsinformatik 2016 (MKWI'16), 2016*, (pp. 1341–1352), Ilmenau, Germany.
- Seyffarth, T., Kühnel, S., & Sackmann, S. (2017a). A taxonomy of compliance processes for business process compliance. In *15th international conference on business process management, business process management forum. In: Lecture Notes in Business Information Processing (LNBIP)* (pp. 71–87), Barcelona, Spain.
- Seyffarth, T., Kühnel, S., & Sackmann, S. (2017b). Welche Compliance-Anforderungen sind für Geschäftsprozessänderungen relevant?: Ein Ansatz zur Modellierung der Beziehungen. In *Proceedings of the Informatik 2017, Lecture Notes in Informatics (LNI)* (pp. 1641–1646), Chemnitz, Germany.
- Seyffarth, T., Kühnel, S., & Sackmann, S. (2018). Business process compliance and business process change: An approach to analyze the interactions. In *Business Information Systems. BIS 2018. Lecture notes in business information processing* (pp. 176–189), Berlin, Germany.
- Seyffarth, T., Kühnel, S., & Sackmann, S. (2019). Business process compliance despite change: Towards proposals for a business process adaption. *Information Systems Engineering in Responsible Information Systems. CAiSE 2019. Lecture Notes in Business Information Processing*, 350, 227–239. https://doi.org/10.1007/978-3-030-21297-1_20
- Seyffarth, T., & Raschke, K. (2018). BCIT: A tool for analyzing the interactions between business process compliance and business process change. *Proceedings of the Dissertation Award and Demonstration, Industrial Track at BPM, 2018*, 81–85. http://ceur-ws.org/Vol-2196/BPM_2018_paper_17.pdf

- Seyffarth, T., & Raschke, K. (2020). BCIT: A tool to recommend compliant business processes based on process adaptation. In *Proceedings of the best dissertation award, doctoral consortium, and demonstration & resources track at BPM 2020 co-located with the 18th International Conference on Business Process Management (BPM 2020)* (pp. 107–111), Vienna, Austria.
- Sillaber, C., & Breu, R. (2012). Managing legal compliance through security requirements across service provider chains: A case study on the German Federal Data Protection Act. *GI-Jahrestagung, Informatik 2012*, (pp. 1306–1318), Braunschweig, Germany.
- Sonnenberg, C., & Vom Brocke, J. (2012). Evaluation patterns for design science research artefacts. In M. Helfert & B. Donnellan (Eds.), *Practical aspects of design science* (Vol. 286, pp. 71–83). Springer Berlin Heidelberg.
- Sturm, B., & Sunyaev, A. (2019). Design principles for systematic search systems: A holistic synthesis of a rigorous multi-cycle design science research journey. *Business & Information Systems Engineering*, 61(1), 91–111. <https://doi.org/10.1007/s12599-018-0569-6>
- The Institut der Wirtschaftsprüfer in Deutschland e.V. [Institute of Public Auditors in Germany, Incorporated Association]. (2002a). *Principles of proper accounting when using information technology* (IDW AcP FAIT 1).
- The Institut der Wirtschaftsprüfer in Deutschland e.V. [Institute of Public Auditors in Germany, Incorporated Association]. (2002b). *The audit of financial statements in an information technology environment* (IDW AuS 330).
- Turetken, O., Elgammal, A., van den Heuvel, W.-J., & Papazoglou, M. (2011). Enforcing compliance on business processes through the use of patterns. *ECIS 2011 Proceedings*, 2011, Helsinki, Finland. <https://aisel.aisnet.org/ecis2011/5/>
- Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: A Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, 25(1), 77–89. <https://doi.org/10.1057/ejis.2014.36>
- Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. In *17th European Conference on Information Systems* (pp. 2206–2217), Verona, Italy.
- Weber, B., Reichert, M., & Rinderle-Ma, S. (2008). Change patterns and change support features: Enhancing flexibility in process-aware information systems. *Data & Knowledge Engineering*, 66(3), 438–466. <https://doi.org/10.1016/j.datak.2008.05.001>
- Webster, J., & Watson, R.T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2), xiii–xxiii.
- Weske, M. (2019). *Business process management: Concepts, languages, architectures* (3rd ed.). Springer-Verlag Berlin Heidelberg.
- Winter, R., & Fischer, R. (2006). Essential layers, artifacts, and dependencies of enterprise architecture. In *2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06)* (pp. 30–37), Hong Kong, China. <https://doi.org/10.1109/EDOCW.2006.33>
- Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., & Wesslén, A. (2012). *Experimentation in software engineering*. Springer Berlin Heidelberg.
- Yousafzai, S.Y., Foxall, G.R., & Pallister, J.G. (2007). Technology acceptance: A meta-analysis of the TAM: Part 1. *Journal of Modelling in Management*, 2(3), 251–280. <https://doi.org/10.1108/17465660710834453>

Eidesstattliche Erklärung über verwendete Hilfsmittel

Hiermit erkläre ich an Eides statt, dass ich die vorliegende Dissertation selbstständig und ohne unerlaubte Hilfe angefertigt sowie keine anderen als die von mir angegebenen Quellen und Hilfsmittel benutzt habe. Alle aus anderen Werken bzw. von anderen Autoren inhaltlich übernommenen Stellen wurden in der vorliegenden Dissertation als solche kenntlich gemacht und entsprechend zitiert.

Tobias Seyffarth

Halle (Saale), den 9. November 2020