Beiträge zu Business Intelligence und IT-Compliance

Von der Wirtschaftswissenschaftlichen Fakultät der
Gottfried Wilhelm Leibniz Universität Hannover
zur Erlangung des akademischen Grades

Doktor der Wirtschaftswissenschaften
– Doctor rerum politicarum –

genehmigte Dissertation

von

Diplom-Ökonom Matthias Kehlenbeck

geboren am 17. Juli 1978 in Verden (Aller)

2011

Betreuer und Gutachten:	Professor Dr. Michael H. Breitner
Gutachten:	Jun.-Professor Dr. Hans-Jörg von Mettenheim
Tag der Promotion:	17. Dezember 2010

Zusammenfassung

Die vorliegende kumulative Dissertation beschäftigt sich mit dem Forschungsgebiet Business Intelligence (BI) / Online Analytical Processing (OLAP) / Data Warehousing (DW), sowie dem Forschungsgebiet IT-Compliance. Ausgehend von Problemstellungen aus der Praxis und Literaturrecherchen sind folgende Forschungsziele definiert worden:

A. Gestaltung von Artefakten zur Verbesserung der Interoperabilität von BI/ OLAP/DW Systemen durch Einsatz von Ontologien und automatisiertes Schlussfolgern,
B. Gestaltung von Artefakten zur automatisierten regelbasierten Überwachung maschineller Kontrollen und zur zielgruppengerechten Berichterstattung von Kontrollausnahmen.

Zur Umsetzung dieser Forschungsziele ist Design Science als Forschungsmethode eingesetzt worden. Die Forschungsergebnisse sind in drei Forschungsbeiträgen zum Forschungsgebiet BI/OLAP/DW und Forschungsziel A sowie fünf Forschungsbeiträgen zum Forschungsgebiet IT-Compliance und Forschungsziel B zusammengefasst worden.

Schlagwörter: Business Intelligence, IT-Compliance, Design Science

Abstract

This cumulative dissertation deals with the research area Business Intelligence (BI) / Online Analytical Processing (OLAP) / Data Warehousing (DW), as well as the research area IT compliance. Based on real life problems and literature reviews, the following research objectives have been defined:

A. Design of artifacts to improve the interoperability of BI/OLAP/DW systems by means of ontologies and automated reasoning,
B. Design of artifacts for the automated ruled-based monitoring of system controls and for the target group appropriate reporting of control exceptions.

In order to achieve these control objectives, design science has been used as the research method. The research results are summarized in three research papers regarding research area BI/OLAP/DW and research objective A as well as five research papers regarding research area IT compliance and research objective B.

Keywords: Business Intelligence, IT compliance, design science

Managementzusammenfassung

Einleitung und Problemstellung

Organisationen setzen zur Unterstützung ihrer Geschäftsprozesse verschiedene Informationssysteme ein. Durch den fortlaufenden Betrieb dieser Systeme entstehen mit der Zeit umfangreiche Datenbestände. Aus diesen Datenbeständen können Informationen gewonnen werden, die für das operative und strategische Management wertvoll sind. Systeme zur Verarbeitung umfangreicher Datenbestände eignen sich aber nur bedingt zu deren Auswertung. Daher gibt es zur Auswertung von Daten eigene Informationssysteme. Diese Systeme werden unter dem Begriff Business Intelligence (BI) zusammengefasst. BI setzt Data Warehousing (DW) für die Überführung und Bereitstellung von Daten sowie Online Analytical Processing (OLAP) für die Analyse von Daten ein. Die Analyse erfordert neben dafür geeigneten Systemen auch wertvolles Expertenwissen hinsichtlich der Bedeutung der Daten. Erhebliche Teile dieses Wissens werden durch die Definition betrieblicher Größen und Objekte im Rahmen von Analysen oder durch das Erstellen von Berichten von den Benutzern der BI/OLAP/DW Systeme in diesen abgelegt. Zum Austausch dieses Wissens gibt es im Gegensatz zum Austausch von Daten jedoch kaum Möglichkeiten. Die vorliegende Dissertation enthält Forschungsbeiträge, die sich mit dem Austausch dieses Wissens beschäftigen. Diese Beiträge gestalten innovative Modelle, Verfahren und Implementierungen zur Verbesserung der Interoperabilität von BI/OLAP/DW Systemen. Zur Beschreibung des Wissens hinsichtlich der Bedeutung von Daten werden Ontologien eingesetzt. Dabei wird das übertragbare Wissen von technischen Details isoliert und durch automatisiertes Schlussfolgern für andere Systeme anwendbar gemacht.

In die Geschäftsprozesse von Organisationen sind zahlreiche Kontrollen eingebettet. Diese Kontrollen sollen unter anderem das Erreichen der betrieblichen Ziele unterstützen, das Einhalten von relevanten Gesetzen sicherstellen sowie Fehler und Manipulationen verhindern. Die Gesamtheit aller Kontrollen einer Organisation bildet ihr internes Kontrollsystem. Ein erheblicher Teil des internen Kontrollsystems kann in die Programmabläufe der unterstützenden Informationssysteme integriert werden. Unter anderem können Systeme das Einhalten von gesetzlichen oder vereinbarten Regelungen sicherstellen, indem sie verschiedene Funktionen und Verantwortungen voneinander trennen sowie bestimmte Verfahren erzwingen. Das Einhalten von gesetzlichen oder

vereinbarten Regelungen durch Systeme wird auch als IT-Compliance bezeichnet. Um sicherzustellen, dass die Kontrollen richtig in den Systemen implementiert sind, müssen die Kontrollen regelmäßig überwacht werden. Aufgrund der Heterogenität und der Komplexität von Systemen kann dieses Überwachen eine schwierige und zeitaufwendige Aufgabe sein. Eine Möglichkeit zur regelmäßigen Überwachung von Kontrollen in Systemen und zur zeitnahen Berichterstattung von Ausnahmen ist der Einsatz entsprechender Informationssysteme. Die vorliegende Dissertation enthält Forschungsbeiträge, die sich mit entsprechenden Systemen beschäftigen. Diese Beiträge gestalten innovative Modelle, Verfahren und Implementierungen zur automatisierten Überwachung von Kontrollen in Systemen. Die automatisierte Überwachung wird durch zuvor hinterlegte Regeln gesteuert. Für die zeitnahe und zielgruppengerechte Berichterstattung von Ausnahmen wird BI eingesetzt.

Forschungsziele und Forschungsmethode

Die vorliegende Dissertation verfolgt ein Forschungsziel im Forschungsgebiet BI/ OLAP/DW und ein Forschungsziel im Forschungsgebiet IT-Compliance. Den Anstoß für diese Ziele haben die in der Einleitung umrissenen Problemstellungen aus der Praxis gegeben. Zu diesen Problemstellungen sind durch systematische Literaturrecherchen bestehende Forschungslücken identifiziert worden. Auf Grundlage der Problemstellungen und der Forschungslücken werden die folgenden Forschungsziele definiert:

A. Gestaltung von Artefakten zur Verbesserung der Interoperabilität von BI/ OLAP/DW Systemen durch Einsatz von Ontologien und automatisiertes Schlussfolgern,
B. Gestaltung von Artefakten zur automatisierten regelbasierten Überwachung maschineller Kontrollen und zur zielgruppengerechten Berichterstattung von Kontrollausnahmen.

Der Begriff des Artefakts bezeichnet unter anderem Konzepte, Modelle und Verfahren sowie deren Implementierungen als Prototypen oder als Produktivsysteme.

Als Forschungsmethode zum Erreichen der Forschungsziele wird Design Science gewählt. Im Design Science werden auf Grundlage des verfügbaren Wissens abduktiv Lösungsvorschläge erarbeitet. Diese Lösungsvorschläge führen zu einem vorläufigen Design. Ausgehend von diesem vorläufigen Design wird das verfügbare Wissen deduktiv zur Entwicklung und anschließenden Evaluation eines Artefaktes eingesetzt. Sowohl

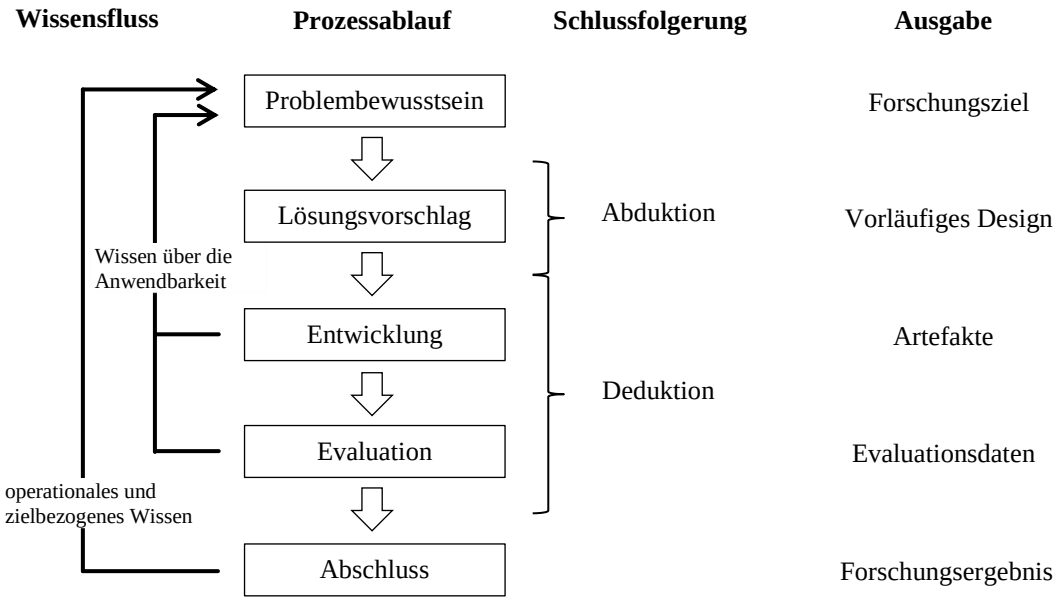

Abbildung I: Design Science als Forschungsmethode.

Quelle: Modifizierte Version von Darstellungen in TAKEDA ET AL. 1990, S. 45 und VAISHNAVI UND KÜCHLER 2009.

durch die Entwicklung als auch durch die Evaluation entsteht Wissen über die Anwendbarkeit von Wissen. Die Anwendbarkeit von Wissen kann aber nur durch das Entdecken von Widersprüchen erkannt werden. Diese Widersprüche treten aufgrund der Unvollständigkeit des verfügbaren Wissens regelmäßig auf. Daher sind in der Regel mehrere Iterationen des beschriebenen Prozesses zum Erreichen der Forschungsziele notwendig. Nach dem Erreichen der Forschungsziele, wird das gewonnene Wissen zusammengefasst und als Forschungsergebnis verbreitet. Abbildung I stellt Design Science als Forschungsmethode grafisch dar.

Forschungsstand

Ausgangspunkt für das Umsetzen der Forschungsziele ist der gegenwärtige Forschungsstand. Um diesen zu bestimmen, ist wie folgt in der Literatur recherchiert worden:

- Um einen Überblick über die zahlreichen Forschungsbeiträge zum Forschungsgebiet BI/OLAP/DW zu gewinnen, sind zunächst weitreichende Suchanfragen in den einschlägigen Internetdatenbanken mit wissenschaftlicher Literatur zur Informatik und Wirtschaftsinformatik durchgeführt worden. Die Titel und Zusammenfassungen von etwa 2.400 Beiträgen sind gelesen und kategorisiert worden. Da es zum Forschungsgebiet IT-Compliance deutlich weniger Forschungsbeiträge gibt, ist ein analoges Vorgehen nicht notwendig gewesen.

- Während der Arbeit an den einzelnen Forschungsbeiträgen sind die Internetdatenbanken sowie die relevanten Zeitschriften und Konferenzbände nach verwandter Literatur durchsucht worden. Auf die relevanten Ergebnisse wird in den einzelnen Forschungsbeiträgen Bezug genommen.
- Schließlich sind alle elektronisch verfügbaren und relevanten Zeitschriften sowie Konferenzbände seit Anfang 2000 beschafft und für die Volltextsuche indiziert worden. Durch Volltextsuchen ist gezielt nach Beiträgen zu den beiden Forschungszielen recherchiert worden. Die Titel und Zusammenfassungen von 385 Beiträgen sind gelesen worden. Auf die relevanten Ergebnisse wird in der Dissertation Bezug genommen.

Zu den beiden Forschungszielen gibt es in der wissenschaftlichen Literatur nur eine überschaubare Anzahl an Beiträgen.

Eigene Forschungsbeiträge und Forschungsergebnisse

Die vorliegende Dissertation enthält drei Forschungsbeiträge zum Forschungsgebiet BI/OLAP/DW und Forschungsziel A sowie fünf Forschungsbeiträge zum Forschungsgebiet IT-Compliance und Forschungsziel B. Innerhalb der Forschungsgebiete und Forschungsziele bauen die einzelnen Forschungsbeiträge aufeinander auf.

Innerhalb des Forschungsgebiets BI/OLAP/DW und Forschungsziels A sind Beiträge mit folgenden Inhalten erstellt worden:

- Strukturierte Literaturrecherche und -klassifizierung zu den Forschungsgebieten BI und DW, veröffentlicht als Discussion Paper (DP) #30 des Instituts für Wirtschaftsinformatik (IWI) der Leibniz Universität Hannover,
- Ontologie-basierter Austausch von Definitionen für Rechenvorschrift und deren unmittelbare Anwendung für BI/OLAP/DW Systeme anhand eines entwickelten Proxys, veröffentlicht bei der International Conference on Data Warehousing and Knowledge Discovery (DaWaK) 2009,
- Integration von Wissensmanagementsystemen und BI-Systemen sowie Isolierung von Geschäftswissen und DW-Metadaten mittels einer Weiterentwicklung des Proxys und einer Reihe eigens entwickelter Werkzeuge, wird eingereicht bei der International Conference on Advanced Information Systems Engineering (CAiSE) 2011.

Zur Evaluation des entwickelten Proxys sind mehrere verbreitete DW-Server und DW-Clients eingesetzt worden, mit diesen arbeitet der Proxy problemlos zusammen.

Innerhalb des Forschungsgebiets IT-Compliance und Forschungsziels B sind Beiträge mit folgenden Inhalten erstellt worden:

- Integriertes Modell, Service-Orientierte Architektur und auf Webservices basierender Prototyp zur Überwachung von Zugriffskontrollen in Systemen sowie zur Berichterstattung von Ausnahmen mittels BI, veröffentlicht bei der Hawaii International Conference on System Sciences (HICSS) 43,
- Weiterentwicklung der Architektur und des Prototypen anhand einer Verbesserung einzelner Webservices und einer Erweiterung um eine automatische Transformation von Zugriffskontrolldaten aus dem proprietären SAP-Modell in ein Standardmodell, veröffentlicht bei der European Conference on Information Systems (ECIS) 2010,
- Diskussion der Anwendung des Prototyps und der entsprechenden Auswirkungen unter Berücksichtigung verschiedener Szenarien und unterschiedlicher Anspruchsgruppen, veröffentlicht bei der International Conference on Availability, Reliability and Security (ARES) 2010,
- Visualisierung von managementrelevanten Informationen, die mit dem Prototyp generiert worden sind, veröffentlicht beim International Workshop on Visualization and Information Security Management (VISM) 2010,
- Weiterentwicklung des Prototyps durch Transfer-, Konvertierungs- und Verarbeitungsverfahren, die besonders geringe Annahmen zu den Modellen und Abläufen in den zu überwachenden Systemen treffen, eingereicht bei der Internationalen Tagung Wirtschaftsinformatik (WI) 2011.

Zur Evaluation des Prototyps sind Daten aus mehreren Mandanten eines produktiven SAP-Systems verwendet worden. Der Prototyp hat die Kontrollen zuverlässig überwacht.

Abbildung II stellt die Zusammenhänge zwischen den Forschungsbeiträgen grafisch dar. Die Größe der Kreise veranschaulicht die Bewertung der Veröffentlichungen in den einschlägigen Ranglisten.

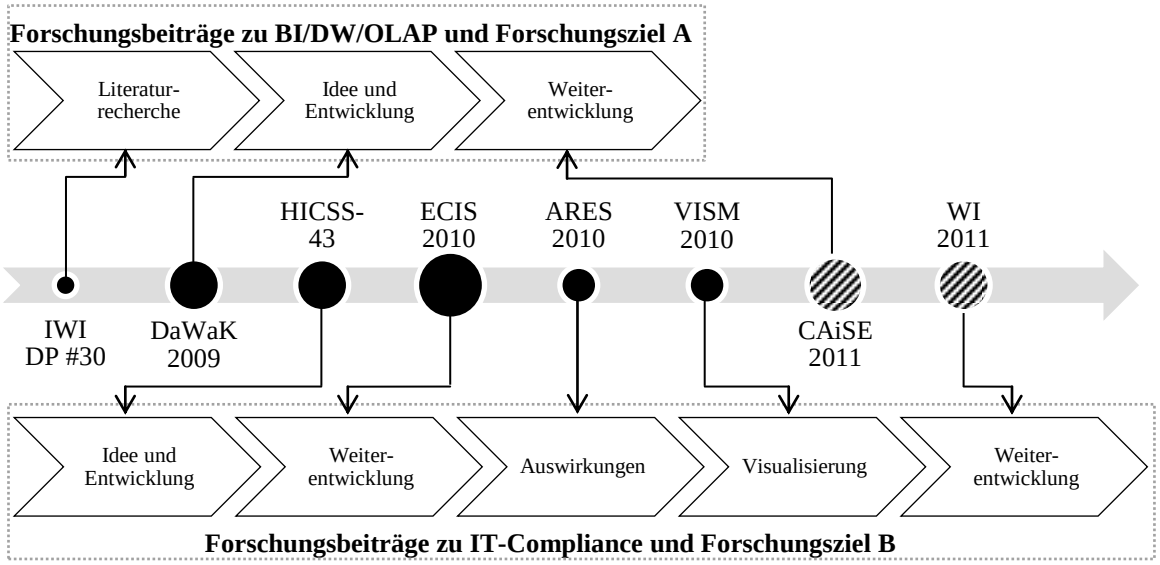

Abbildung II: Darstellung der zeitlichen Abfolge und inhaltlichen Zusammenhänge der Beiträge.

Quelle: Eigene Darstellung.

Fazit und Ausblick

Die vorliegende Dissertation hat jeweils ein Forschungsziel in zwei unterschiedlichen Forschungsgebieten verfolgt. Den Anstoß für diese Forschungsziele ergaben Problemstellungen aus der Praxis. Zu diesen Problemstellungen sind durch systematische Literaturrecherchen bestehende Forschungslücken identifiziert worden.

Innerhalb des Forschungsgebietes BI/OLAP/DW ist das Forschungsziel die Gestaltung von Artefakten zur Verbesserung der Interoperabilität von BI/OLAP/DW Systemen durch Einsatz von Ontologien und automatisiertes Schlussfolgern gewesen. Zur Umsetzung des Forschungsziels ist Design Science betrieben worden. Dabei sind innovative Modelle, Verfahren und Implementierungen entwickelt worden, welche Ontologien und automatisiertes Schlussfolgern einsetzen, um den Austausch von wertvollem Expertenwissen zwischen verschiedenen BI/OLAP/DW Systemen sowie dessen unmittelbare Anwendung zu ermöglichen. Durch diese Modelle, Verfahren und Implementierungen kann erstmals Wissen über Funktionen für Größen (wie z. B. Gewinn vor Zinsen und Steuern) und Definitionen für Objekte (wie z. B. Zinskonto oder Steuerkonto) über Wissensmanagementsysteme zwischen unterschiedlichen BI/OLAP/DW Systemen ausgetauscht werden. Ferner kann das ausgetauschte Wissen mittels eines standardkonformen Proxys ohne Änderungen an diesen Systemen angewendet werden. Dies stellt eine deutliche Verbesserung der Interoperabilität von BI/OLAP/DW Systeme dar. Bisher gibt es in der wissenschaftlichen Literatur keinen vergleichbaren Proxy.

Innerhalb des Forschungsgebietes IT-Compliance ist das Forschungsziel die Gestaltung von Artefakten zur automatisierten regelbasierten Überwachung maschineller Kontrollen und zur zielgruppengerechten Berichterstattung von Kontrollausnahmen gewesen. Zur Umsetzung des Forschungsziels sind auch hier innovative Modelle, Verfahren und Implementierungen durch Design Science entwickelt worden. Diese Modelle, Verfahren und Implementierungen ermöglichen eine homogene Überwachung von Kontrollen in heterogenen Systemen. Der implementierte Prototyp wird durch Regeln gesteuert und leitet die Überwachungsergebnisse (insbesondere identifizierte Kontrollausnahmen) an BI-Systeme weiter. Dies ermöglicht eine zeitnahe und zielgruppengerechte Berichterstattung. Bisher gibt es in der wissenschaftlichen Literatur keinen anderen Prototyp zur Überwachung maschineller Kontrollen, der vergleichbar flexibel auf Unterschiede zwischen den überwachten Systemen eingehen kann und vergleichbar konform zu etablierten Standards ist.

Die aufgeführten Forschungsergebnisse stellen maßgebliche Erfolge für die gesetzten Forschungsziele dar und bieten zugleich mehrere Anknüpfungspunkte für zukünftige Forschung. Innerhalb des Forschungsgebietes BI/OLAP/DW gibt es bisher lediglich vereinzelt Beiträge, die sich mit dem Austausch von Wissen zur Bedeutung von Daten beschäftigen. Auch auf den Einsatz von Ontologien und automatisiertem Schlussfolgern wird nur in Teilgebieten eingegangen. Hier gibt es erhebliches Potential für zukünftige Forschung an innovativen Analysewerkzeugen mit nativer Unterstützung für Ontologien. Entsprechende Werkzeuge könnten bestehende Grenzen zwischen OLAP und künstlicher Intelligenz aufweichen. Innerhalb des Forschungsgebietes IT-Compliance gibt es bisher nicht viele Beiträge, die sich mit der Gestaltung von Artefakten zur Überwachung von Kontrollen in Systemen beschäftigen. Dadurch mangelt es unter anderem an Vorschlägen zu Kontrollmodellen, Einschätzungen zu Regelsprachen und Beurteilungen von Lösungen. Auch auf die Präsentation von Überwachungsergebnissen wird kaum eingegangen. Hier steht die Forschung noch am Anfang.

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACM	Association for Computing Machinery
AIS	Association for Information Systems
AMCIS	Americas Conference on Information Systems
AO	Abgabenordnung
ARES	International Conference on Availability, Reliability and Security
Basel II	Eigenkapitalvorschriften vom Basler Ausschuss für Bankenaufsicht
BDSG	Bundesdatenschutzgesetz
BI	Business Intelligence
BilMoG	Gesetz zur Modernisierung des Bilanzrechts
CAiSE	International Conference on Advanced Information Systems Engineering
CORBA	Common Object Request Broker Architecture
DaWaK	International Conference on Data Warehousing and Knowledge Discovery
DEXA	International Conference on Database and Expert Systems Applications
DP	Discussion Paper
DW	Data Warehousing
ECIS	European Conference on Information Systems
EDI	Electronic Data Interchange
EMEA	Europa, Mittlerer Osten und Afrika
EPK	Ereignisgesteuerte Prozesskette
ERA	Excellence in Research for Australia
ERP	Enterprise Resource Planning
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GI-FB WI	Fachbereich Wirtschaftsinformatik der Gesellschaft für Informatik

GoB	Grundsätze ordnungsmäßiger Buchführung
GoBS	Grundsätze ordnungsmäßiger datenverarbeitungsgestützter Buchführung
GRC	Governance, Risk und Compliance
HICSS	Hawaii International Conference on System Sciences
ICIS	International Conference on Information Systems
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
IT	Informationstechnologie
IWI	Institut für Wirtschaftsinformatik
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
LNCS	Lecture Notes in Computer Science
LUH	Leibniz Universität Hannover
OLAP	Online Analytical Processing
OWL	Web Ontology Language
RDF	Resource Description Framework
SOA	Service-Orientierte Architektur
Solvabilität II	Solvabilitätsvorschriften für die Eigenmittelausstattung von Versicherungsunternehmen
SOX	Sarbanes-Oxley Act
VHB	Verband der Hochschullehrer für Betriebswirtschaft e. V.
VISM	International Workshop on Visualization and Information Security Management
XTM	Extensible Markup Language Topic Maps
W3C	World Wide Web Consortium
WI	Wirtschaftsinformatik
WKWI	Wissenschaftlichen Kommission Wirtschaftsinformatik

1 Einleitung

Organisationen setzen zur Unterstützung ihrer Geschäftsprozesse verschiedene Informationssysteme ein. Geschäftsprozesse sind strukturierte Folgen zusammenhängender Einzelaktivitäten und dienen einem betrieblichen Ziel. Zur Durchführung der einzelnen Prozessaktivitäten werden Daten in den unterstützenden Informationssystemen erfasst, verarbeitet und bereitgestellt. Durch den fortlaufenden Betrieb der Systeme entstehen mit der Zeit umfangreiche Datenbestände. Aus diesen Datenbeständen können Informationen gewonnen werden, die für das operative und strategische Management von Organisationen wertvoll sind. Informationssysteme zur Verarbeitung umfangreicher Datenbestände eignen sich aber nur bedingt zu deren Auswertung. So erfordert die Verarbeitung von Daten ein auf schreibende Zugriffe optimiertes Datenmodell, deren Auswertung hingegen ein auf lesende Zugriffe optimiertes Datenmodell. Insbesondere für strategische Zwecke kann ferner eine gemeinsame Auswertung von Daten aus unterschiedlichen Systemen notwendig sein. Dies erfordert eine Überführung der Daten in ein einheitliches Modell. Daher gibt es zur Auswertung von Daten eigene Informationssysteme. Diese Systeme werden unter dem Begriff Business Intelligence (BI) zusammengefasst. BI setzt Data Warehousing (DW) für die Überführung und Bereitstellung von Daten sowie Online Analytical Processing (OLAP) für die Analyse von Daten ein. Die Analyse erfordert neben dafür geeigneten Systemen auch wertvolles Expertenwissen hinsichtlich der Bedeutung von Daten. Erhebliche Teile dieses Expertenwissens werden durch die Definition betrieblicher Größen und Objekte im Rahmen von Analysen oder durch das Erstellen von Berichten von den Benutzern der BI, OLAP und DW Systeme in diesen abgelegt. Zum Austausch dieses Wissens gibt es im Gegensatz zum Austausch von Daten aber kaum Möglichkeiten. Die vorliegende Dissertation enthält Forschungsbeiträge, welche sich mit dem Austausch dieses Wissens beschäftigen. Die Forschungsbeiträge gestalten innovative Modelle, Verfahren und Implementierungen zur Verbesserung der Interoperabilität von BI, OLAP und DW Systemen. Zur Beschreibung des Wissens hinsichtlich der Bedeutung von Daten werden Ontologien eingesetzt. Dabei wird das übertragbare Wissen von technischen Details isoliert und durch automatisiertes Schlussfolgern für andere Systeme anwendbar gemacht.

In die Geschäftsprozesse von Organisationen sind zahlreiche Kontrollen eingebettet. Diese Kontrollen sollen unter anderem das Erreichen der betrieblichen Ziele unter-

stützen, das Einhalten von relevanten Gesetzen sicherstellen sowie Fehler und Manipulationen verhindern. Die Gesamtheit aller Kontrollen einer Organisation bildet ihr internes Kontrollsystem (IKS). Ein erheblicher Teil des IKS kann in die Programmabläufe der unterstützenden Informationssysteme integriert werden. Unter anderem können Systeme das Einhalten von gesetzlichen oder vereinbarten Regelungen sicherstellen, indem sie verschiedene Funktionen und Verantwortungen voneinander trennen sowie bestimmte Verfahren erzwingen. Das Einhalten von gesetzlichen oder vereinbarten Regelungen durch Systeme wird auch als IT-Compliance bezeichnet. Um sicherzustellen und nachweisen zu können, dass die Kontrollen richtig in den Systemen implementiert und damit wirksam sind, müssen die Kontrollen regelmäßig überwacht werden. Aufgrund der Heterogenität und Komplexität von Systemen kann dieses Überwachen aber eine schwierige und zeitaufwendige Aufgabe sein. Gleichwohl ist eine zeitnahe Berichterstattung über eventuelle Ausnahmen für das rechtzeitige Einleiten von Gegenmaßnahmen und somit für die Wirksamkeit eines IKS notwendig. Eine Möglichkeit zur regelmäßigen Überwachung von Kontrollen in Systemen und zur zeitnahen Berichterstattung von Ausnahmen ist der Einsatz entsprechender Informationssysteme. Die vorliegende Dissertation enthält Forschungsbeiträge, die sich mit entsprechenden Informationssystemen beschäftigen. Diese Forschungsbeiträge gestalten innovative Modelle, Verfahren und Implementierungen zur automatisierten Überwachung von Kontrollen in Systemen. Die automatisierte Überwachung wird durch zuvor hinterlegte Regeln gesteuert. Für die zeitnahe und zielgruppengerechte Berichterstattung von Ausnahmen wird BI eingesetzt.

Durch den Einsatz von BI für die Berichterstattung von Kontrollausnahmen ergeben sich zahlreiche Berührungspunkte zwischen den Forschungsbeiträgen zu BI/OLAP/DW und den Forschungsbeiträgen zu IT-Compliance. Des Weiteren haben die Beiträge zu beiden Forschungsgebieten den Einsatz von Ontologien und Softwarekomponenten zum automatisierten Schlussfolgern, die Berücksichtigung von existierenden Standards und die plattformunabhängige Kommunikation über Webservices gemein.

Die Dissertation ist kumulativer Art und enthält acht verschiedene Forschungsbeiträge. Sechs der acht Forschungsbeiträge sind bereits veröffentlicht. Ein Forschungsbeitrag ist eingereicht und befindet sich gegenwärtig im Begutachtungsverfahren, ein weiterer wird im November 2010 eingereicht. Unter den veröffentlichten Beiträgen sind fünf Konfe-

renzbeiträge und ein Diskussionsbeitrag. Die Konferenzbeiträge haben die Begutachtungsverfahren renommierter internationaler Konferenzen mit Erfolg durchlaufen.

Die Forschungsbeiträge werden auf den folgenden Seiten wissenschaftlich eingeordnet und inhaltlich zusammengefasst. Dabei wird wie folgt vorgegangen: Kapitel 2 geht auf wesentliche Grundlagen zum Forschungsgebiet BI/OLAP/DW sowie zum Forschungsgebiet IT-Compliance ein. Kapitel 3 beschreibt die gesetzten Forschungsziele und eingesetzten Forschungsmethoden. Dazu wird auf ausgewählte philosophische und wissenschaftstheoretische Grundlagen sowie auf die wissenschaftstheoretische Fundierung der Wirtschaftsinformatik eingegangen. Kapitel 4 schildert den Forschungsstand zu den beiden Forschungsgebieten und den gesetzten Forschungszielen. Dazu wird auf die Ergebnisse umfangreicher Literaturrecherchen eingegangen. Kapitel 5 fasst die Forschungsbeiträge zusammen. Dabei werden unter anderem die Aufgabenteilung unter den Autoren, die Veröffentlichung der Beiträge sowie das Ranking der Veröffentlichungen beschrieben. Kapitel 6 enthält eine kritische Würdigung und gibt einen Ausblick. Der Anhang enthält die einzelnen Forschungsbeiträge.

2 Grundlagen

Die vorliegende Dissertation beschäftigt sich mit dem Forschungsgebiet Business Intelligence/Online Analytical Processing/Data Warehousing und dem Forschungsgebiet IT-Compliance. Die folgenden Abschnitte dienen zur Einführung in diese Gebiete.

2.1 Business Intelligence, Online Analytical Processing und Data Warehousing

Der Begriff Business Intelligence wird zwar bereits seit Ende der 1950er Jahre verwendet,[1] in seiner heutigen Bedeutung aber erst Ende der 1980er Jahre durch die Gartner-Gruppe bekannt gemacht. Die heutige Bedeutung von Business Intelligence ist durch die Entwicklung der Führungsinformationssysteme, der Data Warehouse Systeme und des Online Analytical Processing geprägt worden.[2]

Das Massachusetts Institute of Technology prägt Ende der 1970er Jahre den Begriff Führungsinformationssystem.[3] Führungsinformationssysteme sind ein Spezialfall der Entscheidungsunterstützungssysteme.[4] Entscheidungsunterstützungssysteme sind Informationssysteme, die Personen bei der Entscheidungsfindung unterstützen.[5] Führungsinformationssysteme erleichtern die Analyse geschäftskritischer Informationen und unterstützen die strategische Entscheidungsfindung durch Führungskräfte.[6]

Der Begriff Data Warehouse System wird Anfang der 1990er Jahre durch William H. Inmon und Ralph Kimball geprägt.[7] Data Warehouse Systeme übernehmen Daten aus unterschiedlichen Quellsystemen, integrieren diese Daten in ein einheitliches Modell und speichern sie in einer persistenten und zeitgeführten Sammlung.[8]

Anfang der 1990er Jahre wird der Begriff Online Analytical Processing durch Edgar F. Codd bekannt. Codd versteht darunter Verarbeitungsverfahren, mit deren Hilfe Daten nach mehreren Dimensionen konsolidiert, betrachtet und analysiert werden können.[9]

---

[1] Vgl. LUHN 1958, S. 314.
[2] Vgl. POWER 2008, S. 128.
[3] Vgl. MARAKAS 2003, S. 177.
[4] Vgl. MARAKAS 2003, S. 174; SILVER 1991, S. 224.
[5] Vgl. SILVER 1991, S. 13.
[6] Vgl. MARAKAS 2003, S. 174.
[7] Vgl. POWER 2008, S. 128f.
[8] Vgl. INMON 2005, S. 29ff.
[9] Vgl. CODD ET AL. 1993, S. 6.

Die Begriffe BI, OLAP und DW werden in der Literatur nicht einheitlich voneinander abgegrenzt.[10] Insbesondere gibt es sowohl Autoren, die BI als Teil von DW verstehen, als auch Autoren, die DW als Teil von BI verstehen. Für Kimball stellt das Data Warehouse die Daten für BI zur Verfügung. Das Data Warehouse ist also die Grundlage für BI.[11] BI-Systeme ermöglichen die Analyse von Geschäftsinformationen sowie deren Präsentation an Entscheidungsträger.[12] Folglich sind BI-Systeme datengestützte Entscheidungsinformationssysteme.[13]

Im Folgenden wird auf die Begriffe Data Warehousing, Online Analytical Processing und Business Intelligence näher eingegangen. Die Abgrenzung dieser Begriffe folgt dem Verständnis von Codd und Kimball.

2.1.1 Data Warehousing

Data Warehousing ist ein Prozess, in dem Daten beschafft, bereitgestellt und präsentiert werden. Im Rahmen der Beschaffung werden die Daten aus unterschiedlichen Datenquellen extrahiert. Datenquellen können Systeme aber auch einzelne Dateien sein. Des Weiteren können sie unterschiedliche Datenmodelle verwenden. Die Datenmodelle von Quellsystemen sind in der Regel nicht für Analysen, sondern für die Verarbeitung von Transaktionen optimiert. Die Quellsysteme werden daher auch als Online Transaction Processing (OLTP) Systeme bezeichnet. Um die Quellsysteme möglichst wenig zu belasten, werden die extrahierten Daten zunächst in ihrem ursprünglichen Modell in den Operational Data Store übernommen. Um die Daten im Operational Data Store gemeinsam auswerten zu können, werden sie im Rahmen der Bereitstellung aus ihrem ursprünglichen Modell in das einheitliche Modell des Data Warehouse transformiert. Das Modell des Data Warehouse besteht aus Dimensions- und Faktentabellen. Es ist nicht für Transaktionen, sondern für Analysen optimiert. Das Data Warehouse wird daher auch als Online Analytical Processing System bezeichnet. Die Dimensions- und Faktentabellen werden in den Dimensional Data Store geladen. Schließlich werden die Daten im Dimensional Data Store in der Form sogenannter OLAP-Würfel an die Benutzer des Data Warehouse präsentiert. Die OLAP-Würfel können für Analysen und Berichte genutzt werden. Abbildung 1 illustriert den DW-Prozess.

[10] Vgl. KIMBALL 2008, S. 10; POWER 2008, S. 128.
[11] Vgl. KIMBALL 2008, S. 10.
[12] Vgl. NEGASH UND GRAY 2008, S. 176.
[13] Vgl. POWER 2008, S. 128.

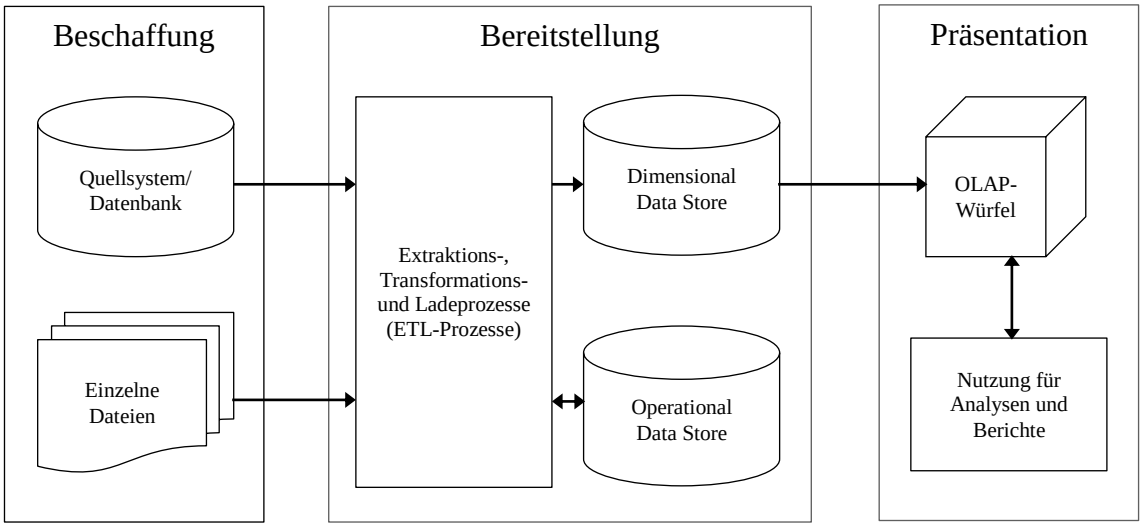

Abbildung 1: Darstellung der Beschaffung, Bereitstellung und Präsentation von Daten im Rahmen des Data Warehousing Prozesses.

Quelle: Modifizierte Version einer Darstellung in KIMBALL 2004, S. 16.

Die Transformation der Daten beinhaltet deren Säuberung und Angleichung. Die Datensäuberung dient der Sicherstellung einer angemessenen Datenqualität. Sie umfasst unter anderem das Überprüfen der Daten auf deren Gültigkeit und Konsistenz sowie das Entfernen von Duplikaten. Durch die Rückmeldung von Qualitätsproblemen kann die Datenqualität auch in den Quellsystemen erhöht werden. Die Datenangleichung dient zur Vereinheitlichung der Repräsentation inhaltlich ähnlicher Daten aus unterschiedlichen Quellen. Diese Repräsentation ist organisationsweit festzulegen.[14]

Die Dimensions- und Faktentabellen werden in der Regel zum Aufbau von OLAP-Würfeln in einem Sternschema oder einem Schneeflockenschema verwendet. Sowohl beim Sternschema als auch beim Schneeflockenschema gibt es eine zentrale Faktentabelle. In den Spalten der Faktentabelle befinden sich die Primärschlüssel mehrerer Dimensionstabellen sowie die Kennzahlen. In den Spalten der Dimensionstabellen befinden sich deren Primärschlüssel und die Attribute. Abbildung 2 zeigt ein Beispiel eines Würfels in einem Sternenschema. Beim Schneeflockenschema werden die Dimensionstabellen weiter aufgeteilt, um Datenredundanz zu vermeiden. Dies spart relativ wenig Speicherplatz, erhöht aber die Komplexität der Präsentation an die Benutzer und reduziert die Performance des Würfels. Aus diesem Grund werden die Dimensionstabellen beim Sternenschema nicht aufgeteilt.[15]

[14] Vgl. KIMBALL 2004, S. 18.
[15] Vgl. KIMBALL 2008, S. 265ff.

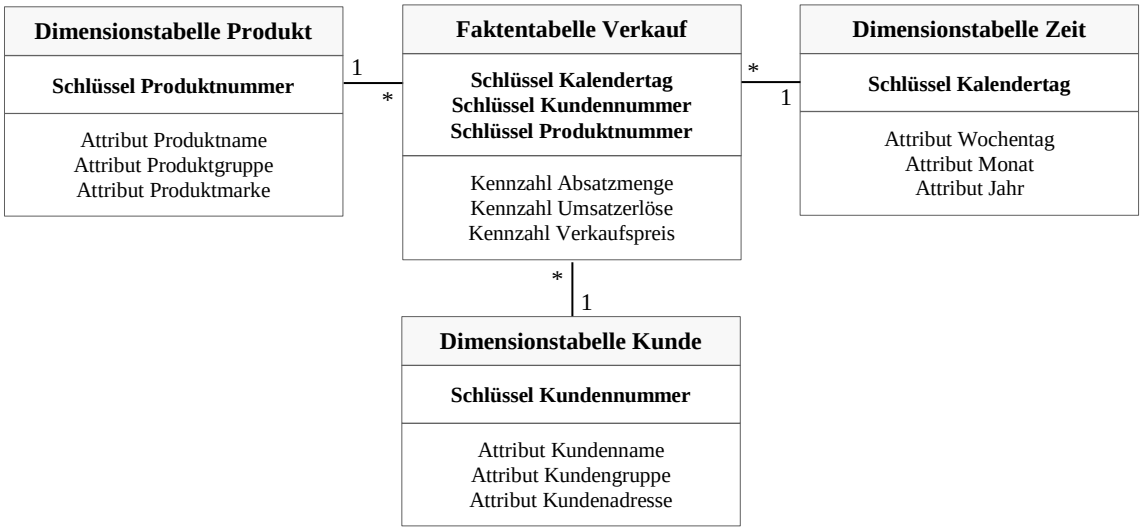

Abbildung 2: Modell eines OLAP-Würfels in einem Sternenschema mit drei Dimensionstabellen und einer Faktentabelle.

Quelle: Eigene Darstellung in Anlehnung an MEREDITH 2008, S. 216.

2.1.2 Online Analytical Processing

Um Online Analytical Processing leichter verständlich zu machen, sei angenommen, dass eine OLAP-Abfrage nur eine Kennzahl verwendet und die Abfrageergebnisse in tabellarischer Form präsentiert werden. Dann enthalten die Vorspalte und die Kopfzeile der Tabelle bestimmte Werte der Schlüssel oder Attribute aus den Dimensionstabellen. Die Felder der Tabellen enthalten die nach der Vorspalte und Kopfzeile aggregierten Werte der Kennzahl. Die Art der Aggregation ist abhängig von der Kennzahl. Beispielsweise kann für Absatzmengen und Umsatzerlöse summiert und für Verkaufspreise der Durchschnitt gebildet werden. Für die Manipulation der Tabelle stehen nun OLAP-Operationen zur Verfügung.

Die Grundoperationen des OLAP sind Slice/Dice, Rotate und Drill-Down/Roll-Up. Mit Hilfe der Slice/Dice-Operation können bestimmte Werte der Schlüssel oder Attribute in der Vorspalte und Kopfzeile hinzugefügt, ersetzt oder entfernt werden.[16] Die aggregierten Werte der Kennzahl werden automatisch aktualisiert. Mit Hilfe der Rotate-Operation können Werte aus den Vorspalten mit Werten aus den Kopfzeilen vertauscht werden.[17] Die Tabelle wird automatisch reorganisiert. Schließlich ermöglicht die Drill-Down/Roll-Up-Operation das Aufteilen und Zusammenfassen von Werten anhand einer

[16] Vgl. JUKIC ET AL. 2008, S. 266.
[17] Vgl. ebd., S. 267.

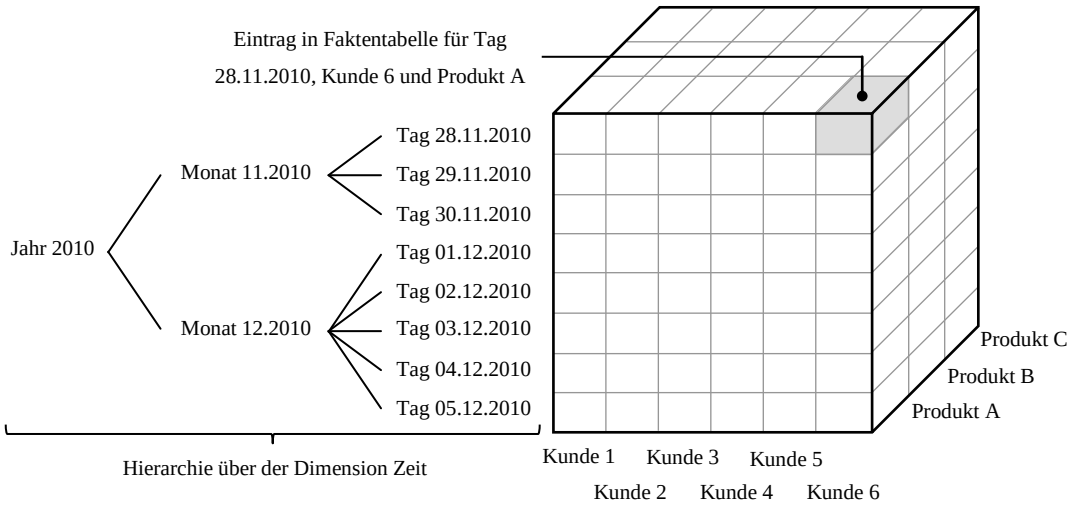

Abbildung 3: Geometrische Darstellung eines OLAP-Würfels mit drei Dimensionen und einer Hierarchie.

Quelle: Eigene Darstellung.

Hierarchie.[18] Dabei werden bestimmte Werte in der Vorspalte oder Kopfzeile in einer Hierarchie dargestellt. Entlang der Knoten in der Hierarchie erfolgt die Aggregation der Kennzahl in den Feldern. Für einen übergeordneten Knoten werden dabei alle Werte der Kennzahl zu den ihm untergeordneten Knoten aggregiert. Abbildung 3 illustriert ein Beispiel eines OLAP-Würfels mit drei Dimensionen und einer Hierarchie. Geometrisch betrachtet werden bei der Slice-Operation Scheiben und bei der Dice-Operation Würfel aus dem OLAP-Würfel herausgeschnitten. Durch die Rotate-Operation können diese Ausschnitte gedreht werden. Die Roll-Up-Operation aggregiert Einträge in der Faktentabelle. Beispielsweise ist eine Aggregation der Einträge zu Tagen nach Monaten und Jahren möglich. Die Drill-Down-Operation nimmt diese Aggregation zurück.

OLAP-Werkzeuge unterstützen noch weitere Operationen, beispielsweise Regressionsanalysen und Zeitreihenanalysen. Diese Operationen stehen aber auch in anderen Werkzeugen zur Verfügung. Kennzeichnend für OLAP-Werkzeuge ist der Zugriff auf OLAP-Würfel in Data Warehouse Systemen. Dies ermöglicht die Ausführung der OLAP-Operationen auf großen Datenmengen.[19]

[18] Vgl. JUKIC ET AL. 2008, S. 268.
[19] Vgl. ebd., S. 270.

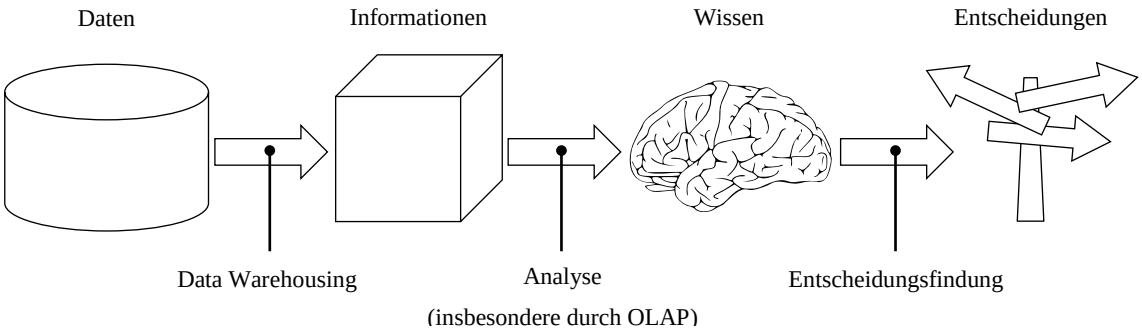

Abbildung 4: Darstellung von Business Intelligence als Prozess, indem Daten in Informationen, Informationen in Wissen und Wissen in Entscheidungen überführt werden.

Quelle: Eigene Darstellung.

2.1.3 Business Intelligence

Business Intelligence kann als Prozess verstanden werden, indem Daten durch DW in Informationen, diese Informationen durch Analysen in Wissen und dieses Wissen im Rahmen der Entscheidungsfindung in Entscheidungen überführt werden.[20] Durch das DW werden Daten aus verschiedenen Quellsystemen in ein einheitliches Modell überführt. Dieses Modell bestimmt die Bedeutung und den Kontext der Daten. Durch Bedeutung und Kontext werden Daten zu Informationen.[21] Im Rahmen von Analysen werden Informationen zu einem bestimmten Zweck sinnvoll miteinander verknüpft. Durch Zweckrichtung und Verknüpfung werden Informationen zu Wissen.[22] Schließlich geht das Wissen in die Entscheidungsfindung ein. Dort führt es zusammen mit anderen Aspekten – wie Regelungen oder Vorgaben – zu Entscheidungen.[23] Der geschilderte Prozess ist in Abbildung 4 dargestellt.

Das Durchführen von Analysen wird durch Analysewerkzeuge unterstützt. Zu diesen Analysewerkzeugen gehören insbesondere OLAP-Werkzeuge zum Erstellen von Abfragen und Berichten, aber auch Data Mining und Visualisierungswerkzeuge. Mit Hilfe von Data Mining können bisher unbekannte Muster in großen Datenmengen entdeckt werden.[24] Für dieses Musterentdecken gibt es beschreibende und vorhersagende Methoden. Beschreibende Methoden versuchen das Verständnis von Daten zu verbessern, beispielsweise durch Clustering oder Visualisierung. Vorhersagende Methoden versuchen ein Vorhersagemodell zu erstellen, beispielsweise durch Neuronale Netze oder

[20] Vgl. NEGASH UND GRAY 2008, S. 177.
[21] Vgl. BODENDORF 2006, S. 1.
[22] Vgl. ebd..
[23] Vgl. NEGASH UND GRAY 2008, S. 177.
[24] Vgl. MAIMON UND ROKACH 2005, S. 1.

Entscheidungsbäume.[25] Mit Hilfe von Visualisierungswerkzeugen kann das menschliche Wahrnehmungs- und Erkenntnisvermögen gefördert werden. Ein verbreitetes Visualisierungswerkzeug ist das Dashboard. Dashboards können viele verschiedene Kennzahlen in einer konsolidierten Sicht darstellen. Für diese Darstellung werden intuitiv verständliche Indikatoren verwendet, beispielsweise rote Ampeln für Probleme.[26]

2.2 Governance und Compliance

Die Begriffe Governance und Compliance werden häufig gemeinsam verwendet.[27] Die folgenden Abschnitte gehen auf die Begriffe ein und grenzen sie voneinander ab. Dazu werden zunächst die Begriffe Corporate Governance und Corporate Compliance eingeführt. Auf dieser Grundlage werden anschließend die Begriffe IT-gestützte Governance und IT-gestützte Compliance sowie IT-Governance und IT-Compliance definiert.

2.2.1 Corporate Governance und Corporate Compliance

Unter dem Begriff der Corporate Governance wird die Sicherstellung einer verantwortungsvollen Führung eines Unternehmens in Bezug zu dessen Anspruchsgruppen verstanden. Zur dieser verantwortungsvollen Führung eines Unternehmens gehört insbesondere die Einhaltung der zu berücksichtigenden Gesetze und Regelungen,[28] wie z. B. das deutsche Bilanzrechtsmodernisierungsgesetz (BilMoG) [29] oder den US-amerikanischen Sarbanes-Oxley Act (SOX)[30]. Die Einhaltung von Gesetzen und Regelungen fällt ebenfalls in den Bereich der Corporate Compliance.

Unter dem Begriff Corporate Compliance wird die Einhaltung von Gesetzen, Regelungen, Normen, Standards oder Vorgaben in einem Unternehmen verstanden. Im Folgenden wird vereinfachend von Regelungen gesprochen. Die Einhaltung von Regelungen ist nicht nur für die Führung, sondern für alle Mitarbeiter eines Unternehmens erforderlich. [31] Folglich müssen auch alle Mitarbeiter für diese Regelungen sensibilisiert werden. Des Weiteren sind die Prozesse im Unternehmen regelkonform zu gestalten.[32] Innerhalb von Prozessen kann Regelkonformität durch das Durchführen von Kontrollen

[25] Vgl. MAIMON UND ROKACH 2005, S. 5ff.
[26] Vgl. NEGASH UND GRAY 2008, S. 184.
[27] Vgl. TEUBNER UND FELLER 2008, S. 400.
[28] Vgl. ebd..
[29] BILMOG 2009.
[30] SOX 2002.
[31] Vgl. TEUBNER UND FELLER 2008, S. 400.
[32] Vgl. RATH 2009, S. 23ff.

Abbildung 5: Das Verhältnis von Corporate Governance und Corporate Compliance.

Quelle: Modifizierte Version einer Darstellung in TEUBNER UND FELLER 2008, S. 401.

sichergestellt werden. Die Funktion dieser Kontrollen und die Einhaltung der Regelungen kann durch sogenannte Audits überprüft werden.

Das Verhältnis zwischen Corporate Governance und Corporate Compliance wird durch Abbildung 5 illustriert. Informationstechnologie kann sowohl ein Instrument zur Ausgestaltung von Governance und Compliance als auch ein Objekt zur Bewertung von Governance und Compliance sein.[33]

2.2.2 IT-gestützte Governance und IT-gestützte Compliance

Die Wissenschaft beschäftigt sich mit den Themen Corporate Governance und Corporate Compliance überwiegend aus rein betriebswirtschaftlicher und nur am Rande auch aus informationstechnischer Perspektive. Die Industrie bietet hingegen unter dem Begriff Governance, Risk und Compliance (GRC) Software verschiedene Lösungen zur Unterstützung von Governance und Compliance durch IT an.[34] Das Thema Risiko ist zentraler Bestandteil einiger wichtiger Regelungen. Dies sind insbesondere die Eigenkapitalvorschriften vom Basler Ausschuss für Bankenaufsicht (Basel II)[35], die Solvabilitätsvorschriften für die Eigenmittelausstattung von Versicherungsunternehmen (Solvabilität II)[36] und das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)[37]. Bei den genannten Regelungen liegt die Verantwortung für die Einhaltung in besonderer Weise bei der Unternehmensführung und somit in der Schnittmenge von Governance und Compliance.[38]

[33] Vgl. TEUBNER UND FELLER 2008, S. 400.
[34] Vgl. ebd., S. 401f.
[35] BASLER AUSSCHUSS FÜR BANKENAUFSICHT 2006.
[36] SOLVABILITÄT II 2009.
[37] KONTRAG 1998.
[38] Vgl. TEUBNER UND FELLER 2008, S. 402.

2.2.3 IT-Governance und IT-Compliance

IT-Governance ist der Teilbereich der Corporate Governance, der sich auf die IT im Unternehmen bezieht.[39] Im Rahmen der IT-Governance wird festgelegt, wer an Entscheidungen zur IT in welcher Form zu beteiligen ist.[40] Insbesondere soll IT-Governance sicherstellen, dass die IT die Unternehmensstrategie und die Unternehmensziele unterstützt.[41] Dazu zählt auch das Einhalten relevanter Regelungen.

IT-Compliance ist der Teilbereich der Corporate Compliance, der sich auf die IT im Unternehmen bezieht. Regelungen mit unmittelbarem Bezug zur IT-Compliance sind beispielsweise das Bundesdatenschutzgesetz (BDSG)[42], die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)[43], die Grundsätze ordnungsmäßiger datenverarbeitungsgestützter Buchführung (GoBS)[44] und SOX.[45] Aufgrund der Bedeutung der IT für das Unternehmen sind aber auch Regelungen mit mittelbarem Bezug zur IT von Bedeutung. Unternehmen können auch ohne explizite Nennung der IT in einem Gesetzestext zu Maßnahmen in Bezug auf die IT verpflichtet sein.[46]

Unternehmen sind durch das Handels- und Steuerrecht zur Einhaltung der Grundsätze ordnungsmäßiger Buchführung (GoB) verpflichtet. Durch die Abgabenordnung (AO) werden die GoB für IT-gestützte Buchführungssysteme durch die GoBS ergänzt. Ein Kriterium für die Einhaltung der GoBS ist die Gestaltung des internen Kontrollsystems. Das interne Kontrollsystem dient der Sicherung und dem Schutz des Vermögens, der Bereitstellung verlässlicher Aufzeichnungen, der Förderung der Effizienz und der Unterstützung der Geschäftspolitik.[47] Es umfasst die Kontrollen eines Unternehmens oder Unternehmensteiles.[48] Hinsichtlich der Kontrollen kann zwischen manuellen und maschinellen Kontrollen unterschieden werden. Maschinelle Kontrollen sind in die Informationssysteme integriert.[49]

IT-Compliance kann sich auch auf die Einhaltung nichtgesetzlicher Regeln beziehen, z. B. auf Vereinbarungen zwischen Organisationen oder innerhalb von Organisationen.

---

[39] Vgl. TEUBNER UND FELLER 2008, S. 403.
[40] Vgl. ebd., S. 405.
[41] Vgl. RATH UND SPONHOLZ 2008, S. 28.
[42] BDSG 2003.
[43] GDPDU 2001.
[44] GOBS 1995.
[45] Vgl. TEUBNER UND FELLER 2008, S. 404.
[46] Vgl. RATH 2009, S. 150.
[47] Vgl. GOBS 1995, Textziffer 4.
[48] Vgl. HÖMBERG 2002, Spalte 1230.
[49] Vgl. GOBS 1995, Textziffer 4.

3 Forschungsdesign

Die Integration der vorliegenden Dissertation in ein wissenschaftstheoretisches Fundament erfordert eine Beschreibung der gesetzten Forschungsziele und der eingesetzten Forschungsmethoden. Die Wissenschaftstheorie ist ein Teilgebiet der Philosophie.[50] Aus diesem Grund geht Abschnitt 3.1 auf philosophische Grundlagen ein, welche für die Einführung der wissenschaftstheoretischen Grundlagen in Abschnitt 3.2 benötigt werden. Die Einführung der wissenschaftstheoretischen Grundlagen ist eine Vorbereitung auf die Diskussion der wissenschaftstheoretischen Fundierung der Wirtschaftsinformatik in Abschnitt 3.3. Insbesondere werden dabei ausgewählte erkenntnistheoretische Positionen beschrieben. Schließlich stellt Abschnitt 3.4 die gesetzten Forschungsziele und die eingesetzten Forschungsmethoden vor.

3.1 Philosophische Grundlagen

Die Philosophie ist eine zu umfangreiche Disziplin, um im Rahmen dieser Dissertation eine angemessene Einführung geben zu können. Daher werden im Folgenden nur die Begriffe eingeführt, welche für die weitere Diskussion benötigt werden.

Folgende Bereiche der Philosophie werden für die weitere Diskussion benötig:

- Die **Ontologie** ist die Lehre vom Sein als solches.[51] Sie beschäftigt sich mit der Natur der Realität und des Erkennbaren.[52]
- Die **Epistemologie** ist die Lehre von der Erkenntnis.[53] Sie beschäftigt sich mit der Natur des Verhältnisses zwischen dem Erkennenden und dem Erkennbaren bzw. dem Wissenden und dem Erkannten.[54]
- Die **Methodologie** ist die Lehre von den wissenschaftlichen Methoden.[55] Sie beschäftigt sich damit, wie Wissen erlangt werden kann.[56]
- Die **Axiologie** ist die Lehre von den Werten.[57]

[50] Vgl. MITTELSTRASS ET AL. 1996, S. 738ff.
[51] Vgl. SCHMIDT 1974, S. 476f.
[52] Vgl. GUBA 1990, S. 18.
[53] Vgl. SCHMIDT 1974, S. 153.
[54] Vgl. GUBA 1990, S. 18.
[55] Vgl. MITTELSTRASS UND WOLTERS 1995B, S. 887.
[56] Vgl. GUBA 1990, S.18.
[57] Vgl. SCHMIDT 1974, S. 51.

In der weiteren Diskussion werden ferner die Bezeichnungen für die unterschiedlichen Arten des logischen – das bedeutet richtigen – [58] Schlussfolgerns verwendet. Dies sind die Folgenden:

- Als **Deduktion** wird das Schlussfolgern vom Allgemeinen auf das Besondere bezeichnet.[59] Es ist die Ableitung von Konsequenzen aus einer Regel und ihren Voraussetzungen.[60]
- Als **Induktion** wird das Schlussfolgern vom Besonderen auf das Allgemeine bezeichnet.[61] Es ist die Ableitung einer Regel aus Voraussetzungen und Konsequenzen.[62]
- Als **Abduktion** wird das Schlussfolgern von der Wirkung auf die Ursache bezeichnet.[63] Es ist die Ableitung von Voraussetzungen aus einer Regel und ihren Konsequenzen.[64]

Der Begriff der Abduktion wurde erst zu Beginn des 20. Jahrhunderts eingeführt. Die Abduktion kann als praktischer Schluss zur Bildung von Hypothesen aufgefasst werden.[65] Genauso wie induktive Schlüsse,[66] sind abduktive Schlüsse nicht sicher.

3.2 Wissenschaftstheoretische Grundlagen

Innerhalb der Wissenschaftstheorie sind besonders die unterschiedlichen erkenntnistheoretischen Positionen von Bedeutung. Diese haben einen entscheidenden Einfluss auf die verschiedenen Forschungsmethoden. Für die weitere Diskussion sind folgende Positionen relevant:

- Der **Rationalismus** bezeichnet Positionen, welche die Vernunft in den Mittelpunkt ihrer Betrachtungen stellen.[67] Im Rationalismus kann Erkenntnis nicht nur aus Sinneserfahrungen sondern auch aus vernünftigen Theorien abgeleitet werden.[68]

[58] Vgl. SCHMIDT 1974, S. 390f.
[59] Vgl. ebd., S. 103f.
[60] Vgl. MENZIEST 1996, S. 311.
[61] Vgl. SCHMIDT 1974, S. 296f.
[62] Vgl. MENZIEST 1996, S. 311.
[63] Vgl. SCHMIDT 1974, S. 2.
[64] Vgl. MENZIEST 1996, S. 311.
[65] Vgl. SANDKÜHLER 1999A, S. 7ff.
[66] Vgl. ebd., S. 629ff.
[67] Vgl. SCHMIDT 1974, S. 536f.
[68] Vgl. MITTELSTRASS ET AL. 1995, S. 464ff.

- Der **Empirismus** ist eine Position, die alle Erkenntnis aus Sinneserfahrungen ableitet. Folglich ist der Empirismus eine Gegenposition zum Rationalismus.[69]
- Der **Positivismus** ist eine Position, die Forschung und Darstellung allein auf Tatsachenbehauptungen beschränkt.[70] Auf diese Weise soll die Wissenschaft die wahre Natur der Realität und ihre wahren Gesetzte entdecken.[71]
- Der **logische Empirismus** ist durch den Empirismus und den Positivismus beeinflusst worden. Wie beim Empirismus wird alle Erkenntnis aus Sinneserfahrungen abgeleitet. Dabei wird die moderne Logik als Analysewerkzeug verwendet. Sie dient auch zur Identifizierung sogenannter Scheinprobleme und -sätze, welche insbesondere in der Philosophie und Theologie vermutet werden. Wie beim Positivismus erfolgt so eine Konzentration auf Tatsachen. Der logische Empirismus wird daher auch als logischer Positivismus bezeichnet.[72]
- Der **kritische Rationalismus** ist eine Gegenreaktion auf Probleme innerhalb des logischen Empirismus. Insbesondere wird der Versuch kritisiert, allgemeine Aussagen einer Theorie durch einzelne Sinneserfahrungen verifizieren zu wollen.[73] An die Stelle der induktiven Verifizierung von Theorien tritt deren Bewährung durch erfolglose deduktive Falsifizierungsversuche.[74] Der **Postpositivismus** geht auf Kritik wie den kritischen Rationalismus ein, ohne die Grundvorstellungen des Positivismus aufzugeben.[75]
- Der **Behaviorismus** ist eine Position der Psychologie, welche das Verhalten von lebenden Organismen mit Hilfe naturwissenschaftlicher Methoden untersucht. Der Behaviorismus orientiert sich am Positivismus und am Vorbild der Naturwissenschaften.[76]
- Der **Konstruktivismus** ist eine Position, die jegliche Erkenntnistätigkeit als konstruierende begreift.[77] Anstatt einer wahren Realität gibt es ausschließlich subjektive und kontextbezogene Realitäten.[78] Damit ist er eine Gegenposition zum Positivismus und Postpositivismus.

---

[69] Vgl. SCHMIDT 1974, S. 476f.
[70] Vgl. SCHMIDT 1974, S. 520; MITTELSTRASS ET AL. 1995, S. 301ff.
[71] Vgl. GUBA 1990, S. 19.
[72] Vgl. SANDKÜHLER 1999A, S. 322ff.
[73] Vgl. SANDKÜHLER 1999B, S. 1333ff.
[74] Vgl. MITTELSTRASS ET AL. 1995, S. 464ff.
[75] Vgl. GUBA 1990, S. 108f.
[76] Vgl. MITTELSTRASS UND WOLTERS 1995A, S. 274.
[77] Vgl. SANDKÜHLER 1999B, S. 722ff.
[78] Vgl. GUBA 1990, S. 25ff.

Tabelle 1: Unterschiede in den Grundvorstellungen im Positivismus, Postpositivismus und Konstruktivismus

Philosophische Bereiche	Erkenntnistheoretische Positionen		
	Positivismus	**Postpositivismus**	**Konstruktivismus**
Ontologie	naiver Realismus, reale Welt entspricht der sinnlichen Wahrnehmung	kritischer Realismus, reale Welt entspricht der sinnlichen Wahrnehmung, ist durch die menschliche Wahrnehmung aber nicht unmittelbar erkennbar	Relativismus, lokal und spezifisch konstruierte Wirklichkeiten
Epistemologie	Objektivität, Ergebnisse sind wahr	Objektivität, kritische Community, Ergebnisse könnten wahr sein	Subjektivität, erstellte Ergebnisse
Methodologie	Experiment, Verifizierung von Hypothesen, hauptsächlich quantitative Methoden	modifiziertes Experiment, Falsifizierung von Hypothesen, zusätzlich qualitative Methoden	Hermeneutik, Dialektik

Quelle: Modifizierte Version einer Tabelle in GUBA UND LINCOLN 1994, S. 109.

Von besonderer Bedeutung für die weitere Diskussion sind die erkenntnistheoretischen Positionen des Positivismus, des Postpositivismus und des Konstruktivismus. Tabelle 1 erläutert wesentliche Unterschiede in den Grundvorstellungen dieser erkenntnistheoretischen Positionen. Dabei wird nach den philosophischen Bereichen der Ontologie, Epistemologie und Methodologie untergliedert. Besonders anschaulich werden dabei die Ähnlichkeiten zwischen dem Positivismus und dem Postpositivismus sowie deren Unterschiede zum Konstruktivismus.

3.3 Wissenschaftstheoretische Fundierung der Wirtschaftsinformatik

Die Wirtschaftsinformatik ist eine interdisziplinäre Wissenschaft. Sie hat vor allem Schnittmengen mit der Betriebswirtschaftslehre und der Informatik, aber auch mit den Ingenieurswissenschaften und der Mathematik. Gleichwohl hat die Wirtschaftsinformatik einen eigenen Kern. Sie beinhaltet somit mehr als die Vereinigung der genannten Schnittmengen.[79] Zur Erläuterung der wissenschaftstheoretischen Fundierung der Wirtschaftsinformatik wird zunächst auf ihren Forschungsgegenstand und ihr Forschungsziel eingegangen. Anschließend werden ihre Forschungsmethoden umrissen.

[79] Vgl. FINK ET AL. 2005, S. 1f.; MERTENS ET AL. 2005, S. 5.

3.3.1 Forschungsgegenstand und Forschungsziel

Forschungsgegenstand der Wirtschaftsinformatik ist die Untersuchung betrieblicher Informationssysteme und den für ihre Nutzung bedeutsamen Kontext des Handlungssystems.[80] Informationssysteme manipulieren Informationen und stellen diese für ihre Benutzer bereit.[81] Sie verwenden Informationstechnologien, beziehen aber auch Menschen und deren organisatorisches Umfeld mit ein. Informationssysteme sind also soziotechnische Systeme in denen menschliche und technische Elemente arbeitsteilig zusammenwirken.[82] In einem Handlungssystem werden Objekte durch Handlungen von Akteuren manipuliert. Zu den Handlungssystemen gehören auch die betrieblichen Organisationen. Die Mitarbeiter einer Organisation führen Handlungen zur Erbringung von Leistungen durch. Informationssysteme sind in Handlungssysteme eingebettet und unterstützen diese.[83] Der für ein Informationssystem bedeutsame Kontext des Handlungssystems ist dessen Handlungskontext.

Forschungsziel der Wirtschaftsinformatik ist Wissen, welches eine höhere Wirtschaftlichkeit der Gestaltung und Nutzung von Informationssystemen in Aussicht stellt.[84] Besonders hervorzuheben ist die Dynamik der Informationssysteme und des Handlungskontextes. So führt die Entwicklung oder Weiterentwicklung von Informationssystemen zu Reaktionen im Handlungskontext. Der Handlungskontext beeinflusst wiederum die Entwicklung und Weiterentwicklung von Informationssystemen.[85]

3.3.2 Forschungsmethoden

In der Wirtschaftsinformatik kommt eine Vielzahl an Forschungsmethoden zum Einsatz. Folgende Methoden werden besonders häufig eingesetzt:[86]

- **Deduktive Analysen** basieren auf deduktiven Schlüssen. Die deduktiven Schlüsse werden im Rahmen von formalen, konzeptionellen oder rein sprachlichen Modellen vorgenommen.
- **Prototyping** beschäftigt sich mit der Entwicklung und Evaluation von Informationssystemen.

[80] Vgl. FRANK 2007, S. 157.
[81] Vgl. MYRACH 2008, S. 100.
[82] Vgl. ebd., S. 101ff.
[83] Vgl. ebd., S. 103f.
[84] Vgl. FRANK 2007, S. 157.
[85] Vgl. ebd., S. 158.
[86] Vgl. hier und im Folgenden WILDE UND HESS 2007, S. 282ff.

- **Fallstudien** untersuchen komplexe Phänomene in ihrem natürlichen Kontext.
- **Quantitative Querschnittsanalysen** erheben Daten über mehrere Individuen hinweg und werten diese mit quantitativen Methoden aus.

Die am häufigsten eingesetzte Methode in der Wirtschaftsinformatik ist die deduktive Analyse im Rahmen von rein sprachlichen Modellen. Diese Methode wird auch als argumentativ-deduktive Analyse bezeichnet.[87]

Die anglo-amerikanische und international dominierende Schwesterdisziplin der Wirtschaftsinformatik wird „Information Systems" genannt.[88] In der Disziplin Information Systems kommt die argumentativ-deduktive Analyse deutlich weniger zum Einsatz. Auf Prototyping wird nahezu ganz verzichtet. Die am häufigsten eingesetzte Methode ist die quantitative Querschnittsanalyse. Deutlich häufiger finden auch Labor- und Feldexperimente statt.[89] Diese Experimente untersuchen bestimmte Kausalzusammenhänge in kontrollierten Umgebungen.[90]

Der Verzicht auf Prototyping ist kennzeichnend für Information Systems. Information Systems beschäftigt sich im Vergleich zur Wirtschaftsinformatik weniger mit der Gestaltung innovativer Informationssysteme als mit der Untersuchung existierender Informationssysteme. Für die Untersuchung werden vorzugsweise positivistische Methoden eingesetzt. Die vorherrschende erkenntnistheoretische Position in Information Systems ist der Behaviorismus.[91] Die Gestaltung von Informationssystemen wird auch als Design Science, die Untersuchung von Informationssystemen als Behavioral Science bezeichnet.[92]

Gerade die Konferenzen und Zeitschriften mit der höchsten internationalen Sichtbarkeit sind durch Behavioral Science geprägt. Die Chancen für die Publikation von Design Science sind vergleichsweise gering.[93] Innerhalb der Wirtschaftsinformatik aber auch innerhalb Information Systems gibt es Anstrengungen, die internationale Akzeptanz von Design Science zu erhöhen.

[87] Vgl. WILDE UND HESS 2007, S. 282.
[88] Vgl. FRANK 2007, S. 156.
[89] Vgl. WILDE UND HESS 2007, S. 285.
[90] Vgl. ebd., S. 282.
[91] Vgl. FRANK 2007, S. 161ff.
[92] Vgl. HEVNER ET AL. 2004, S. 75.
[93] Vgl. HEVNER UND CHATTERJEE 2010, S. IX; WKWI UND GI-FB WI 2008, S. 155.

3.4 Forschungsziele und Forschungsmethoden

Informationssysteme werden für eine Vielzahl an Anwendungsgebieten eingesetzt. Ferner werden ständig neue Informationssysteme entwickelt oder bestehende Informationssysteme weiterentwickelt. Die Konzentration auf einzelne Anwendungsgebiete erleichtert das Verfolgen des dortigen Wandels und damit dessen Gestaltung durch eigene Forschungsbeiträge. Der Anstoß für diese Gestaltung kann sowohl durch Problemstellungen aus der Praxis als auch aus der Wissenschaft erfolgen. Auf Grundlage dieser Problemstellungen werden Forschungsziele formuliert.[94] Zur Verfolgung dieser Forschungsziele werden Forschungsmethoden eingesetzt. Im Folgenden wird auf die Forschungsziele und Forschungsmethoden der vorliegenden Dissertation eingegangen.

3.4.1 Forschungsziele

Die Forschungsziele sind durch praktische Erfahrungen und wissenschaftliche Recherchen beeinflusst worden. Die praktischen Erfahrungen sind im Rahmen der aktuellen Arbeit als Anwendungsbetreuer für SAP NetWeaver Business Intelligence Systeme und durch die ehemalige Arbeit als System- und Prozessprüfer in einer Wirtschaftsprüfungsgesellschaft gewonnen worden. Dabei sind Problemstellungen hinsichtlich der Interoperabilität von BI/OLAP/DW Systemen und hinsichtlich der Überwachung von maschinellen Kontrollen identifiziert worden.

Die Analyse von Daten erfordert neben dafür geeigneten Systemen auch umfangreiches Wissen hinsichtlich der Bedeutung der Daten. Erhebliche Teile dieses Wissens werden durch die Definition von Funktionen (für Kennzahlen) und Mengen (von Schlüssel- oder Attributwerten) durch die Benutzer von BI/OLAP/DW Systemen in diesen abgelegt. Für einen Austausch dieses Wissens gibt es im Gegensatz zum Austausch von Daten aber kaum Möglichkeiten. Dies beeinträchtigt die Interoperabilität der Systeme. Als Interoperabilität wird die Fähigkeit von zwei oder mehr Systemen oder Systemteilen (Komponenten) verstanden, Informationen untereinander austauschen und die ausgetauschten Informationen nutzen zu können.[95]

Erhebliche Teile von internen Kontrollsystemen können als maschinelle Kontrollen in unterstützende Informationssysteme integriert werden. Um sicherzustellen, dass die maschinellen Kontrollen richtig in den Systemen implementiert und damit wirksam

[94] Vgl. ÖSTERLE ET AL. 2010, S. 4.
[95] Vgl. IEEE 1990, S. 114.

sind, müssen sie regelmäßig überwacht werden. Aufgrund der Heterogenität und Komplexität der Systeme kann dies eine schwierige und zeitaufwendige Aufgabe sein. Gleichwohl ist eine zeitnahe Berichterstattung eventueller Ausnahmen für das rechtzeitige Einleiten von Gegenmaßnahmen und somit für die Wirksamkeit eines internen Kontrollsystems notwendig. Eine Möglichkeit zur regelmäßigen Überwachung von Kontrollen und zur zeitnahen Berichterstattung von Ausnahmen ist der Einsatz entsprechender Informationssysteme.

Die wissenschaftlichen Recherchen sind im Rahmen der Einarbeitung in die Literatur zum Forschungsgebiet BI/OLAP/DW und zum Forschungsgebiet IT-Compliance durchgeführt worden. Dabei sind Forschungslücken hinsichtlich der Problemstellungen identifiziert worden. Auf Grundlage der Problemstellungen und der Forschungslücken sind folgende Forschungsziele definiert worden:

A. Gestaltung von Artefakten zur Verbesserung der Interoperabilität von BI/ OLAP/DW Systemen durch Einsatz von Ontologien und automatisiertes Schlussfolgern,
B. Gestaltung von Artefakten zur automatisierten regelbasierten Überwachung maschineller Kontrollen und zur zielgruppengerechten Berichterstattung von Kontrollausnahmen.

In den folgenden Absätzen findet zunächst eine Begriffsdefinition statt.

Unter einem Artefakt wird in der Wirtschaftsinformatik ein Konstrukt, ein Modell, eine Methode oder eine Instanz verstanden. Konstrukte sind Konzepte, Terminologien oder Sprachen. Instanzen sind Implementierungen von Konstrukten, Modellen und Methoden als Prototypen oder produktive Informationssysteme.[96]

Anders als in der Philosophie und Wissenschaftstheorie wird unter einer Ontologie in der Informatik und Wirtschaftsinformatik eine explizite Spezifizierung einer Konzeptualisierung verstanden. Eine Konzeptualisierung bezeichnet wiederum eine abstrakte und vereinfachte Sicht auf einen Ausschnitt der zu repräsentierenden Welt.[97] Für die Konstruktion und den Austausch von Ontologien gibt es eigene Ontologiesprachen. Diese Ontologiesprachen dienen der Repräsentation des Wissens in einer Ontologie. Ferner ermöglichen sie automatisiertes Schlussfolgern,[98] wodurch die Konsistenz des

[96] Vgl. ÖSTERLE ET AL. 2010, S. 4.
[97] Vgl. GRUBER 1993, S. 199ff.
[98] Vgl. CORCHO UND GÓMEZ-PÉREZ 2000, S. 80ff.

Wissens in einer Ontologie überprüft und implizit enthaltenes Wissen explizit gemacht werden kann.[99]

Unter einer Regel wird eine Verknüpfung von Voraussetzungen mit Konsequenzen verstanden. Sofern die Voraussetzungen einer Regel erfüllt sind, müssen auch die Konsequenzen dieser Regel erfüllt sein. Somit sind Regeln zum deduktiven Schlussfolgern geeignet.

Schließlich wird unter einer Kontrollausnahme eine nicht wirksame Kontrolle verstanden, die das interne Kontrollsystem einer Organisation beeinträchtigen kann. Mängel im internen Kontrollsystem bergen Risiken für die Anspruchsgruppen einer Organisation.

3.4.2 Forschungsmethoden

Da die Forschungsziele nicht auf die Untersuchung von Informationssystemen, sondern auf deren Gestaltung gerichtet sind, kommt nicht Behavioral Science sondern Design Science als Forschungsmethode zum Einsatz. Innerhalb eines Design Science Rahmens wird in den Forschungsbeiträgen des Weiteren argumentativ-deduktiv oder konzeptionell-deduktiv für die Gestaltung von Konstrukten, Modellen und Methoden vorgegangen. Für die Implementierung dieser Konstrukte, Modelle und Methoden durch Instanzen wird Prototyping eingesetzt.

In den folgenden Abschnitten wird auf Design Science als Forschungsmethode eingegangen. Diese Forschungsmethode vertritt eine eigene erkenntnistheoretische Position, die beschrieben wird. Die Diskussion orientiert sich weitgehend an der grundlegenden Arbeit von VAISHNAVI UND KÜCHLER 2009.

Design Science als Forschungsmethode beginnt mit einem Problembewusstsein. Dieses Bewusstsein für eine Problemstellung kann in der Praxis oder in der Wissenschaft entstanden sein. Die Lösung dieser Problemstellung ist das Forschungsziel. Zum Erreichen dieses Forschungsziels werden auf Grundlage des verfügbaren Wissens abduktiv Lösungsvorschläge erarbeitet. Diese Lösungsvorschläge führen zu einem vorläufigen Design. Ausgehend von diesem vorläufigen Design wird das verfügbare Wissen deduktiv zur Entwicklung und anschließenden Evaluation eines Artefaktes eingesetzt. Sowohl durch die Entwicklung als auch durch die Evaluation entsteht Wissen über die Anwendbarkeit von Wissen. Dies wird als Circumscription bezeichnet. Circumscription ist eine

[99] Vgl. W3C 2009.

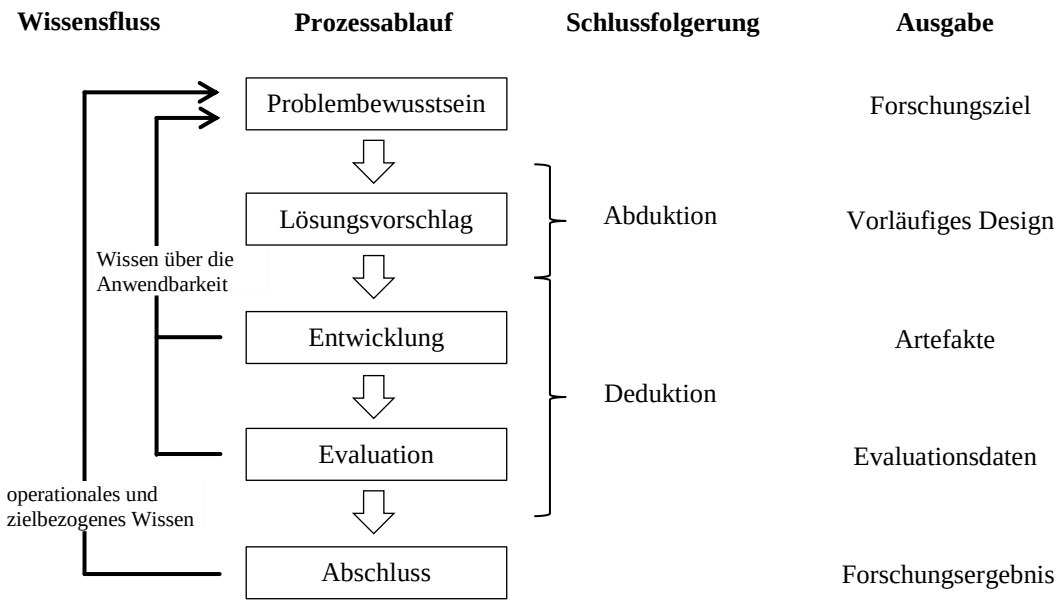

Abbildung 6: Design Science als Forschungsmethode.

Quelle: Modifizierte Version von Darstellungen in TAKEDA ET AL. 1990, S. 45 und VAISHNAVI UND KÜCHLER 2009.

Methode der formalen Logik. Diese Methode nimmt an, dass jegliches Wissen nur in bestimmten Situationen anwendbar ist. Die Anwendbarkeit von Wissen kann aber nur durch das Entdecken von Widersprüchen erkannt werden. Diese Widersprüche treten aufgrund der Unvollständigkeit des verfügbaren Wissens regelmäßig auf. Daher sind in der Regel mehrere Iterationen des beschriebenen Prozesses zum Erreichen des Forschungsziels notwendig. Nachdem das Forschungsziel erreicht worden ist, wird das gewonnene Wissen zusammengefasst und als Forschungsergebnis verbreitet. Abbildung 6 stellt Design Science als Forschungsmethode grafisch dar.

Als erkenntnistheoretische Position unterscheidet sich Design Science sowohl vom Positivismus und Postpositivismus, als auch vom Konstruktivismus. Durch die Gestaltung von Informationssystemen verändert Design Science den Zustand eines Ausschnittes der Welt. Folglich müssen alternative Weltzustände möglich sein. Im Design Science sind diese alternativen Weltzustände das Sein und das Erkennbare. Die möglichen Weltzustände werden durch die Naturgesetze der Realität begrenzt. Beispielsweise wird die Kommunikationsgeschwindigkeit von Systemen durch die Lichtgeschwindigkeit

Tabelle 2: Unterschiede in den Grundvorstellungen im Positivismus/Postpositivismus, Konstruktivismus und Design Science

Philosophische Bereiche	Erkenntnistheoretische Positionen		
	Positivismus/Postpositivismus	**Konstruktivismus**	**Design Science**
Ontologie	eine einzige Realität, erkennbar	mehrere Realitäten, sozial konstruiert	mehrere alternative Welt-zustände, sozialtechnologisch ermöglicht
Epistemologie	Objektivität, leidenschaftslose und losgelöste Betrachter der Wahrheit	Subjektivität, Werte und Wissen beeinflusst durch die Interaktion zwischen Forschern und Teilnehmern	Wissen durch Gestalten, Gestaltung von Artefakten, Erkennen der Anwendbarkeit von Wissen durch Circumscription
Methodologie	Betrachtung, quantitative/statistische Methoden	Mitwirkung, qualitative Methoden, Hermeneutik, Dialektik	Entwicklung, Auswirkungen des Artefakts auf das Informations-system und den Handlungs-kontext
Axiologie	universelle Wahrheit, Vorhersage	situationsbezogenes Verstehen	Erschaffung, Fortschritt

Quelle: Modifizierte Version von Tabellen in GREGG ET AL. 2001, S. 172 und VAISHNAVI UND KÜCHLER 2009.

begrenzt. Diese Realität steht im Design Science aber nicht im Mittelpunkt. Hingegen ist sie im Positivismus und Postpositivismus das Sein und das Erkennbare. Im Konstruktivismus wird von mehreren sozialkonstruierten Realitäten ausgegangen.

Im Design Science entsteht Wissen durch Gestalten. Durch die Gestaltung von Artefakten entsteht Wissen über die Lösung von Problemstellungen und durch Circumscription entsteht Wissen über die Anwendbarkeit dieses Wissens. Das Wissen kann objektiv hergeleitet sein (beispielsweise ein Algorithmus) oder subjektiv geprägt sein (beispielsweise eine Realisierung in einem Handlungskontext). Design Science dient der Erschaffung und dem Fortschritt. Weder versucht Design Science wie im Positivismus und Postpositivismus, die Wahrheit zu finden oder vorherzusagen, noch beschränkt sich Design Science wie im Konstruktivismus auf das Verstehen von Systemen.

Tabelle 2 fasst die unterschiedlichen Grundvorstellungen im Positivismus/Postpositivismus, Konstruktivismus und Design Science zusammen.

4 Forschungsstand

Ausgangspunkt für das Erreichen der Forschungsziele ist der gegenwärtige Forschungsstand. Um diesen richtig zu bestimmen, ist strukturiert in der vorhandenen Literatur recherchiert worden. Die folgenden Abschnitte untergliedern die Literaturrecherche nach den Forschungsgebieten.

4.1 Forschungsgebiet BI/OLAP/DW und Forschungsziel A

Ausgangspunkt für die Einarbeitung in das Forschungsgebiet BI/OLAP/DW sind Suchanfragen in einschlägigen Internetdatenbanken mit Literatur zur Informatik und Wirtschaftsinformatik gewesen. Die Suchanfragen wurden Mitte 2008 durchgeführt. Dabei sind Begriffe verwendet worden, die eine Zugehörigkeit zum Forschungsgebiet nahelegen. Dies sind insbesondere verschiedene Ausprägungen der Begriffe BI, OLAP und DW gewesen. Als Internetdatenbanken sind der Association for Computing Machinery (ACM) Guide to Computing Literature[100], Engineering Village[101], IngentaConnect[102], ScienceDirect[103] und SpringerLink[104] ausgewählt worden. Die Suchergebnisse sind aus den einzelnen Internetdatenbanken in eine gemeinsame Literaturdatenbank übernommen und von redundanten Datensätzen bereinigt worden. Anschließend sind die Titel und Zusammenfassungen aller Beiträge, die ab Anfang 2006 veröffentlicht wurden, gelesen worden. Dies sind in etwa 2.400 Beiträge gewesen. Nach dem Lesen sind die Beiträge inhaltlich kategorisiert worden. Auf diese Weise sind sowohl aktuelle Forschungsthemen als auch relevanten Zeitschriften und Konferenzen identifiziert worden.[105]

Im Rahmen der Arbeit an den Forschungsbeiträgen zum Forschungsgebiet BI/ OLAP/DW sind die genannten Internetdatenbanken, die relevanten Zeitschriften und die Tagungsbände der relevanten Konferenzen sowohl Anfang 2009 als auch Anfang 2010 erneut nach Begriffen zu Forschungsziel A durchsucht worden. Zu den relevanten Ergebnissen wird in den Forschungsbeiträgen Bezug genommen.[106] Zu den Herausforderungen bei der Suche nach verwandter Literatur gehört deren unterschiedliche

[100] ACM 2010.
[101] ELSEVIER 2010a.
[102] PUBLISHING TECHNOLOGY 2010.
[103] ELSEVIER 2010b.
[104] SPRINGER 2010b.
[105] Vgl. Abschnitt 5.1 und Anhang A.
[106] Vgl. Anhang B und G.

Verbreitung. So werden Zeitschriften und Tagungsbände über verschiedene Verlage, verschiedene Organisationen oder eigene Auftritte im Internet verbreitet. Zwar gibt es Metadatenbanken wie das Digital Bibliography & Library Project (DBLP)[107], welche Beiträge aus verschiedenen Quellen einbeziehen, diese sind aber nicht vollständig. Weder enthalten sie alle Beiträge, noch alle Daten zu den enthaltenen Beiträgen. Dies betrifft insbesondere die Volltexte. Für einen Zugriff auf diese verlangen die Verlage, Organisationen und Zeitschriften häufig eine Gebühr. In der Konsequenz müssen Volltextsuchen in vielen verschiedenen Datenbanken durchgeführt werden. Diese Datenbanken verwenden eine unterschiedliche Anfragesyntax und setzten unterschiedliche Suchverfahren ein. Folglich sind die Ergebnisse nur bedingt vergleichbar. Zum Teil sind auch gar keine Volltextsuchen möglich.

Um die relevante Literatur gleichzeitig umfassend und tiefgehend nach verwandten Beiträgen zu durchsuchen, sind Mitte 2010 alle über institutionelle Zugänge wissenschaftlicher Bibliotheken in Hannover elektronisch verfügbaren Ausgaben relevanter Zeitschriften und Tagungsbände relevanter Konferenzen seit Anfang 2000 beschafft und durch ein leistungsfähiges Suchprogramm für eine Volltextsuche indiziert worden. Dabei sind die Zeitschriften und Konferenzen in den WI-Orientierungslisten[108] der Wissenschaftlichen Kommission Wirtschaftsinformatik (WKWI) im Verband der Hochschullehrer für Betriebswirtschaft e.V. (VHB) und des Fachbereiches Wirtschaftsinformatik der Gesellschaft für Informatik (GI-FB WI) berücksichtigt worden, sofern sich diese mit der Wirtschaftsinformatik im Allgemeinen oder mit einem der beiden Forschungsgebiete im Besonderen beschäftigen. Für das Forschungsgebiet BI/OLAP/DW sind zusätzlich die durch die strukturierte Literaturrecherche identifizierten Zeitschriften und Konferenzen berücksichtigt worden. Tabelle 3 enthält eine Übersicht der indizierten Ausgaben von Zeitschriften und Tabelle 4 eine Übersicht der indizierten Tagungsbände von Konferenzen. Insgesamt sind in etwa 63.000 Dateien indiziert worden.

Für die Suche in den indizierten Dateien ist zunächst hinsichtlich des Forschungsgebietes BI/OLAP/DW eingeschränkt worden. Die Beiträge sind nur in die Suchergebnisse aufgenommen worden, wenn im Volltext eine der Zeichenketten „Business Intelligence“, „Data Warehouse“, „Data Warehousing“, „Online Analytical Processing“ oder „OLAP“ vorkommt. Diese Bedingung ist von 6.129 Dateien erfüllt worden.

[107] UNI TRIER 2010.
[108] WKWI UND GI FB-WI 2008.

Tabelle 3: Übersicht der für die Volltextsuche indizierten Ausgaben von Zeitschriften.

Zeitschrift	Jahre
ACM Transactions on Information and System Security (TISSEC, ACM)	2000-2010
ACM Transactions on Information Systems (TOIS, ACM)	2000-2010
ACM Transactions on Knowledge Discovery from Data (TKDD, ACM)	2007-2010
Australasian Journal of Information Systems (AJIS, AAIS)	2000-2010
Communications of the ACM (CACM, ACM)	2000-2010
Communications of the Association for Information Systems (CAIS, AIS)	2000-2010
Computers & Security (COSE, Elsevier)	2000-2010
Data & Knowledge Engineering (DATAK, Elsevier)	2000-2010
Decision Sciences (DSJ, Wiley)	2000-2010
Decision Support Systems (DECSUP, Elsevier)	2000-2010
Expert Systems with Applications (ESWA, Elsevier)	2000-2010
IEEE Intelligent Systems Magazine (M-IS, IEEE)	2000-2010
IEEE Transactions on Data and Knowledge Engineering (T-KDE, IEEE)	2000-2010
Information & Management (INFMAN, Elsevier)	2000-2010
Information Processing & Management (IPM, Elsevier)	2000-2010
Information Sciences (INS, Elsevier)	2000-2010
Information Systems (INFOSYS, Elsevier)	2000-2010
Information Systems Frontiers (ISF, Springer)	2000-2010
Information Systems Journal (ISJ, Wiley)	2000-2010
Information Systems Research (ISR, INFORMS)	2000-2010
Intelligent Systems in Accounting, Finance & Management (ISAF, Wiley)	2000-2010
International Journal of Accounting Information Systems (ACCINF, Elsevier)	2001-2010
International Journal of Information Management (IJIM, Elsevier)	2000-2010
International Journal of Information Security (IJIS, Springer)	2000-2010
Journal of Computational Information Systems (JOFCIS, Binary Information Press)	2007-2010
Journal of Computer Information Systems (JCIS, IACIS)	2007-2009
Journal of Intelligent Information Systems (JIIS)	2000-2010
Journal of Strategic Information Systems (JSIS, Elsevier)	2000-2010
Journal of the Association for Information Systems (JAIS, AIS)	2000-2010
Knowledge and Information Systems (KAIS, Springer)	2000-2010
Knowledge-Based Systems (KNOSYS, Elsevier)	2000-2010
The VLDB Journal (VLDB Journal)	2000-2010
Wirtschaftsinformatik (WI Zeitschrift)	2006-2010
WSEAS Transactions in Information Science and Applications (TISA, WSEAS)	2004-2010

Quelle: Eigene Daten.

Ausgehend von den 6129 Dateien ist weiter hinsichtlich des Forschungsziels A eingeschränkt worden. Dabei wurden folgende Gruppen von Zeichenketten gebildet:

(1) „Interoperability“, „Interoperabilität“, „Exchange“, „Austausch“, „Compatibility“ oder „Kompatibilität“
(2) „Ontology“, „Ontologies“, „Ontologie“ oder „Ontologien“
(3) „Reasoning“, „Schlussfolgern“, „Inference“ oder „Inferenz“

Tabelle 4: Übersicht der für die Volltextsuche indizierten Tagungsbände von Konferenzen.

Konferenzen	Jahre
ACM SIGMOD Conference on Management of Data (ACM SIGMOD)	2000-2010
ACM Symposium on Applied Computing (ACM SAC)	2000-2010
Advances in Databases and Information Systems (ADBIS)	2000-2010
Advances in Information Systems (ADVIS)	2000, 2002, 2004, 2006
Americas Conference on Information Systems (AMCIS)	2000-2009
British National Conference on Databases (BNCOD)	2000-2009
Business Intelligence for the Real-Time Enterprises (BIRTE)	2006
Data Warehousing and Knowledge Discovery (DaWaK)	2000-2009
Database and Expert Systems Applications (DEXA)	2000-2009
Database Systems for Advanced Applications (DASFAA)	2004-2010
Design and Management of Data Warehouses (DMDW)	2000-2003
European Conference on Information Systems (ECIS)	2000-2010
European Symposium Research Computer Security (ESORICS)	2000, 2002-2009
Hawaii International Conference on System Sciences (HICSS)	2000-2010
IEEE Symposium on Security and Privacy (IEEE SP)	2000-2010
International Conference on Advanced Information Systems (CAiSE)	2000-2009
International Conference on Availability, Reliability and Security (ARES)	2009-2010
International Conference on Business Process Management (BPM)	2000, 2003-2009
International Conference on Computational Science (ICCS)	2001-2009
International Conference on Data Engineering (ICDE)	2000-2009
International Conference on Extending Database Technology (EDBT)	2000, 2002-2010
International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)	2007-2008
International Conference on Information and Knowledge (CIKM)	2000-2009
International Conference on Information Systems (ICIS)	2000-2009
International Conference on Knowledge Discovery and Data Mining (KDD)	2000-2009
International Conference on Scientific and Statistical Database Management (SSDBM)	2000-2010
International Conference on the Entity-Relationship Approach (ER)	2000-2009
International Conferences on Very Large Databases (VLDB Conference)	2000-2009
International Symposium on Database Engineering & Applications (IDEAS)	2000-2009
International Workshop on Data Warehousing and OLAP (DOLAP)	2000-2009
Multikonferenz Wirtschaftsinformatik (MKWI)	2008, 2010
Wirtschaftsinformatik (WI Konferenz)	2001, 2003, 2005, 2007, 2009

Quelle: Eigene Daten.

Abbildung 7 illustriert die Anzahl der Suchergebnisse zu den einzelnen Gruppen. In der Gruppe (1) gibt es 1.927, in der Gruppe (2) 807 und in der Gruppe (3) 1.427 Beiträge. In der Schnittmenge von Gruppe (1) und (2) gibt es 408, in der von Gruppe (1) und (3) 555 und in der von Gruppe (2) und (3) 385 Beiträge. Schließlich gibt es 216 Beiträge in der Schnittmenge von Gruppe (1), (2) und (3). Hinsichtlich der Beiträge in dieser Gesamtschnittmenge ist der größte Bezug zu Forschungsziel A zu erwarten. Daher sind die Titel und Zusammenfassungen dieser Beiträge gelesen worden. Abbildung 8 stellt dar, bei welchen Konferenzen und Zeitschriften die Beiträge veröffentlicht worden sind.

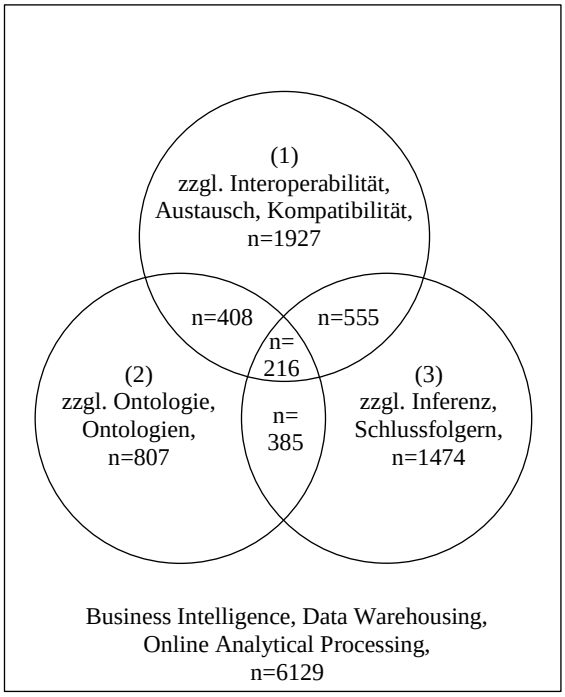

Abbildung 7: Anzahl der Suchergebnisse zu den gebildeten Gruppen. Der größte Bezug zu Forschungsziel A ist für die Beiträge in der Schnittmenge von (1), (2) und (3) zu erwarten.

Quelle: Eigene Darstellung.

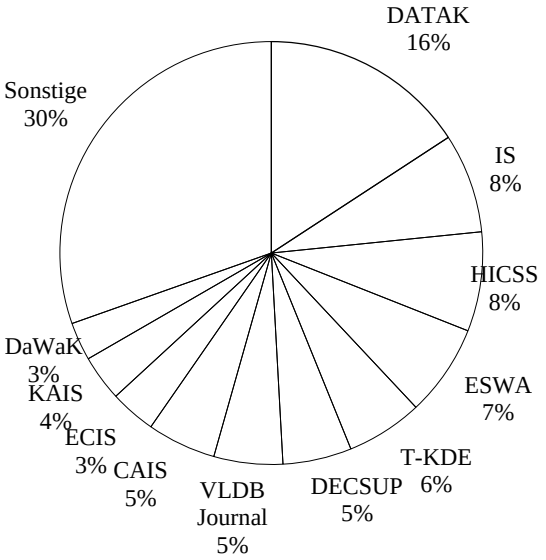

Abbildung 8: Gruppierung der Beiträge in der Schnittmenge von (1), (2) und (3) nach Konferenzen / Zeitschriften.

Quelle: Eigene Darstellung.

Auffallend viele Beiträge in der Schnittmenge beschäftigen sich mit den Themen Datenintegration, Datenmodellierung und Modellmanagement. In Bezug auf das Forschungsgebiet BI/OLAP/DW können diese Themen den Bereichen ETL-Prozesse und multidimensionale Modellierung zugeordnet werden. Nur wenige Beiträge haben einen starken Bezug zu Forschungsziel A. Im Folgenden wird auf diese Beiträge eingegangen.

Ein Modell und eine Architektur zur Integration von Wissensmanagement und Data Warehousing beschreibt KERSCHENBERG 2001. Modell und Architektur werden allgemein beschrieben. Auf die für eine Implementierung notwendigen Details wird nicht eingegangen.

NGUYEN ET AL. 2003 beschreiben einen Ansatz zur Integration von heterogenen Data Warehouse Systemen auf Grundlage von XML Topic Maps (XTM)[109]. Durch den Einsatz der Topic Maps soll den semantischen Unterschieden in den verschiedenen Modellen Rechnung getragen werden. Topic Maps sind ein Standard der International Organization for Standardization (ISO)[110]. Sie haben Gemeinsamkeiten mit dem Resource

[109] ISO / IEC 2006.
[110] ISO 2010.

Description Framework (RDF)[111] und der Web Ontology Language (OWL)[112] des World Wide Web Consortiums (W3C)[113]. Ferner gibt es Ansätze zur Kombination von Topic Maps und RDF/OWL.[114] Auf Möglichkeiten zum automatisierten Schlussfolgern wird nicht eingegangen.

Das Design und die Entwicklung eines Tools zur Integration von heterogenen Data Warehouse Systemen beschreiben TORLONE UND PANELLA 2005. Das Tool überprüft die Gültigkeit von Zuordnungen zwischen verschiedenen Dimensionen. Danach werden mit Hilfe der Zuordnungen übergreifende Anfragen oder Sichten erstellt. Ontologien werden nicht eingesetzt.

SKOUTAS UND SIMITSIS 2006 gehen auf den Einsatz von Ontologien für das Design von Extraktions-, Transformations- und Ladeprozessen ein. Ausgehend von einer semantischen Annotation verschiedener Datenquellen wird eine Ontologie erstellt. Anschließend wird durch Schlussfolgern ermittelt, welche Arten von Transformationen durchzuführen sind. Eine konkrete Definition dieser Transformationen wird aber nicht erstellt.

Schließlich schlagen ROMERO UND ABELLÓ 2007 eine Methode zur teilautomatisierten Erstellung des multidimensionalen Modells von Data Warehouse Systemen vor. Ausgehend von einer Beschreibung verschiedener Datenquellen durch eine Ontologie werden mehrere Stern- oder Schneeflockenschemata einschließlich Hierarchien erstellt. Dabei wird auch auf Möglichkeiten zum automatischen Schlussfolgern eingegangen.

Die Beiträge sind ausnahmslos über Konferenzen zum Forschungsgebiet BI/OLAP/ DW veröffentlicht worden. Insgesamt gibt es nur wenige Beiträge zu Forschungsziel A.

4.2 Forschungsgebiet IT-Compliance und Forschungsziel B

Im Rahmen der Arbeit an den Forschungsbeiträgen zum Forschungsgebiet IT-Compliance sind die einschlägigen Internetdatenbanken zwischen Anfang 2009 und Mitte 2010 mehrfach nach Begriffen zu Forschungsziel B durchsucht worden. Zu den relevanten Ergebnissen wird in den Forschungsbeiträgen Bezug genommen.[115] Zusätzlich ist Mitte 2010 – analog zum Vorgehen für das Forschungsgebiet BI/OLAP/DW und Forschungsziel A – eine Volltextsuche in den elektronisch verfügbaren Ausgaben rele-

[111] W3C 2004.
[112] W3C 2009.
[113] W3C 2010.
[114] W3C 2006A; W3C 2006B.
[115] Vgl. Anhang C, D, E, F und H.

vanter Zeitschriften und Tagungsbände relevanter Konferenzen seit Anfang 2000 durchgeführt worden.

Für die Suche in den indizierten Dateien ist zunächst hinsichtlich des Forschungsgebietes IT-Compliance eingeschränkt worden. Die Beiträge sind nur aufgenommen worden, wenn im Volltext eine der Zeichenketten „IT-Compliance“, „IT Compliance“, „Internal Control“, „Interne Kontrolle“, „Internal Control System“, „Internes Kontrollsystem“, „IT-Audit“ oder „IT Audit“ vorkommt. Diese Bedingung ist von 473 Dateien erfüllt worden. Ausgehend von diesen Dateien ist weiter hinsichtlich des Forschungsziels B eingeschränkt worden. Dabei sind folgende Gruppen gebildet worden:

(1) „Monitoring”, „Überwachung, „monitor” oder „überwachen”
(2) „Reporting“, „Berichterstattung“, „report“ oder „berichten“
(3) „Rules”, „Regeln”, „rule”, „Regel”, „Policies”, „Richtlinien”, „Policy” oder „Richtlinie“

Abbildung 9 illustriert die Anzahl der Suchergebnisse zu den einzelnen Gruppen. In der Gruppe (1) gibt es 237, in der Gruppe (2) 344 und in der Gruppe (3) 371 Beiträge. In der Schnittmenge von Gruppe (1) und (2) gibt es 196, in der von Gruppe (1) und (3) 199 und in der von Gruppe (2) und (3) 288 Beiträge. Schließlich gibt es 169 Beiträge in der Schnittmenge von Gruppe (1), (2) und (3). Die Titel und Zusammenfassungen der Beiträge in der Gesamtschnittmenge sind gelesen worden. Abbildung 10 kann entnommen werden, bei welchen Konferenzen und Zeitschriften sie veröffentlicht worden sind. Auf Beiträge mit starkem Bezug zu Forschungsziel B wird im Folgenden eingegangen.

Auf ein prototypisches System zur Unterstützung der Prüfung von Electronic Data Interchange (EDI)[116] Kontrollen gehen LEE UND HAN 2000 ein. Das System kann zum Erfassen von Kontrollen, Risiken und Kontrolltests eingesetzt werden. Es ermöglicht aber keine automatisierte Überwachung von Kontrollen.

LIANG ET AL. 2001 beschreiben ein prototypisches System zur automatischen Durchführung von IT-Audits über das Internet. Zur Verbindung der überwachten Systeme mit dem überwachenden System wird die Common Object Request Broker Architecture (CORBA)[117] eingesetzt. Für die Abbildung der Überwachungslogik werden Programme benötigt. Anstelle von CORBA werden heute häufig Webservices eingesetzt.

[116] UNECE 2010.
[117] OMG 2004.

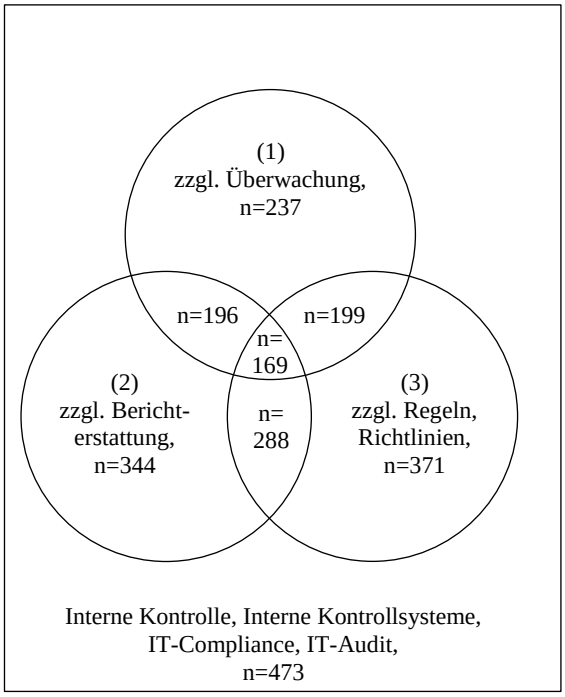

Abbildung 9: Anzahl der Suchergebnisse zu den gebildeten Gruppen. Der größte Bezug zu Forschungsziel B ist für die Beiträge in der Schnittmenge von (1), (2) und (3) zu erwarten.

Quelle: Eigene Darstellung.

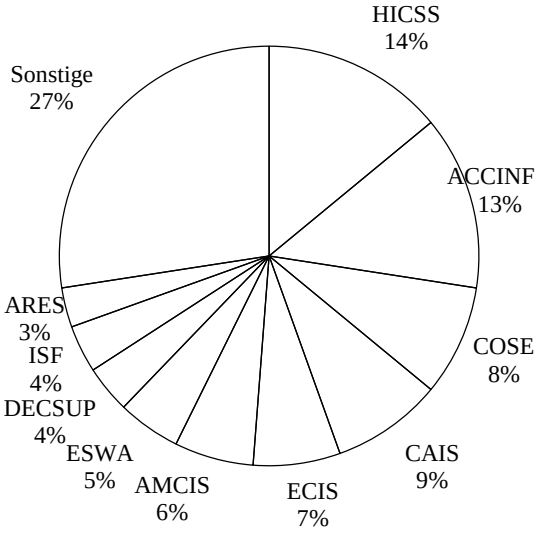

Abbildung 10: Gruppierung der Beiträge in der Schnittmenge von (1), (2) und (3) nach Konferenzen / Zeitschriften.

Quelle: Eigene Darstellung.

Auf eine ganzheitliche Compliance mit dem Sarbanes-Oxley Act gehen VOLONINO ET AL. 2004 ein. Diese betrifft insbesondere die Informationstechnologie und die Geschäftsprozesse. Die Autoren identifizieren entsprechende Forschungsgebiete. Zu diesen gehören unter anderem der Einsatz von BI und Wissensmanagement für die Dokumentation interner Kontrollen.

FLOWERDAY UND VON SOLMS 2005 diskutieren, wie Entscheidungsträger in Echtzeit mit Sicherheiten hinsichtlich der Richtigkeit, Vertrauenswürdigkeit und Zuverlässigkeit von Informationen versorgt werden können. Dabei werden eine fortlaufende Kontrolle von Geschäftsprozessen sowie eine fortlaufende Prüfung der Kontrollen vorgeschlagen.

Einen Ansatz zur Unterstützung der Compliance mit SOX auf Basis von Datenbanktechnologie schlagen AGRAWAL ET AL. 2006 vor. Dabei werden zunächst die Prozesse modelliert. Anschließend soll das Ausführen nicht gestatteter Transaktionen datenbanktechnisch unterbunden oder zumindest protokolliert werden. Ferner sollen die tatsächlichen Prozessdurchläufe auf Grundlage von Transaktionsdaten rekonstruiert und mit den vorgesehenen Prozessdurchläufen verglichen werden. Schließlich sollen mit Hilfe von OLAP-Analysen eventuell vorhandene Anomalien in Finanzdaten aufgespürt werden.

ALLES ET AL. 2006 beschreiben eine Implementierung eines Systems zur fortlaufenden Prüfung von Kontrollen in den SAP-Systemen eines Unternehmens. Aufgrund der gemachten Erfahrungen wird besonders auf die Notwendigkeit einer Formalisierung des Prüfungsvorgehens und der Prüfungseinschätzungen hingewiesen.

Einen Vergleich verschiedener Modelle zur fortlaufenden Prüfung von Informationssystemen ziehen FLOWERDAY ET AL. 2006. Dabei wird ein Mangel an konkreten und umfassenden Modellen festgestellt. Als mögliche Ursache für diesen Mangel wird unter anderem die Vielfalt der verschiedenen Datenformate genannt.

LI ET AL. 2007 schlagen einen Ansatz zur Unterstützung von Systemprüfern vor. Dieser Ansatz soll den Einsatz von Systemen zur IT-gestützten Prüfung erleichtern. Dabei werden Anwendungsfalldiagramme zur Beschreibung von Prüfungszielen, Datenflussdiagrammen zur Identifikation von Kontrollen und Entitity-Relationship-Diagramme zur Unterstützung des Entwurfs von Regeln eingesetzt. Auf Grundlage der Regeln werden Datenbanktrigger erstellt. Trigger sind Programme, die bei bestimmten Ereignissen in der Datenbank automatisch ausgeführt werden.

Ein agentenbasiertes System zur fortlaufenden Überwachung beschreiben CHAU ET AL. 2007. Die einzelnen Agenten können unabhängig von den überwachten Systemen entwickelt und relativ leicht angepasst werden. Gleichwohl stellt das System hohe Anforderungen an die Performance der überwachten Systeme und den Zugriff auf diese.

SADIQ ET AL. 2007 vertreten die Auffassung, dass beim Entwurf von Geschäftsprozessen stärker auf regulatorische Anforderungen einzugehen ist. Daher beschäftigen sie sich mit der Modellierung von Kontrollzielen und deren Einbeziehung in Geschäftsprozessmodelle. Zur Modellierung von Kontrollzielen wird eine deklarative Sprache vorgeschlagen. Die Arbeit an Methoden zur Interpretation dieser Sprache steht noch aus.

Mit der Entwicklung eines Frühwarnsystems zur Entdeckung von Verletzungen der Privatsphäre beschäftigen sich ACCORSI ET AL. 2008. Die Voraussetzungen für diese Verletzungen werden in einer Richtliniensprache definiert. Diese Richtliniensprache unterstützt nicht nur Berechtigungen, sondern auch Verpflichtungen.

KARAGIANNIS 2008 beschreibt einen Ansatz zur Integration von Compliance Management und Geschäftsprozessmanagement auf Grundlage der Metamodellierung. Ferner wird die technische Realisierung des Ansatzes mit Hilfe einer Metamodellierungsplattform vorgestellt und anhand einer Fallstudie zu SOX verdeutlicht.

Einen Ansatz zum regelbasierten und fallbasierten Schlussfolgern für interne Prüfungen in Banken stellt LEE 2008 vor. Dabei werden durch regelbasiertes Schlussfolgern Anomalien oder Risiken in Transaktionsdaten identifiziert. Zu diesen Anomalien werden anschließend durch fallbasiertes Schlussfolgern ähnliche Fälle ermittelt. Der Ansatz ist implementiert und getestet worden.

RIEKE UND WINKELMANN 2008 beschäftigen sich mit der Dokumentation und der Visualisierung von operativen Risiken entlang von Prozessmodellen. Diese Prozessmodelle basieren auf der Ereignisgesteuerten Prozesskette (EPK)[118]. Die Möglichkeit einer Hinterlegung von Regeln wird nur im Ausblick angesprochen.

Mit einer Definition und Abgrenzung der Begriffe IT-Governance und IT-Compliance beschäftigen sich TEUBNER UND FELLER 2008. Dabei wird auch angesprochen, in wie weit sich die Wissenschaft und die Industrie mit der Gestaltung von Informationssystemen zur Unterstützung von Governance und Compliance beschäftigen.

YE ET AL. 2008 beschreiben einen Ansatz zur fortlaufenden Prüfung auf Grundlage von Webservices. Dieser sieht vor, dass Prüfungsgesellschaften ihre Dienste in Form von Webservices anbieten und in kundenseitigen Registrierungsstellen bekannt machen. Ein entsprechender Prototyp ist nicht erstellt worden.

Einen Ansatz zur Prüfung von webbasierten Informationssystemen präsentieren AKOKA UND COMYN-WATTIAU 2010. Dieser organisiert die Prüfung in einem hierarchischen Prozess. Auf die Durchführung der Schritte dieses Prozesses wird nicht eingegangen.

GEHRKE 2010 beschreibt einen Prototyp zur automatisierten Prüfung von Einstellungen in SAP-Systemen. Dieser ermöglicht die Definition von Kontrolltests ohne Änderungen am Programmcode. Für die Definition wird eine eigene Regelsyntax verwendet.

Den Aufbau einer Audit-Plattform auf Grundlage von Web 2.0 Prinzipien schlagen GEHRKE UND WOLF 2010 vor. Über diese Plattform sollen kleine Audit-Routinen für unterschiedliche Systeme ausgetauscht werden.

Die genannten Beiträge sind über Konferenzen und Zeitschriften zur Wirtschaftsinformatik im Allgemeinen und zum Forschungsgebiet IT-Compliance im Besonderen veröffentlicht worden. Zu Forschungsgebiet B gibt es zwar schon einige aber noch nicht viele Beiträge.

[118] KELLER ET AL. 1992; SCHEER 1997.

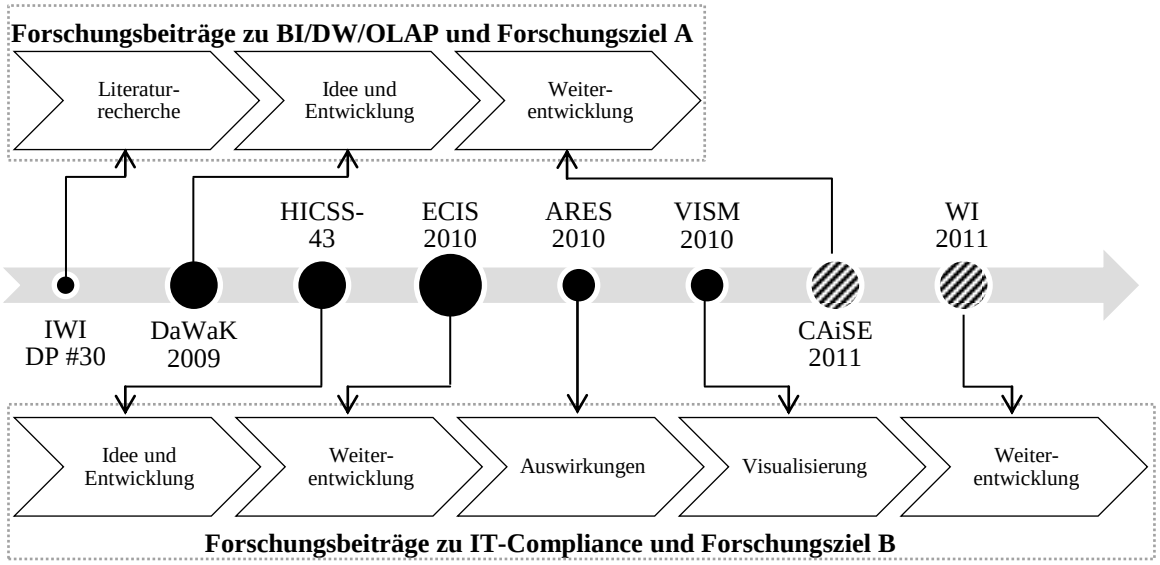

Abbildung 11: Darstellung der zeitlichen Abfolge und inhaltlichen Zusammenhänge der Beiträge.

Quelle: Eigene Darstellung.

5 Eigene Forschungsbeiträge

Die vorliegende Dissertation enthält drei Forschungsbeiträge zum Forschungsgebiet BI/OLAP/DW und Forschungsziel A sowie fünf Forschungsbeiträge zum Forschungsgebiet IT-Compliance und Forschungsziel B. Innerhalb der Forschungsgebiete und -ziele bauen die einzelnen Forschungsbeiträge aufeinander auf. Die einzelnen Forschungsbeiträge werden in den folgenden Abschnitten vorgestellt. Dies erfolgt in der Reihenfolge, in der an den Forschungsbeiträgen gearbeitet worden ist. Dabei wird kurz auf den Hintergrund, den Inhalt und die Veröffentlichung der Forschungsbeiträge eingegangen. Bei Beiträgen, an denen mehrere Autoren geschrieben haben, wird zusätzlich die Aufgabenteilung unter den Autoren skizziert. Die Angaben zur Veröffentlichung enthalten auch Informationen zur Kategorisierung anhand einschlägiger Ranglisten.

Zur Kategorisierung der Veröffentlichungen werden die WI-Orientierungslisten, das VHB-JOURQUAL 2 Ranking von betriebswirtschaftlich relevanten Zeitschriften[119] sowie die Excellence in Research for Australia (ERA) Ranked Conference List[120] verwendet.

Abbildung 11 stellt die Reihenfolge der Forschungsbeiträge und deren inhaltliche Zusammenhänge grafisch dar. Die Größe der Kreise veranschaulicht das Renommee der Veröffentlichungen gemäß den Kategorisierungen.

[119] SCHRADER UND HENNIG-THURAU 2009.
[120] ARC 2010.

5.1 Strukturierte Literaturrecherche und -klassifizierung zu den Forschungsgebieten Business Intelligence und Data Warehousing

Um Synergieeffekte zwischen praktischer Tätigkeit und Dissertation zu ermöglichen, ist nach geeigneten Forschungsthemen innerhalb BI und DW gesucht worden. Die hohe Anzahl und das fortlaufende Wachstum der wissenschaftlichen Veröffentlichungen hat die Einarbeitung erheblich erschwert. Um den Diskussionen zu aktuellen Forschungsthemen nicht nur folgen, sondern diese auch durch eigene Beiträge bereichern zu können, ist eine frühe Konzentration auf einzelne Themen erforderlich gewesen. Die dafür erforderliche Auswahl von einzelnen Forschungsthemen hat Kenntnisse über die Gesamtheit der aktuellen Themen und somit eine aktuelle Übersicht über das Forschungsgebiet vorausgesetzt. Zur Erfüllung dieser Voraussetzungen ist eine strukturierte Literaturrecherche und -klassifizierung durchgeführt worden.

5.1.1 Inhalt

Ausgangspunkt für die Einarbeitung in das Forschungsgebiet und die Identifikation aktueller Forschungsthemen sind Suchanfragen in einschlägigen Internetdatenbanken mit Literatur zur Informatik und Wirtschaftsinformatik gewesen. In diesen Literaturdatenbanken ist nach Begriffen gesucht worden, die eine Zugehörigkeit zum Forschungsgebiet nahelegen. Insbesondere waren dies verschiedene Ausprägungen der Begriffe BI und DW. Die Suchergebnisse sind aus den einzelnen Literaturdatenbanken in Dateien exportiert und in eine gemeinsame Literaturdatenbank importiert worden. Vor dem Import sind in der Regel automatisierte und/oder manuelle Nachbearbeitungsschritte an den Dateien notwendig gewesen. Nach dem Import ist die gemeinsame Literaturdatenbank von redundanten Datensätzen bereinigt worden.

Um eine aktuelle Übersicht über das Forschungsgebiet zu gewinnen, sind die Titel und Zusammenfassungen aller ab dem 1. Januar 2006 veröffentlichten Beiträge gelesen worden. Zur Identifikation der Forschungsthemen sind die Beiträge unmittelbar nach dem Lesen kategorisiert worden. Mit Hilfe der gemeinsamen Literaturdatenbank sind verschiedene Auswertungen zu den für das Forschungsgebiet inhaltlich relevanten Beiträgen erstellt worden. Die Auswertungen fassen die Anzahl der Beiträge nach den gebildeten Kategorien, dem Veröffentlichungsjahr und der Veröffentlichungsform zusammen. Für die Veröffentlichungsformen Zeitschriften- und Konferenzartikel wird

zusätzlich nach der Zeitschrift bzw. Konferenz zusammengefasst. Für die Zeitschriften und Konferenzen sind außerdem Ranking-Kategorien angegeben.

Das Lesen der Zusammenfassungen hat zu einer gründlichen und umfassenden Einarbeitung geführt und somit die Identifikation von Forschungslücken ermöglicht. Eine Wiederholung der Vorgehensweise für einzelne Forschungsthemen ist nicht mehr notwendig gewesen. Die Auswertungen stellten sich als sehr hilfreich für die Auswahl geeigneter Veröffentlichungsmedien heraus.

5.1.2 Veröffentlichung

Die Literaturrecherche ist zunächst als Teil einer Präsentation im Doktorandenkolloquium des Instituts für Wirtschaftsinformatik der Leibniz Universität Hannover (LUH) vorgestellt und anschließend in einem IWI-Diskussionsbeitrag beschrieben worden. Er ist Teil der IWI Discussion Paper (DP) Series. Die IWI Discussion Paper Series umfasst mehr als 30 Beiträge und wird unter anderem über das Research Papers in Economics (RePEc) Projekt verbreitet.[121] Das RePEc Projekt hat die Verbesserung der Verbreitung wirtschaftswissenschaftlicher Forschung zum Ziel. Kern des Projektes ist die RePEc Datenbank. Die RePEc Datenbank umfasst gegenwärtig mehr als 355.000 Arbeitspapiere und 550.000 Zeitschriftenartikel.[122]

5.2 Ontology-Based Exchange and Immediate Application of Business Calculation Definitions for Online Analytical Processing

Im Anschluss an die Einarbeitung in das Forschungsgebiet BI/OLAP/DW im Rahmen des vorherigen Beitrags ist unmittelbar mit der Arbeit an einem eigenen Forschungsbeitrag begonnen worden.

5.2.1 Inhalt

Der Forschungsbeitrag beschreibt ein Verfahren zum organisationsübergreifenden und implementierungsunabhängigen Austausch von Rechenvorschriften für BI/OLAP/DW Systeme. Die Benutzer dieser Systeme verwenden Rechenvorschriften, um auf Grundlage bereits vorhandener Kennzahlen und Dimensionen weitere abgeleitete Kennzahlen zu definieren. Diese Rechenvorschriften enthalten somit Wissen über die quantitativen Zusammenhänge zwischen betriebswirtschaftlichen Größen. In den Systemen sind diese

[121] Vgl. IWI 2010.
[122] Vgl. BAUM UND ZIMMERMANN 2010.

Rechenvorschriften gegenwärtig nicht ausreichend von Data Warehouse Metadaten isoliert. Des Weiteren wird nicht ausreichend zwischen organisationsunabhängigen und -abhängigen Rechenvorschriften sowie zwischen implementierungsunabhängigen und -abhängigen Metadaten unterschieden. Schließlich fehlt es auch an Austauschformaten für Rechenvorschriften. In der Konsequenz können die Rechenvorschriften und damit das in ihnen enthaltene Wissen nur mit großem Aufwand ausgetauscht werden.

Der Forschungsbeitrag beschreibt ein Modell zur Isolierung der einzelnen Bestandteile der Rechenvorschriften in unterschiedliche Ontologien. In diesem Modell wird insbesondere zwischen der Geschäftsontologie und der DW-Ontologie unterschieden. Die Geschäftsontologie enthält die betriebswirtschaftlichen Größen und Objekte sowie deren Beziehungen untereinander. Die DW-Ontologie enthält die informationstechnischen Data Warehouse Metadaten. Diese Ontologien müssen nicht manuell angelegt werden. In die Geschäftsontologie können betriebswirtschaftliche Definitionen, die in einer Standardsprache für mathematische Formeln beschrieben sind, importiert werden. In die DW-Ontologie können DW-Metadaten über eine DW-Standardschnittstelle importiert werden.

Die Geschäftsontologie und die DW-Ontologie können unabhängig voneinander gepflegt und ausgetauscht werden. Erst für ihre gemeinsame Nutzung zu Analyse- und Berichtszwecken ist eine Kombination erforderlich. Diese Kombination erfolgt mittels der Zuordnungsontologie. Diese Zuordnungsontologie ordnet den Größen und Objekten der Geschäftsontologie die entsprechenden Kennzahlen und Dimensionen der DW-Ontologie zu. Das Zuordnen kann manuell oder mit Hilfe von Regeln erfolgen. Durch automatisiertes Schlussfolgern werden auf Grundlage dieser Regeln automatisch Zuordnungen getroffen. Ferner wird ermittelt, welcher OLAP-Würfel welche abgeleiteten Kennzahlen mit Hilfe welcher Definitionen bereitstellen kann. Für abgeleitete Kennzahlen ist somit kein Zuordnen erforderlich.

Der Forschungsbeitrag beschreibt einen Prototyp, welcher das beschriebene Verfahren und das beschriebene Modell implementiert. Dieser Prototyp wird zwischen die Kommunikation eines DW-Clients und eines DW-Servers über eine DW-Standardschnittstelle geschaltet. Auf Grundlage der Ontologien injiziert der Prototyp zusätzliche Kennzahlenbeschreibungen in die Data Warehouse Metadaten, die der Server an den Client sendet, sowie zusätzliche Kennzahlendefinitionen in die Abfragen, die der Client an den Server sendet. Die Kennzahlen können somit ohne jegliche Änderungen an DW-

Clients oder DW-Servern verwendet werden. Folglich sind das Verfahren, das Modell und der Prototyp unmittelbar einsetzbar.

Abschließend wird die Funktionsweise des Prototyps anhand eines Beispiels erläutert. Der Prototyp ist erfolgreich mit mehreren verbreiteten Clients und Servern getestet worden.

5.2.2 Veröffentlichung

Der Forschungsbeitrag ist bei der 11th International Conference on Data Warehousing and Knowledge Discovery (DaWaK 2009) in Linz, Österreich eingereicht worden. Nach einem Review durch drei Gutachter ist der Beitrag angenommen worden. Besonders positiv haben die Gutachter die hohe Relevanz der Problemstellung bewertet. Verbesserungsvorschläge hat es zur Beschreibung des Erzeugens von Kennzahlendefinitionen und zur Präsentation des Beispiels gegeben. Diese Vorschläge sind in der Überarbeitung des Beitrags umgesetzt worden. Der überarbeitete Beitrag ist in der Serie Lecture Notes in Computer Science (LNCS) von Springer Science+Business Media veröffentlicht worden.

Nach eigenen Angaben ist die DaWaK-Konferenz eine der wichtigsten internationalen Tagungen zu den Forschungsgebieten Data Warehousing und Knowledge Discovery.[123] Die DaWaK-Konferenz findet zusammen mit der International Conference on Database and Expert Systems Applications (DEXA) statt.[124] In der strukturierten Literaturrecherche hat die DaWaK-Konferenz die meisten und die DEXA-Konferenz die drittmeisten relevanten Konferenzbeiträge.[125] In den WI-Orientierungslisten ist die DaWaK-Konferenz der Kategorie C und in der ERA Ranked Conference List der Kategorie B zugeordnet.

Die LNCS-Serie ist ein etabliertes Medium für die Veröffentlichung von Informatikbeiträgen und insbesondere Konferenzbeiträgen.[126] In den WI-Orientierungslisten ist LNCS der Kategorie B zugeordnet.

[123] Vgl. DEXA 2010a.
[124] Vgl. DEXA 2010b.
[125] Vgl. Anhang A, S. 9.
[126] Vgl. SPRINGER 2010A.

5.3 Managing Internal Control in Changing Organizations through Business Process Intelligence – A Service Oriented Architecture for the XACML based Monitoring of Supporting Systems

Kurz vor der Fertigstellung des vorherigen Forschungsbeitrages und vor dem Eindruck einiger Vorträge zu IT-Compliance und IT-Sicherheit bei der Internationalen Tagung Wirtschaftsinformatik 2009 (WI 2009) haben Thorben Sandner und der Autor der vorliegenden Dissertation zusammen den Entschluss getroffen, gemeinsam an Forschungsbeiträgen zur Überwachung von Zugriffskontrollen in Systemen zu arbeiten.

5.3.1 Inhalt

Der Forschungsbeitrag verknüpft ein Modell für Geschäftsprozesse, ein Modell für Zugriffskontrollen und ein Modell für interne Kontrollsysteme zu einem integrierten Gesamtmodell. Zur Modellierung der Geschäftsprozesse und Zugriffskontrollen kommen formal beschriebene und standardisierte Modelle zum Einsatz. Die Verwendung formal beschriebener Modelle ermöglicht den Einsatz von Werkzeugen zur modellgetriebenen Softwareentwicklung. Diese Werkzeuge generieren auf Grundlage von Modellen automatisch Quellcode.[127] Die Verwendung standardisierter Modelle ermöglicht den Einsatz bereits existierender Softwarekomponenten. Formal beschriebene und standardisierte Modelle reduzieren somit die Entwicklungszeit. Da keine formal beschriebenen und standardisierten Modelle für interne Kontrollsysteme verfügbar sind, wird zu deren Modellierung zunächst ein etabliertes Modell formal beschrieben. Das formal beschriebene Modell unterstützt auch die Definition von Kontrollausnahmen mit Hilfe einer Regelsprache.

Zur Überwachung von Zugriffskontrollen auf Grundlage des integrierten Gesamtmodells beschreibt der Forschungsbeitrag eine Service-Orientierte Architektur (SOA). SOA trennt Funktionalität in unterschiedliche Dienste auf.[128] Die beschriebene Architektur sieht einen Überwachungsdienst, einen Zugriffskontrollentscheidungsdienst, einen Schlussfolgerungsdienst und einen DW-Dienst vor. Der Überwachungsdienst kann Instanzen des integrierten Gesamtmodells einlesen. Zunächst benutzt er den Zugriffskontrollentscheidungsdienst, um zu ermitteln, welche Benutzer über welche Zugriffsberechtigungen verfügen. Anschließend benutzt er den Schlussfolgerungsdienst,

[127] Vgl. STAHL ET AL. 2007, S. 4.
[128] Vgl. BELL 2009, S. 7.

um zu ermitteln, welche Kontrollausnahmen sich daraus ergeben. Schließlich benutzt er den DW-Dienst, um die eingelesenen und die geschlussfolgerten Daten für Analyse- und Berichtszwecke bereitzustellen.

Der Forschungsbeitrag beschreibt eine prototypische Implementierung der Architektur in einer SAP-Umgebung. Die einzelnen Dienste der Architektur sind als Webservices implementiert worden. Webservices ermöglichen die Zusammenarbeit von Softwarekomponenten über Standardprotokolle im Internet.[129] Der Überwachungswebservice ist komplett eigenentwickelt worden. Für den Zugriffskontrollentscheidungs- und den Schlussfolgerungswebservice sind freie und quelloffene Softwarekomponenten wiederverwendet worden. Für diese sind Webserviceschnittstellen erstellt worden. Für das DW wird ein verfügbares SAP NetWeaver BI System eingesetzt. Die Datenbereitstellung erfolgt über den DW Import Webservice. Dieser ist im Rahmen der Arbeit als SAP-Anwendungsbetreuer entwickelt worden. Auch er wird wiederverwendet.

Abschließend wird die Funktionsweise des Prototyps anhand eines Beispiels erläutert. Die abgebildeten Beispielabfragen dienen zur Darstellung der Realisierung.

5.3.2 Aufgabenteilung

Thorben Sandner ist bereits vor der Arbeit an dem Forschungsbeitrag umfassend in die Themen Sicherheit und Zugriffskontrolle eingelesen gewesen. Er hat den überwiegenden Teil der Literaturarbeit geleistet. Der Autor der vorliegenden Dissertation hat durch die ehemalige Arbeit als System- und Prozessprüfer praktische Erfahrungen in der Modellierung von Geschäftsprozessen und der Prüfung darin eingebetteter Kontrollen gesammelt. Durch den vorherigen Beitrag ist er zudem in Softwarekomponenten zum automatisierten Schlussfolgern und Webservices eingearbeitet gewesen. Er hat das integrierte Gesamtmodell, die Architektur und den Prototyp entwickelt. Die Einarbeitung in das verwendete Zugriffskontrollmodell und die entsprechende Softwarekomponente ist zu gleichen Teilen erfolgt.

5.3.3 Veröffentlichung

Der Forschungsbeitrag ist bei der 43th Hawaii International Conference on System Sciences (HICSS-43) in anonymisierter Form eingereicht worden. Nach einem Review durch drei Gutachter ist der Beitrag angenommen worden. Der Forschungsbeitrag hat

[129] Vgl. W3C 2004B.

von zwei Gutachtern hohe Bewertungen bekommen. Der dritte Gutachter hat den Beitrag als etwas zu technisch eingeordnet. In der Überarbeitung des Beitrages ist daher stärker auf organisatorische Aspekte eingegangen worden. Der überarbeitete Beitrag ist in der IEEE Digital Library der IEEE Computer Society des Institute of Electrical and Electronics Engineers (IEEE) veröffentlicht worden.

Nach eigenen Angaben ist die HICSS eine der am längsten bestehenden und dauerhaft durchgeführten wissenschaftlichen Konferenzen.[130] In einem Artikel der Zeitschrift Communications of the ACM nimmt die HICSS den zweiten von elf Plätzen unter den betrachteten Information System Konferenzen[131] und in einem Artikel der Zeitschrift Information & Management den dritten von dreizehn Plätzen unter den betrachteten Management Information Systems Konferenzen[132] ein. Dies sind gemäß den WI-Orientierungslisten und der ERA Zeitschriftenliste[133] Top-Zeitschriften. Die HICSS Konferenz selbst ist in den WI-Orientierungslisten der Kategorie B und in der ERA Ranked Conference List der Kategorie A zugeordnet.

Die IEEE Digital Library enthält mehr als 2,7 Millionen Dokumente.[134] Darunter sind alle vom IEEE veröffentlichen Konferenz- und Zeitschriftenartikel seit dem Jahr 1988.[135]

5.4 An Implementation of a Process-Oriented Cross-System Compliance Monitoring Approach in a SAP ERP and BI Environment

Im Rahmen der Arbeiten am vorherigen Beitrag hat sich herausgestellt, dass eine Überführung der Daten aus dem von SAP verwendeten proprietären Zugriffskontrollmodell in das vom Prototyp verwendete standardisierte Zugriffskontrollmodell aufgrund der hohen Datenmenge kaum manuell durchführbar ist. Aus diesem Grund ist der Prototyp aus dem vorherigen Beitrag um einen entsprechenden Konvertierungswebservice erweitert worden. Darüber hinaus hat es umfassende Änderungen am Überwachungs- und am Schlussfolgerungswebservice gegeben.

[130] Vgl. UNI HAWAII 2010.
[131] Vgl. HARDGRAVE UND WALSTROM 1997, S. 123.
[132] Vgl. WALSTROM UND HARDGRAVE 2001, S. 121.
[133] ARC 2010.
[134] IEEE 2010B.
[135] IEEE 2010A.

5.4.1 Inhalt

Der Forschungsbeitrag führt zunächst weiterentwickelte Versionen des Modells und der Architektur aus dem vorherigen Beitrag ein. Anschließend wird auf die Implementierung eingegangen.

Für den Schlussfolgerungswebservice wird nun eine andere quelloffene Softwarekomponente eingesetzt. Diese unterstützt modernere Standards, für die es eine größere Auswahl an Entwicklungswerkzeugen gibt. Dadurch wird das Erstellen von Definitionen für Kontrollausnahmen deutlich vereinfacht. Außerdem können Anfragen an den Schlussfolgerungswebservice nun in einer Standardsprache formuliert werden.

Über den hinzugekommenen Konvertierungswebservice werden SAP-Zugriffskontrolldaten exportiert und konvertiert. Der Export kann wahlweise über die grafische SAP-Benutzeroberfläche, einen Webservice oder eine Datenbankschnittstelle erfolgen. Die Konvertierung leitet die exportierten Daten vollautomatisch aus dem SAP-Zugriffskontrollmodell in das Standardzugriffskontrollmodell über. Im Beitrag werden die dafür erforderlichen Schritte beschrieben.

Die Änderungen am Schlussfolgerungswebservice und die Einführung des Konvertierungswebservices erfordern Anpassungen am Überwachungswebservice. Aus diesem Grund wird das Zusammenspiel zwischen den einzelnen Komponenten des Prototyps, insbesondere zwischen dem Konvertierungswebservice und dem Überwachungswebservice erläutert.

Abschließend wird der Prototyp mit Hilfe eines produktiven SAP-Systems evaluiert. Die aufgeführten Angaben zu den konvertierten Zugriffskontrolldaten belegen die Notwendigkeit einer automatischen Konvertierung.

5.4.2 Aufgabenteilung

Thorben Sandner hat den überwiegenden Teil der Literaturarbeit geleistet und die Motivation sowie die Vorzüge des erstellten Prototyps herausgearbeitet. Der Autor der vorliegenden Dissertation hat den Prototypen weiterentwickelt, die Diagramme erstellt und die Evaluation durchgeführt.

5.4.3 Veröffentlichung

Der Forschungsbeitrag ist bei der 18th European Conference on Information Systems (ECIS) in anonymisierter Form eingereicht worden. Nach einem Review durch drei Gutachter ist er angenommen worden. Als besonders positiv sind die transparente Methodologie, der klare Argumentationsfluss und die hohe Relevanz hervorgehoben worden. Einer der Gutachter hat eine stärkere Abgrenzung zu den in SAP eingebauten Überwachungsmöglichkeiten empfohlen. Dies ist in der Überarbeitung berücksichtigt worden. Der überarbeitete Beitrag ist durch die Konferenz veröffentlicht worden.

Nach eigenen Angaben ist die ECIS die größte und prestigereichste Konferenz für Wirtschaftsinformatik in Europa. Ferner ist sie die Regionalkonferenz der Association for Information Systems (AIS) für Europa, den Mittleren Osten und Afrika (EMEA).[136] Die AIS hat etwa 4.000 Mitglieder aus 90 Ländern.[137] Sie organisiert auch die Americas Conference on Information Systems (AMCIS)[138] und die International Conference on Information Systems (ICIS).[139] Im VHB-JOURQUAL 2 Ranking sind die ECIS-Konferenzbände der Kategorie B zugeordnet. In den WI-Orientierungslisten und in der ERA Ranked Conference List ist die Konferenz der Kategorie A zugeordnet. Die ECIS, die ICIS und die Internationale Tagung Wirtschaftsinformatik sind die einzigen Konferenzen der Kategorie A in den WI-Orientierungslisten.

5.5 Application and Economic Implications of an Automated Requirement-Oriented and Standard-Based Compliance Monitoring and Reporting Prototype

Die für einen Forschungsbeitrag zur Verfügung stehende Anzahl an Seiten in wissenschaftlichen Publikationen ist üblicherweise stark beschränkt. In gestaltungsorientierten Forschungsbeiträgen erfordert eine gewissenhafte Beschreibung der entwickelten Artefakte zum Teil einen so hohen Umfang, dass nur noch am Rande auf die Anwendung dieser Artefakte sowie die entsprechenden Auswirkungen eingegangen werden kann. Gleichwohl sind nicht nur die technologieorientierten, sondern auch die managementorientierten Aspekte wichtig.[140] Aus diesem Grund geht dieser Forschungsbeitrag

[136] Vgl. UNI PRETORIA 2010.
[137] Vgl. AIS 2010.
[138] ESAN UNI 2010.
[139] UNI SAINT LOUIS 2010.
[140] Vgl. HEVNER 2004, S. 90.

schwerpunktmäßig auf die Anwendung des Prototyps aus den Forschungsbeiträgen für die HICSS-43 und die ECIS 2010 sowie die entsprechenden Auswirkungen ein.

5.5.1 Inhalt

Der Forschungsbeitrag geht zunächst auf das Geschäftsumfeld für die Anwendung des Prototyps ein. Dazu werden typische Personenkreise, die an der Überwachung interner Kontrollsysteme beteiligt sind, charakterisiert. Sie unterscheiden sich insbesondere durch ihre Verantwortungsbereiche und Informationsbedürfnisse. Ferner wird auf Unterschiede in den Eigenschaften von Organisationen eingegangen. Für die Überwachung interner Kontrollsysteme sind insbesondere der Umfang der Prozessdokumentation und die Heterogenität der Systemlandschaft entscheidend. Anhand dieser Eigenschaften wird zwischen vier Szenarien unterschieden. Diese Szenerien entsprechen unterschiedlichen Geschäftsanforderungen. Damit kann die Relevanz des Prototyps aus der Befriedigung der unterschiedlichen Informationsbedürfnisse und Geschäftsanforderungen abgeleitet werden. Die Rigorosität ergibt sich aus der effektiven Nutzung wissenschaftlicher Ergebnisse im Rahmen der Entwicklung und Evaluation des Prototyps.

Die Entwicklung und Evaluation des Prototyps wird im Beitrag kurz beschrieben. Dabei wird auch die Weiterentwicklung des ersten Prototyps zum zweiten Prototyp dargestellt. Wie in den vorherigen Beiträgen wird nach Modell, Architektur und Implementierung untergliedert. Hinzugekommen ist eine Würdigung der in der Literatur beschriebenen kritischen Erfolgsfaktoren zu IT-Compliance. Im Rahmen dieser Würdigung wird auch auf die unterschiedlichen Einsatzphasen entsprechender Software eingegangen. Diese Ergebnisse werden im Folgenden ergänzend zu den Informationsbedürfnissen und Geschäftsanforderungen diskutiert.

Die Diskussion der Anwendung des Prototyps ist nach der Einsatzphase, den Geschäftsanforderungen und kritischen Erfolgsfaktoren sowie den Informationsbedürfnissen untergliedert. Im Rahmen dieser Diskussion werden die entsprechenden Auswirkungen herausgearbeitet.

5.5.2 Aufgabenteilung

Der überwiegende Teil der Literaturarbeit wurde von Thorben Sandner geleistet. Insbesondere hat er die kritischen Erfolgsfaktoren sowie die Einsatzphasen identifiziert und erläutert. Der Autor der vorliegenden Dissertation hat die methodische Einordnung

übernommen, die verschiedenen Personenkreise charakterisiert, die unterschiedlichen Szenarien definiert und die Darstellungen erstellt. An der Diskussion zur Anwendung des Prototyps und der entsprechenden Auswirkungen ist zu gleichen Teilen gearbeitet worden.

5.5.3 Veröffentlichung

Der Forschungsbeitrag ist beim First Workshop on Economics of Compliance Control and Automation (ECCA 2010) der Fifth International Conference on Availability, Reliability and Security (ARES 2010) eingereicht worden. Aufgrund einer zu geringen Anzahl geeigneter Beiträge ist der ECCA-Workshop durch die Workshop Co-Chairs abgesagt worden. Einige geeignete Beiträge sind aber auf andere Workshops verteilt worden. So ist der Beitrag nach einem Review durch zwei Gutachter für den Second International Workshop on Organizational Security Aspects (OSA 2010) angenommen worden. Die Aktualität und Relevanz des Beitrages ist besonders gewürdigt worden. Einzelne Stellen sind als etwas schwer verständlich eingeordnet und daher in der Überarbeitung des Beitrages klarer formuliert worden. Der überarbeitete Beitrag ist in der IEEE Digital Library veröffentlicht worden.

Die ARES-Konferenz beschäftigt sich schwerpunktmäßig mit der Stabilität von Systemen sowie den Wirkungsbeziehungen zwischen deren Verfügbarkeit, Zuverlässigkeit und Sicherheit. In den WI-Orientierungslisten taucht die Konferenz nicht auf. Gleichwohl fällt sie sowohl durch die vergleichsweise geringen Annahmequoten (zuletzt von etwa 25%)[141] als auch durch die von führenden Sicherheitsforschern (wie Ross Anderson und Elisa Bertino) gehaltenen Key-Notes[142] auf. In der ERA Ranked Conference List ist die Konferenz der Kategorie B zugeordnet.

5.6 Visualization of Automated Compliance Monitoring and Reporting

Nachdem die technologieorientierten Aspekte des Prototyps in den Beiträgen für die HICSS-43 und die ECIS 2010 beschrieben worden sind, ist der Beitrag für die ARES 2010 auf die managementorientierten Aspekte des Prototyps eingegangen. Selbst ausgefeilte Lösungen können sich ohne die Aufmerksamkeit des Managements nur schwer durchsetzen. Eine Möglichkeit zur Steigerung dieser Aufmerksamkeit ist die Visuali-

[141] Vgl. SECURE BUSINESS AUSTRIA 2010A.
[142] Vgl. SECURE BUSINESS AUSTRIA 2010B.

sierung von managementrelevanten Informationen.[143] Aus diesem Grund geht dieser Beitrag schwerpunktmäßig auf eine Möglichkeit zur Visualisierung von managementrelevanten Informationen ein, die mit dem Prototyp generiert worden sind.

5.6.1 Inhalt

Der Forschungsbeitrag führt zunächst den Begriff der Informationsvisualisierung ein. Informationsvisualisierung wird zur Förderung des menschlichen Wahrnehmungs- und Erkenntnisvermögens eingesetzt. Beispielsweise kann Visualisierung die Mustererkennung und Informationssuche erleichtern. Eine Möglichkeit zur Erleichterung der Informationssuche ist das Dashboard. Ein Dashboard enthält die wichtigsten Informationen zur Erreichung eines bestimmten Ziels in konsolidierter Form auf einem einzigen Bildschirm. Dies erleichtert die Überwachung der Zielerreichung für das Management. Zur Gestaltung von Dashboards gibt es verschiedene Leitfäden.

Der Prototyp wird im Forschungsbeitrag nur kurz beschrieben. Im Rahmen dieser Beschreibung wird auch dargestellt, wie die Informationen durch den Prototyp für Visualisierungswerkzeuge bereitgestellt werden. Mit Hilfe dieser Werkzeuge und der Leitfäden ist ein Dashboard zur Unterstützung des Compliance Managements entwickelt worden. Die Entwicklung des Dashboards ist in einem iterativen Prozess unter Beteiligung verschiedener Interessenvertreter erfolgt. Zur Evaluation ist es mit Informationen beladen worden. Das Dashboard ist zur Darstellung der Realisierung im Beitrag abgebildet.

5.6.2 Aufgabenteilung

Die Einarbeitung in das Thema der Informationsvisualisierung und die Konsolidierung der Inhalte von Leitfäden hat Thorben Sandner übernommen. Die Beschreibung der Informationsbereitstellung und die Umsetzung des Dashboards hat der Autor der vorliegenden Dissertation herausgearbeitet.

5.6.3 Veröffentlichung

Der Forschungsbeitrag ist beim First International Workshop on Visualization and Information Security Management (VISM 2010) der 21st International Conference on Database and Expert Systems Applications (DEXA 2010) eingereicht und nach einem Review durch drei Gutachter angenommen worden. Besonders positiv ist die Originalität und Relevanz des Beitrages bewertet worden. Der Beitrag ist in der IEEE Digital

[143] Vgl. DEXA 2010C.

Library veröffentlicht worden. Der VISM-Workshop beschäftigt sich schwerpunktmäßig mit der Visualisierung sicherheitsrelevanter Informationen. In den WI-Orientierungslisten ist die DEXA-Konferenz der Kategorie C und in der ERA Ranked Conference List der Kategorie B zugeordnet.

5.7 Integrating Knowledge Management and Business Intelligence Using Semantic Middleware and Established Standards

Im Rahmen der Arbeiten am Forschungsbeitrag für die DaWaK 2009 sind mehrere Möglichkeiten zur Ergänzung und Erweiterung der entwickelten Artefakte erkannt worden. Nach der Veröffentlichung des Beitrages und dem Besuch der DaWaK und HICSS Konferenzen ist an der Umsetzung dieser Möglichkeiten zur Weiterentwicklung gearbeitet worden.

5.7.1 Inhalt

Der Forschungsbeitrag beschreibt Modelle, Verfahren und Implementierungen zur Verbesserung der Integration von Wissensmanagementsystemen und BI-Systemen, zur Isolierung von Geschäftswissen und Data Warehouse Metadaten sowie zur Unterstützung von Benutzern.

Wie beim Beitrag für die DaWaK 2009 werden die Inhalte aus der Geschäftsdomäne und der DW-Domäne in separate Ontologien übernommen. Die Geschäftsontologie und die DW-Ontologie werden lediglich für Analyse- und Berichtszwecke durch die Zuordnungsontologie miteinander verknüpft.

Das Modell der Geschäftsontologie ist um zusätzliche Klassen und Beziehungen erweitert worden. Neben der Definition von Größen unterstützt es nun auch die Definition von Objekten. Zum Erstellen der Geschäftsontologie steht nun ein entwickeltes Werkzeug zur Verfügung. Dieses Werkzeug ist über entwickelte Erweiterungen in den Microsoft Internet Explorer und Mozilla Firefox, die beiden am weitesten verbreiteten Internet-Browser,[144] integriert. Das Werkzeug ermöglicht den Import von Funktionen und Definitionen aus Wiki-Seiten. Wikis werden unter anderem für gemeinschaftliche Webseiten, Intranet-Seiten und Wissensmanagementsysteme genutzt.[145]

[144] Vgl. W3SCHOOLS 2010.
[145] Vgl. WIKIMEDIA 2010.

Das Modell der DW-Ontologie wurde ebenfalls erweitert. Insbesondere unterstützt es nun Hierarchien und Ebenen. Zum Erstellen der DW-Ontologie wurde ein Werkzeug entwickelt. Dieses greift über eine Standardschnittstelle auf ein Data Warehouse zu und erstellt vollautomatisch die DW-Ontologie.

Die Zuordnungen in der Zuordnungsontologie können unverändert von Hand oder durch Regeln erstellt werden. Ein entwickeltes Werkzeug evaluiert die Regeln und ermittelt durch automatisiertes Schlussfolgern, welche OLAP-Würfel welche Größen und Objekte mit Hilfe welcher Funktionen und Definitionen bereitstellen können. Zusätzlich ermittelt das Werkzeug, welche Objekte Unterklassen von welchen anderen Objekten sind. Die Ergebnisse des Schlussfolgerns werden für die automatische Bereitstellung von Größen und Objekten im Rahmen von OLAP sowie für die werkzeugunterstützte Durchsicht von Definitionen eingesetzt.

Der Proxy zur automatischen Bereitstellung von Größen und Objekten im Rahmen von OLAP ist intensiv überarbeitet worden. Die Bereitstellung erfordert die Injektion von komplizierten und umfangreichen Definitionen in den Datentransfer zwischen DW-Servern und DW-Clients. Die Definitionen werden nun mit Hilfe entsprechender Textvorlagen erstellt.

Zur Unterstützung von Benutzern bei der Durchsicht von Definitionen ist ein weiteres Werkzeug entwickelt worden. Das Werkzeug stellt die vorhandenen Definitionen in einer Hierarchie dar. Die Darstellung erleichtert das Identifizieren von inkonsistenten, redundanten und fehlerhaften Definitionen.

5.7.2 Veröffentlichung

Eine Veröffentlichung des Forschungsbeitrages steht noch aus. Der Beitrag wird bei der 23rd International Conference on Advanced Information Systems Engineering (CAiSE 2011) eingereicht. Die CAiSE-Konferenz hat das Ziel, den Austausch von Erfahrungen, Forschungsergebnissen, Ideen und Prototypen zwischen Forschung und Industrie zu fördern.[146]

Im VHB-JOURQUAL 2 Ranking sind die CAiSE-Konferenzbände der Kategorie C zugeordnet. In den WI-Orientierungslisten ist die Konferenz der Kategorie B und in der ERA Ranked Conference List der Kategorie A zugeordnet.

[146] Vgl. CAiSE 2010.

5.8 Ein modellunabhängiges und ontologiebasiertes Informationssystem zur Überwachung automatisierter Kontrollen in heterogenen Systemlandschaften

Die beiden Konferenzbeiträge zum Forschungsgebiet BI/OLAP/DW basieren weitgehend auf dem Einsatz von Ontologien. Auch der Prototyp aus dem Forschungsbeitrag zum Forschungsgebiet IT-Compliance bei der ECIS 2010 setzt Ontologien ein. Während der Arbeiten an der Zusammenfassung der vorliegenden Dissertation ist eine Idee zur stärkeren Nutzung von Ontologien für den Prototyp zur Überwachung von Kontrollen entwickelt worden. Die Umsetzung dieser Idee erhöht die Flexibilität des Prototyps und verknüpft die Forschungsbeiträge zum Forschungsgebiet BI/OLAP/DW stärker mit den Forschungsbeiträgen zum Forschungsgebiet IT-Compliance.

5.8.1 Inhalt

Der Forschungsbeitrag beschreibt ein Transfer-, ein Konvertierungs- und ein Verarbeitungsverfahren zur einheitlichen Überwachung automatisierter Kontrollen in unterschiedlichen Systemen. Diese Verfahren treffen möglichst geringe Annahmen hinsichtlich der Modelle und Abläufe in den zu überwachenden Systemen. Auf diese Weise können sie besonders flexibel auf die in realen Systemlandschaften vorhandene Heterogenität eingehen. Die Verfahren sind prototypisch implementiert und mit Daten aus einem produktiven SAP-System evaluiert worden.

Das Transferverfahren überführt die Daten aus den überwachten Systemen in das überwachende System. Durch die Unterstützung separater Datenbanken können Verarbeitungsprozesse im überwachenden System ablaufen, ohne die Performance der überwachten Systeme zu beeinträchtigen. Ferner können verschiedene Datenstände vorgehalten werden. Für den Export und Import von Daten sind Komponenten entwickelt worden, die auf unterschiedlichen softwarearchitektonischen Schichten arbeiten, zur Sicherstellung der Interoperabilität aber ein einheitliches Format verwenden.

Das Konvertierungsverfahren kann Daten in unterschiedlichen Modellen automatisch in Ontologien umwandeln. Dafür müssen die Modelle auf bestimmten Standards zur Definition von Modellen basieren. Sofern diese Bedingung erfüllt ist, kann die dafür entwickelte Komponente auch Daten in zukünftigen Modellen ohne Programmänderungen in Ontologien konvertieren.

Für das Verarbeitungsverfahren ist eine Standardregelsprache um Funktionen für die effiziente Abfrage von Datenbanken und Zugriffsentscheidungspunkten erweitert worden. Die Regelsprache dient der Definition von Kontrollausnahmen. Die definierten Kontrollausnahmen werden auf Grundlage der Ontologien durch automatisiertes Schlussfolgern evaluiert. Die Ergebnisse werden in einer Wissensdatenbank bereitgestellt. Diese Wissensdatenbank kann über zwei verschiedenen Verfahren abgefragt werden. Das sogenannte Push-Verfahren übernimmt die Ergebnisse in ein Data Warehouse. Das Pull-Verfahren stellt die Ergebnisse als Datenquelle bereit. Auf die Ergebnisse im Data Warehouse oder in der Datenquelle kann mit BI-Werkzeugen zugegriffen werden.

Eine Konvertierung in Ontologien ist nur für Daten und Modelle erforderlich, die für die Definition von Kontrollausnahmen oder Abfragen an die Wissensdatenbank benötigt werden. Die Klassen und Beziehungen in den Modellen stehen nach der Konvertierung als Sprachelemente für die Definition von Kontrollausnahmen und Abfragen zur Verfügung. Eine Konvertierung ist nicht für Daten notwendig, auf welche ausschließlich über die zusätzlichen Funktionen zugegriffen wird, wodurch die Performance erhöht wird.

Die Definition von Kontrollausnahmen wird anhand von Beispielen verdeutlicht. Der Prototyp wird zur Überwachung von Kontrollen in einem produktiven SAP-System eingesetzt. Zur Abbildung der Kontrollen ist das Kontrollmodell aus dem Forschungsbeitrag für die ECIS 2010 leicht erweitert worden. Insbesondere gibt es nun Klassen für Benutzer, Mandanten sowie Systeme und es wird zwischen Konfigurations- und Zugriffskontrollen unterschieden. Um eine effiziente Überwachung von SAP-Zugriffskontrollen zu ermöglichen, werden verschiedene Alternativen für Zugriffsentscheidungspunkte diskutiert. Eine der Alternativen ist ausgewählt und implementiert worden.

5.8.2 Veröffentlichung

Der Forschungsbeitrag ist bei der 10. Internationalen Tagung Wirtschaftsinformatik (WI 2011) eingereicht worden. Die Benachrichtigung über die Annahme wird Ende November 2010 erfolgen.

Die Internationale Tagung Wirtschaftsinformatik ist die renommierteste Konferenz zur Wirtschaftsinformatik im deutschsprachigen Raum. Sie wird alle zwei Jahre ausgerichtet. Im VHB-JOURQUAL 2 Ranking sind die Tagungsbände der Kategorie C zugeordnet. Die WI-Orientierungslisten ordnen die Konferenz der Kategorie A und die ERA Ranked Conference List der Kategorie C zu.

6 Kritische Würdigung und Ausblick

Die Forschungsbeiträge der vorliegenden Dissertation sind durch die Kapitel 1 bis 4 wissenschaftlich eingeordnet und durch das Kapitel 5 inhaltlich zusammengefasst worden. Abschließend soll diese Dissertation kritisch gewürdigt werden. Die kritische Würdigung orientiert sich dabei zunächst an der Arbeit von ÖSTERLE ET AL. 2010. In dieser Arbeit treten zahlreiche einflussreiche Professoren für Wirtschaftsinformatik im deutschsprachigen Raum für eine gestaltungsorientierte Wirtschaftsinformatik ein und erläutern ihr gemeinsames Verständnis dieser. Diese Erläuterung beschreibt den Prozess und definiert die Prinzipien der gestaltungsorientierten Wirtschaftsinformatik. Der beschriebene Prozess ist als Grundlage für eine Würdigung der Vorgehensweise und die definierten Prinzipien sind als Grundlage für eine Würdigung der Forschungsergebnisse genommen worden. Im Anschluss folgt eine Würdigung der Ergebnisveröffentlichung. Schließlich wird ein Fazit gezogen und ein Ausblick auf mögliche Anknüpfungspunkte für zukünftige Forschung gegeben.

6.1 Vorgehensweise

Der Prozess der gestaltungsorientierten Wirtschaftsinformatik kann in die Phasen der Analyse, des Entwurfs, der Evaluation und der Diffusion untergliedert werden:[147]

Die **Analysephase** umfasst die Beschreibung der Problemstellung, die Formulierung der Forschungsziele, die Erhebung des Forschungsstandes und die Auswahl der Forschungsmethode. Die Analysephase beginnt mit einem Anstoß durch die Praxis oder die Wissenschaft. Wie im Abschnitt zu den Forschungszielen[148] beschrieben, haben diesen Anstoß Problemstellungen aus der Praxis und entsprechende Forschungslücken in der Wissenschaft gegeben. Diese Problemstellungen und Forschungslücken haben zur Formulierung der Forschungsziele geführt. Die Problemstellungen sind in der Einleitung[149] kurz umrissen und in den Einleitungen der einzelnen Forschungsbeiträge detailliert beschrieben. Auf den Forschungsstand und die Forschungslücken wird im Kapitel zum Forschungsstand[150], in der strukturierten Literaturrecherche zu BI und DW[151] und in den

[147] Vgl. hier und im Folgenden ÖSTERLE ET AL. 2010, S. 4f.
[148] Abschnitt 3.4.1.
[149] Kapitel 1.
[150] Kapitel 4.
[151] Anhang A.

einzelnen Forschungsbeiträgen intensiv eingegangen. Die Auswahl der Forschungsmethode ist im Abschnitt zu den Forschungsmethoden[152] begründet.

Die **Entwurfsphase** umfasst die Herleitung der Artefakte anhand von anerkannten Methoden, deren Begründung sowie deren Abgrenzung zu bereits bekannten Lösungen aus Praxis und Wissenschaft. Für die Herleitung der Artefakte wird Design Science eingesetzt. Innerhalb eines Design Science Rahmens ist für die Gestaltung der erstellten Konstrukte, Modelle und Methoden argumentativ-deduktiv oder konzeptionell-deduktiv vorgegangen worden. Für die Implementierung dieser Konstrukte, Modelle und Methoden durch Instanzen ist Prototyping eingesetzt worden. Design Science und Prototyping umfassen sowohl die Entwurfsphase als auch die Evaluationsphase. In Bezug auf die Entwurfsphase ist die Auswahl möglicher Alternativen für Teile der entwickelten Prototypen an den entsprechenden Stellen in den einzelnen Forschungsbeiträgen begründet worden. Sofern es für diese Teile in der Praxis oder der Wissenschaft bereits geeignete Artefakte gegeben hat, sind keine funktionsgleichen Artefakte erstellt, sondern die verfügbaren Artefakte in die Gesamtentwürfe der Prototypen integriert worden. Diese Gesamtentwürfe sind in den einzelnen Forschungsbeiträgen von bekannten Lösungen aus Praxis und Wissenschaft abgegrenzt worden.

Die **Evaluationsphase** umfasst die Überprüfung der geschaffenen Artefakte hinsichtlich der gesetzten Forschungsziele und mittels der eingesetzten Methoden. Durch die Implementierung der erstellten Modelle und Verfahren in Prototypen ist deren Eignung für das Umsetzen der Forschungsziele überprüft worden. Auf diese Überprüfung ist innerhalb der einzelnen Forschungsbeiträge durch Fallbeispiele mit Daten aus z. T. produktiven Systemen eingegangen worden. Ferner ist auch die Annahme der Beiträge im Rahmen von Begutachtungsverfahren als eine erfolgreiche Evaluation anzusehen.

In der **Diffusionsphase** werden die wissenschaftlichen Ergebnisse möglichst weitreichend verbreitet. Diese Ergebnisverbreitung erfolgt durch die einzelnen Konferenzbeiträge, die dazugehörigen Vorträge und den Diskussionsbeitrag. Auch die vorliegende Dissertation dient unter anderem der Verbreitung von Ergebnissen.

Zusammenfassend befindet sich das gewählte Vorgehen zur Umsetzung der gesetzten Forschungsziele im vollen Einklang mit dem Prozess der gestaltungsorientierten Wirtschaftsinformatik.

[152] Abschnitt 3.4.2.

6.2 Forschungsergebnisse

Die Prinzipien der gestaltungsorientierten Wirtschaftsinformatik sind Abstraktion, Originalität, Begründung und Nutzen:[153]

Das **Abstraktionsprinzip** fordert die Anwendbarkeit eines Artefakts auf eine Klasse von Problemen. Die erstellen Artefakte verwenden etablierte Standards und vermeiden einen Bezug zu einzelnen Plattformen. Zwar sind auch wenige Artefakte mit einem Bezug zu einzelnen Plattformen (wie SAP) erstellt worden, ohne diese Artefakte wäre aber auch keine Evaluation mit Daten aus produktiven Systemen möglich gewesen. Abstraktion und Evaluation befinden sich insofern in einem Spannungsverhältnis.

Das **Originalitätsprinzip** fordert einen innovativen Beitrag zum bereits publizierten Wissensstand. Auf den publizierten Wissensstand ist im Kapitel zum Forschungsstand[154], in der strukturierten Literaturrecherche zu BI und DW[155] und in den einzelnen Forschungsbeiträgen intensiv eingegangen worden. In Bezug auf die einzelnen Forschungsbeiträge ist auf einen angemessenen Anteil innovativen Materials besonders geachtet worden. Eine verständliche Präsentation des innovativen Materials kommt ohne dessen Einordnung in einen bekannten Kontext aber schwer aus. Darüber hinaus befinden sich Originalität und Diffusion in einem gewissen Spannungsverhältnis. In den Gutachten zu den Beiträgen bei der DaWaK 2009, HICSS-43, ARES 2010 und VISM 2010 wurde explizit auf die Originalität eingegangen. Die Originalität ist dabei positiv bewertet worden.

Das **Begründungsprinzip** fordert eine nachvollziehbare Begründung der Artefakte sowie deren Validierbarkeit. Der soziotechnische Charakter von Informationssystemen schließt eine deterministische Lösung von Problemstellungen sowie deren formale Beweisbarkeit weitgehend aus. Die Auswahl möglicher Alternativen zur Lösung wird jedoch an den entsprechenden Stellen in den einzelnen Forschungsbeiträgen begründet. Durch die Annahme der Beiträge im Rahmen von Begutachtungsverfahren ist diese Begründung von Experten akzeptiert worden. Da die Beiträge umfassend auf die zur Rekonstruktion der Artefakte notwendigen technischen Details eingehen, sind die erstellten Artefakte überprüfbar.

[153] Vgl. hier und im Folgenden ÖSTERLE ET AL. 2010, S. 5f.
[154] Kapitel 4.
[155] Anhang A.

Das **Nutzenprinzip** fordert, dass ein Artefakt einen Nutzen für die Anspruchsgruppen der gestaltungsorientierten Wirtschaftsinformatik erzeugen kann. Nutzen entsteht durch die Befriedigung von Bedürfnissen. Ein solches Bedürfnis kann für die Lösung einer Problemstellung bestehen. Beiträge, welche zur Lösung real existierender Problemstellungen beisteuern, werden als relevant bezeichnet. Auf die Relevanz wird in den Gutachten zu den veröffentlichten Beiträgen explizit eingegangen. Die Relevanz ist sehr positiv bewertet worden.

Zusammenfassend befinden sich die erarbeiteten Forschungsergebnisse im vollen Einklang mit den Prinzipien der gestaltungsorientierten Wirtschaftsinformatik.

6.3 Ergebnisveröffentlichung

Die Veröffentlichung der Forschungsergebnisse ist insbesondere durch den Wandel von der Monografie zur kumulativen Dissertation beeinflusst worden. Ferner ist der Einfluss von Ranglisten bedeutsam gewesen.

Im deutschsprachigen Raum ist die Monografie eine weitverbreitete Dissertationsform. Gleichwohl gewinnt die kumulative Dissertation zunehmend an Bedeutung.[156] Die Arbeiten an der vorliegenden Dissertation haben mit der Anmeldung zur Promotion Mitte 2008 begonnen. Zu diesem Zeitpunkt ist noch von einer Monografie ausgegangen worden. Der Wechsel zur kumulativen Dissertation ist erst Ende 2009 erfolgt. Ausgehend von einer kumulativen Dissertation wäre es strategisch günstiger gewesen, die als Diskussionsbeitrag veröffentlichte strukturierte Literaturrecherche zu BI und DW[157] weiter auszubauen und bei einer Konferenz einzureichen. So hätten früher Erfahrungen mit dem Prozess der Begutachtung von wissenschaftlichen Beiträgen gesammelt werden können. Des Weiteren hätten einzelne Forschungsbeiträge bei Konferenzen mit höherer Sichtbarkeit und Bewertung eingereicht werden können.

Der erste Konferenzbeitrag zu BI/OLAP/DW[158] wurde bei der DaWaK 2009 eingereicht und angenommen. Die DaWaK hat eine besonders hohe Sichtbarkeit für das Gebiet BI/OLAP/DW. Ausgehend von einer kumulativen Dissertation wäre es eventuell günstiger gewesen, den Beitrag bei der CAiSE oder HICSS einzureichen. Diese Konferenzen haben zwar eine geringere Sichtbarkeit für das Forschungsgebiet BI/OLAP/DW,

[156] Vgl. DASKE ET AL. 2009.
[157] Anhang A.
[158] Anhang B.

beschäftigen sich aber auch mit deren Inhalten und haben eine höhere Sichtbarkeit für die gesamte Wirtschaftsinformatik. Für den zweiten Konferenzbeitrag zu BI/OLAP/ DW[159] ist die CAiSE ausgewählt worden.

Der erste Konferenzbeitrag zu IT-Compliance[160] ist bei der HICSS 2010, der zweite[161] bei der ECIS 2010 angenommen worden. Diese Konferenzen sind aufgrund ihrer hohen Sichtbarkeit für die gesamte Wirtschaftsinformatik und ihrer hohen Bewertung in den einschlägigen Ranglisten hervorragend zur Ergebnisveröffentlichung geeignet. Der dritte Konferenzbeitrag zu IT-Compliance[162] ist bei der ARES 2010, der vierte[163] bei der VISM 2010 angenommen worden. Beides sind fachbezogene Konferenzen zur IT-Sicherheit die auch auf IT-Compliance eingehen. Fachbezogene Konferenzen haben durchaus Stärken. Sie ermöglichen eine Präsentation vor einem besonders fachkundigen Publikum und gewährleisten somit gute Möglichkeiten zur Vernetzung. Der fünfte Konferenzbeitrag zu IT-Compliance[164] wurde bei der WI 2011 eingereicht und befindet sich gegenwärtig im Begutachtungsverfahren. Diese Konferenz hat im deutschsprachigen Raum sowohl eine hohe Sichtbarkeit als auch eine hohe Bewertung.

6.4 Fazit und Ausblick

Die vorliegende Dissertation hat ein Forschungsziel im Forschungsgebiet BI/OLAP/ DW und ein Forschungsziel im Forschungsgebiet IT-Compliance verfolgt. Den Anstoß für diese Forschungsziele gaben Problemstellungen aus der Praxis. Zu diesen Problemstellungen sind durch systematische Literaturrecherchen bestehende Forschungslücken identifiziert worden.

Innerhalb des Forschungsgebietes BI/OLAP/DW ist das Forschungsziel die Gestaltung von Artefakten zur Verbesserung der Interoperabilität von BI/OLAP/DW Systemen durch Einsatz von Ontologien und automatisiertem Schlussfolgern gewesen. Als Forschungsmethode ist Design Science ausgewählt worden. Im Rahmen von Design Science sind innovative Modelle, Verfahren und Implementierungen entwickelt worden. Die Modelle und Verfahren, ermöglichen den Austausch von wertvollem Expertenwissen zwischen verschiedenen BI/OLAP/DW Systemen. Dieses Wissen wird von

[159] Anhang G.
[160] Anhang C.
[161] Anhang D.
[162] Anhang E.
[163] Anhang F.
[164] Anhang H.

technischen Details isoliert, in Ontologien überführt und durch automatisiertes Schlussfolgern unmittelbar für andere Systeme anwendbar gemacht. Zur Umsetzung der Modelle und Verfahren sind eine Reihe von Werkzeugen und ein Proxy implementiert worden. Die entwickelten Werkzeuge dienen zur Automatisierung der Verfahren zum Wissensaustausch. Dadurch kann erstmals Wissen über Funktionen für Größen (wie z. B. Gewinn vor Zinsen und Steuern) und Definitionen für Objekte (wie z. B. Zinskonto oder Steuerkonto) über Wissensmanagementsysteme zwischen unterschiedlichen BI/OLAP/DW Systemen ausgetauscht werden. Ferner kann das ausgetauschte Wissen mittels des entwickelten Proxys unmittelbar angewendet werden. Dazu verändert der Proxy die Kommunikation von Servern und Clients über eine Standardschnittstelle. Daher sind keine Änderungen an existierenden Systemen erforderlich. Somit wird auch für existierende BI/OLAP/DW Systeme eine deutliche Verbesserung der Interoperabilität erreicht. Bisher gibt es in der wissenschaftlichen Literatur keinen vergleichbaren Proxy. Zur Evaluation des entwickelten Proxys sind mehrere verbreitete Server und Clients eingesetzt worden.

Innerhalb des Forschungsgebietes IT-Compliance ist das Forschungsziel die Gestaltung von Artefakten zur automatisierten regelbasierten Überwachung maschineller Kontrollen und zur zielgruppengerechten Berichterstattung von Kontrollausnahmen gewesen. Auch hier ist Design Science als Forschungsmethode ausgewählt worden und auch hier sind innovative Modelle, Verfahren und Implementierungen entwickelt worden. Die Modelle und Verfahren ermöglichen eine homogene Überwachung von Kontrollen in heterogenen Systemen. Die Überwachung wird durch Regeln gesteuert und leitet die Überwachungsergebnisse (insbesondere identifizierte Kontrollausnahmen) an BI-Systeme weiter. Dies ermöglicht eine zeitnahe und zielgruppengerechte Berichterstattung. Zur Umsetzung der Modelle und Verfahren ist eine Reihe von Webservices implementiert worden. Diese Webservices werden durch eine fortlaufend weiterentwickelte Architektur miteinander zu einem Prototyp verknüpft. Der Prototyp verwendet Standardschnittstellen und kann flexibel in die bestehende IT-Infrastruktur integriert werden. Bisher gibt es in der wissenschaftlichen Literatur keinen anderen Prototyp zur Überwachung maschineller Kontrollen, der vergleichbar flexibel auf Unterschiede zwischen den überwachten Systemen eingehen kann und vergleichbar konform zu etablierten Standards ist. Zur Evaluation des entwickelten Prototyps sind Daten aus mehreren Mandanten eines produktiven SAP ERP Systems verwendet worden.

Die Vorgehensweise zur Umsetzung der Forschungsziele ist im vollen Einklang mit dem Prozess und die erarbeiteten Forschungsergebnisse sind im vollen Einklang mit den Prinzipien der gestaltungsorientierten Wirtschaftsinformatik. Dieser Prozess und diese Prinzipien sind Konsens unter zahlreichen einflussreichen Professoren für Wirtschaftsinformatik im deutschsprachigen Raum. Die Veröffentlichung der Forschungsergebnisse ist vor allem bei internationalen Konferenzen erfolgt. Somit sind Vorgehensweise und Forschungsergebnisse auch im internationalen Raum gewürdigt worden. Die Forschungsergebnisse konnten sich sowohl gegen die starke Konkurrenz bei allgemeinen Konferenzen durchsetzen, als auch den hohen fachlichen Anforderungen bei fachbezogenen Konferenzen gerecht werden. Somit sind die Forschungsergebnisse sowohl in der gesamten Wirtschaftsinformatik als auch in den einzelnen Forschungsgebieten sichtbar.

Die aufgeführten Forschungsergebnisse stellen maßgebliche Erfolge für die gesetzten Forschungsziele dar und bieten zugleich mehrere Anknüpfungspunkte für zukünftige Forschung. Innerhalb des Forschungsgebiets BI/OLAP/DW ist das Thema der Interoperabilität in den letzten Jahren vor allem in Bezug auf Daten und weniger in Bezug auf Metadaten diskutiert worden. Dabei ist insbesondere die Anbindung von Daten aus unterschiedlichen Quellen und deren Transformation in ein einheitliches Modell diskutiert worden. Der Austausch von Metadaten zu diesem Modell wird hingegen kaum angesprochen. Des Weiteren gibt es außerhalb des Data Mining bisher nur wenige Beiträge im Forschungsgebiet BI/OLAP/DW, die sich mit dem Einsatz von Ontologien und automatisiertem Schlussfolgern beschäftigen. Dabei gibt es in Bezug auf alle Phasen des DW-Prozesses bereits Ansätze, an die angeknüpft werden könnte. Erhebliches Potential gibt es für zukünftige Forschung an innovativen Analysewerkzeugen mit nativer Unterstützung für Ontologien. Entsprechende Werkzeuge könnten bestehende Grenzen zwischen OLAP und künstlicher Intelligenz aufweichen. Innerhalb des Forschungsgebiets IT-Compliance gibt es bisher nicht viele Beiträge, die sich mit der Gestaltung von Artefakten zur Überwachung von Kontrollen in Systemen beschäftigen. Dadurch mangelt es unter anderem an Vorschlägen zu Kontrollmodellen, Einschätzungen zu Regelsprachen und Beurteilungen von Lösungen. Auch auf die Präsentation von Überwachungsergebnissen wird kaum eingegangen. Obwohl der regulatorische Druck in den letzten Jahren spürbar zugenommen hat, steht die Forschung hier noch am Anfang.

Literaturverzeichnis

ACCORSI ET AL. 2008 ACCORSI, R.; SATO, Y.; KAI, S.: *Compliance Monitor for Early Warning Risk Determination*. In: Wirtschaftsinformatik 50 (2008), Nr. 5, 375-382.

AGRAWAL ET AL. 2006 AGRAWAL, R.; JOHNSON, C.; KIERNAN, J.; LEYMANN, F.: *Taming Compliance with Sarbanes-Oxley Internal Controls using Database Technologie*. In: Proceedings of the 22nd International Conference on Data Engineering (ICDE 2006, Atlanta, GA, USA, 3. - 7. April 2006). IEEE, 2006.

AKOKA UND COMYN-WATTIAU 2010 AKOKA, J.; COMYN-WATTIAU, I.: *A Framework for Auditing Web-Based Information Systems*. In: Proceedings of the 18th European Conference on Information Systems (ECIS 2010, Pretoria, Südafrika, 6. - 9. Juni 2010). URL http://web.up.ac.za/ecis/ECIS2010PR/ECIS2010/toc.htm. Aktualisierungsdatum: 13. Juli 2010.

ALLES ET AL. 2006 ALLES, M.; BRENNAN, G.; KOGAN, A.; VASARHELYI, M. A.: *Continuous Monitoring of Business Process Controls: A Pilot Implementation of a Continuous Auditing System at Siemens*. In: International Journal of Accounting Information Systems 7 (2006), Nr. 2, 137-161.

ACM 2010 ASSOCIATION FOR COMPUTER MACHINERY (ACM): *ACM Guide to Computing Literature*. URL http://portal.acm.org/guide.cfm. Aktualisierungsdatum: 6. September 2010.

AIS 2010 ASSOCIATION FOR INFORMATION SYSTEMS (AIS): *About the Association for Information Systems*. URL http://home.aisnet.org/displaycommon.cfm?an=3. Aktualisierungsdatum: 8. September 2010.

ARC 2010 AUSTRALIAN RESEARCH COUNCIL (ARC): The Excellence in Research for Australia (ERA) Ranked Outlets, URL http://www.arc.gov.au/era/era_journal_list.htm. Aktualisierungsdatum: 19. Juli 2010.

BASLER AUSSCHUSS FÜR BANKENAUFSICHT 2006 BASLER AUSSCHUSS FÜR BANKENAUFSICHT; BANK FÜR INTERNATIONALEN ZAHLUNGSAUSGLEICH (Hrsg.): *Internationale Konvergenz der Eigenkapitalmessung und Eigenkapitalanforderungen*. 2006. ISBN 92-9197-325-4.

BDSG 2003 *Bekanntmachung der Neufassung des Bundesdatenschutzgesetzes vom 14. Januar 2003*. Bundesgesetzblatt 2003, Teil I, Nr. 3, S. 66-88.

BILMOG 2009 *Gesetz zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz - BilMoG) vom 25. Mai 2009*. Bundesgesetzblatt 2009, Teil I, Nr. 27, S. 1102-1136.

BAUM UND ZIMMERMANN 2010 BAUM, K.; ZIMMERMANN, C.: *Research Papers in Economics (RePEc)*. URL http://repec.org. Aktualisierungsdatum: 29. Juli 2010.

BELL 2008 BELL, M.: *Service-Oriented Modeling: Service Analysis, Design, and Architecture*. Hoboken, NJ: Wiley, 2008.

BODENDORF 2006 Bodendorf, F.: *Daten- und Wissensmanagement*. 2. Auflage. Berlin (u. a.): Springer, 2006.

CAISE 2010 CONFERENCE ON ADVANCED INFORMATION SYSTEMS ENGINEERING (CAISE): CAiSE. URL http://www.caise.org. Aktualisierungsdatum: 18. September 2010.

CHAU ET AL. 2007 CHOU, C. L.; DU, T.; LAI, V. S.: *Continuous Auditing with a Multi-Agent System.* In: Decision Support Systems 42 (2007), Nr. 4, S. 2274-2292.

CODD ET AL. 1993 CODD, E. F.; CODD S. B.; SALLEY C. T.: *Providing OLAP (On-line Analytical Processing) to User-Analysts: An IT Mandate*. San Jose, CA: Codd & Date, 1993.

CORCHO UND GÓMEZ-PÉREZ 2000 CORCHO, S.; GÓMEZ-PÉREZ, A.: *A Roadmap to Ontology Specification Languages*. In: Proceedings of the 12th International Conference on Knowledge Engineering and Knowledge Management Methods, Models and Tools (EKAW 2000, Juan-les-Pins, Frankreich, 2. - 6. Oktober 2000), Lecture Notes in Artificial Intelligence 1937, Berlin (u. a.): Springer, 2000, S. 80-96.

DASKE ET AL. 2009 DASKE, H.; NEUS, W.; KORMANN, H.; SADOWSKY, D.; WAGENHOFER, A.: Symposium Kumulative Dissertation. VHB Pfingsttagung 2009 (Erlangen, Deutschland, 5. Juli 2009). URL http://vhbonline.org/uploads/media/kum-Dissertation.pdf. Aktualisierungsdatum: 20. 7. 2009.

DEXA 2010A DATABASE & EXPERT SYSTEMS APPLICATIONS (DEXA) SOCIETY: *Call for Papers DaWaK 2010*. URL http://www.dexa.org/dawak_cfp. Aktualisierungsdatum: 21. August 2010.

DEXA 2010B DATABASE & EXPERT SYSTEMS APPLICATIONS (DEXA) SOCIETY: *Previous Conferences*. URL http://www.dexa.org/history. Aktualisierungsdatum: 21. August 2010.

DEXA 2010C DATABASE & EXPERT SYSTEMS APPLICATIONS (DEXA) SOCIETY: *VISM - International Workshop on Visualization and Information Security Management*. URL http://www.security-conference.eu/VISM. Aktualisierungsdatum: 8. September 2010.

ELSEVIER 2010A ELSEVIER: *Engineering Village*. URL http://www.engineeringvillage.com. Aktualisierungsdatum: 6. September 2010.

ELSEVIER 2010B ELSEVIER: *ScienceDirect*. URL http://www.sciencedirect.com. Aktualisierungsdatum: 6. September 2010.

ESAN UNI 2010 ESAN UNIVERSITY: *About AIS and AMCIS*. URL http://www.amcis2010.org/home/index.php?option=com_content&task=view&id=12&Itemid=27, Aktualisierungsdatum: 7. September 2010.

FINK ET AL. 2005 FINK, A.; Schneidereit, G.; Voß, S.: *Grundlagen der Wirtschaftsinformatik*. Heidelberg: Physica-Verlag, 2005.

FLOWERDAY UND VON SOLMS 2005 FLOWERDAY, S.; VON SOLMS, R.: *Real-Time Information Integrity = System Integrity + Data Integrity + Continuous Assurances*. In: Computers & Security 24 (2005), Nr. 8, S. 604-613.

FLOWERDAY ET AL. 2006 FLOWERDAY, S.; BLUNDELL, A. W.; VON SOLMS, R.: *Continuous Auditing Technologies and Models: A Discussion*. In: Computers & Security 25 (2006), Nr. 5, S. 325-331.

FRANK 2007 FRANK, U.: Ein Vorschlag zur Konfiguration von Forschungsmethoden in der Wirtschaftsinformatik. In: LEHNER, F. (Hrsg.); ZELEWSKI, S. (Hrsg.): *Wissenschaftliche Fundierung und wissenschaftliche Orientierung der Wirtschaftsinformatik*, Berlin: GITO-Verlag, 2007.

GDPDU 2001 *Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) vom 16. Juli 2001*. Bundessteuerblatt 51 (2001), Teil I, Nr. 11, S. 415-417.

GEHRKE 2010 GEHRKE, N.: *The ERP Audit-Lab – A Prototypical Framework for Evaluating Enterprise Resource Planning System Assurance*. In: Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS-43, Koloa, Hawaii, USA, 5. - 8. Januar 2010). IEEE, 2010.

GEHRKE UND WOLF 2010 GEHRKE, N.; WOLF, P.: *Towards Audit 2.0 – A Web 2.0 Community Platform for Auditors*. In: Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS-43, Koloa, Hawaii, USA, 5. - 8. Januar 2010). IEEE, 2010.

GOBS 1995 *Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)*. Bundessteuerblatt 45 (1995), Teil I, Nr. 18, S. 738-746.

GREGG ET AL. 2001 GREGG, D. G.; KULKARNI, U. R.; VINZÉ, A. S.: *Understanding the Philosophical Underpinnings of Software Engineering Research in Information Systems*. In: Information Systems Frontiers 3 (2001), Nr. 2, S. 169-183.

GRUBER 1993 GRUBER, T.R.: *A Translation Approach to Portable Ontology Specifications*. In: Knowledge Acquisition 5 (1993), Nr. 3, S. 100-220.

GUBA 1990 GUBA, E. G.: *The Paradigm Dialog*. Newbury Park (u. a.): Sage, 1990.

GUBA UND LINCOLN 1994 GUBA, E. G.; Lincoln, Y.S.: Competing Paradigms in Qualitative Research. In: Denzin, N. (Hrsg.); Lincoln, Y. (Hrsg.): *Handbook of Qualitative Research*, Newbury Park (u. a.): Sage, 1994, S. 105-117.

HARDGRAVE UND WALSTROM 1997 HARDGRAVE, B. C., WALSTROM, K. A.: *Forums for MIS Scholars*. In: Communications of the ACM 40 (1997), Nr. 11, S. 119-124.

HEVNER ET AL. 2004 HEVNER, A. R.; MARCH, S. T.; PARK, J.: *Design Science in Information Systems Research*. In: MIS Quarterly 28 (2004), Nr. 1, S. 75-105.

HEVNER UND CHATTERJEE 2010 HEVNER, A. R. (Hrsg.), CHATTERJEE, S. (Hrsg.): *Design Research in Information Systems*. Berlin (u. a.): Springer, 2010.

HÖMBERG 2002 HÖMBERG, R.: Internes Kontrollsystem. In: BALLWIESER, W. (Hrsg.); COENENBERG, A. G. (Hrsg.); V. WYSOCKI, K. (Hrsg.): *Handwörterbuch der Rechnungslegung und Prüfung*. Stuttgart : Schäffer-Poeschler, 2002.

INMON 2005 INMON, W. H.: *Building the Data Warehouse*. 4. Auflage. Indianapolis, Ind.: Wiley, 2005.

IEEE 1990 Institute of Electrical and Electronics Engineers (IEEE): *IEEE Standard Computer Dictionary*. 1990. ISBN 1-55937-079-3.

IEEE 2010A INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE): *Collections in the IEEE Xplore Database*. URL http://ieeexplore.ieee.org/Xplorehelp/Help_Collections_IEEE_Xplore_Database.html. Aktualisierungsdatum: 17. Juni 2010.

IEEE 2010B INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE): *IEEE Xplore*. URL http://ieeexplore.ieee.org/Xplore/dynhome.jsp. Aktualisierungsdatum: 7. September 2010.

IWI 2010 INSTITUT FÜR WIRTSCHAFTSINFORMATIK (IWI) DER GOTTFRIED WILHELM LEIBNIZ UNIVERSITÄT HANNOVER: *IWI Discussion Paper Series*. URL http://econpapers.repec.org/paper/ifwiwidps. Aktualisierungsdatum: 21. August 2010.

ISO 2010 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): *About ISO*. URL http://www.iso.org/iso/about.htm. Aktualisierungsdatum: 27. August 2010.

ISO / IEC 2006 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) / INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): *Information Technology - Topic Maps - Part 3: XML Syntax, ISO/IEC FDIS 13250-3.* URL http://www.isotopicmaps.org/sam/sam-xtm/xml-syntax.pdf. Aktualisierungsdatum: 19. Juni 2006.

JUKIC ET AL. 2008 JUKIC, N.; JUKIC, B.; MALLARIS, M.: Online Analytical Processing (OLAP) for Decision Support, in: BURSTEIN, F. (Hrsg.); HOLSAPPLE, C. W. (Hrsg.): *Handbook on Decision Support Systems 1*. Berlin (u. a.): Springer, 2008, S. 259-276.

KARAGIANNIS 2008 KARAGIANNIS, D.: *A Business Process-Based Modelling Extension for Regulatory Compliance*. In: Tagungsbände der Multikonferenz Wirtschaftsinformatik (MKWI 2008, München, Deutschland, 26. - 28. 2. 2008). Berlin: GITO-Verlag, 2008, S. 1159-1173.

KELLER ET AL. 1992 KELLER, G.; NÜTTGENS, M.; SCHEER, A.-W.: *Semantische Prozeßmodellierung auf Grundlage „Ereignisgesteuerter Prozeßketten (EPK)“*. Veröffentlichungen des Instituts für Wirtschaftsinformatik (IWI), Universität des Saarlandes, Heft 89. URL http://www.iwi.uni-sb.de/Download/iwihefte/heft89.pdf, 1992.

KERSCHENBERG 2001 KERSCHENBERG, L.: *Knowledge Management in Heterogeneous Data Warehouse Environments.* In: Proceedings of the 3rd International Conference on Data Warehousing and Knowledge Discovery (DaWaK 2001, München, Deutschland, 5. - 7. September 2001), Lecture Notes in Computer Science 2114. Berlin (u. a.): Springer, 2001, S. 1-10.

KIMBALL 2004 KIMBALL, R.: *The Data Warehouse ETL Toolkit*. Indianapolis, Ind.: Wiley 2004.

KIMBALL 2008 KIMBALL, R.: *The Data Warehouse Lifecycle Toolkit*. 2. Auflage. Indianapolis, Ind.: Wiley, 2008.

KONTRAG 1998 *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)*. Bundesgesetzblatt 1998, Teil I, Nr. 24, S. 786-794.

LEE 2008 LEE, G. H.*: Rule-Based and Case-Based Reasoning Approach for Internal Audit of Bank*. In: Knowledge-Based Systems 21 (2008), Nr. 2, S. 140-147.

LEE UND HAN 2000 LEE, S.; HAN, I.: *EDI Controls Design Support System using Relational Database System*. In: Decision Support Systems 29 (2000), Nr. 2, S. 169-193.

LI ET AL. 2007 LI, S.-H.; HUANG, S.-M.; LIN, Y.-C. G.: *Developing a Continuous Auditing Assistance System Based on Information Process Models*. In: Journal of Computer Information Systems 48 (2007), Nr. 1, S. 2-13.

LIANG ET AL. 2001 LIANG, D.; LIN, F.: WU, S.: *Electronically Auditing EDP Systems with the Support of Emerging Information Technologies*. In: International Journal of Accounting Information Systems 2 (2001), Nr. 2, S. 130-147.

LUHN 1958 LUHN, H. P.: *A Business Intelligence System*. In: IBM Journal of Research and Development 2 (1958), Nr. 4, S. 314-319.

MARAKAS 2003 MARAKAS, G. M.: *Decision Support Systems In the 21st Century*. Upper Saddle River, NJ: Prentice Hall, 2003.

MAIMON UND ROKACH 2005 MAIMON, O.; ROKACH, L.: Introduction to Knowledge Discovery in Databases. In: MAIMON, O. (Hrsg.); ROKACH, L. (Hrsg): *Data Mining and Knowledge Discovery Handbook*, Belin (u.a.): Springer, 2005, S. 1-17.

MENZIEST 1996 Menziest, T.: *Applications of Abduction: Knowledge-Level Modelling*. In: International Journal of Human-Computer Studies 45 (1996), Nr. 3, S. 305-335.

MEREDITH ET AL. 2008 MEREDITH, R.; O'DONNELL, P.; ARNOTT, D.: Databases and Data Warehouses for Decision Support. In: BURSTEIN, F. (Hrsg.); HOLSAPPLE, C. W. (Hrsg.): *Handbook on Decision Support Systems 1*, Berlin (u. a.): Springer, 2008, S. 207-229.

MERTENS ET AL. 2005 MERTENS, P.; BODENDORF, F.; KÖNIG, W.; PICOT, A.; SCHUMANN, M.; HESS, T.: *Grundzüge der Wirtschaftsinformatik*. Neunte, überarbeitete Auflage. Berlin (u. a.): Springer, 2005.

MITTELSTRASS UND WOLTERS 1995A MITTELSTRASS, J. (Hrsg.); WOLTERS, G. (Hrsg.): *Enzyklopädie Philosophie und Wissenschaftstheorie, Band 1: A-G*. Korrigierter Nachdruck. Stuttgart: Metzler, 1995.

MITTELSTRASS UND WOLTERS 1995B MITTELSTRASS, J. (Hrsg.); WOLTERS, G. (Hrsg.): *Enzyklopädie Philosophie und Wissenschaftstheorie, Band 2: H-O*. Korrigierter Nachdruck. Stuttgart: Metzler, 1995.

MITTELSTRASS ET AL. 1995C MITTELSTRASS, J. (Hrsg.); CARRIER, M. (Hrsg.); WOLTERS, G. (Hrsg.): *Enzyklopädie Philosophie und Wissenschaftstheorie, Band 3: P-So*. Stuttgart: Metzler, 1995.

MITTELSTRASS ET AL. 1996 MITTELSTRASS, J. (Hrsg.); CARRIER, M. (Hrsg.); WOLTERS, G. (Hrsg.): *Enzyklopädie Philosophie und Wissenschaftstheorie, Band 4: Sp-Z*. Stuttgart: Metzler, 1996.

MYRACH 2008 MYRACH, T.: Perspektiven auf die Wirtschaftsinformatik: Eine Disziplin im Spannungsfeld von Mensch und Maschine. In: Jung, R. (Hrsg.); Myrach, T. (Hrsg.): *Quo vadis Wirtschaftsinformatik?*. Wiesbaden: Gabler, 2008, S. 95-124.

NEGASH UND GRAY 2008 NEGASH, S.; GRAY, P.: Business Intelligence. In: BURSTEIN, F. (Hrsg.); HOLSAPPLE, C. W. (Hrsg.) *Handbook on Decision Support Systems 2*, Berlin (u. a.): Springer, 2008, S. 175-193.

NGUYEN ET AL. 2003 NGUYEN, T. B.; TJOA, A. M.; MANGISENGI, O.: *MetaCube XTM: A Multidimensional Metadata Approach for Semantic Web Warehousing Systems*. In: Proceedings of the 5th International Conference on Data Warehousing and Knowledge Discovery (DaWaK 2003, Prag, Tschechische Republik, 3. - 5. September 2003), Lecture Notes in Computer Science 2737. Berlin (u. a.): Springer, 2003, S. 76-88.

OMG 2004 Object Management Group (OMG): *Common Object Request Broker Architecture: Core Specification.* URL http://www.omg.org/cgi-bin/doc?formal/04-03-12.pdf. Aktualisierungsdatum: 12. März 2004.

ÖSTERLE ET AL. 2010 ÖSTERLE, H.; BECKER, J.; FRANK, U.; HESS, T.; KARAGIANNIS, D.; KRCMAR, H.; LOOS, P.; MERTENS, P.; OBERWEIS, A.; SINZ, E.J.: Memorandum zur

gestaltungsorientierten Wirtschaftsinformatik. In: ÖSTERLE, H. (Hrsg.); WINTER, R. (Hrsg.); BRENNER, W. (Hrsg.): *Gestaltungsorientierte Wirtschaftsinformatik, Ein Plädoyer für Rigor und Relevanz*. 2010. ISBN 978-3-00-030310-4.

POWER 2008 POWER, J. P.: Decision Support Systems: A Historical Overview, In: BURSTEIN, F. (Hrsg.); HOLSAPPLE, C. W. (Hrsg.): *Handbook on Decision Support Systems 1*. Berlin (u. a.): Springer, 2008, S. 121-139.

PUBLISHING TECHNOLOGY 2010 Publishing Technology: *ingentaconnect*. URL http://www.ingentaconnect.com. Aktualisierungsdatum: 6. September 2010.

RATH 2009 RATH, M.: Rechtliche Aspekte von IT-Compliance. In: WECKER, G. (Hrsg.); VAN LAAK, H. (Hrsg.): *Compliance in der Unternehmerpraxis*. 2. Auflage. Wiesbaden: Gabler, 2009.

RATH UND SPONHOLZ 2008 RATH, M.; SPONHOLZ, R.: *IT-Compliance*. Belin (u. a.): Schmidt, 2008.

RIEKE UND WINKELMANN 2008 RIEKE, T.; WINKELMANN, A.: *Modellierung und Management von Risiken – Ein prozessorientierter Risikomanagement-Ansatz zur Identifikation und Behandlung von Risiken in Geschäftsprozessen.* In: Wirtschaftsinformatik 50 (2008), Nr. 5, S. 346-356.

ROMERO UND ABELLÓ 2007 ROMERO, O.; ABELLÓ, A.: *Automating Multidimensional Design from Ontologies*. In: Proceedings of the 10th International Workshop on Data Warehousing and OLAP (DOLAP 2007, Lissabon, Portugal, 9. November 2007). ACM, 2007, S. 1-8.

SADIQ ET AL. 2007 SADIQ, S.; GOVERNATORI, G.; NAMIRI, K.: *Modeling Control Objectives for Business Process Compliance*. In: Proceedings of the 5th International Conference on Business Process Management (Brisbane, Australien, 24. - 28. September 2007). Lecture Notes in Computer Science 4714, Berlin (u. a.): Springer, 2007, S. 149-164.

SANDKÜHLER 1999A SANDKÜHLER, H. J. (Hrsg.): *Enzyklopädie Philosophie, Band 1: A-N*. Hamburg: Meiner, 1999.

SANDKÜHLER 1999B SANDKÜHLER, H. J. (Hrsg.): *Enzyklopädie Philosophie, Band 2: O-Z*. Hamburg: Meiner, 1999.

SCHEER 1997 SCHEER, A.-W.: *Referenzmodelle für industrielle Geschäftsprozesse*. 7. Auflage. Berlin (u. a.): Springer, 1997.

SCHMIDT 1974 SCHMIDT, H.: *Philosophisches Wörterbuch*. Neunzehnte Auflage. Stuttgart: Kröner, 1974.

SCHRADER UND HENNIG-THURAU 2009 SCHRADER, U.; HENNIG-THURAU, T.: *VHB-JOURQUAL2: Method, Results, and Implications of the German Academic Association for Business Research's Journal Ranking*. In: BuR – Business Research 2 (2009), Nr. 2, S. 180-204.

SECURE BUSINESS AUSTRIA 2010A SECURE BUSINESS AUSTRIA: *ARES Conference*. URL http://www.ares-conference.eu/conf/index.php/previous-conferences. Aktualisierungsdatum: 8. September 2010.

SECURE BUSINESS AUSTRIA 2010B SECURE BUSINESS AUSTRIA: *ARES Conference*, URL http://www.ares-conference.eu/conf/index.php/previous-keynotes. Aktualisierungsdatum: 8. September 2010.

SILVER 1991 SILVER, M. S.: *Systems That Support Decision Makers*, Chichester (u.a.): Wiley, 1991.

SKOUTAS UND SIMITSIS 2006 SKOUTAS, D.; SIMITSIS, A.: *Designing ETL Processes Using Semantic Web Technologies*. In: Proceedings of the 9th International Workshop on Data Warehousing and OLAP (DOLAP 2006, Arlington, VA, USA, 10. November 2006). ACM, 2006, S. 67-74.

SOLVABILITÄT II 2009 *Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II)*. Amtsblatt L 335 vom 17.12.2009, S. 1-155.

SOX 2002 *Sarbanes-Oxley Act of 2002*. Public Law 107–204.

SPRINGER 2010A SPRINGER SCIENCE+BUSINESS MEDIA (SPRINGER): *Lecture Notes in Computer Science (LNCS) Overview*. URL *http://www.springer.com/computer/lncs?SGWID=0-164-6-73659-0*. Aktualisierungsdatum: 21. August 2010.

SPRINGER 2010B SPRINGER SCIENCE+BUSINESS MEDIA (SPRINGER): *SpringerLink*. URL http://www.springerlink.de. Aktualisierungsdatum: 6. September 2010.

STAHL 2007 STAHL, T.; VÖLTER, M.; EFFTINGE, S.; HAASE, A.: *Modellgetriebene Softwareentwicklung*. 2. Auflage. Heidelberg: dpunkt.verlag, 2007.

TAKEDA ET AL. 1990 TAKEDA, H.; VEERKAMP, P.; TOMIYAMA, T.; YOSHIKAWA, H.: *Modeling Design Processes*. In: AI Magazine 11 (1990), Nr. 4, S. 37-48.

TEUBNER UND FELLER 2008 TEUBNER, A.; FELLER, T.: Informationstechnologie, Governance und Compliance. In: *Wirtschaftsinformatik* 5, 2008, S. 400-407.

TORLONE UND PANELLA 2005 TORLONE, R.; PANELLA, I.: *Design and Development of a Tool for Integrating Heterogeneous Data Warehouses*. In: Proceedings of the 7th International Conference on Data Warehousing and Knowledge Discovery (DaWaK 2005, Kopenhagen, Dänemark, 22. - 26. August 2005), Lecture Notes in Computer Science 3589. Berlin (u. a): Springer, 2005, S. 105-114.

UNECE 2010 UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE (UNECE): *United Nations Directories for Electronic Data Interchange for Administration, Commerce and Transport*. URL http://www.unece.org/trade/untdid/welcome.htm. Aktualisierungsdatum: 3. September 2010.

UNI HAWAII 2010 UNIVERSITY OF HAWAI'I AT MANOA: *Hawaii International Conference on System Sciences*. URL http://www.hicss.hawaii.edu. Aktualisierungsdatum: 31. August 2010.

UNI PRETORIA 2010 UNIVERSITY OF PRETORIA: *ECIS2010*. URL http://web.up.ac.za/default.asp?ipkCategoryID=8136. Aktualisierungsdatum: 7. September 2010.

UNI SAINT LOUIS 2010 UNIVERSITY OF SAINT LOUIS: *About ICIS 2010*. http://icis2010.aisnet.org/about.htm. Aktualisierungsdatum: 16. August 2010.

UNI TRIER 2010 UNIVERSITÄT TRIER: *The DBLP Computer Science Bibliography*. http://www.informatik.uni-trier.de/~ley/db. Aktualisierungsdatum: 6. September 2010.

VAISHNAVI UND KÜCHLER 2009 VAISHNAVI, V.; KÜCHLER, W.: *Design Research in Information Systems*. URL http://desrist.org/design-research-in-information-systems. Aktualisierungsdatum: 16. August 2009.

VOLONINO ET AL. 2004 VOLONINO, L.; GESSNER, G. H.; KERMIS, G. F.: *Holistic Compliance with Sarbanes-Oxley*. In: Communications of the Association for Information Systems 14 (2004), Nr. 1, S. 219-233.

WALSTROM UND HARDGRAVE 2001 WALSTROM, K. A.; HARDGRAVE, B. C.: *Forums for Information Systems Scholars: III*. In: Information & Management 39 (2001), Nr. 2, S. 117-124.

WIKIMEDIA 2010 WIKIMEDIA FOUNDATION: *Wiki*. URL http://en.wikipedia.org/wiki/Wiki. Aktualisierungsdatum: 6. September 2010.

WILDE UND HESS 2007 WILDE, T.; HESS, T.: *Forschungsmethoden der Wirtschaftsinformatik: Eine empirische Untersuchung*. In: Wirtschaftsinformatik 49 (2007), Nr. 4, S. 280-287.

WKWI UND GI-FB WI 2008 Wissenschaftliche Kommission Wirtschaftsinformatik im Verband der Hochschullehrer für Betriebswirtschaft e.V. (WKWI); Fachbereich Wirtschaftsinformatik der Gesellschaft für Informatik (GI-FB WI): *WI-Orientierungslisten*. In: Wirtschaftsinformatik 50 (2008), Nr. 2, S. 155-163.

W3C 2004A WORLD WIDE WEB CONSORTIUM (W3C): *Resource Description Language (RDF).* URL http://www.w3.org/TR/2004/REC-rdf-concepts-20040210. Aktualisierungsdatum: 10. Februar 2004.

W3C 2004B WORLD WIDE WEB CONSORTIUM (W3C): *Web Services Architecture*. URL http://www.w3.org/TR/ws-arch. Aktualisierungsdatum: 11. Februar 2004.

W3C 2006A WORLD WIDE WEB CONSORTIUM (W3C): *A Survey of RDF/Topic Maps Interoperability Proposals*. URL http://www.w3.org/TR/rdftm-survey. Aktualisierungsdatum: 10. Februar 2006.

W3C 2006B WORLD WIDE WEB CONSORTIUM (W3C): *Guidelines for RDF/Topic Maps Interoperability*. URL http://www.w3.org/2001/sw/BestPractices/RDFTM/guidelines-20060630.html. Aktualisierungsdatum: 30. Juni 2006.

W3C 2009 WORLD WIDE WEB CONSORTIUM (W3C): *OWL 2 Web Ontology Language Primer*, URL http://www.w3.org/TR/2009/REC-owl2-primer-20091027. Aktualisierungsdatum: 27 Oktober 2009.

W3C 2010 WORLD WIDE WEB CONSORTIUM (W3C): *About W3C*. URL http://www.w3.org/Consortium. Aktualisierungsdatum: 11. August 2010.

W3SCHOOLS 2010 W3SCHOOLS: *Browser Statistics*. URL http://www.w3schools.com/browsers/browsers_stats.asp. Aktualisierungsdatum: 8. September 2010.

YE ET AL. 2008 YE, H.; HE, Y.; XIANG, Z.: *Continuous Auditing System Based on Registration Center*. In: WSEAS Transactions on Information Science & Applications 5 (2008), Nr. 5, S. 746-755.

IWI Diskussionsbeiträge
#30 (19. Dezember 2008)[1]
ISSN 1612-3646

Strukturierte Literaturrecherche und -klassifizierung zu den Forschungsgebieten Business Intelligence und Data Warehousing

Matthias Kehlenbeck[2] und Michael H. Breitner[3]

1 Kurzfassung

Zur Entwicklung einer aktuellen Übersicht über die Forschungsgebiete Business Intelligence und Data Warehousing und zur Identifikation aktueller Forschungsthemen wurden etwa 2400 ab dem Jahr 2006 veröffentlichte Beiträge systematisch gesammelt, durchgesehen, kategorisiert und klassifiziert. Die für die Forschungsgebiete inhaltlich relevanten Beiträge wurden nach Kategorien, Konferenzen und Zeitschriften ausgewertet und tabellarisch dargestellt.

Die in diesem Beitrag enthaltenen Tabellen stellen eine aktuelle und kompakte Übersicht über die Forschungsgebiete und deren Forschungsthemen dar.

[1] Kopien oder eine PDF-Datei sind auf Anfrage erhältlich: Institut für Wirtschaftsinformatik, Leibniz Universität Hannover, Königsworther Platz 1, 30167 Hannover (www.iwi.uni-hannover.de).

[2] Diplom-Ökonom, Niedersächsisches Hochschulkompetenzzentrum für SAP (CCC), Welfengarten 1 (PF 114), 30167 Hannover (kehlenbeck@iwi.uni-hannover.de).

[3] Professor für Wirtschaftsinformatik und Betriebswirtschaftslehre und Direktor des Instituts für Wirtschaftsinformatik der Leibniz Universität Hannover (breitner@iwi.uni-hannover.de).

2 Einführung und Motivation

Der Begriff Business Intelligence ist mehr als fünfzig Jahre alt[4] und bezeichnet datenbasierte Entscheidungsunterstützungssysteme.[5] Zur Bereitstellung der entscheidungsrelevanten Daten werden seit etwa zwanzig Jahren Data Warehouse Systeme eingesetzt.[6] Data Warehouse Systeme übernehmen Daten aus unterschiedlichen Quellsystemen, integrieren diese in ein einheitliches Modell und speichern sie in einer persistenten und zeitgeführten Sammlung.[7]

Die Anzahl der wissenschaftlichen Veröffentlichungen zu den Forschungsgebieten Business Intelligence und Data Warehousing ist hoch und die Forschergemeinschaft produktiv. Um den Diskussionen zu aktuellen Forschungsthemen nicht nur folgen sondern diese durch eigene Beiträge auch bereichern zu können, ist eine Konzentration auf einzelne Forschungsthemen sinnvoll. Eine solche Konzentration setzt die Kenntnis aktueller Forschungsthemen und somit eine aktuelle Übersicht über die Forschungsgebiete voraus. Zur Erfüllung dieser Voraussetzungen wurde die im nächsten Abschnitt beschriebene Vorgehensweise gewählt.

3 Vorgehensweise und Begründung

Ausgangspunkt der Einarbeitung in das Forschungsgebiet und der Identifikation aktueller Forschungsthemen waren Suchanfragen in folgenden Online-Literaturdatenbanken:

- Association for Computing Machinery (ACM)[8],
- Engineering Village[9],
- IngentaConnect[10],
- ScienceDirect[11] sowie
- SpringerLink[12].

ACM ist die weltweit größte wissenschaftliche Gesellschaft für Informatik, organisiert Tagungen und publiziert Zeitschriften. Engineering Village und ScienceDirect gehören zu Elsevier, SpringerLink zu Springer Science+Business Media und IngentaConnect zu Publishing Technology. Elsevier[13] und Springer Science+Business Media[14] sind weltweit

[4] Vgl. LUHN, H. P. (1958), S. 314.
[5] Vgl. Power, D. J. (2007).
[6] Vgl. DEVLIN, B. A.; MURPHY, P. T. (1988), S. 60.
[7] VGL. INMON, W. H. (2005), S. 29-33.
[8] Online verfügbar unter http://www.acm.org.
[9] Online verfügbar unter http://www.engineeringvillage.org.
[10] Online verfügbar unter http://www.ingentaconnect.com.
[11] Online verfügbar unter http:// www.sciencedirect.com.
[12] Online verfügbar unter http://www.springerlink.com.
[13] Online verfügbar unter http://www.elsevier.com.

führende wissenschaftliche Verlage. Publishing Technology[15] ist ein Hersteller für Veröffentlichungstechnologie. Die Datenbanken wurden mit dem Ziel ausgewählt, möglichst viele der für die Forschungsgebiete relevanten Beiträge abzudecken.

In den Online-Literaturdatenbanken wurde in den Schlüsselwörtern, Titeln und Zusammenfassungen der Beiträge nach folgenden Begriffen gesucht:

- „Business Intelligence“,
- „Business“ und „Intelligence“,
- „Common Warehouse Metamodel“,
- „Common“ und „Warehouse“ und „Metamodel“,
- „Data Warehouse“,
- „Data“ und „Warehouse“,
- „Data Warehousing“,
- „Data“ und „Warehousing“ sowie
- „OLAP“[16].

Um zu vermeiden, dass die Vorgabe der Suchbegriffe zu einer Einschränkung auf bestimmte Forschungsthemen führt, wurden bewusst allgemeine Begriffe aus den Forschungsgebieten gewählt. Aufgrund der noch fehlenden Übersicht über die Forschungsgebiete war die Verwendung von speziellen Begriffen auch gar nicht möglich. Die aufgeführten englischen Begriffe werden in der Regel auch im deutschsprachigen Raum verwendet.[17]

Die Suchergebnisse wurden aus den einzelnen Online-Literaturdatenbanken in Dateien exportiert, automatisiert und / oder manuell nachbearbeitet sowie in eine gemeinsame Literaturdatenbank importiert. Anschließend wurde diese Literaturdatenbank auf Grundlage von Titel und Veröffentlichungsjahr automatisiert auf Dubletten hin überprüft. Nach Abzug der Dubletten enthielt die gemeinsame Literaturdatenbank 8678 Beiträge. Die Veröffentlichungsjahre dieser Beiträge reichten aber zum Teil bis in die zwanziger Jahre des letzten Jahrhunderts zurück. Da eine *aktuelle* Übersicht über die Forschungsgebiete entwickelt und *aktuelle* Forschungsthemen identifiziert werden sollten, wurde auf die 2383 Beiträge ab dem Jahr 2006 – dies entspricht 27,5% aller Beiträge – eingegrenzt. Tabelle 1 enthält eine Übersicht der gemeinsamen Literaturdatenbank vor, Tabelle 2 nach der Eingrenzung.

[14] Online verfügbar unter http://www.springer-sbm.de.
[15] Online verfügbar unter http:/www.publishingtechnology.com.
[16] Online Analytical Processing, vgl. CODD, E. F. et al. (1993).
[17] Beispielsweise für die Beschreibungen der Tracks der 8. Internationalen Tagung Wirtschaftsinformatik, online verfügbar unter http://www.aifb.uni-karlsruhe.de/Forschungsgruppen/BIK/wi2007/tracks.htm.

Tabelle 1: Alle Beiträge

Datenbank	alle Beiträge			
	Beiträge	Reduzierung durch		verbleibende Beiträge
		interne[18] Dubletten	externe[19] Dubletten	
ACM	2607	118	0	2489
ScienceDirect	766	2	193	571
SpringerLink	1056	29	171	856
Engineering Village	5496	77	1263	4156
IngentaConnect	980	7	367	606
			Summe	**8678**

Tabelle 2: Beiträge ab 2006

Datenbank	Beiträge ab 2006			
	Beiträge	Reduzierung durch		verbleibende Beiträge
		interne Dubletten	externe Dubletten	
ACM	569	8	0	561
ScienceDirect	196	0	74	122
SpringerLink	427	10	24	393
Engineering Village	1627	16	457	1154
IngentaConnect	214	1	60	153
			Summe	**2383**

Um eine aktuelle Übersicht über die Forschungsgebiete zu entwickeln wurden die Titel und Zusammenfassungen aller Beiträge ab dem Jahr 2006 gelesen. Zur Identifizierung aktueller Forschungsthemen wurden die Beiträge unmittelbar nach dem Lesen ihrer Titel und Zusammenfassungen kategorisiert. Da sich die Übersicht über die Forschungsgebiete erst während des Lesens entwickelt hat, konnten die Kategorien nicht davor festgelegt werden, sondern wurden währenddessen gebildet.

85 Beiträge konnten aufgrund von Titel und Zusammenfassung nicht kategorisiert werden. Fünf weitere Beiträge waren Dubletten, die im Rahmen der automatisierten Prüfung nicht entdeckt wurden. Die Kategorien zu den übrigen 2293 Beiträgen wurden zurück in die gemeinsame Literaturdatenbank übernommen. Auf Grundlage dieser Literaturdatenbank wurden Auswertungen erstellt. Abbildung 1 fasst das Vorgehen zusammen.

[18] Beiträge, die innerhalb der Datenbank mehrfach aufgeführt waren.
[19] Beiträge, die bereits in den zuvor aufgenommenen Datenbanken aufgeführt waren.

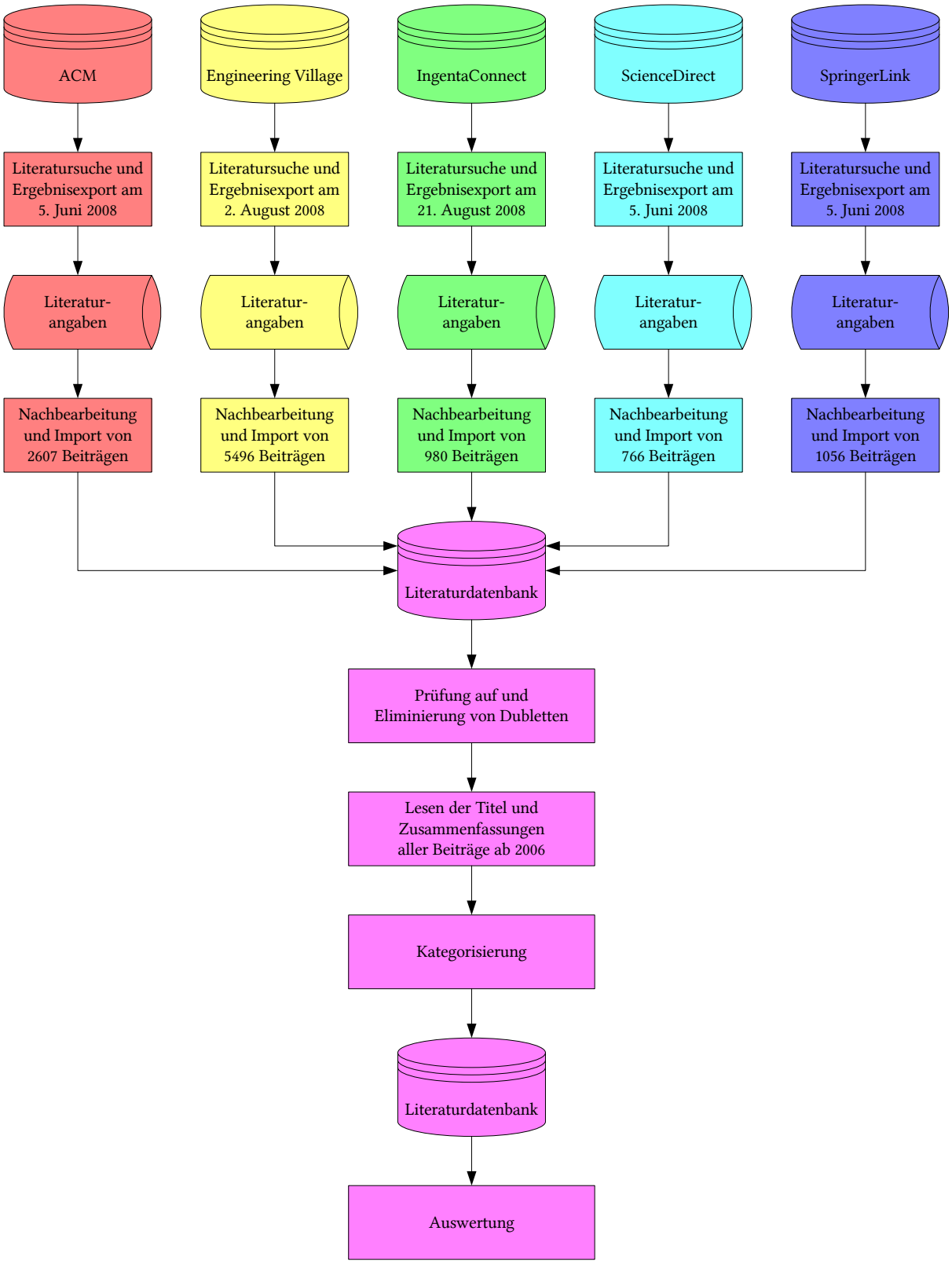

Abbildung 1: Prozess der Literatursammlung, -durchsicht, -kategorisierung und –klassifizierung

Im Rahmen der Kategorisierung wurden Haupt- und Unterkategorien gebildet. Alle Beiträge wurden einer Haupt- und bis zu zwei Unterkategorien zugeordnet. Die Zuordnung zu einer Hauptkategorie war in der Regel problemlos möglich.

Tabelle 3: Beiträge nach Veröffentlichungsform

Veröffentlichungsform	Anzahl
Artikel in Zeitschrift	465
Artikel in Konferenzband	583
Artikel in Fachbuch	88
Dissertation	29
Fachbuch	7
Summe	1172

Tabelle 4: Beiträge nach Veröffentlichungsjahr

Jahr	Anzahl
2006	492
2007	479
2008	201
Summe	1172

1121 Beiträge wurden als inhaltlich für die Forschungsgebiete nicht relevant kategorisiert. Diese Beiträge sind vorwiegend aufgrund der zerteilten Suchbegriffe wie „Data“ und „Warehousing“ in die Suchergebnisse geraten. Mit Hilfe der gemeinsamen Literaturdatenbank wurde jedoch festgestellt, dass bei ausschließlicher Verwendung der nicht zerteilten Suchbegriffe wie „Data Warehousing“ 203 relevante Beiträge nicht unter die Suchergebnisse geraten wären.

4 Ergebnisse und Diskussion

Tabelle 3 enthält eine Übersicht der relevanten Beiträge nach Veröffentlichungsformen, Tabelle 4 nach Veröffentlichungsjahren. Der überwiegende Teil der Beiträge wurde in Zeitschriften oder Konferenzbänden veröffentlicht. 162 Konferenzbeiträge wurden in der Online-Literaturdatenbank des Verlages der entsprechenden Konferenzbände als Fachbuchartikel gekennzeichnet. Diese Beiträge wurden den Konferenzbeiträgen zugeordnet.

Tabelle 5 enthält eine Übersicht der relevanten Beiträge nach Hauptkategorien. Einige der Hauptkategorien wurden zusammengefasst. Hauptkategorien mit weniger als fünf Beiträgen sowie Unterkategorien sind nicht aufgeführt. Die Unterkategorien eignen sich zur näheren Beschreibung der besonders umfangreichen Kategorien „Anwendungen“ und „Performance“. Von den 279 Beiträgen zu „Anwendungen“ wurden 37 Beiträge der Unterkategorie „Gesundheit und Medizin“, 22 Beiträge der Unterkategorie „Marketing und Vertrieb“ sowie 20 Beiträge der Unterkategorie „Biologie und Landwirtschaft“ zugeordnet. Von den 130 Beiträgen zur „Performance“ wurden 97 Beiträge der Unterkategorie „materialisierte Views und Queries“ zugeordnet. Abschließend wurden einige der Unterkategorien zusammengefasst.

Tabelle 5: Beiträge nach Kategorien

Kategorien	**Anzahl**
Anwendungen (Data Warehousing, Data Mining und / oder Business Intelligence)	279
Performance von Data Warehouses / Data Warehouse Systemen	130
Data Mining / Entdeckung von Erkenntnissen in Datenbanken	87
Business Intelligence	65
Verarbeitung komplexer Daten in Data Warehouse Systemen	37
Usability und Visualisierung von / in Data Warehouse und / oder Business Intelligence Systemen	36
Multidimensionale Modellierung von Data Warehouses	32
Verteilte Data Warehouse Systeme	28
Extraktions-, Transformations- und Ladeprozess von Data Warehouse Systemen	26
Design von Data Warehouse Systemen	25
Änderungen an Data Warehouses	24
Business Process Intelligence	22
Sicherheit von Data Warehouses / Data Warehouse Systemen	22
Verarbeitung von räumlichen Daten in Data Warehouse Systemen	21
Real-Time Business Intelligence / Real-Time Data Warehousing	20
Komprimierung in Data Warehouse Systemen	18
Datenqualität	17
Integration von Data Warehouses	16
Verarbeitung von unpräzisen oder unsicheren Daten in Data Warehouse Systemen	15
Verarbeitung von Datenströmen	14
Forschungsanalysen und offene Forschungsfragen	14
Auswirkungen des Einsatzes von Data Warehousing und / oder Business Intelligence	13
Business Performance Management	13
Erfolgsfaktoren für den Einsatz von Data Warehouse und / oder Business Intelligence Systemen	11
Physische Datenspeicherung in Data Warehouse Systemen	10
Einsatz von Ontologien und semantisches Schlussfolgern	10
Betrieb von Data Warehousing Systemen	10
Datenschutz	10
Data Warehousing und / oder Business Intelligence Plattformen	9
Verarbeitung von Webdaten in Data Warehouse Systemen	9
Verarbeitung von räumlichen und zeitlichen Daten in Data Warehouse Systemen	8
Verarbeitung von zeitlichen Daten in Data Warehouse Systemen	8
Mobile Business Intelligence / Mobile Data Warehousing	8
Service-Orientierte Architekturen	6
Fallstudien	5
Vorgehensmodelle	5
Verarbeitung von Textdaten in Data Warehouse Systemen	5
Sonstige (verteilt auf 54 Kategorien)	84
Nicht relevante Beiträge	1121
Summe	**2293**

Tabelle 6 enthält eine Übersicht der relevanten Zeitschriftartikel nach Zeitschriften, Tabelle 7 eine Übersicht der relevanten Konferenzartikel nach Konferenzen. Zeitschriften und Konferenzen mit weniger als fünf Beiträgen sind nicht aufgeführt. Auffällig ist, dass eine spezialisierte Zeitschrift, wie das „International Journal of Business Intelligence and Data Mining" lediglich mit sechs relevanten Beiträgen vertreten ist. Exemplarisch wurde für diese Zeitschrift kontrolliert und bestätigt, dass alle Beiträge, deren Schlüsselwörter, Titel und Zusammenfassungen die Suchbegriffe enthielten, exportiert wurden. Die übrigen Beiträge enthielten speziellere Begriffe.

Tabelle 6: Zeitschriftenartikel nach Zeitschriften

	Ranking				
Zeitschriften	**ABDC[20]**	**CORE[21]**	**VHB[22]**	**WI[23]**	**Anzahl**
Decision Support Systems	**A+**	**A***	**C**	**A**	26
Data & Knowledge Engineering	**A**	**B**	**C**	**A**	23
IEEE Transactions on Knowledge and Data Engineering		**A**		**A**	9
Information Systems	**A**	**A**	**C**	**A**	9
Jisuanji Jicheng Zhizao Xitong / Computer Integrated Manufacturing Systems					7
Journal of Intelligent Information Systems		**B**			7
Jisuanji Yanjiu yu Fazhan / Computer Research and Development		**A**			7
Jisuanji Gongcheng / Computer Engineering					7
Information Sciences		**B**			7
International Journal of Business Intelligence and Data Mining		**C**			6
DB2 Magazine					6
WSEAS Transactions on Information Science and Applications		**C**			6
Journal of Computational Information Systems					6
Journal of Database Management	**B**	**A**			5
IEEE Transactions on Systems, Man, and Cybernetics		**B**		**A**	5
International Journal of Computational Science and Engineering		**A***			5
Communications of the ACM	**A**	**B**	**C**	**A**	5
The International Journal on Very Large Data Bases		**A***			5
Sonstige (verteilt auf 218 Zeitschriften)					314
Summe					465

[20] Vgl. ABDC (2008).
[21] Vgl. CORE (2008).
[22] Vgl. SCHRADER, U.; HENNIG-THURAU, T. (2008).
[23] Vgl. HEINZL, A. et al. (2008), S. 161-162.

Tabelle 7: Konferenzartikel nach Konferenzen

Konferenzen	Ranking		Anzahl
	CORE[24]	WI[25]	
International Conference on Data Warehousing and Knowledge Discovery (DaWaK)	B	C	36
International Workshop on Data Warehousing and OLAP (DOLAP)	C		25
International Conference on Database and Expert Systems Applications (DEXA)	A	C	24
International Conference on Data Engineering (ICDE)	A+		18
International Conference on Extending Database Technology (EDBT)	A	B	14
International Conference on Very Large Data Bases (VLDB)	A+		14
Hawaii International Conference on System Sciences (HICSS)	B	B	11
International Conference on Availability, Reliability and Security (ARES)	B		11
International Conference on Conceptual Modeling (ER)	B	B	11
International Conference on Data, Text and Web Mining and their Business Applications and Management Inform. Eng. (DATA)			11
Symposium on Applied Computing (SAC)	B		11
International Conference on Database Systems for Advanced Applications (DASFAA)	A		10
International Conference on Management of Data (SIGMOD)	A+	B	9
British National Conference on Databases (BNCOD)	B		8
East-European Conference on Advances in Databases and Information Systems (ADBIS)	B		8
OnTheMove (OTM)			8
International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)			7
International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)			7
International Conference on Machine Learning and Cybernetics (ICMLC)			6
International Database Engineering and Applications Symposium (IDEAS)	B		6
Advances in Information Systems (ADVIS)			5
International Conference on Computational Science (ICCS)	A		5
International Workshop on Business Intelligence for the Real Time Enterprise (BIRTE)			5
International Conference on Computational Intelligence and Multimedia Applications (ICCIMA)	C		5
International Conference on Computer and Information Technology (ICCIT)	C		5
International Conference on Industrial Informatics (INDIN)			5
Conference on Information and Knowledge Management (CIKM)	A		5
International Conference on Knowledge Discovery and Data Mining (SIGKDD)	A+	B	5
International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD)			5
International Conference on Scientific and Statistical Database Management (SSDBM)	A		5
Sonstige (verteilt auf 183 Konferenzen)			278
Summe			583

[24] Vgl. CORE (2007).
[25] Vgl. HEINZL et al. (2008), S. 162-163.

5 Zusammenfassung und Ausblick

Zur Entwicklung einer aktuellen Übersicht über die Forschungsgebiete Business Intelligence und Data Warehousing und zur Identifikation aktueller Forschungsthemen wurden etwa 2400 ab dem Jahr 2006 veröffentlichte Beiträge aus einer Suche in fünf Online-Literaturdatenbanken systematisch gesammelt und auf Grundlage der Titel und Zusammenfassungen kategorisiert und klassifiziert. Die für die Forschungsgebiete inhaltlich relevanten Beiträge wurden nach Kategorien, Konferenzen und Zeitschriften ausgewertet und tabellarisch dargestellt.

Die in diesem Beitrag enthaltenen Tabellen stellen eine aktuelle und kompakte Übersicht über die Forschungsgebiete und deren Forschungsthemen dar und sind somit eine wertevolle Hilfe für die Einarbeitung in diese.

Da die in den Tabellen aggregierten Beiträge auf Ergebnissen von Suchanfragen in einer Auswahl von Online-Literaturdatenbanken basieren und bei diesen Suchanfragen für die Forschungsgebiete allgemeine und nicht für deren Forschungsthemen spezielle Suchbegriffe verwendet wurden, besteht kein Anspruch auf eine vollständige Berücksichtigung aller relevanten Beiträge.

Zur Entwicklung einer aktuellen Übersicht über einzelne Forschungsthemen und zur Identifikation aktueller Forschungsfragen empfiehlt sich, die Vorgehensweise mit für die Forschungsthemen speziellen Suchbegriffen und unter Einbeziehung der gewichtigsten Konferenzen und Zeitschriften zu wiederholen.

Literaturverzeichnis

AUSTRALIAN BUSINESS DEAN COUNCIL (ABDC): ABDC JOURNAL LIST (2008), online verfügbar unter http://www.abdc.edu.au/3.36.0.0.1.0.htm.

CODD, E. F. et al.: Providing OLAP to User-Analysts: An IT Mandate, online verfügbar unter http://dev.hyperion.com/resource_library/white_papers/providing_olap_to_user_analysts.pdf.

Computing Research & Education (CORE): 2007 Ranking of ICT Conferences (2007), online verfügbar unter http://www.core.edu.au.

Computing Research & Education (CORE): Journal Ranking July 2008 (2008), online verfügbar unter http://www.core.edu.au.

DEVLIN, B. A.; MURPY, P. T.: An architecture for a business and information system, in: IBM Systems Journal. Vol. 27, No. 1, 1988.

HEINZL et al.: WI-Orientierungsliste, in: WIRTSCHAFTSINFORMATIK. Vol. 50, No 2, 2008.

IMMON, W. H.: Building the Data Warehouse. Wiley, Indianapolis 2005.

LUHN, H. P.: A Business Intelligence System, in: IBM Journal. Oktober 1958.

POWER, D. J.: A Brief History of Decision Support Systems. DSSResources.COM, online verfügbar unter http://dssresources.com/history/dsshistory.html, Version 4.0, 10. März 2007.

SCHRADER, U.; HENNIG-THURAU, T.: VHB-JOURNAL 2, online verfügbar unter http://pbwi2www.uni-paderborn.de/WWW/VHB/VHB-Online.nsf/id/DE_Jourqual_2.

Ontology-Based Exchange and Immediate Application of Business Calculation Definitions for Online Analytical Processing

Matthias Kehlenbeck and Michael H. Breitner

Institut für Wirtschaftsinformatik, Leibniz Universität Hannover
{kehlenbeck,breitner}@iwi.uni-hannover.de

Abstract. Business users define calculated facts based on the dimensions and facts contained in a data warehouse. These business calculation definitions contain necessary knowledge regarding quantitative relations for deep analyses and for the production of meaningful reports. The business calculation definitions are implementation and widely organization independent. But no automated procedures facilitating their exchange across organization and implementation boundaries exist. Separately each organization currently has to map its own business calculations to analysis and reporting tools. This paper presents an innovative approach based on standard Semantic Web technologies. This approach facilitates the exchange of business calculation definitions and allows for their automatic linking to specific data warehouses through semantic reasoning. A novel standard proxy server which enables the immediate application of exchanged definitions is introduced. Benefits of the approach are shown in a comprehensive case study.

1 Introduction

For decision support business users have to perform analyses and create reports based on large data sets from heterogeneous sources. Data warehouses (DW) facilitate this decision support by integrating data from different systems and providing them in a consistent multidimensional (MD) model to analysis and reporting tools [1][2]. With the help of these tools business users build queries using the dimensions and facts contained in the MD model and define additional calculated facts based on them. These business calculation definitions contain necessary knowledge regarding quantitative relations for the performance of deep analyses and the production of meaningful reports. Although they are implementation and, to a large extend, organization independent, no automated procedures facilitating their exchange across organization and implementation boundaries exist. Therefore, each organization currently has to map its own business calculations to online analytical processing (OLAP) tools separately.
A major obstacle for the exchange of business calculation definitions is its missing division into organization independent and organization specific parts as well as its missing abstraction from implementation specific details. Moreover, organizations and implementations use different names for entities with the same

DOI: 10.1007/978-3-642-03730-6_24

meaning and describe the relations between these entities in different languages. In order to overcome these obstacles, this paper presents an innovative approach which structures business calculation definitions for OLAP into distinct layers of ontologies and enables business users to exchange definitions using standard technologies, e. g. by means of office documents or web pages. Exchanged definitions are automatically linked to specific data warehouses and immediately provided for OLAP.
The benefits of this proposal are demonstrated in a comprehensive case study in which business calculation definitions are created, exchanged and consolidated as well as automatically linked to a specific data warehouse and used as a semantic middleware layer while querying Microsoft Analysis Services (MSAS) [3], Penhao Analysis Services (PAS) [4] and SAP NetWeaver Business Intelligence (SAPBI) [5].
The remainder of this paper is structured as follows: Section 2 presents an overview of related work. Section 3 describes the approach for the ontology-based exchange and immediate application of business calculation definitions for OLAP. A comprehensive case study is provided in section 4. Finally, section 5 points out the conclusions.

2 Related Work

In the last few years, there has been a growing interest in metamodels and ontologies [6]. As these terms are closely related [7], the most relevant approaches are briefly described for both of them.
The Common Warehouse Metamodel (CWM) is a standardized metamodel for data warehouse metadata [8] and can be used in conjunction with the CWM Metadata Interchange Patterns (CWM MIP) [9] and XML Metadata Interchange (XMI) [10] for exchange. Januszewski and Pankowski use the Behavioral Metamodel part of the CWM to create an implementation independent description of a calculation function for a business quantity [11]. This description is primarily intended for the subsequent implementation of the function on a data warehouse platform and does not distinguish between business entities and their data warehouse representations. Futhermore, the description does not define the meaning of the contained terms. The authors suggest to use the Business Nomenclature part of the CWM to define those terms. However, this part is far less expressive than the available ontology languages.
The Model-Driven Architecture (MDA) is an approach which emphasizes the use of models in software development [12]. The requirements and the vocabularity of business users are described in the Computation Independent Model (CIM), which forms the basis to create the Platform Independent Model (PIM). Finally, the PIM is used to derive a Platform Specific Model (PSM). These models can be described using the Unified Modeling Language (UML) [13], transformed using Query/View/Transformations (QVT) [14] and exchanged using XMI. Mazón and Trujillo describe a comprehensive MDA approach for the development of data warehouses [15]. They use UML profiles to create a PIM for the multidimensional

DOI: 10.1007/978-3-642-03730-6_24

model and derive a corresponding PSM in the CWM using QVT transformations. A similar approach for queries is presented by Pardillo et al. [16]. None of these approaches deals with the modeling of calculated facts.
The Web Ontology Language (OWL) is a machine interpretable knowledge representation language [17]. OWL provides its three sublanguages OWL Lite, OWL DL and OWL Full. As OWL Lite and DL are both based on description logics (DL), they can be used in conjunction with available semantic reasoners. Xie et al. use an extended OWL DL to represent a conceptual enterprise data model and a conceptual multidimensional model [18]. Based on these models, business users define analysis requirements. Afterwards IT specialists map new entities to the data warehouse model and use a deployment engine to create a dedicated data mart. As an exchange of entities and their relations is not intended, the approach does not distinguish between organization independent and organization specific parts and provides for the definition of calculated facts in a proprietary language.
Diamantini and Potena propose to annotate data cubes by describing the contained facts with a business and a mathematic ontology [19]. The business ontology is described using OWL while the mathematic ontology is described using MathML [20] and OpenMath [21]. Both ontologies are maintained exclusively by IT specialists after they made changes to data cubes. The exchange of entities and their relations is not discussed.
This contribution is the first approach which facilitates the exchange of business calculation definitions between business users across organization and implementation boundaries and enables their immediate application to specific data warehouses. Moreover, the approach exclusively uses standard technologies and is therefore easy to implement and maintain.

3 Ontology-Based Exchange and Immediate Application of Business Calculation Definitions for OLAP

As business and data warehousing are different domains, their entities and relations are mapped to distinct ontologies. Business entities and their relations are only contained in the business ontology while data warehouse entities and their relations are only contained in the data warehouse ontology. The business ontology is divided into an organization independent and an organization specific part to facilitate the exchange of business calculation definitions. Likewise, the data warehouse ontology is divided into an implementation independent and an implementation specific part to increase its reusability. Business and data warehouse ontology are combined with each other by the mapping ontology. The mapping ontology consists of a manually created and an automatically inferred part. All ontologies are defined in OWL DL and are used in conjunction for OLAP. This is illustrated in Figure 1 and concisely described in the following subsections.

DOI: 10.1007/978-3-642-03730-6_24

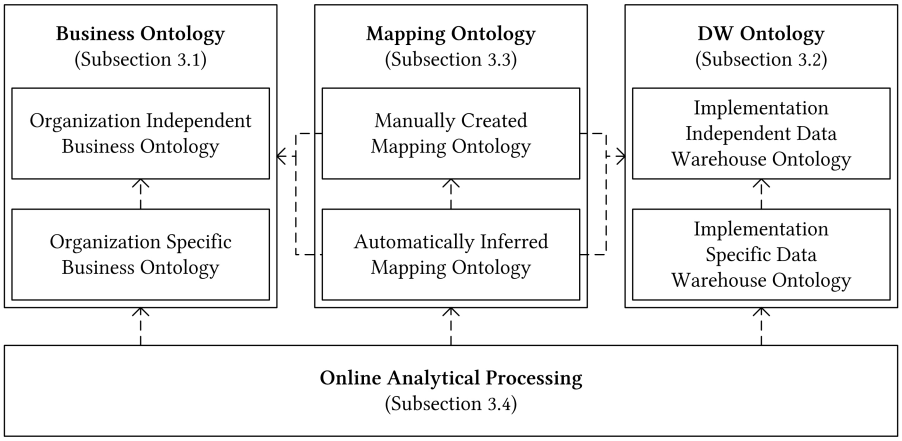

Fig. 1. Business calculation definitions and DW models are structured into distinct ontologies. They are solely combined with each other by the mapping ontology. All ontologies are used in conjunction for OLAP. Arrows (−→) correspond to dependencies.

3.1 Business Ontology

The business ontology is based on the concepts function, term, operator, quantity, object and set. Functions have exactly one calculation term and return a quantity with its result. Additionally, functions may have one restriction term which constrains the domain of application. Terms are either single quantities, objects or sets, or they have exactly one operator and at least one other term as an operand. Operands may take on different roles, e. g. the role of a dividend or divisor, depending on the used operator. Operators, quantities, objects and sets are uniquely identified by their name. Individuals are sorted into the organization independent respectively specific ontology according to their nature. Figure 2 illustrates the concepts and relations of the business ontology.
Provided that an ontology is defined in a prevalent language, like OWL, it is well suited for its exchange and consolidation with other ontologies [22]. However, it is also desirable to facilitate the exchange of single functions. Prevalent languages for the description of mathematical functions are MathML and OpenMath. MathML provides its sublanguages MathML Presentation and MathML Content. MathML Presentation focuses on the display of expressions while MathML Content and OpenMath focus on their semantic meaning. Functions of the business ontology can be transformed to MathML Content or OpenMath expressions and vice versa. Therefore, it is also possible to use business calculation definitions which were originally created for other purposes than OLAP, e. g. for their description on wiki pages. As MathML and OpenMath provide for the definition of symbols in Content Dictionaries (CD), operators may refer to a corresponding CD and CD base. Additionally, terms may possess a corresponding MathML Content, MathML Presentation and/or OpenMath expression.

DOI: 10.1007/978-3-642-03730-6_24

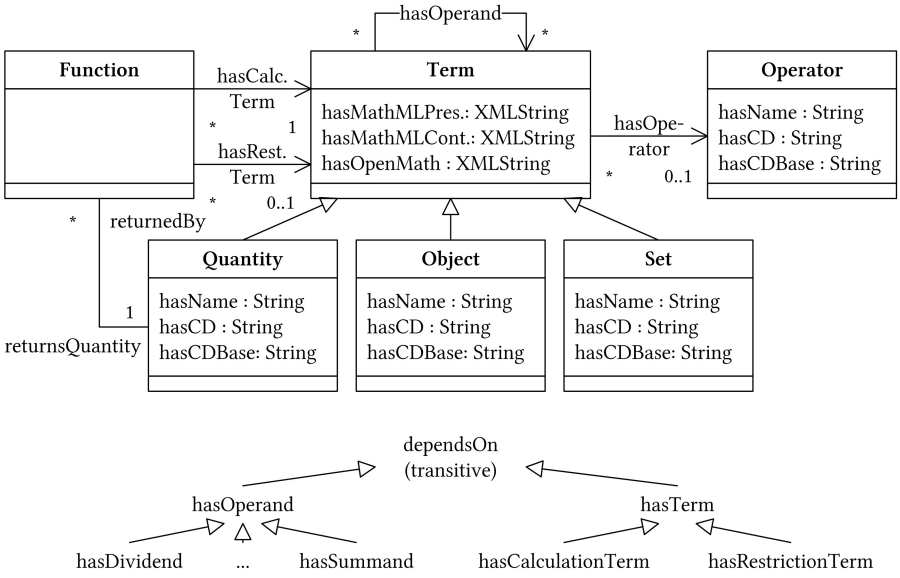

Fig. 2. Concepts, associations (→) and generalizations (⊳) of the business ontology. OWL supports many relation types, e. g. generalized as well as transitive relations.

As MathML and OpenMath expressions can be embedded in any Extensible Markup Language (XML) [23] document, e. g. office documents [24] or web pages [26], their technical exchange is simple. However, their businesslike exchange requires the consolidation of external and internal terms. Therefore, business users have to decide for every external quantity, object or set referred by an exchanged expression whether it has to be replaced by an already existing or taken over as a new individual. To allow for the globally unique identification of these individuals, they may refer to a corresponding CD and CD base as well.
Although functions are stored in a tree structure, the quantities, objects and/or sets required for their evaluation can be inferred using a transitive relation. The business ontology contains an object property `dependsOn` which is transitive and is a super property of the object properties `hasOperand` and `hasTerm`. The inverse object property of `dependsOn` is `requiredBy`. Using these relations, the set of quantities required for the evaluation of on individual function F can be defined in Manchester OWL Syntax [25] by the class expression `Quantity and requiredBy value F`.

3.2 Data Warehouse Ontology

The data warehouse ontology is based on the concepts cube, fact and dimension. Cubes possess an arbitrary number of facts and dimensions. However, each of them may only belong to one cube. All individuals possess a unique identifier.

DOI: 10.1007/978-3-642-03730-6_24

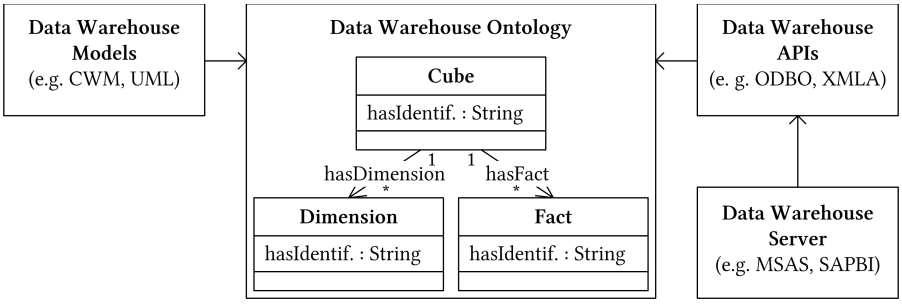

Fig. 3. Alternative information flows (⟶) for the generation of the DW ontology

Individuals can be generated from data warehouse models, e. g. based on CWM or UML, or using data warehouse application programming interfaces (APIs), e. g. OLE DB for OLAP (ODBO) [27] or XML for Analysis (XMLA) [28], with an OWL API [29] and sorted into the implementation independent respectively specific ontology according to their nature. Figure 3 illustrates the generation of the data warehouse ontology.

3.3 Mapping Ontology

The manually created mapping ontology solely consists of the symmetric object property `isMappedTo` which maps objects to dimensions respectively quantities to facts. These mappings can be either created manually by IT specialists or, if possible, inferred from Semantic Web Rule Language (SWRL) [30] rules. E. g., the SWRL rule `Quantity(?q)` ∧ `hasName(?q, ?n)` ∧ `Fact(?f)` ∧ `hasIdent(?f, ?i)` ∧ `equal(?n, ?i)` → `isMappedTo(?q, ?f)` maps a quantity to a fact, if quantity name and fact identifier equal.
Based on the other ontologies, a semantic reasoner creates the automatically inferred mapping ontology. In particular, it infers which quantities can be provided by which cubes using which functions and mappings. A cube is able to provide an object if it is mapped to one of its dimensions and is able to provide a quantity if it is mapped to one of its facts and/or returned by one of its supported functions. This can be defined by the property chains `hasDimension` ∘ `isMappedTo` → `isAbleToProvideObject`, `hasFact` ∘ `isMappedTo`→ `isAbleToProvideQuantity` and `supportsFunction` ∘ `returnsQuantity` → `isAbleToProvideQuantity`. A cube supports a function if it only uses quantities and objects which the cube is able to provide. The class of functions supported by a cube C can be defined by the expression `Function and dependsOn only ((not Object and not Quantity) or (isObjectAvailableForCube value C) or (isQuantityAvailableForCube value C))` and is a subclass of `Function` and `isSupportedByCube value C`, where `isObjectAvailableForCube` is the inverse of `isAbleToProvideObject`, `isQuantityAvailableForCube` the inverse of `isAbleToProvideQuantity` and `isSupportedByCube` the inverse of `supportsFunction`.

DOI: 10.1007/978-3-642-03730-6_24

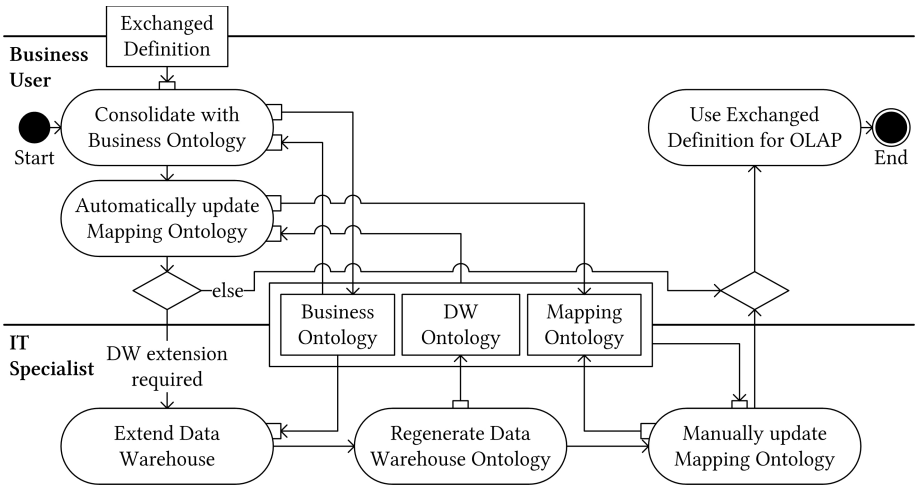

Fig. 4. Workflow from the exchange of a business calculation definition to its utilization for OLAP. Business users predominantly exchange definitions without IT specialists.

As these definitions use universal quantifiers, a semantic reasoner which makes the open world assumption requires closure axioms in order to infer the supported functions. These closure axioms can be created automatically by a tool which enumerates all objects, quantities and sets and complements the object property assertions based on `dependsOn` for all functions with corresponding negative object property assertions. Likewise, the class of supported functions can be defined automatically for each cube.

3.4 Online Analytical Processing

A workflow which describes the activities from the exchange of a definition to its utilization for OLAP is illustrated in Figure 4. It allows for a predominant exchange of business calculation definitions between business users without the participation of IT specialists. As the aforementioned ontologies contain all required information, a defined quantity can be provided automatically, if a data warehouse supports the corresponding function. This provision may take place on the client side, on the server side or in between. A provision on the client or server side would probably require as many different implementations as platforms. However, a provision in between may achieve platform independence by using a data warehouse API. Prevalent data warehouse APIs are ODBO and XMLA. ODBO is based on the proprietary Component Object Model (COM) [31] while XMLA is based on the platform independent SOAP [32] standard. SOAP web services can be described using the Web Services Definition Language (WSDL) [33]. As WSDL documents are available for several data warehouse servers, like MSAS and SAPBI, corresponding client and server side inter-

DOI: 10.1007/978-3-642-03730-6_24

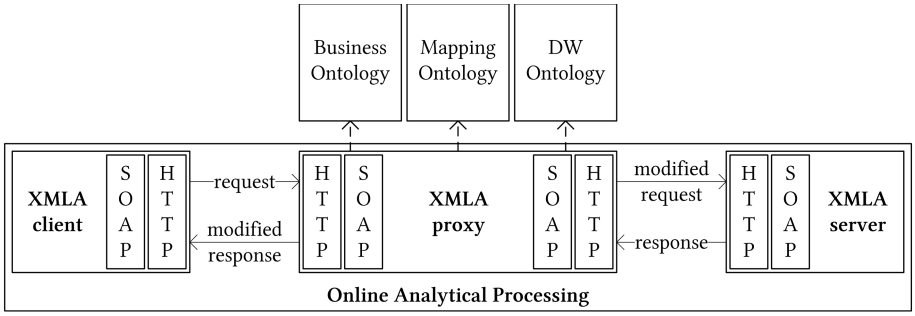

Fig. 5. Immediate application of definitions via XMLA compliant proxy server

faces can be created automatically using a web service framework, e. g. Apache CXF [34]. These interfaces enable the implementation of an XMLA proxy which provides the defined quantities by modifying the communication between client and server. In particular, the responses of XMLA discovery methods and the requests to XMLA execute methods can be modified. Figure 5 illustrates this approach. As a bridge driver which allows to use an ODBO client in conjunction with an XMLA server exists [35], a wide variety of clients can be used.

4 Case Study

This section contains a case study in which the definitions for two business quantities are produced using a MathML editor, exchanged as an XML document, consolidated with an existing ontology and immediately made available by means of semantic reasoning and an XMLA proxy.
A business user defines the quantities *EBIT Margin* and *EBIT* using a MathML editor, e. g. Integre MathML Equation Editor [36].

$$EBIT\ Margin = \frac{EBIT}{Net\ Sales}\ . \tag{1}$$

$$EBIT = Net\ Income - (Interest\ Income + Tax\ Income)\ . \tag{2}$$

They are saved to an XML document. E. g., the quantity *EBIT Margin* may be represented by the following MathML Content fragment:

```
<mml:apply>
  <mml:csymbol cd="relation1">eq</mml:csymbol>
  <mml:ci>EBIT Margin</mml:ci>
  <mml:apply>
    <mml:csymbol cd="arith1">divide</mml:csymbol>
    <mml:ci>EBIT</mml:ci>
    <mml:ci>Net Sales</mml:ci>
  </mml:apply>
</mml:apply>
```

DOI: 10.1007/978-3-642-03730-6_24

A different business user adopts these definitions. The quantities as well as their corresponding functions and terms are created in the organization independent business ontology. E. g., the quantity *EBIT Margin* may be represented by the following OWL DL fragment:

```
<Quantity rdf:about="#EBITMarginQuantity">
  <hasName>EBIT Margin</hasName>
</Quantity>
<Function rdf:about="#EBITMarginFunction">
  <hasCalculationTerm rdf:resource="#EBITMarginCalculationTerm"/>
  <returnsQuantity rdf:resource="#EBITMarginQuantity"/>
</Function>
<Term rdf:about="#EBITMarginCalculationTerm">
  <hasOperator rdf:resource="#DivisionOperator"/>
  <hasDividend rdf:resource="#EBITQuantity"/>
  <hasDivisor rdf:resource="#NetSalesQuantity"/>
</Term>
```

In this case study, the referred quantity *Interest Income* is already defined in the organization independent business ontology by the calculation term *Interest Revenue − Interest Expense*. Likewise, the referred quantities *Net Income*, *Net Sales* and *Tax Income* as well as the required quantities *Interest Revenue* and *Interest Expense* are already defined in the organization specific business ontology by calculation terms based on the quantity *Account Balance* and restriction terms based on the object *Account* and a corresponding set. E. g., the quantity *Interest Expense* is defined by the calculation term − *Account Balance* and the restriction term *Account* ∈ *Interest Expense Accounts*. Therefore, the quantities *EBIT Margin* and *EBIT* ultimately only depend on the quantity *Account Balance*, the object *Account* and the sets *Net Income Accounts*, *Net Sales Accounts*, *Tax Income Accounts*, *Interest Revenue Accounts* and *Interest Expense Accounts*. The quantity *Account Balance* is mapped to a corresponding fact and the object *Account* is mapped to a corresponding dimension of the cube `AdventureWorksCube`. Therefore, a semantic reasoner, e. g. Pellet [37], infers that `AdventureWorksCube supportsFunction EBITMarginFunction` as well as `AdventureWorksCube supportsFunction EBITFunction` and therefore `AdventureWorksCube isAbleToProvideQuantity EBITMarginQuantity` as well as `AdventureWorksCube isAbleToProvideQuantity EBITQuantity`. These axioms are saved to the automatically inferred mapping ontology.

An XMLA proxy makes the quantities immediately available for OLAP. It was implemented as a web service based on the Java API for XML Web Services (JAX-WS) [38] and is currently able to access MSAS, PAS and SAPBI as a web service consumer. XMLA defines two methods: discover and execute. Requests to the discover method of the XMLA proxy are passed unmodified to the responsible server. However, the proxy modifies the received results for the request types `MDSCHEMA_MEASUREGROUPS` and `MDSCHEMA_MEASURES` before passing them on to the client. Results for the request type `MDSCHEMA_MEASUREGROUPS` are complemented by an XMLA fragment like

DOI: 10.1007/978-3-642-03730-6_24

```
<MEASUREGROUP_NAME>XMLA Proxy</MEASUREGROUP_NAME>
<MEASUREGROUP_CAPTION>XMLA Proxy</MEASUREGROUP_CAPTION>
```

in order to create an additional measure group. Similarly, results for the request type `MDSCHEMA_MEASURES` are complemented by XMLA fragments like

```
<MEASURE_NAME>EBIT Margin</MEASURE_NAME>
<MEASURE_UNIQUE_NAME>[Measures].[EBIT Marg.]</MEASURE_UNIQUE_NAME>
<MEASURE_CAPTION>EBIT Margin</MEASURE_CAPTION>
<MEASURE_AGGREGATOR>127</MEASURE_AGGREGATOR>
<MEASUREGROUP_NAME>XMLA Proxy</MEASUREGROUP_NAME>
```

which correspond to the facts that can be additionally provided based on the information contained in the ontologies. This information is used to create expression trees, as illustrated in Figure 6, which are subsequently supplemented with the original results for the request type `MDSCHEMA_MEASURES` to determine the corresponding values of the `MEASURE_AGGREGATOR`. The latter indicates whether a measure was derived using a single aggregation function (e.g. SUM), a combination of aggregation functions, or using a more complex function. Due to the complementary XMLA fragments, the OLAP client regards the additional facts as available on the data warehouse server.

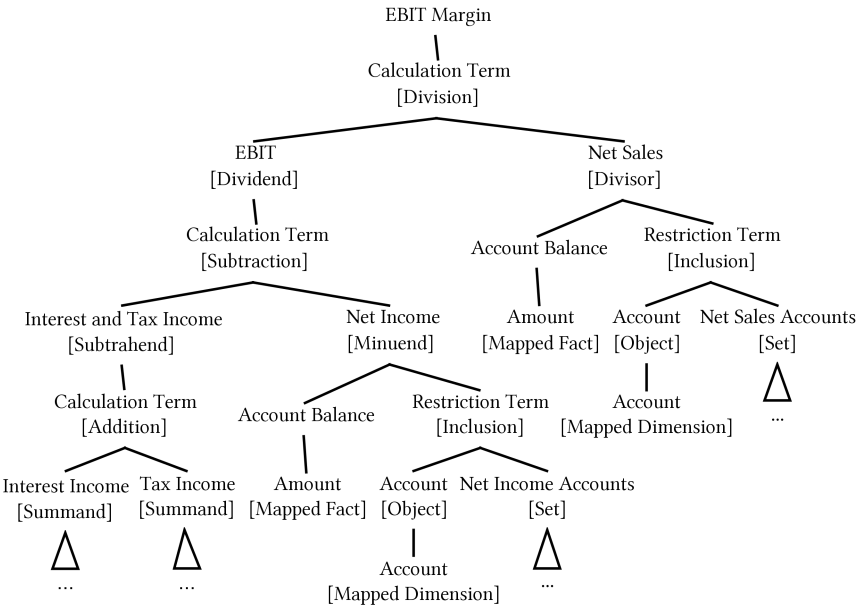

Fig. 6. Expression tree for the exchanged quantity *EBIT Margin*. Triangles represent parts which are not shown in full details due to space restrictions.

DOI: 10.1007/978-3-642-03730-6_24

Requests to the execute method of the XMLA proxy contain commands which can contain queries defined using Multidimensional Expressions (MDX) [39]. The XMLA proxy modifies the queries before passing them on to the responsible data warehouse server by complementing them with MDX fragments like

```
MEMBER [Measures].[EBIT Marg.] AS
  [Measures].[EBIT] / [Measures].[Net Sales]
```

which result from transformations of the supplemented expression trees. The received results are passed on unmodified to the client. Due to the MDX fragments, queries can use the additional facts from the ontologies just like the original facts from the data warehouse.
The proxy has been successfully tested with the MSAS, PAS and SAPBI servers as well as the IBM DataQuant for Workstation XMLA [40] and Microsoft Excel [41] ODBO clients. A positive side effect is that the proxy increases compatibility by unifying web service definitions, e. g. enabling to use IBM DataQuant for Workstation with SAPBI. Figure 7 contains a screenshot of Microsoft Excel connected to MSAS through the XMLA proxy and an ODBO bridge.

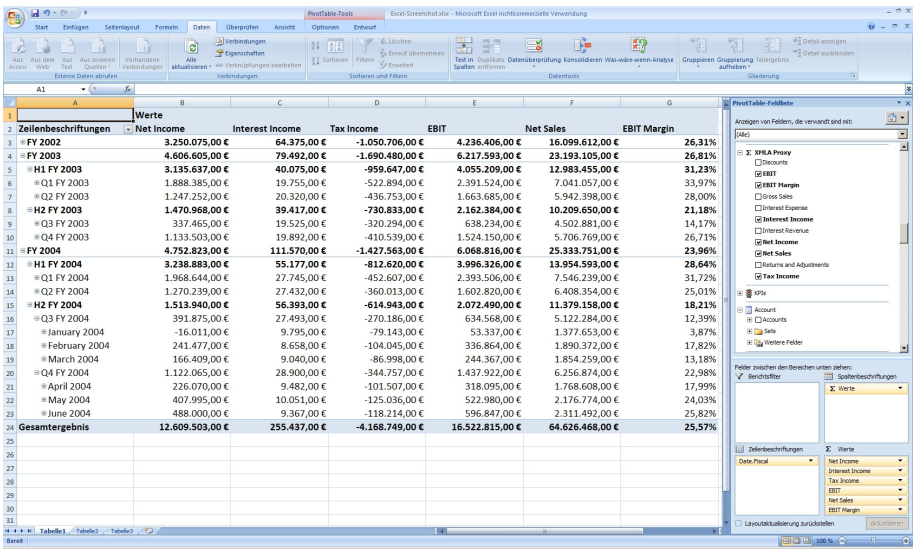

Fig. 7. Microsoft Excel connected to MSAS through the XMLA proxy and an ODBO bridge. Queries may use facts that can be additionally provided based on the information contained in the ontologies just like the original facts from a data warehouse.

DOI: 10.1007/978-3-642-03730-6_24

5 Conclusions and Outlook

This paper focuses on the problem of exchanging business calculation definitions across organization and implementation boundaries. An innovative approach based on Semantic Web technologies which facilitates the exchange of business calculation definitions is presented. This approach also supports the utilization of definitions which were created for other purposes than OLAP. Automatic linking of business calculation definitions to specific data warehouse models through semantic reasoning is enabled. A novel standard proxy server between analysis and reporting clients as well as data warehouse servers is introduced. This proxy server immediately provides exchanged definitions and enables business users to exchange their definitions independently from IT specialists. The benefits of the approach have been outlined in a comprehensive case study.
Research is now dedicated to the design, implementation and evaluation of more advanced analysis and reporting tools with direct support for Semantic Web technologies. In particular, the presented approach will be extended to facilitate the exchange of entire queries. This will require the inclusion of further parts of the multidimensional model.

References

1. Inmon, W. H.: Building the Data Warehouse. Wiley, New York (2005)
2. Kimball, R.: The Data Warehouse Lifecycle Toolkit. Wiley, New York (2008)
3. Microsoft Corporation: Microsoft Analysis Services, http://www.microsoft.com/sql/technologies/analysis/default.mspx
4. Pentaho Corporation: Pentaho Analysis Services, http://mondrian.pentaho.org
5. SAP AG: SAP NetWeaver Business Intelligence http://www.sap.com/germany/plattform/netweaver/components/businessintelligence/index.epx
6. Guizzardi, G.: On Ontology, ontologies, Conceptualizations, Modeling Languages, and (Meta)Models. Frontiers in Artificial Intelligence and Applications. **155** (2007) 18–35
7. Object Management Group (OMG): Ontology Definition Metamodel (ODM) Beta 2 (2007), http://www.omg.org/cgi-bin/doc?ptc/07-09-09
8. Object Management Group (OMG): Common Warehouse Metamodel (CWM) 1.1 (2003), http://www.omg.org/spec/CWM/1.1/PDF/
9. Object Management Group (OMG): CWM Metadata Interchange Patterns (2004), http://www.omg.org/cgi-bin/doc?formal/04-03-25
10. Object Management Group (OMG): XML Metadata Interchange 2.1.1 (2007), http://www.omg.org/docs/formal/07-12-01.pdf
11. Januszewski, A., Pankowski, T.: Modeling Analytical Indicators Using Data Warehouse Metamodel. Proceedings of the 17th International Conference on Database and Expert Systems Applications (DEXA 2006). IEEE. 642–646
12. Object Management Group (OMG): MDA Guide 1.0.1 (2003), http://www.omg.org/docs/omg/03-06-01.pdf
13. Object Management Group (OMG): Unified Modeling Language 2.2 Beta 1 (2008), http://www.omg.org/docs/pct/08-04-04.pdf
14. Object Management Group (OMG): MOF Query / View / Transformations 1.0 (2008), http://www.omg.org/docs/formal/08-04-03.pdf

DOI: 10.1007/978-3-642-03730-6_24

15. Mazón, J.-N., Trujillo, J.: An MDA approach for the development of data warehouses. Decision Support Systems **45** (2008) 41–58
16. Pardillo, J., Mazón, J.-N., Trujillo, J.: Bridging the Semantic Gap in OLAP Models: Platform-independent Queries Proceedings of the 11th International Workshop on Data Warehousing and OLAP (DOLAP 2008). ACM. 89–96
17. World Wide Web Consortium (W3C): OWL Web Ontology Language, http://www.w3.org/TR/2004/REC-owl-features-20040210/
18. Xie, G., Yang, Y., Liu, S., Qiu, Z., Pan, Y., Zhou, X.: EIAW: Towards a Business-friendly Data Warehouse Using Semantic Web Technologies. Proceedings of the 6th International Semantic Web Conference (ISWC 2007). IEEE. 857–870
19. Diamantini, C., Potena, D.: Semantic Enrichtment of Strategic Datacubes. Proceedings of the 11th International Workshop on Data Warehousing and OLAP (DOLAP 2008). ACM. 81–88
20. World Wide Web Consortium (W3C): Mathematical Markup Language (MathML) 3.0, http://www.w3.org/TR/2008/WD-MathML3-20081117/
21. The OpenMath Standard 2.0, http://www.openmath.org/standard/om20-2004-06-30/omstd20.pdf
22. de Laborda, C. P., Conrad, S.: Relational.OWL - A Data and Schema Representation Format Based on OWL. Proceedings of the 2nd Asia-Pacifc Conference on Conceptual Modelling (APCCM2005).
23. World Wide Web Consortium (W3C): Extensible Markup Language(XML) 1.0, http://www.w3.org/TR/2008/REC-xml-20081126/
24. Organization for the Advancement of Structured Information Standards (OASIS): The OpenDocument v1.0 Specification, http://www.oasis-open.org/committees/download.php/12572/OpenDocument-v1.0-os.pdf
25. University of Manchester: The Manchester OWL Syntax, http://www.co-ode.org/resources/reference/manchester_syntax/
26. World Wide Web Consortium (W3C): XHTML 1.0: The Extensible HyperText Markup Language, http://www.w3.org/TR/2000/REC-xhtml1-20000126/
27. Microsoft Corporation: OLE DB for Online Analytical Processing (OLAP), http://msdn.microsoft.com/en-us/library/ms717005(VS.85).aspx
28. Microsoft Corporation, Hyperion Solutions Corporation: XML for Analysis Specification 1.1, http://www.xmlforanalysis.com/xmla1.1.doc
29. Horridge, M., Bechhofer, S., Noppens, O.: Igniting the OWL 1.1 Touch Paper: The OWL API. Proceedings of the OWLED 2007 Workshop on OWL: Experiences and Directions. CEUR-WS.org
30. World Wide Web Consortium (W3C): SWRL: A Semantic Web Rule Language Combining OWL and RuleML, http://www.w3.org/Submissions/2004/SUBM-SWRL-20040521/
31. Microsoft Corporation: COM: Component Object Model Technologies, http://www.microsoft.com/com/default.mspx
32. World Wide Web Consortium (W3C): SOAP 1.2, http://www.w3.org/TR/2007/REC-soap12-part1-20070427/
33. World Wide Web Consortium (W3C): Web Services Definition Language (WSDL) 2.0, http://www.w3.org/TR/2007/REC-wsdl20-primer-20070626/
34. The Apache Software Foundation: Apache CXF: An Open Source Service Framework, http://cxf.apache.org/
35. Simba Technologies: SimbaO2X, http://www.simba.com/odbo-to-xmla.htm
36. Integre Technical Publishing Co., Inc.: MathML Equation Editor, http://www.integretechpub.com/zed/

DOI: 10.1007/978-3-642-03730-6_24

37. Clark & Parsia, LLC: Pellet: The Open Source OWL DL Reasoner, http://clarkparsia.com/pellet/
38. Sun Microsystems, Inc: JSR 224: Java API for XML-Based Web Services (JAX-WS) 2.0, http://jcp.org/en/jsr/detail?id=224
39. Microsoft Corporation: Multidimensional Expressions (MDX) Reference, http://msdn.microsoft.com/en-us/library/ms145506.aspx
40. International Business Machines Corp. (IBM): Dataquant, http://www-01.ibm.com/software/data/db2imstools/db2tools/dataquant/index.html
41. Microsoft Corporation: Microsoft Office Excel, http://office.microsoft.com/en-us/excel/FX100487621033.aspx

DOI: 10.1007/978-3-642-03730-6_24

Managing Internal Control in Changing Organizations through Business Process Intelligence – A Service Oriented Architecture for the XACML based Monitoring of Supporting Systems

Matthias Kehlenbeck, Thorben Sandner, Michael H. Breitner
Leibniz Universität Hannover
{kehlenbeck,sandner,breitner}@iwi.uni-hannover.de

Abstract

Organizations respond to opportunities and risks by strategic decisions. Strategic decisions ensure the sustainable existence of organizations, but require continuous organizational change. Organizational change includes the redesign of business processes. Processes are subject to internal and external requirements. Requirements include the alignment to strategic goals, the effective and efficient use of resources and the compliance with applicable laws and regulations. Their achievement is assured by embedding internal controls into processes. Many controls can be incorporated into supporting systems, as their access control functions allow the modeling of authorization and segregation of duties.

A model for the annotation of processes with controls, permissions and roles based on BPMN, COSO and XACML is presented. Additionally, a Service Oriented Architecture for the automated monitoring of controls and the timely communication of thereby detected control exceptions is proposed. The benefits of the approach are demonstrated in a prototype implementation and a corresponding case study.

1. Introduction

In order to achieve their strategic goals, to make effective and efficient use of their resources and to secure their reliability of financial reporting as well as their compliance with applicable laws and regulations, organizations perform risk management. Risk management is an ongoing process at every level of an organization designed to identify, assess and respond to potential risks for the entity [1]. Risk responses are incorporated into business processes by means of control activities. The management of internal control is therefore an integral part of risk management [2]. This management includes the design and implementation of monitoring procedures which ensure the effective operation of internal control over time as well as the identification and communication of internal control exceptions. Monitoring procedures include – amongst others – the periodic evaluation and testing of controls, the use of continuous monitoring software as well as the analysis of appropriate reports [3].

Provided that an organization utilizes IT systems to support its business processes, many control activities can be incorporated into these systems. In particular, their access control functions typically allow for the modeling of authorization and segregation of duties controls by means of permissions and roles. However, continuous organizational change (and increasing process orientation) entails frequent adjustments to business processes and thereby requires corresponding changes to systems and controls. Moreover, organizations often possess heterogeneous system landscapes and are thereby forced to model these controls in distinct repositories and using different access control languages. Therefore, the monitoring of these controls is complex and often time-consuming and compliance validation as a whole is still mainly a manual task [4], [5]. Thus, there is a need for capable automated detection and monitoring tools.

Corresponding approaches can be roughly distinguished by their employment phase: "after-the-fact" or "before-the-fact" [6], [7]. The after-the-fact phase is the classic application area of (i) manual audits (by consultants) and (ii) automated detection (with application support). A major drawback of after-the-fact approaches is that they entail adjustment costs. However, the before-the-fact phase contains (iii) compliance aware design and (iv) post design verification approaches which proactively try to avoid non compliance situations and thereby strive for the reduction of these costs. Due to the heterogeneous system landscapes, the implementation of these approaches is estimated as "extremely difficult" [6] though.

As the frequency of monitoring and reporting correlates with the success of compliance management [8],

DOI: 10.1109/HICSS.2010.262

it is important that control exceptions are timely communicated to the right decision-makers. This timeliness provides the decision-makers with the necessary latitude for corresponding measures. An absence of these measures may lead to far-reaching consequences, e.g. damage to the organizations reputation, decline of the organizations credit rating or market value, fraud and fines. Consequently, the achievement of the organizations objectives is put at risk.

This paper addresses the aforementioned issues by means of Design Science Research [9] and presents a synthesis between (ii) and (iv), as it enables the automated detection of control exceptions both after-the-fact and before-the-fact. In order to reduce complexity and time required, a model for the annotation of business processes with internal controls, critical permissions and roles based on existing standards is proposed. Additionally, an architecture for automated monitoring of authorization and segregation of duties controls as well as the timely communication of thereby detected control exceptions based on existing technologies is presented. Business processes are described using the Business Process Modeling Notation (BPMN) [10] in conjunction with the XML Process Definition Language (XPDL) [11], access control is described using the Extensible Access Control Markup Language (XACML) [12], internal control is described following the established Internal Control – Integrated Framework [13] respectively Enterprise Risk Management – Integrated Framework [2] (COSO) and control exceptions are formally defined using an Extensible Markup Language (XML) [14] based rule language, like the Rule Markup Language (RuleML) [15].

Decision-makers require meaningful information concerning the implications of control exceptions. In order to increase their acceptance, internal control can be presented in a coherent way with other characteristics and facts using a business intelligence (BI) system, thereby enabling a comprehensive view. Additionally, this enables IT specialists and process specialists to exploit drill-down functionalities for the location of the corresponding causes. To demonstrate the merits of this approach, we present a prototype implementation which enables the automated monitoring of controls and the timely communication of thereby detected control exceptions. It is realized by an orchestration of task-specific web services and employed in a SAP Enterprise Resource Planning (ERP) [16] and BI [17] environment. A practical application of the prototype is shown in a case study which refers to a typical financial business process which must consider several segregations of duties.

Section 2 presents an overview of related work. Section 3 describes the proposed model and section 4 the proposed architecture. The prototype implementation is presented in section 5 and a corresponding case-study is provided in section 6. Finally, section 7 concludes this paper.

2. Related Work

The IT infrastructure of today's organizations consists predominantly of heterogeneous distributed systems. To stay abreast of this development, there have been several attempts to centralize the definition and control of access and authorization (e.g. [18], [19] and [20]). The step towards a standardized and platform independent approach was affected by the Organization for the Advancement of Structured Information Standards (OASIS) with XACML. Amongst others, this standard provides for a processing engine which makes authorization policies interpretable and delivers decisions about acceptance or rejection: the so-called "Policy Decision Point" (PDP).

Alam et al. [21] use XACML in their approach to make the provisioning of security policies among different domains easier. They present SECTET-PL, a specification language for permissions in the context of UML models which transforms access and authorization information. But being part of the SECTET framework for model driven security for B2B-workflows, their work put a focus on specifying permissions for web services.

Pistoia et al. [22] develop a formal model for Role Based Access Control (RBAC) policy validation and a static analysis model for RBAC systems which is capable to analyze static policy models. Through the use of XACML, the present approach allows the use of other access control models than RBAC. Additionally, it enables not only a static analysis but also a runtime analysis of policies (as described in subsection 5.3).

A method for integrating risks in business processes is presented by zur Muehlen and Rosemann [23]. The authors developed a taxonomy of process related risks and capture the risk-related information with an extended Event-driven Process Chain (EPC) Notation. Furthermore, Sadiq et al. [6] developed a language for the representation of control objectives and propose to annotate business processes with corresponding control tags. However, the present approach includes an access control model, uses an internal control model, which resembles the COSO model more closely and prefers a standard rule language.

There has been a couple of work on developing approaches or tools for analyzing BPMN or Unified Modeling Language (UML) [24] models with regard to security requirements, including [25], [26], [27] and [28]. However, no tools for the verification of role or user permissions against security policies are proposed.

DOI: 10.1109/HICSS.2010.262

Höhn and Jürjens presented Rubacon [29], an implementation to support model-based development and evaluation of software configurations to indemnify compliance with security policies. In particular, they analyze UML models of business applications and corresponding configuration data in terms of their relevance for security policies and compliance requirements. Limitations are the use of proprietary XML formats for access control and rule data and a tightly coupled architecture.

3. Proposed Model

Organizations structure their activities in business processes. Business processes embed controls and are partially supported by IT systems. Authorization and segregation of duties controls can be incorporated into these IT systems using their access control functions. The proposed model therefore consists of a business process sub model, an access control sub model and an internal control sub model. Figure 1 contains an overview of the proposed model.

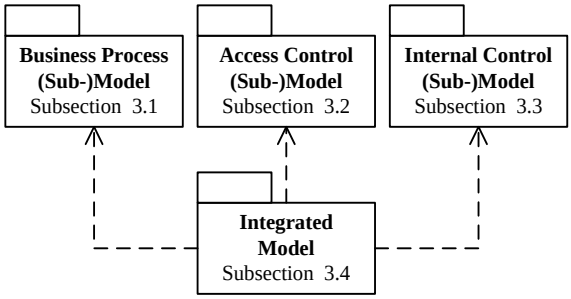

Figure 1: Overview of the proposed model and its sub-models as a UML package diagram

3.1. Business Process Model

The analysis and the optimization of their business processes are essential abilities for organizations in competition. For this reason, process owners often possess extensive knowledge regarding their processes. However, in terms of the alignment of processes with regulatory requirements (e.g. Sarbanes-Oxley Act (SOX), Euro-SOX, Basel II) and the design and implementation of corresponding controls, they often require external assistance. Moreover, process owners require the assistance of IT specialists to adjust their supporting IT systems. In summary, the design and implementation of processes requires the participation of numerous people with different backgrounds.
The BPMN has been developed to facilitate efficient communication between participants with different backgrounds. Additionally, it provides a mapping to the Web Services Business Process Execution Language (WSBPEL) [30]. UML activity diagrams are considered less suitable, as they were developed for a different problem domain – software engineering – and do not provide a mapping to web services.
BPMN defines a diagram notation, but not an exchange format. However, XPDL can be used to exchange BPMN diagrams. As an XML Schema Definition (XSD) [31] is available for XPDL, code generators may be used to create the model implementation.

3.2. Access Control Model

XACML can be used to centralize the definition and control of access and authorization in organizations. Whenever an authorization request is made, the PDP delivers one of four possible decisions (permit, deny, not applicable or indeterminate). An important advantage arises when using the RBAC profile for XACML [32]. Without any adjustments to XACML, this profile enables to model the relationship between roles and permissions as they are typically found in IT systems.
The XACML core concepts and relations used within the scope of this paper are specified in [12] but can be briefly described as follows:

- A rule refers to a target (i.e. actions, resources and subjects) and evaluates a condition (an expression) to an effect (permit or deny)
- A policy contains multiple rules and combines their effects to its decision.
- A policy set contains multiple policies and combines their decisions to its own. It may also include policies from other policy sets.

The features supported by the standardized XACML render the development of a proprietary format for the exchange between monitored systems and monitoring systems obsolete. There is also an XML Schema Definition (XSD) available for XACML.

3.3. Internal Control Model

While formally defined and standardized models for business processes and access control exist, corresponding models for internal control do – for the best of our knowledge – not. For this reason, the core concepts and relations of the established COSO model required within the scope of this paper were formally defined by an XSD. They are specified in [2] but can be concisely described as follows:

- Organizations set and pursue objectives. Their achievement can be endangered by risks.
- The organizations risk management identifies risks, prepares risk assessments and develops risk responses.

DOI: 10.1109/HICSS.2010.262

- Risk responses are incorporated into business processes by means of control activities.

To allow for the automatic detection of control exceptions, this paper additionally provides for the enhancement of control activities by formal definitions of control exceptions using a rule definition language. This internal control model does not impose any restrictions with respect to the concrete rule language except that it should support an XML representation, e.g. like RuleML. The rule language is used to describe which combinations of critical permission sets (and optionally other entities whose inclusion is beyond the scope of this paper) imply a control exception. Permissions are linked to XACML targets, in particular to actions (e.g. register) and resources (e.g. documents or transactions), by means of extended attributes. The use of a rule language renders the monitoring of segregation of duties controls easy and therefore countervails a weakness of XACML.

In the following, the developed formal definition of the internal control model is referred to as the Extensible Business Risk Description Language (XBRDL). It is presented as one possible internal control model. However, it bases upon the established COSO model and facilitates the formal definition of control exceptions.

3.4. Integrated Model

The integration of the defined internal control model (XBRDL) and the relevant parts of the adopted models (XACML, XPDL and e.g. RuleML) for the creation of the proposed model is illustrated in Figure 2. XPDL processes contain activities (e.g. post document) and participants (e.g. roles). These may possess extended attributes just like XBRDL permissions which are used to link XPDL participants to XACML (role) policy sets and XPDL activities to XBRDL control sets and permission sets. This approach enables the use of existing business process modeling tools, e.g. TIBCO Business Studio [33]. The proposed model is presented as one possible solution for the problem domain. However, it excels at the seamless integration and efficient reutilization of existing and prevalent models and thereby enables the use of existing components and tools.

4. Proposed Architecture

In order to minimize possible dependencies between components and to maximize their exchangeability and reusability, a Service Oriented Architecture (SOA) [34] is proposed for implementations of the proposed model. Its individual components as well as their interfaces are illustrated in Figure 3 and are concisely described in the following subsections.

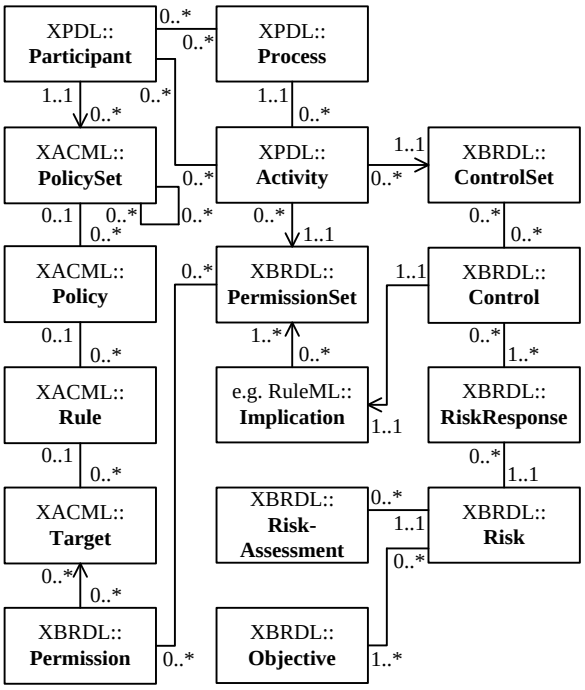

Figure 2: Overview of the proposed model as a UML class diagram. The defined internal control model (XBRDL) and the relevant parts of the adopted business process model (XPDL), access control model (XACML) and rule model (e.g. RuleML) are integrated with each other.

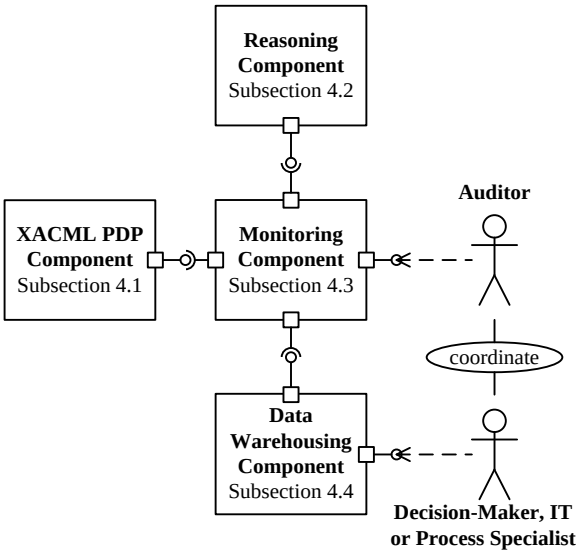

Figure 3: Overview of the proposed Service Oriented Architecture as a combined UML component and use case diagram

DOI: 10.1109/HICSS.2010.262

4.1. XACML PDP Component

The XACML PDP component evaluates which persons possess which permissions. It accepts incoming XACML requests, processes a repository of XACML (role and permission) policy sets and returns thereby evaluated decisions. Its repository may consist of policy sets concerning a single system or multiple systems and may refer to single or multiple system levels, e.g. operation system level, database level and / or application level. These policy sets may originate from the transformation of data from systems using proprietary access control models or represent data from systems with native XACML support. In the latter case, the productive XACML PDP may be used.

4.2. Reasoning Component

The reasoning component evaluates which persons infringe which controls. It accepts incoming XML encoded assertions and queries. With respect to queries, it returns the inferred results. The reasoner may be based on any suitable kind of logic, e.g. predicate logic or deontic logic. It may natively use a human readable logic programming language, e.g. Prolog [35], and translate between XML and this language, e.g. using Extensible Stylesheet Language Transformations (XSLT) [36], or natively use an XML based logic programming language. A distinct advantage which arises from the choice of a standardized language is the possibility to use existing tools.

4.3. Monitoring Component

The monitoring component detects control exceptions and publishes information to the data warehousing (DW) component. It accepts incoming XPDL business processes, XBRDL control and permission sets as well as XACML role (to user) assignment policy sets. The actions and resources linked to the XBRDL permission sets are combined with the subjects referred in the XACML role assignment policy sets and passed to the XACML PDP component. The latter evaluates these requests and returns corresponding decisions. These decisions as well as the definitions of control exceptions linked to the XBRDL control sets are passed to the reasoning component. Based on the corresponding assertions, the reasoning component infers and returns existing control exceptions. Finally, these control exceptions are published together with the original XPDL and XBRDL information to the DW component. The monitoring component may be configured by auditors.

4.4. Data Warehousing Component

The DW component is used for deep analyses and meaningful reports. It accepts data from the monitoring component and optionally other sources and provides this data in a consistent multidimensional model to analysis and reporting tools. Decision-makers use high level reports and encounter control exceptions with corresponding measures, while IT specialists and process specialists exploit available drill-down functionalities in order to identify their cause.

5. Prototype Implementation

In order to increase the degree of confirmation with respect to the feasibility and suitability of the proposed model and architecture, a prototype implementation in a SAP environment has been developed. Figure 4 contains an overview of the implemented prototype and the following subsections detail on its individual components.

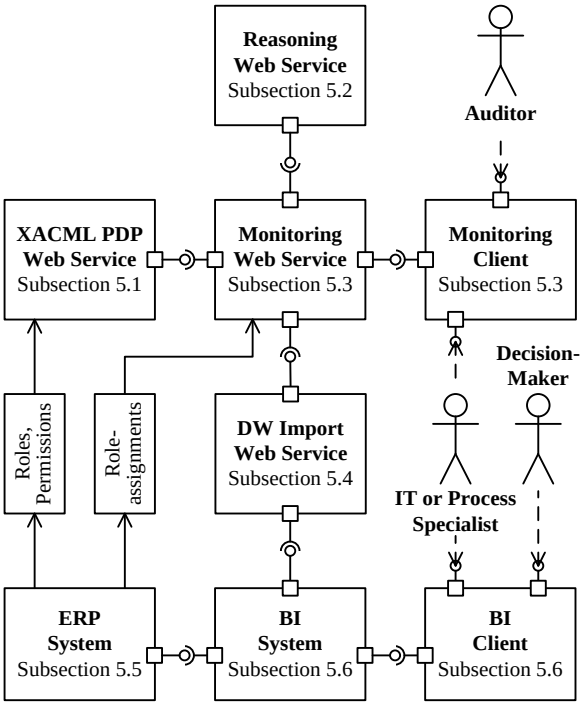

Figure 4: Overview of the implemented prototype as a combined UML component and use case diagram

5.1. XACML PDP Web Service

There are different XACML PDP implementations, each with different technical implementation details,

DOI: 10.1109/HICSS.2010.262

conformity and performance levels [37]. The prototype employs the implementation from SUN (SUNXACML) [38], because it offers a high level of conformity and its performance shortcomings [39] are of no significance to the following case study. Furthermore, it's comprehensive documentation and open source license has rendered the development of an encapsulating web service easy.

5.2. Reasoning Web Service

Several industry standards for the definition of rules exist. The Rule Markup Initiative [40] develops RuleML to increase the interoperability between these standards and thereby the corresponding rule engines. RuleML is formally defined by several XSDs and can be translated to other rule language, e.g. to JESS [41], using XSLT. Furthermore, it represents an integral part of the Semantic Web Rule Language (SWRL) [42]. The reasoning web service encapsulates OO jDREW [43], an open source reasoning engine with native support for RuleML.

5.3. Monitoring Web Service and Client

As the proposed model solely consists of formally defined sub-models, it was easily possible to generate a model implementation based on the corresponding XSDs using Model Driven Architecture (MDA) [44] tools. The monitoring web service uses this implementation to parse XACML, XBRDL as well as XPDL documents. Subsequently, it invokes the XACML PDP and the reasoning web service in order to detect control exceptions. Moreover, it performs an object-relational mapping for the entire model, creates an archive file containing corresponding flat files, and passes this file to the DW import web service.
The monitoring web service may be invoked regularly, e.g. on a daily basis, and / or after changes. Relevant changes are, amongst others:

- an application developer changes the permissions required for an activity,
- a role administrator changes the permissions contained in a role,
- a user administrator changes the assignment of users and roles,
- a business process developer changes the participant associated with an activity or the role associated with a participant or
- an internal control auditor changes a control.

Provided that these changes are not immediately effective but consecutively transported through the stages of a multistage system concept (e.g. with separate test, quality and productive systems), control exceptions can already be detected before-the-fact. Therefore, problematic changes (e.g. caused by process optimization) can be prevented before they affect the productive system and thereby business objectives.
The monitoring client is used to configure and invoke the monitoring web service. It outputs a brief report regarding detected control exceptions. However, the business intelligence system is used for deep analyses and meaningful reports.

5.4. Data Warehousing Import Web Service

The DW import web service uncouples the monitoring web service from a particular BI system. In addition, it unpacks the received archive file to the right destination and optionally schedules a dedicated extraction, transformation and loading (ETL) process chain.

5.5. Enterprise Resource Planning System

The XACML role and permission policy sets used by the XACML web service and the XACML role assignment policy sets used by the monitoring web service originate from the access control data of a SAP ERP system. As SAP ERP is a leading business application and possesses a very sophisticated access control model, it is well suited for the following case study.

5.6. Business Intelligence System and Client

SAP ERP and the DW import web service are the data suppliers for a SAP BI system. Based on a history of snapshots, the SAP BI enables to analyze internal control under temporal aspects. Moreover, it is well suited for the provision of internal control information in a coherent way with other characteristics and facts to analysis and reporting tools. In particular, decision-makers, IT and process specialists may use the analysis and reporting clients of the SAP Business Explorer.

6. Case Study

The case study has been conducted for a subset financial process of an organization. This process is subject to compliance requirements and continuously supported by a SAP ERP system. The system is a multitenant system with over 1,200 users and is operated by the organization for about nine years. Figure 5 illustrates the activities performed for the case study from the description of the process to the creation of a report containing the detected control exceptions. These activities are detailed in the following subsections.

DOI: 10.1109/HICSS.2010.262

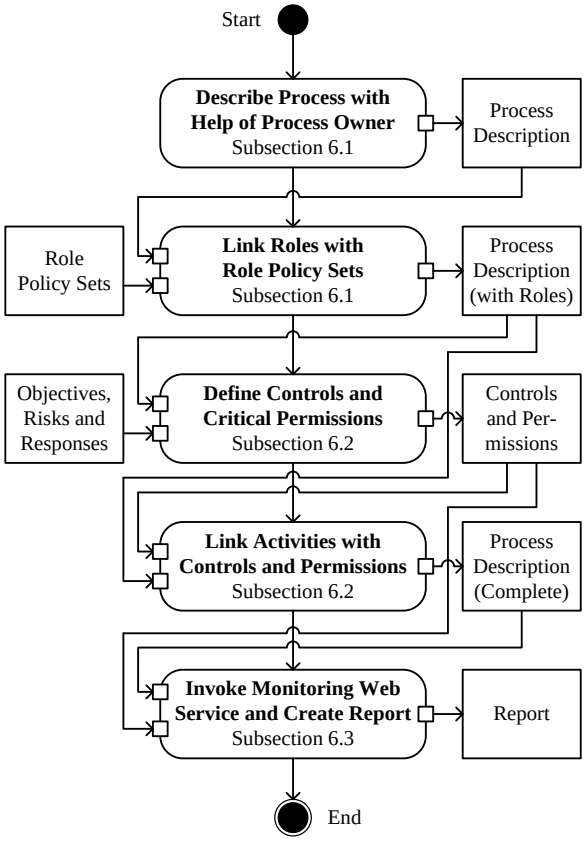

Figure 5: Overview of the conducted case study as a UML activity diagram.

6.1. Process Description

In order to ensure information value, two requirements have been defined for the selection of a process for the case study: the process must contain (i) several participants and (ii) differentiated authorization assignments.
In cooperation with the financials process owner of the organization, the "Documents and Payments" process has been selected and illustrated as in Figure 7. The process covers the registration and posting of documents as well as the preparation, review and execution of corresponding payment proposals. These activities correspond to transaction calls in the SAP ERP system. The use of a transaction requires certain permissions. These permissions are bundled up in roles and assigned to the different process participants in SAP ERP. Additionally, the role names are linked to the participants in the BPMN process description using standard modeling tools by means of XPDL extended attributes.
In this process, a compliance requirement which needs differentiated authorization assignments is to ensure segregation of duties. Some authorizations / roles must not overlap, e.g. a "Secretary of Department" may only register a document but is not allowed to post it.

6.2. Control Definition

Internal control is defined using XBRDL, e.g. the aforementioned segregation of duties control may be represented as illustrated in Figure 6.

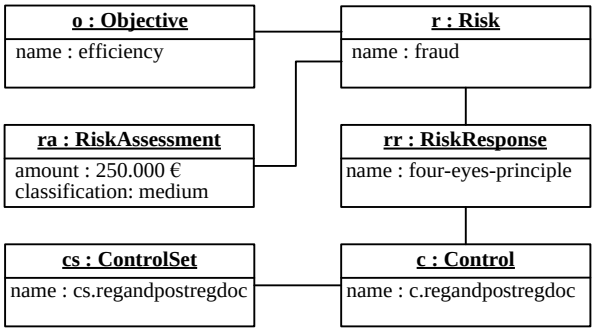

Figure 6: Example XBRDL control as a UML object diagram

This control is linked to a formal definition of a control exception in RuleML. RuleML can be transformed from and to the Positional-Slotted Language (POSL) [45], which is easier to read for humans. The rule may be represented by the following POSL fragment:

```
subject_infringes_c (?S c.regandpostregdoc) :-
  subject_has_ps (?S, ps.registerdoc),
  subject_has_ps (?S, ps.postregistereddoc).
```

The control (c.`regandpostregdoc`) is infringed by each person (`S`) which has both the permissions to register a document (ps.`registerdoc`) and the permissions to post a registered document (ps.`postregistereddoc`). These critical permission sets are defined using XBRDL as well and linked to corresponding XACML targets. E.g. the permission to register a document may be represented by a XACML target with the action "register" and the resource "FV60". Subsequently, process activities are linked to the names of controls and critical permissions using standard modeling tools by means of XPDL extended attributes.
While the definition of controls is a core competence of auditors, the definition of therein referred critical permissions may also be performed by IT specialists, in particular application developers.

6.3. Monitoring and Reporting

The monitoring web service combines the action values (e.g. "register") and resource values (e.g. "FV60") from the critical permissions with the subject values (e.g. a person "Copper, J." with a role "secretaryofdepartment") from the XACML role assignment policy sets and invokes the XACML PDP web service with respective XACML requests.

DOI: 10.1109/HICSS.2010.262

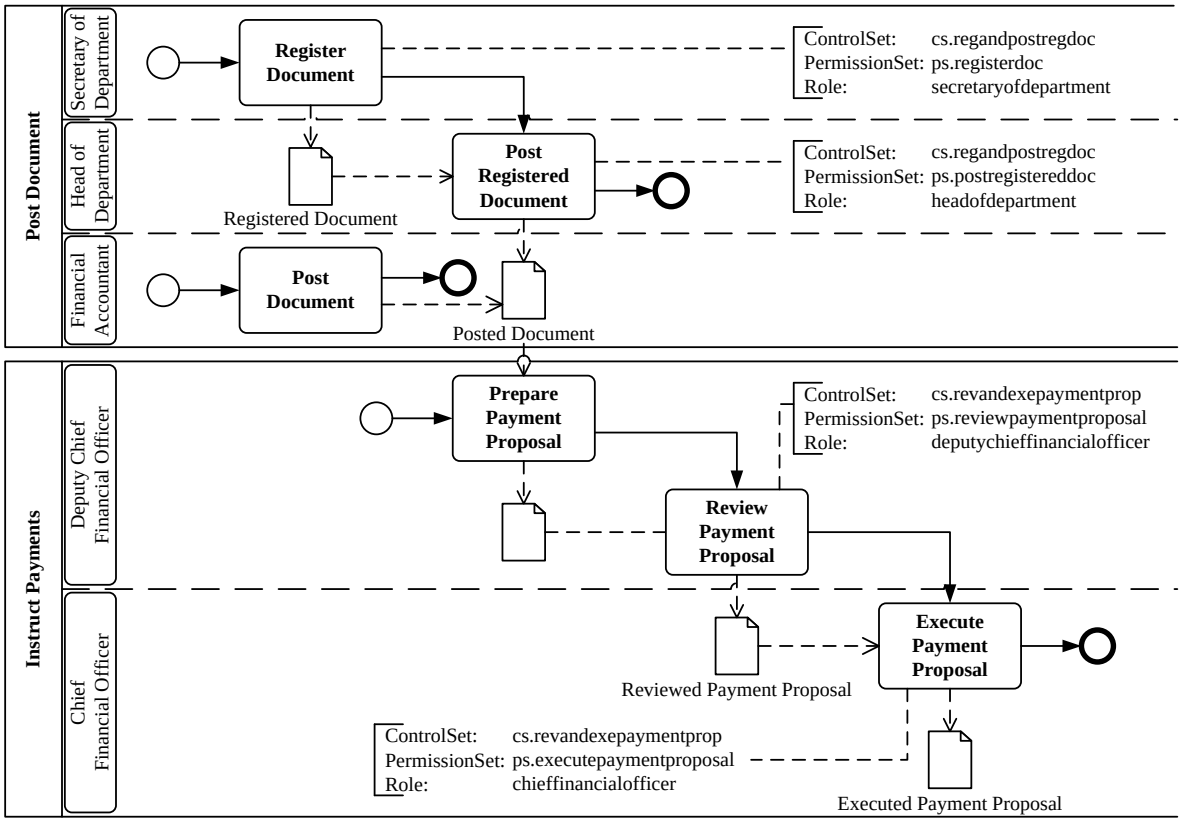

Figure 7: Example process in Business Process Modeling Notation

Based on the corresponding decisions, the monitoring web service passes assertions like the following to the reasoning web service:

```
subject_has_ps ('Cooper, J.', ps.registerdoc).
```

The rules contained in the controls are passed to the reasoning web service likewise. The reasoning web service therefore has the required information to infer answers for the query:

```
subject_infringes_c(?S, c.regandpostregdoc).
```

These answers are combined with the other information and passed to the DW import web service. The latter coordinates their import into SAP BI.
Figure 8 contains a screenshot of SAP Business Explorer Analyzer showing some example queries regarding processes, internal control, control exceptions and permissions. The presentation in a BI tool enables process owners to work with internal control reports within their familiar analysis environment. This has potential to increases the acceptance and usage rate. Furthermore, process owners are now independently and timely in the position to recognize control exceptions within their area of responsibility. In contrast to periodical audits made by varying consultants, BI reports deliver homogeneous information tailored to individual requirements for people with different backgrounds at any time. Furthermore, data histories enable process owners to analyze the status of their business processes under temporal aspects. This enables an easy monitoring of internal control, e.g. controls related to objectives set by the organizations business strategy.

7. Conclusion

Although the importance of risk management and the monitoring of business processes and internal control in organizations lately get recognized and high awareness is attached, the implementation of corresponding approaches remains difficult. These difficulties are addressed by a Design Science Research approach.
A model for the enrichment of business processes with internal controls, user roles and permissions is presented. Additionally, an architecture for the automated monitoring of internal controls and the timely communication and deep analysis of thereby detected control exceptions using business intelligence (BI) is proposed.

DOI: 10.1109/HICSS.2010.262

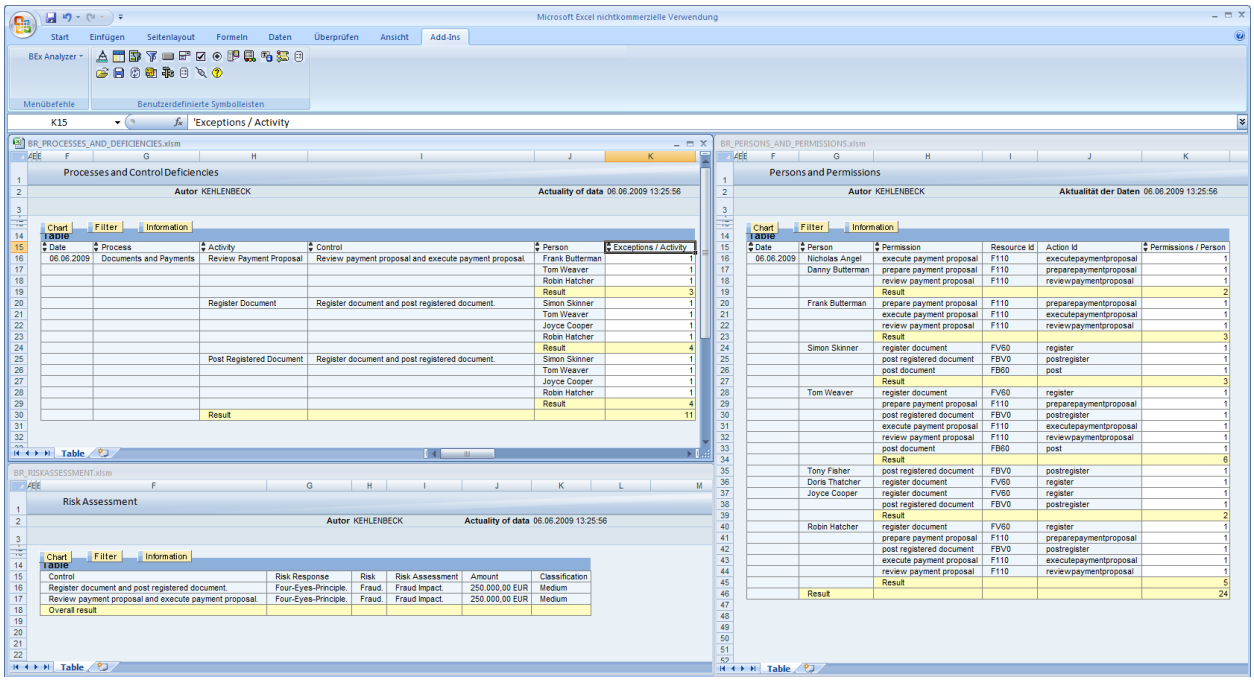

Figure 8: Example queries regarding business processes, internal control, control exceptions and permissions created using the implemented prototype and the SAP Business Explorer Analyzer.

The major advantage of this approach is the combination of a widely understandable business process notation (BPMN) with an established internal control model (COSO), an XML based rule language (e.g. RuleML) and a platform independent access control policy standard (XACML). The adherence to this standard models and technologies enables the reuse of existing components and tools. Furthermore, the use of BI offers merits for participants with different professions on multiple organizational levels. Amongst others, the easy access to information facilitates the individual development of competencies and problem awareness. Therefore, the approach does not only meet particular (short term) information needs which are considered important at the launch of corresponding projects (e.g. by sponsors from the top management), but thoroughly meet the needs of many participants in the long term. Consequently, both strategic and operational information needs can be adequately addressed likewise. This appropriately integrates risk management into the decision-making process and thereby contributes to the improvement of security, the mitigation of risks and the achievement of business objectives.

To increase the degree of confirmation with respect to the feasibility and suitability of the proposed model and architecture, a prototype with a Service Oriented Architecture (SOA) has been implemented in a SAP ERP and BI environment using model-driven architecture (MDA) principles. This prototype has been used in a comprehensive case study to outline the benefits of this approach.

Future research will be dedicated to the evaluation of the prototype with real-life workloads. The performance of the individual components will be measured in order to identify potential bottlenecks. Furthermore, the prototype is currently extended with automated transformations from proprietary access control models to XACML.

References

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management - Integrated Framework, Executive Summary, 2004, http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

[2] Committee of Sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management - Integrated Framework, 2004, http://www.coso.org/guidance.htm

[3] Committee of Sponsoring Organizations of the Treadway Commission (COSO): Guidance on Monitoring Internal Control Systems, 2009, http://www.coso.org/guidance.htm

[4] J. Bace, C. Rozwell, "Understanding the Components of Compliance", Gartner Report: G00137902, 2006.

[5] R. Agrawal, C. Johnson, J. Kiernan, F. Leymann, "Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology", Proceedings of the 22nd

DOI: 10.1109/HICSS.2010.262

International Conference on Data Engineering, IEEE, Washington, 2006, pp. 92-102.
[6] S. Sadiq, G. Governatori, K. Namiri, "Modeling Control Objectives for Business Process Compliance", Business Process Management, Springer, Berlin, 2007, pp. 149-164.
[7] A. Awad, G. Decker, M. Weske, „Efficient Compliance Checking Using BPMN-Q", Business Process Management, Springer, Berlin, 2008, pp. 326-341.
[8] J. Liebenau, P. Kärrberg, "International Perspectives on Information Security Practices", London School of Economics and Political Science, McAfee, 2006.
[9] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research", MIS Quaterly, vol. 28, no. 1, 2004, pp. 75-105.
[10] Object Management Group (OMG): Business Process Modeling Notation (BPMN), http://www.bpmn.org/
[11] Workflow Management Coalition (WfMC): XML Process Definition Language (XPDL), http:// www.wfmc.org/xpdl.html
[12] Organization for the Advancement of Structured Information Standards (OASIS): eXtensible Access Control Markup Language (XACML), http://www.oasis-open.org/ committees/xacml/
[13] Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control - Integrated Framework (1992), http://www.coso.org/guidance.htm
[14] World Wide Web Consortium (W3C): Extensible Markup Language (XML), http://www.w3.org/XML/
[15] The Rule Markup Initiative: Rule Markup Language (RuleML), http://ruleml.org
[16] SAP AG: SAP ERP 6.0, http://www.sap.com/ germany/solutions/businesssuite/erp/index.epx
[17] SAP AG: SAP NetWeaver Business Intelligence, http://www.sap.com/germany/plattform/netweaver/ components/businessintelligence/index.epx
[18] N. Damianou, N. Dulay, E. Lupu, M. Sloman, "The Ponder Policy Specification Language", Proceedings of the International Workshop on Policies for Distributed Systems and Networks, Springer, London, 2001, pp. 18-38.
[19] The Web Services Policy Framework (WS-Policy), www.w3.org/Submission/WS-Policy/
[20] PrivilEge and Role Management Infrastructure Standards Validation (PERMIS), www.permis.org
[21] M. Alam, R. Breu, M. Hafner, "Modeling permissions in a (u/x)ml world", In: ARES 2006. Proceedings of the First International Conference on Availability, Reliability and Security, Washington, DC, USA, IEEE Computer Society Press, Los Alamitos, 2006, pp. 685–692.
[22] M. Pistoia, S.J. Fink, R.J. Flynn, E. Yahav, "When Role Models Have Flaws", ICSE 2007 Proceedings, 2007, pp. 478-488.
[23] M. zur Muehlen, M. Rosemann, "Integrating Risks in Business Process", *ACIS 2005 Proceedings*, 2005.
[24] Object Management Group (OMG): Unified Modeling Language (UML), http://www.uml.org/
[25] C. Wolter, A. Schaad, C. Meinel, "Deriving XACML Policies from Business", Web Information Systems Engineering – WISE 2007 Workshops, Springer, Berlin, 2007, pp. 142-153.
[26] X. Wang, Y. Zhang, H. Shi, J. Yang, " BPEL4RBAC: An Authorisation Specification for WS-BPEL", Web Information Systems Engineering - WISE 2008, Springer, Berlin, 2008, pp. 381-395.
[27] D. Basin, J. Doser, T. Lodderstedt, "Model Driven Security for Process-Oriented Systems", In SACMAT '03: Proceedings of the eighth ACM Symposium on Access Control Models and Technologies, ACM, NY, 2003, pp. 100–109.
[28] J. Jürjens, "UMLsec: Extending UML for Secure Systems Development", In UML '02: Proceedings of the 5th International Conference on The Unified Modeling Language, Springer, London, 2002, pp. 412–425.
[29] S. Höhn, J. Jürjens, "Rubacon: automated support for model-based compliance engineering", Proceedings of the 30th international conference on Software engineering, ACM, NY, 2008, pp. 875-878.
[30] Organization for the Advancement of Structured Information Standards (OASIS): Web Services Business Process Execution Language (WSBPEL), www.oasis-open.org/ committees/wsbpel/
[31] World Wide Web Consortium (W3C): XML Schema, http://www.w3.org/XML/Schema
[32] Core and hierarchical role based access control (RBAC) profile of XACML v2.0, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf, 02.2005.
[33] TIBCO Software Inc.: TIBCO Business Studio, http://developer.tibco.com/business_studio/
[34] Organization for the Advancement of Structured Information Standards (OASIS): SOA Reference Model, http://www.oasis-open.org/committees/soa-rm/
[35] International Organization for Standardization (ISO): ISO/IEC 13211-1:1995, http://www.iso.org/iso/ catalogue_detail.htm?csnumber=21413
[36] World Wide Web Consortium (W3C): XSL Transformations, http://www.w3.org/TR/xslt
[37] P.G. Scaglioso, C. Basile, A. Lioy, "Modern Standard-based Access Control in Network Services: XACML in action", IJCSNS International Journal of Computer Science and Network Security Vol. 8 No. 12, 2008, pp. 296-305.
[38] Sun's XACML implementation, Version 1.2, http://sourceforge.net/projects/sunxacml, 2004.
[39] N. Li, J. Hwang, T. Xie, "Multiple-implementation testing for XACML implementations", Proceedings of the 2008 workshop on Testing, analysis, and verification of web services and applications, ACM, NY, 2008, pp. 27-33.
[40] The Rule Markup Initiative, http://ruleml.org
[41] Sandia National Laboratories, Jess, the Rule Engine for the Java Platform, http://www.jessrules.com/
[42] World Wide Web Consortium (W3C): SWRL: A Semantic Web Rule Language Combining OWL and RuleML, http://www.w3.org/Submission/SWRL/
[43] M. Ball, B. Craig: Object Oriented jDREW, http://www.jdrew.org/oojdrew/
[44] Object Management Group (OMG): Model Driven Architecture, http://www.omg.org/mda/
[45] H. Boley, "POSL: An Integrated Positional-Slotted Language for Semantic Web Knowledge", http:// ruleml.org/submission/ruleml-shortation.html

DOI: 10.1109/HICSS.2010.262

AN IMPLEMENTATION OF A PROCESS-ORIENTED CROSS-SYSTEM COMPLIANCE MONITORING APPROACH IN A SAP ERP AND BI ENVIRONMENT

Sandner, Thorben, Leibniz Universität Hannover, Institut für Wirtschaftsinformatik, Königsworther Platz 1, 30167 Hannover, Germany, sandner@iwi.uni-hannover.de

Kehlenbeck, Matthias, Leibniz Universität Hannover, Institut für Wirtschaftsinformatik, Königsworther Platz 1, 30167 Hannover, Germany, kehlenbeck@iwi.uni-hannover.de

Breitner, Michael H., Leibniz Universität Hannover, Institut für Wirtschaftsinformatik, Königsworther Platz 1, 30167 Hannover, Germany, breitner@iwi.uni-hannover.de

Abstract

Compliance to regulatory demands has become a crucial matter for organizations. Non-observance may lead to far-reaching consequences, e.g. damage to reputation, decline of credit rating or market value, fraud and fines. The success of compliance management correlates with the frequency of monitoring and reporting and is affected by complex and often time-consuming manual validation tasks. To address this problem, organizations implement corresponding IT solutions. However, the often heterogeneous system landscapes, the different information sources and their integration represent major challenges.

This paper presents an implementation of a novel process-oriented and cross-system compliance monitoring approach. The approach is based on a model which provides for the annotation of business processes with internal controls, critical permissions and roles as well as an architecture which provides for the automatic detection, timely communication and deep analysis of control exceptions. It solely relies on established standards (i.e. XACML, BPMN, COSO and SWRL) and existing technologies. The implementation has been deployed in a productive SAP ERP and BI environment. It automatically converts access control data from the proprietary SAP model and publishes control exceptions to the BI system. The effects and causes of these control exception can be appropriately analyzed using BI queries and reports.

Keywords: IT compliance, IT risk management, IS security, business process management, SAP R/3

1 INTRODUCTION

Triggered by a set of enterprise scandals as for example Enron or WorldCom, the compliance standards considerably raised during the last years. Many additional regulations such as Sarbanes-Oxley Act (SOX) or EuroSOX were released to ensure the reasonable acting of organizations. The implementation of these regulations is often a prerequisite for organizations to continue their work. The resulting investment cost required to introduce and operate corresponding measures is estimated in the U.S. as 32 billion U.S. dollars for the year 2008 (McGreevy et al. 2008).

Compliance management can be defined as the use of frameworks, standards and software to ensure compliance with legal requirements (Kharbili et al. 2008). Compliance may be achieved by embedding control activities into business processes and supporting systems. However, dynamic environments frequently require changes to processes and systems. The maintenance and monitoring of controls is a complex, time-consuming and often manual task (Bace et al. 2006), (Agrawal et al. 2006). As compliance management depends on the frequency of monitoring and reporting, the timely communication of control exceptions is an important success factor (Liebenau et al. 2006). Further factors are central approaches, proactive responses and automated processes (Chatterjee et al. 2008).

The present paper focuses on the use of software to ensure compliance. This software forms the technical infrastructure for the realization and traceability of compliance management. In most Information Systems (IS) publications to this subject, the research focus rather lies on exploratory problem-indentifying instead of developing concrete solutions (Syed et al. 2009). It is also criticized that the solutions to compliance issues are often implemented in isolation and do not adequately address the need for information from different data sources as well as the need for analytic data (Gericke et al. 2009). Although some systems provide strong internal control features, heterogeneous system landscapes render an integrated monitoring and reporting very difficult.

Echoing these criticisms, the present paper describes a prototypical implementation in a productive SAP environment. The prototype enables the automated and central monitoring of controls distributed over multiple heterogeneous systems. Compliance information is integrated into a central repository and forms the basis for the creation of homogeneous analyses and reports. This may prevent the definition of redundant controls and bundle competencies. Noncompliance situations may be avoided by analyzing the impact of changes to processes, permissions and roles on internal control before these changes become productive. The prototype relies on a Service-Oriented Architecture (SOA) and uses a Business Intelligence (BI) system for analysis. It is based on a model which provides for the annotation of business processes with internal controls, critical permissions and roles as well as an architecture which provides for the automatic detection, timely communication and deep analysis of control exceptions. Both are based on existing standards and technologies. Processes are described using the Business Process Modeling Notation (BPMN) (OMG 2009a) in combination with the XML Process Definition Language (XPDL) (WfMC 2009). Access control information is specified using the Extensible Access Control Markup Language (XACML) (OASIS 2009). Internal control is described following the established Internal Control – Integrated Framework (COSO 1992) respectively Enterprise Risk Management – Integrated Framework (COSO) (COSO 2004) and control exceptions are formally defined using the Semantic Web Rule Language (SWRL) (W3C 2004). Furthermore, access control information is automatically transformed from the proprietary SAP model to XACML. Other relevant information (e.g. customizations and parameters) can be transformed to OWL.

In the IS Research, there are two fundamental types of approaches: (1) the behavioral and (2) the design science research (DSR) approach (Hevner et al. 2004). Here, the DSR approach is selected. It focuses on the heuristic search for new and innovative artifacts. Artifacts consist of constructs, models, and methods and are converted to problem-related instances (March et al. 1995). In this paper, a situational adjustment of a generic artifact (to an SAP ERP and BI environment) is made and the usefulness of this developed artifact is evaluated using dynamic and architecture analysis.

The remainder of the paper is structured as follows. Section 2 gives an overview about the related work. In section 3 a model, architecture and implementation of a control monitoring system is presented. The transformation process from the monitored systems to the monitoring system is described in section 4. Section 5 contains an evaluation of the monitoring system. We conclude with a discussion about future work in section 6.

2 RELATED WORK

The increasing process orientation in consideration of business perspectives and security requirements let several works, e.g. Wolter et al. (2007), Wang et al. (2008), Basin et al. (2003) and Jürjens (2002), examine the implications of Unified Modeling Language (UML) (OMG 2009b) models or BPMN models in conjunction with security policies. However, they have different focuses and do not detail on control monitoring. Höhn and Jürjens (2008) deal with the analysis of UML models of business applications and corresponding configuration data in terms of their relevance for security policies and compliance requirements. Thematically closer are Wolter et al. (2007), that describe a mapping between BPMN and XACML meta-models for the automated derivation of authorization constraints, specifically an XSL Transformation (XSLT) (W3C 1999) that converts security constraints into XACML policies. However, the present approach contains a transformation between different access control models, not between a process and an access control model.

Pistoia et al. (2007) and Sadiq et al. (2007) discuss some other aspects of the topic. Pistoia et al. (2007) focus on the static policy validation for a Role Based Access Control (RBAC) model. However, the present approach uses XACML which allows the use of other access control models than RBAC. Additionally, not only a static analysis is possible but also a runtime analysis of policies. Sadiq et al. (2007) concentrate on a language for the representation of control objectives and annotate business processes with corresponding control tags. However, the present approach includes an access control model, uses a standard rule language and resembles the COSO model more closely.

Other approaches that have different intentions but are related to the employed technologies are Ferrini and Bertino (2009) as well as Kolovski et al. (2007). Ferrini and Bertino (2009) extend XACML with a framework that integrates OWL ontologies and XACML policies to support static and dynamic segregation of duties. Like the present approach, they combine XACML with OWL. However their main focus lays on the improvement of RBAC. Kolovski et al. (2007) have developed a description logic based analysis service for XACML policies. They combine XACML and description logic along with the reasoner Pellet (Clark and Parsia 2009) for verifying properties of XACML policies.

Kehlenbeck et al. (2010) describe an approach for the annotation of business processes with controls, permissions and roles based on BPMN, COSO and XACML. Additionally, they propose an architecture for the automated monitoring of controls and the timely communication of thereby detected control exceptions. The present approach adopts their model and architecture, supplements it with a conversion web service which automatically transforms access control data from the proprietary SAP model to XACML, implements this supplemented approach in a productive ERP and BI environment and evaluates this implementation.

3 MODEL, ARCHITECTURE AND IMPLEMENTATION

3.1 Model

Clearly structured business processes help organizations to achieve their goals. Many controls contained in these processes can be supported by IT systems. In particular, authorization and segregation of duties controls can be mapped to systems by means of their access control functions. This abets transparency and traceability. The present approach adopts the model developed by Kehlenbeck et al. (2010). It is illustrated in Figure 1 and concisely described in the following subsections.

3.1.1 Process Model

The design and implementation of business processes requires the participation of numerous people with different backgrounds. The process owner often possesses extensive knowledge regarding his processes but frequently needs help with their alignment to regulatory requirements (e.g. SOX and EuroSOX) and the design and implementation of corresponding controls. Moreover, IT specialists have to map a substantial part of these controls to supporting IT systems. To facilitate efficient communication between these participants, the BPMN has been developed. BPMN may be exchange using XPDL, which is formally defined by an XML Schema Definition (XSD) (W3C 2008b).

3.1.2 Access Control Model

A variety of heterogeneous distributed systems exist in organizations. Consequently, there are efforts to centralize the administration and enforcement of access control (e.g. Damianou et al. 2001, W3C 2006 and PERMIS 2003). To tackle this problem, the Organization for the Advancement of Structured Information Standards (OASIS) offers XACML, a platform independent access control standard. It provides for a Policy Decision Point (PDP), which is a processing engine that makes authorization policies interpretable and delivers decisions about acceptance or rejection. A further interesting aspect arises by using the RBAC profile for XACML (OASIS 2005), which makes it possible to map the relationships between roles and permissions as they are typically contained in supporting IT systems. XACML is formally defined by several XSDs. Its comprehensive function range let it appear suitable for the exchange between monitored systems and monitoring systems.

3.1.3 Internal Control Model

In contrast to business process models and access control models, formally defined and standardized internal control models do not exist. To close this gap, the established COSO model has been formally defined by an XSD. Additionally, this XSD provides for the definition of control exceptions by any XML based rule definition language. The present approach uses SWRL as this rule definition language. SWRL combines the Rule Markup Language (RuleML) (RuleML Initiative 2009) and OWL. It is supported by several editors (e.g. Protégé) and reasoners (e.g. Pellet). SWRL rules are used to describe, which combinations of critical permissions and optionally other information (e.g. customizing and parameters) imply which control exceptions. Permissions can be linked to XACML actions and resources. Actions, resources and subjects are parts of XACML targets. The formal definition of control exceptions (e.g. infringed segregation of duties) is a precondition for their automatic detection. The internal control and permission model is referred to as the Extensible Business Risk Description Language (XBRDL).

3.2 Architecture and Implementation

The described model has been prototypically implemented in a SAP ERP and BI environment. The implementation is based on a Service-Oriented Architecture (SOA) (OASIS 2009b). This architecture provides for the loose coupling of components and thereby increases flexibility and facilitates reutilization. It is a variation of the architecture developed by Kehlenbeck et al. (2010), illustrated in Figure 2 and concisely described in the following subsections.

3.2.1 XACML PDP Web Service

The PDP is the core component of an XACML engine. The PDP examines incoming requests, determines applicable policy sets and returns a corresponding decision. It thereby decides whether a person is permitted to perform an action on a resource or not. Policy sets may originate from one or more systems of the IT landscape and may refer to single or multiple system levels, e.g. operation system level, database level and / or application level. Systems may either natively use XACML or a

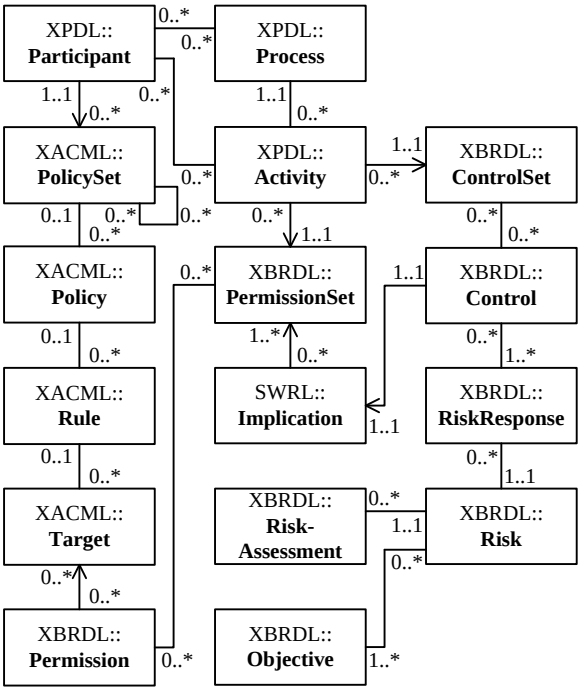

Figure 1. Used model as a UML diagram.

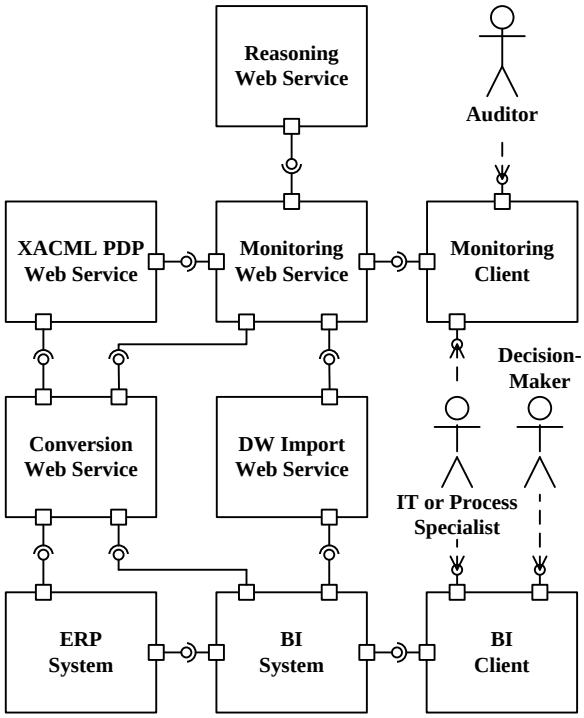

Figure 2. Used architecture as a UML diagram.

The diagrams are adopted from Kehlenbeck et al. (2010) except for the conversion web service.

proprietary access control model. The latter case requires a transformation from the proprietary model to XACML. Several implementations of XACML are available. They differ in licensing terms, technical maturity and performance (Scaglioso et al. 2008). The XACML PDP web service encapsulates the implementation by SUN (SUNXACML) (SUN 2004), as it offers a high level of conformity (Li et al. 2008), a comprehensive documentation and an open source license.

3.2.2 Reasoning Web Service

The reasoning web service accepts incoming OWL and SWRL assertions and builds up a corresponding knowledge base. Based on this knowledge base, it processes incoming SPARQL (W3C 2008a) queries and returns their result. In particular, it thereby evaluates which persons infringe which controls. The reasoning web service employs the Jena API (Jena 2009) in conjunction with Pellet.

3.2.3 Conversion Web Service

The conversion web service extracts access control and other information (i.e. customizations and parameters) from the SAP ERP and BI systems and transforms these to XACML permission policy sets, role policy sets and role assignment policies as well as OWL ontologies. SAP ERP and BI use the same proprietary access control model. The transformation is detailed in section 4.

3.2.4 Monitoring Web Service and Client

The monitoring web service accepts incoming XPDL business processes, XBRDL control and permission sets, XACML role assignment policy sets as well as OWL ontologies containing other information. As the model solely consists of formally defined sub models, it was easily possible to generate a model implementation based on the corresponding XSDs using Model Driven Architecture (MDA) (Ball and Craig 2008) tools. The actions and resources contained in the XBRDL permission sets are combined with the subjects contained in the XACML role assignment policy sets and passed to the XACML PDP web service. The latter evaluates these requests and returns corresponding

decisions. These decisions are converted to OWL and passed to the reasoning web service along with the received OWL ontologies and the SWRL rules contained in the XBRDL control sets. Based on this, the reasoning web service infers and returns existing control exceptions. Finally, these control exceptions are published together with the original XPDL and XBRDL information to the data warehousing (DW) web service. The monitoring web service may be configured and invoked using the monitoring client.

3.2.5 Data Warehousing Import Web Service

The information needs and their levels of granularity differ significantly for the involved participants. Decision-makers employ high level reports to survey the effects of control exceptions whereas IT and process specialists exploit drill-down functionalities to identify their specific causes. These requirements are met by the delivery of data to a corresponding warehouse and the subsequent use of business intelligence tools. The data warehousing import web services is used to uncouple this delivery from the monitoring web service to a particular business intelligence system.

3.2.6 Enterprise Resource Planning System

In order to test the prototype implementation in a meaningful and realistic environment, a commonly used business application has been selected, an Enterprise Resource Planning system. From the market of ERP vendors, a leading system, SAP ERP has been chosen. SAP ERP offers a very sophisticated access control model. Its transformation to XACML policies is therefore considered interesting.

3.2.7 Business Intelligence System and Client

Business Intelligence systems enable the performance of deep analyses and the production of meaningful reports. The provision of internal control information in a BI environment is considered suitable, as this allows its presentation in a coherent way with other characteristics and facts. Another inherent benefit of BI is the ability to analyze internal control under temporal aspects. The SAP BI system receives internal control data from the DW import web service and other data from the SAP ERP system. Decision-makers, IT and process specialists use the SAP Business Explorer as a client.
The interaction of the individual components from the invocation of the monitoring web service to the import into SAP BI is illustrated in Figure 3.

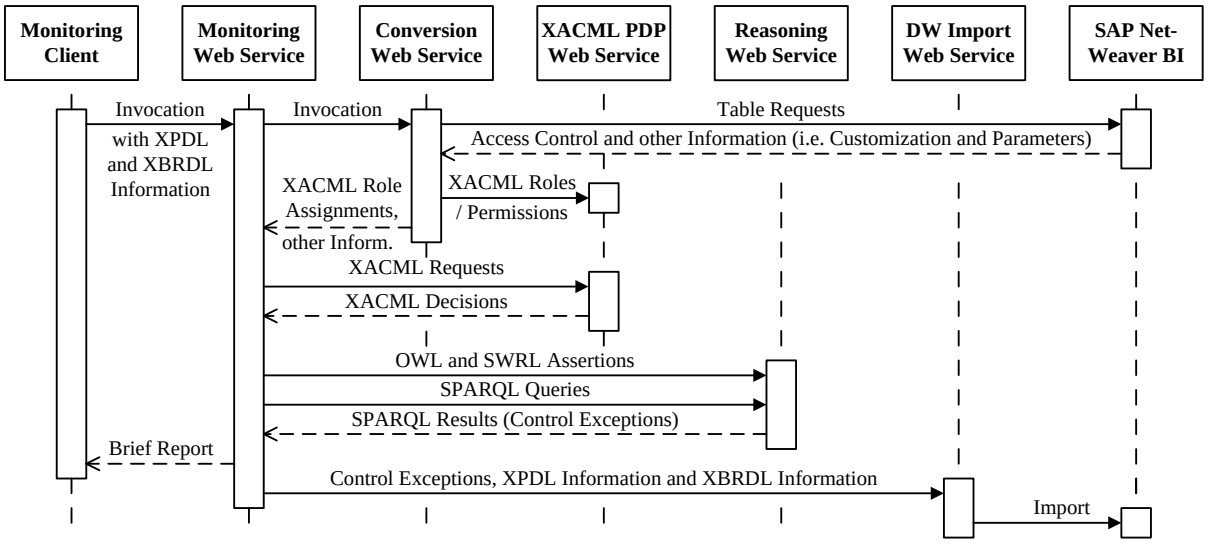

Figure 3. Interaction of the individual prototype components as a UML diagram. SAP BI and SAP ERP share the same access control model. The illustration therefore omits SAP ERP.

4 TRANSFORMATION

The developed conversion web service is able to extract access control data from SAP ERP and BI systems using (1) a SOAP connection to a corresponding web service, (2) a Java Database Connectivity (JDBC) connection to a database and / or (3) a folder of ALV files (a SAP internal XML format) which have been saved with the SAP GUI. At first, data is converted to an internal XML table format. ALV files are transformed to it using XSLT. The XML table format has been formally defined by an XSD. As the same XSD has been embedded into the Web Service Description Language (WSDL) file of the web service, extracted data can be directly marshalled to the XML table format using the Java Architecture for XML Binding (JAXB). The XSD has also been used to create a model implementation by means of the Eclipse Modelling Framework (EMF). This implementation is used to write data which has been extracted using JDBC to the XML table format and to read from data in the XML table format created by any of the three ways.

After the data has been converted to the internal XML table format, it is used to create (1) XACML role assignment policies, (2) XACML role and permission policy sets and (3) OWL ontologies. The role assignment policies and ontologies are sent to the monitoring, the role and permission policy sets to the XACML PDP web service. Figure 4 illustrates the activities performed by the conversion web service and its relation to other components, in particular the monitoring web service. The following subsections describe the SAP access control model and its transformation to XACML and OWL.

4.1 SAP Access Control Model

SAP access control is stored in a relational model and distinguishes between profiles and roles. Both profiles and roles are assigned to users and contain authorizations. Authorizations link permission objects with field values. However, profiles are used for access control enforcement, while roles are used for access control administration. When an administrator maintains a role, the SAP system automatically updates corresponding profiles. When these roles are assigned to users, these profiles are automatically assigned, too. In order to reduce overhead, only profiles are transformed to XACML policies. However, roles can be transformed to OWL ontologies. Figure 5 illustrates this model.

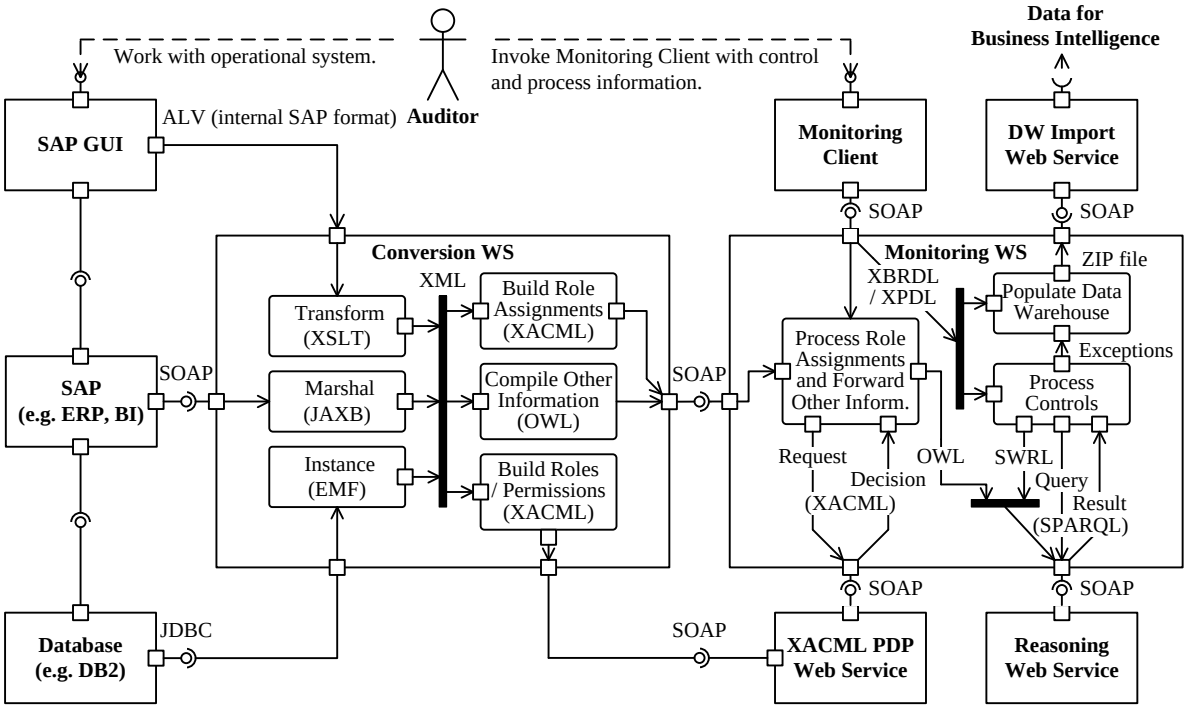

Figure 4. Conversion and monitoring web service as a UML diagram.

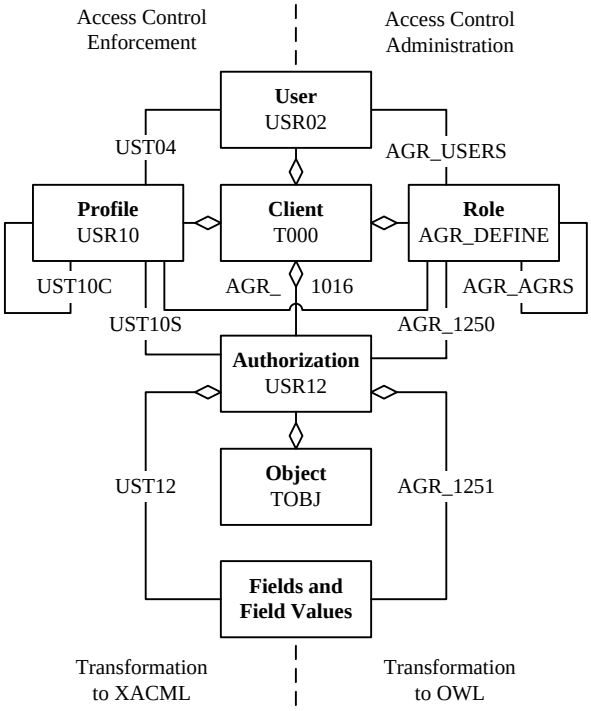

Figure 5. SAP access control model as a UML diagram.

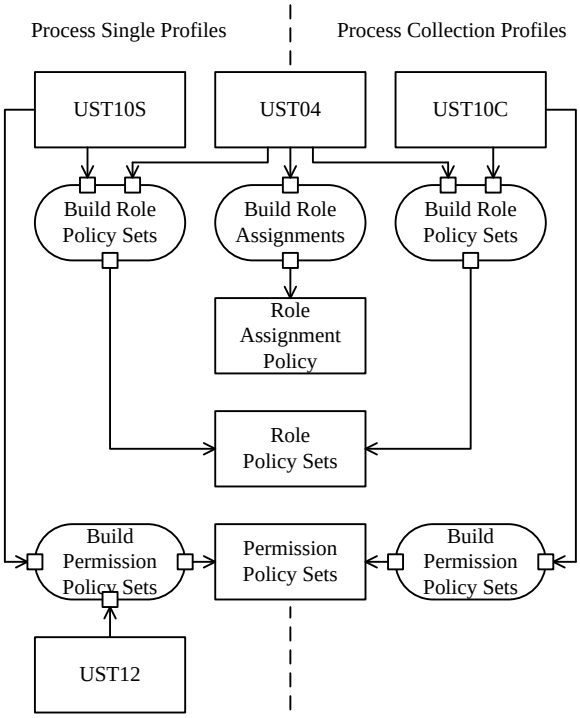

Figure. 6. Transformation from SAP to XACML as a UML diagram.

4.2 Transformation to XACML and OWL

The required information for the transformation of SAP profiles to XACML role assignment policies as well as XACML role and permission policy sets are contained in the tables UST04 (users and profiles), UST10C (collection profiles), UST10S (single profiles and authorizations) and USR12 (authorizations and field values). The transformation from SAP to XACML is illustrated in Figure 6 and consists of the following steps:

1. Table UST04 is converted to an XACML role assignment policy. SAP user names are mapped to XAMCL subjects and SAP profile names to XACML role policy set ids.
2. For each single profile in UST10S, a permission policy set is created. Mappings are as follows:
   a. SAP profile names are mapped to XACML policy and policy set ids,
   b. SAP authorization and object names are concatenated and mapped to XACML rule ids,
   c. SAP objects names are mapped to XACML resources and
   d. SAP field names and their values are concatenated and mapped to XACML actions.
3. For each collection profile in UST10C, an XACML permission policy set is created. The XACML permission policy sets corresponding to the contained profiles are included by reference.
4. For each profile in UST10S and UST04 or UST10C and UST04, an XACML role policy set is created. The corresponding XACML permission policy set is included by reference.

MANDT	PROFN	AKTPS	OBJCT	AUTH
700	T-P1281126	A	S_TCODE	T-P128112601

Table 1. A single profile in table UST10S.

MANDT	OBJCT	AUTH	AKTPS	FIELD	VON	BIS
700	S_TCODE	T-P128112601	A	TCD	F110	

Table 2. A field and field value in table UST12.

SAP field values support ranges and may contain wildcards. However, the numerous available XACML functions have made the mapping easy. Table 1 and Table 2 show a single profile and a field value in SAP, a corresponding XACML fragment is:

```
...
<Policy PolicyId="PP_T-P1281126"
 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
 <Target/>
 <Rule Effect="Permit" RuleId="S_TCODE_T-P128112601">
  <Target>
   <Resources>
    <Resource>
     <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
       DataType="http://www.w3.org/2001/XMLSchema#string">S_TCODE</AttributeValue>
      ...
     </ResourceMatch>
    </Resource>
   </Resources>
   <Actions>
    <Action>
     <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
       DataType="http://www.w3.org/2001/XMLSchema#string">TCD_F110</AttributeValue>
      ...
     </ActionMatch>
    </Action>
    ...
   </Actions>
  </Target>
 </Rule>
 ...
</Policy>
...
```

The SAP access control enforcement is also influenced by certain customizations and parameters. E.g. transaction codes listed in the system parameter "auth/tcodes_not_checked" are not checked at all. A transaction code is an object (S_TCODE). These issues have to be addressed in the SWRL rules. The conversion web service uses OWL to add corresponding information to the knowledge base of the reasoning web service. OWL may also be used to add information regarding SAP access control administration.

5 EVALUATION

The evaluation of the developed artifact depends on the requirements of the business environment and its corresponding technical infrastructure (Hevner et al. 2004). For the present artifact, appropriate steps are to perform an architecture analysis, which examines how well it fits into the technical infrastructure and a dynamic analysis, which addresses qualities such as performance (Hevner et al. 2004). Another key aspect is to verify the feasibility of the chosen approach.

The business environment used for the evaluation is a SAP ERP multitenant system with more than 1,200 users. It is productive for about nine years. To simplify the technical evaluation of the controls with reference to a concrete organization structure, the evaluation focuses on the biggest client with 586 users. This client uses the SAP modules for finance, human-resources, controlling and materials management and has some central and several decentralized structures, which make a differentiated authorization concept with multiple segregations of duties necessary. To map these requirements to the system, the client maintains 1,190 roles. In order to enforce these roles, the SAP system automatically updates 1,197 profiles in the background.

The integration of the artifact into the technical infrastructure can be divided into three different parts: (1) its incorporation into the existing system landscape, (2) its upstream connection to the monitored systems and (3) its downstream connection to the BI system. The architecture of the artifact made it easy to deploy it to an existing application server and establish connections to the SAP ERP and BI systems. The flexible web services facilitate extensibility and maintainability. Upstream connections to the monitored system were established using SOAP but would have also been possible using JDBC.

Characteristic	Number	Kilobyte
Role Policy Set to User Assignments (RPAs)	1,200	3,342
Role Policy Sets (RPS)	1,200[1]	1,165
Collection Permission Policy Sets (CPPS)	140	159
Single Permission Policy Sets (SPPS)	2,780	128,375

[1] 3 RPS for CPPS and 1197 RPS for SPPS

Characteristic	Average	Minimum	Maximum	Standard Deviance
Number of Users per RPA	4.30	1	586	23.41
Number of SPPS per CPPS	5.71	1	81	7.59
Number of Permissions per SPPS	12.75	1	170	23.46

Table 3 and 4. Information regarding the XACML created by the conversion web service.

Downstream connections were established using SOAP as well. Additional systems may be easily connected without significant adjustments to model or architecture.

Table 3 and 4 contain quantitative information regarding the role assignment policies, role policy sets and permissions policy sets created by the conversion web service. Particularly interesting is the number of users per role policy set assignment. There exists a basis profile which is assigned to all users. Furthermore, each profile is assigned to at least one user. Finally, the discrepancy between the average and the standard deviation may be explained by the very sophisticated access control concept. The majority of the users only possess the basis and a few other profiles for their specific area of work. However, a few key users with several profiles and three technical users with almost all profiles exist in the system. The latter are the only users that possess collection permission policy sets.

The export of access control data from the productive ERP system to equivalent XACML policies resulted in a large number of files. This large number entails two negative implications. First, the large number of files impairs the performance. This has already been described in a similar extent by Liu et al. (2008) as well as Turkmen and Crispo (2008). Most other available PDPs have a scaling problem, too. Second, the large number of files let a manual administration appear extremely time-consuming. However, both implications are rather unimportant for the present approach.

Business processes and controls have been defined in cooperation with the financials process owner. The generated policy sets and the control exceptions detected by the monitoring system have been verified against the source data from the monitored system by random checks.

As the approach is based on established standards and existing technologies, standard software such as TIBCO Business Studio (TIBCO 2009) may be used. This renders the development of individual software unnecessary and thereby increases cost effectiveness.

6 CONCLUSION

Although compliance standards considerably raised during the last years, most corresponding IS publications focus on exploratory problem-identifying instead of developing concrete solutions. Even the few developed solutions are often implemented in isolation and do not adequately address the need for information from different data sources as well as the need for analytic data. In order to meet the need for suitable solutions, a prototypical implementation of an innovative compliance monitoring approach in a productive SAP environment is presented. The prototype enables the automated, central and proactive monitoring of controls distributed over multiple heterogeneous systems. It is based on a model which provides for the annotation of BPMN business processes with COSO inspired internal controls, critical permissions and roles as well as an Service-Oriented Architecture which provides for the automatic detection, timely communication and deep analysis of control exceptions. Both are based on existing standards and technologies. Control exceptions are formally defined using the SWRL rule language. Permissions and roles are defined using the XACML access control modeling language. They may originate from one or more systems of the IT landscape and may refer to single or multiple system levels, e.g. operation system level, database level and / or application level.

As the implementation has been deployed in a SAP ERP and BI environment, an automatic transformation from their proprietary access control model to XACML have been developed. Other relevant information (e.g. customizations and parameters) may be transformed to OWL ontologies.

The deployed implementation has been evaluated with access control data from an organization with 586 users and 1,190 roles. Business processes and controls have been defined in cooperation with the financials process owner. The results of the transformation and the monitoring processes have been verified against the source data from the monitored system by random checks.

Future research will be dedicated to the evaluation of the implementation in a field study. Furthermore, it will be extended with additional transformations from other proprietary access control models to XACML.

REFERENCES

Agrawal, R., Johnson, C., Kiernan, J. and Leymann F. (2006): Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology. In Proceedings of the 22nd International Conference on Data Engineering, pp. 92-102, IEEE, Washington.

Bace, J. and Rozwell, C. (2006): Understanding the Components of Compliance, Gartner Report: G00137902.

Ball, M. and Craig, B. (2008): Object Oriented jDREW, http://www.jdrew.org/oojdrew/

Basin, D., Doser, J. and Lodderstedt, T. (2003): Model Driven Security for Process-Oriented Systems. In Proceedings of the eighth ACM Symposium on Access Control Models and Technologies, pp. 100–109, ACM, NY.

Chatterjee, A. and Milam, D. (2008): Gaining Competitive Advantage from Compliance and Risk Management. In Pantaleo, D. and Pal, N. (Eds.): From Strategy to Execution, pp. 167-183, Springer, Berlin.

Clark and Parsia (2009): Pellet: The Open Source OWL Reasoner, http://clarkparsia.com/pellet

COSO (1992): Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework, http://www.coso.org/guidance.htm

COSO (2004): Committee of Sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management - Integrated Framework, Executive Summary, http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

Damianou, N., Dulay, N., Lupu, E. and Sloman, M. (2001): The Ponder Policy Specification Language. In Proceedings of the International Workshop on Policies for Distributed Systems and Networks, pp. 18-38, Springer, London.

Ferrini, R. and Bertino E. (2009): Supporting RBAC with XACML+OWL. In Proceedings of the 14th ACM symposium on Access control models and technologies, pp. 145-154, ACM, NY.

Gericke, A., Fill, H.-G., Karagiannis, D. and Winter, R. (2009): Situational Method Engineering for Governance, Risk and Compliance Information Systems. In Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, ACM, NY.

Hevner, A. R., March, S. T., Park, J. and Ram, S. (2004): Design Science in Information Systems Research. MIS Quarterly. 28, 1, 75-105.

Höhn, S. and Jürjens, J. (2008): Rubacon: automated support for model-based compliance engineering. In Proceedings of the 30th international conference on Software engineering, pp. 875-878, ACM, NY.

Jena (2009): Jena – A Semantic Web Framework for Java, http://jena.sourceforge.net/

Jürjens, J. (2002): UMLsec: Extending UML for Secure Systems Development. In Proceedings of the 5th International Conference on The Unified Modeling Language, pp. 412–425, Springer, London.

Kehlenbeck, M., Sandner, T. and Breitner, M. H. (2010): Managing Internal Control in Changing Organizations through Business Process Intelligence – A Service Oriented Architecture for the XACML based Monitoring of Supporting Systems. In Proceedings of the 43th Hawaii International Conference on System Sciences (HICSS-43), 10 pages, CD-ROM, IEEE, Washington.

Kolovski, V., Hendler, J. and Parsia, B. (2007): Analyzing web access control policies. In Proceedings of the 16th international conference on World Wide Web, pp. 677-686, ACM, NY.
Kharbili, M. E., Stein, S., Markovic, I. and Pulvermüller, E. (2008): Towards a Framework for Semantic Business Process Compliance Management. In Proceedings of GRCIS 2008.
Li, N., Hwang, J. and Xie, T. (2008): Multiple-implementation testing for XACML implementations, In Proceedings of the 2008 workshop on Testing, analysis, and verification of web services and applications, pp. 27-33, ACM, NY.
Liebenau, J. and Kärrberg, P. (2006): International Perspectives on Information Security Practices. London School of Economics and Political Science, McAfee.
March, S. T. and Smith, G. F. (1995): Design and Natural Science Research on Information Technology. Decision Support Systems. 15, 4, 251-266.
McGreevy, M. (2008): AMR Research Finds Spending on Governance, Risk Management, and Compliance Will Exceed $32B in 2008. http://www.amrresearch.com/Content/View.aspx?pmillid=21310
OASIS (2005): Core and hierarchical role based access control (RBAC) profile of XACML v2.0, http://docs.oasisopen.org/xacml/2.0/access_control-xacml-2.0-rbacprofile1-spec-os.pdf
OASIS (2009a): eXtensible Access Control Markup Language (XACML), http://www.oasis-open.org/committees/xacml/
OASIS (2009b): SOA Reference Model, http://www.oasis-open.org/committees/soa-rm/
OMG (2009a): Business Process Modeling Notation (BPMN), http://www.bpmn.org/
OMG (2009b): Unified Modeling Language (UML), http://www.uml.org/
PERMIS (2003): PrivilEge and Role Management Infrastructure Standards Validation (PERMIS), http://www.permis.org/
Pistoia, M., Fink, S.J., Flynn, R.J. and Yahav, E. (2007): When Role Models Have Flaws. In Proceedings of the 29th international conference on Software Engineering, pp. 478-488, IEEE, Washington.
RuleML Initiative (2009): Rule Markup Language (RuleML), http://ruleml.org
Sadiq, S., Governatori, G. and Namiri, K. (2007): Modeling Control Objectives for Business Process Compliance. Business Process Management. pp. 149-164, Springer, Berlin.
Scaglioso, P.G., Basile, C. and Lioy, A. (2008): Modern Standard based Access Control in Network Services: XACML in action. IJCSNS International Journal of Computer Science and Network Security Vol. 8 No. 12, pp. 296-305.
SUN (2004): Sun's XACML implementation, Version 1.2, http://sourceforge.net/projects/sunxacml.
Syed, A., Syed, N. H., Indulska, M. and Sadiq, S. (2009): A STUDY OF COMPLIANCE MANAGEMENT IN INFORMATION SYSTEMS RESEARCH. In Proceedings of the 17th European Conference on Information Systems.
TIBCO (2009): TIBCO Business Studio, http://developer.tibco.com/business_studio/default.jsp
Turkmen, F. and Crispo, B. (2008): Performance evaluation of XACML PDP implementations. In Proceedings of the 2008 ACM workshop on Secure web services. pp. 37-44, ACM, NY.
TIBCO (2009): TIBCO Business Studio, http://developer.tibco.com/business_studio/default.jsp
W3C (1999): XSL Transformations, http://www.w3.org/TR/xslt
W3C (2004): SWRL: A Semantic Web Rule Language Combining OWL and RuleML, http://www.w3.org/Submission/SWRL/
W3C (2006): Web Services Policy Framework, www.w3.org/Submission/WS-Policy/
W3C (2008a): SPARQL Query Language for RDF, http://www.w3.org/TR/rdf-sparql-query/
W3C (2008b): XML Schema, http://www.w3.org/XML/Schema
Wang, X., Zhang, Y., Shi, H. and Yang J. (2008): BPEL4RBAC: An Authorisation Specification for WS-BPEL. In Proceedings of the 9th international conference on Web Information Systems Engineering, pp. 381-395, Springer, Berlin.
WfMC (2009): XML Process Definition Language (XPDL), http://www.wfmc.org/xpdl.html
Wolter, C., Schaad, A. and Meinel, C. (2007): Deriving XACML Policies from Business Process Models. WISE 2007 Workshops, LNCS 4832, 142–153.

Application and Economic Implications of an Automated Requirement-Oriented and Standard-Based Compliance Monitoring and Reporting Prototype

Matthias Kehlenbeck, Thorben Sandner, Michael H. Breitner
Institut für Wirtschaftsinformatik
Leibniz Universität Hannover
Hannover, Germany
{kehlenbeck,sandner,breitner}@iwi.uni-hannover.de

***Abstract*—Compliance management is a challenging task affected by continuously increasing legal requirements. Compliance with legal requirements can be assured by the incorporation of control activities into business processes. But the maintenance and monitoring of these control activities is a complex, time-consuming and often manual task. However, the timely communication of control exceptions is an important factor for the success of compliance management. The present paper presents an innovative prototypical implementation of an automated compliance monitoring and reporting system. This system is based on established standards and existing technologies. In particular, business processes are notated in BPMN and modeled in XPDL, control activities are linked to risks using COSO, control exceptions are defined using SWRL and access control data is transformed from proprietary models to XACML. The development of the prototype was aligned with common design-science research. The application of the developed prototype and its economic implications are concisely discussed with respect to different business requirements and information needs.**

***Keywords*—IT compliance, IT risk management, IS security, business process management**

I. Introduction

Compliance management can be defined as the use of frameworks, standards and software to ensure compliance with legal requirements [1]. These legal requirements considerably increased during the last years and entailed high investment costs [2]. These costs result from the embedding of control activities into business processes as well as from their ongoing maintenance and monitoring, which is a complex, time-consuming and often manual task [3], [4]. However, the timely communication of control exceptions is an important factor for the success of compliance management [5].

Compliance software forms the technical infrastructure for compliance management. Although business possesses a current need for compliance software, academia either focuses on exploratory problem-identifying [6] or neglects actual information needs [7]. Consequently, business demand and academic supply diverge [8].

The present paper presents an innovative prototypical implementation of an automated compliance monitoring and reporting system. This system is based on established standards and existing technologies. Its development has been aligned with common design-science research guidelines. According to these guidelines, design-science research must be presented to both technology-oriented and management-oriented audiences [9]. Sufficient detail for the construction of the system has been presented in a previous paper [10]. The present paper details on the application of the system and its economic implications, in particular with respect to different business requirements and information needs.

The remainder of this paper is structured as follows: Section II introduces the problem domain and the research approach. The design and evaluation process of the prototype is described in section III. The application of this prototype and corresponding economic implications are discussed in section IV. Section V contains the related work. Finally, section VI concludes with a discussion about future work.

II. Problem Domain and Research Approach

A. Business Environment and Problem Relevance

Compliance monitoring and reporting involves several participants. Typical participants are:

- Decision-makers (e.g. chief financial officer) define business objectives and require highly aggregated strategic information.
- Process-owners (e.g. head of accounting) are in operative charge and require detailed process information regarding their area of responsibility.
- Control specialists (e.g. auditor) inspect processes and systems with respect to compliance issues and develop corresponding recommendations.
- IT specialists (e.g. application administrator) maintain systems and incorporate controls.

Table I characterizes these participants by means of their responsibilities and information needs in more detail.

Information needs considerably differ in their focus and granularity. For example, decision-makers require highly aggregated information regarding effects, while IT specialists require detailed information regarding causes.

Process-owners bear the responsibility for their area as a whole. Therefore, they initiate adjustments to processes, controls and systems, while control specialists only develop corresponding recommendations.

The suitability of software depends not least on its adaptability to specific organizations. Organizations differ in certain characteristics. With respect to compliance monitoring and reporting, two especially influential characteristics have been identified:

DOI: 10.1109/ARES.2010.88

TABLE I. PARTICIPANTS, RESPONSIBILITIES AND USER REQUIREMENTS WITH RESPECT TO COMPLIANCE MONITORING AND REPORTING

Participants	Responsibilities	Information Needs
Decision-makers	• Definition of business objectives • Identification and assessment of risks	• Highly aggregated risk, control and process information • Coherent presentation with other strategic information
Process-owners	• Development of responses corresponding to risks • Initiation of adjustments to processes, controls and systems	• Detailed process, some risk, control and system information • Coherent presentation with other operative information
Control specialists	• Development of controls corresponding to risk responses • Monitoring of controls and reporting of exceptions	• Detailed control, some risk, process and system information • Collaboration with process owner and IT specialists
IT specialists	• Incorporation of controls into systems • Maintenance of systems	• Detailed system, some process, control and risk information • Collaboration with process owner and control specialists

1. As control activities are embedded into business processes, the comprehensiveness of existing process documentation is characteristic.
2. As numerous control activities are implemented into supporting systems, the heterogeneity of the system landscape is characteristic.

These characteristics are used to classify organizations into four different scenarios, as illustrated in Fig. 1. These scenarios correspond to different business requirements. For example, scenario 2 organizations require compliance software which incorporates existing process documentation, monitors the embedded controls in heterogeneous systems and consistently reports thereby detected control exceptions. On the contrary, scenario 3 organizations possess neither process documentation nor system heterogeneity.

The relevance of the presented prototype arises from its ability to meet the different business requirements and information needs.

B. Scientific Knowledge and Research Rigor

The scientific knowledge base offers a plethora of foundations and methodologies. Concerning the prototype, data models, software architectures, design methods and evaluation techniques are particularly helpful. Design-science research is perceived as an ongoing design and evaluation process. Consequently, the present paper concisely describes both the current prototype and its development so far. The rigor of the presented ongoing research arises from the effective use of scientific knowledge for the design and evaluation process.

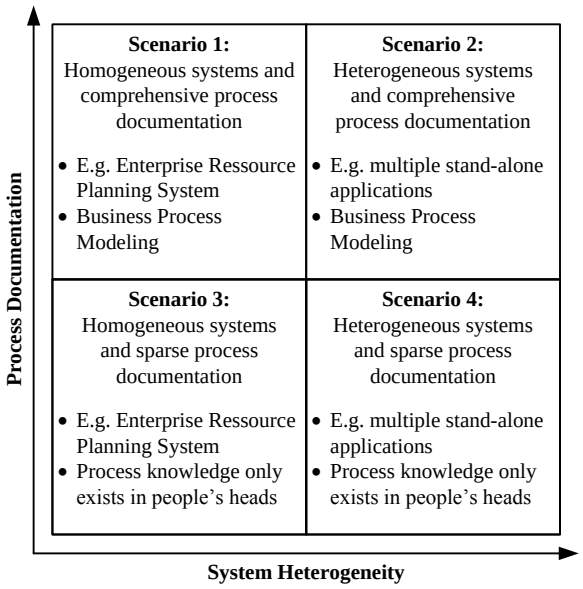

Figure 1. Process Documentation, System Heterogeneity and Scenarios

III. DESIGN AND EVALUATION PROCESS

The design of the prototype allowed for critical success factors and followed Model-Driven Architecture (MDA) [11] and Service-Oriented Architecture (SOA) [12] principles. Consequently, it has been divided into model, architecture and implementation design phases. The design phases have entailed evaluation phases. Fig. 2 illustrates the design and evaluation process for the current and previous prototype.

A. Critical Success Factors

One of the key questions for organizations is how to effectively and efficiently respond to continuously changing legal requirements with adjustments to processes and systems [13]. Moreover, dynamic business environments require continuously changing processes and systems although these have to comply with legal requirements. Chatterjee et al. [14] have established critical factors for the success of compliance management. They argue for (1) central approaches, (2) proactive responses, and (3) automated processes.

Central approaches to compliance management possess several advantages. They provide for the central definition of requirements and the central analysis of compliance. This mitigates challenges associated with heterogeneous system landscapes (scenario 1 and 2) and enables a bundling of competences which allows for a lean staff, a steep learning curve and comparably low costs. Aside of these effects, a central compliance repository may prevent system-oriented silos and thereby reveals overlapping between already existing controls and new controls. Thus, recurrent reinventing the wheel effects which cause additional work and expense for every additionally regarded system are encountered. The integration of compliance information from several systems into a central repository also forms a basis for the creation of homogeneous analyses and reports. In order to reduce time and effort for learning and to dispel potential reservations, these analyses and reports may be provided in an environment which is familiar to the participants. The prototype has to support such a central approach.

DOI: 10.1109/ARES.2010.88

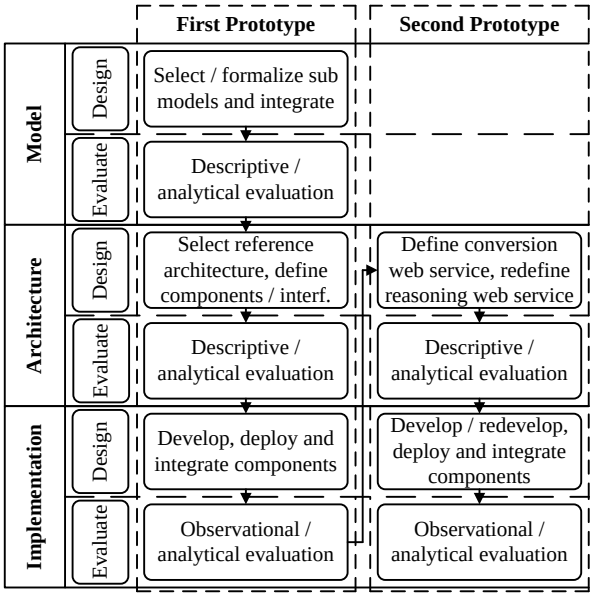

Figure 2. Design and Evaluation Process for the Prototypes

Compliance solutions can generally be divided by their employment phase: "before-the-fact" or "after-the-fact" [15]. The before-the-fact phase contains (i) compliance aware design and (ii) post design verification approaches which proactively try to avoid noncompliance situations and thereby strive for the reduction of subsequent adjustment costs. The after-the-fact phase is the classic application area of (iii) manual audits and (iv) automated detection which reactively try to discover noncompliance situations and thereby entail adjustment costs. The prototype has to facilitate the avoidance of these costs.

Automation is a crucial factor with respect to the cost and the feasibility of compliance monitoring. Cost and time intensive manual audit processes can be partially replaced by automated processes, which increase the possibilities as well as the productivity of auditors. Up to date analyses and reports assure a continuous effect of compliance monitoring. However, they also require a continuous monitoring technology that runs in the back-ground of the organizations systems. The prototype has to support continuous monitoring.

An additional critical success factor for the success of compliance management is its seamless integration in the organizational design. In particular, organizations have to strike a balance between trust and control to secure the acceptance of control monitoring. Organization cultures of trust are considered as more productive than cultures of control [16]. However, the legal requirements or the risk environment may suggest a reasonable trade off.

B. Model

Control activities are embedded into business processes. Business processes change and evolve over time. In order to account for this, the model includes a process model. Understanding of business processes is very important for compliance monitoring and reporting. The Business Process Modeling Notation (BPMN) [17] was developed to ease this understanding for participants. The XML Process Definition Language (XPDL) [18] is used to store BPMN processes.

Many control activities can be incorporated into supporting systems by means of their access control functions. Supporting systems typically use proprietary access control models. In order to avoid dependencies on these proprietary models, the standardized Extensible Access Control Markup Language (XACML) [19] is used to store access control data. Access control data from proprietary models is transformed to XACML.

Sensible control activities respond to business risks and support the achievement of business objectives. The predominant approach to internal control is described in the Internal Control – Integrated Framework [20] respectively the Enterprise Risk Management – Integrated Framework [21] (COSO). The core concepts of the COSO model were formalized and supplemented with definitions of control exceptions. Control exceptions may be defined using any Extensible Markup Language (XML) [22] based rule language, e.g. RuleML [23] or SWRL [24].

Business process, access control and internal control models were integrated. An overview of the integrated model is presented in Fig. 3. This model was evaluated as semantically rich but yet not too complex. Moreover, its composition of existing sub models enables the use of existing tools for process modeling, access control processing and control definition and thereby reduces implementation expenditure.

The integrated model enables the post design verification of changes to processes, controls and systems with respect to compliance issues. Therefore, problematic changes may be detected before they become productive. This avoids potential adjustment costs and thereby addresses success factor (2), proactive responses.

C. Architecture

In order to increase flexibility and facilitate reuse, the prototype was divided into distinct components:

- The XACML Policy Decision Point (PDP) web service (WS) accepts incoming access control requests, processes a repository of policies and returns decisions.
- The reasoning WS accepts incoming assertions, evaluates rules, and answers queries to the thereby established knowledge base.

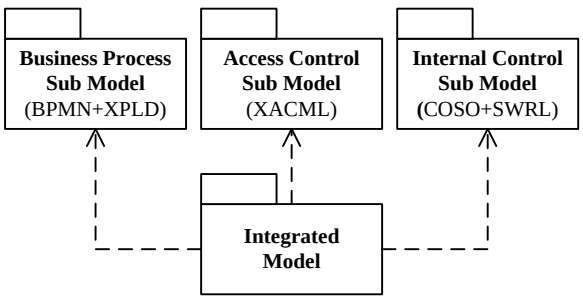

Figure 3. Business Process, Access Control and Internal Control Model

DOI: 10.1109/ARES.2010.88

- The conversion WS transforms access control data from proprietary models to XACML. Permissions and roles are passed to the XACML PDP WS, while role assignments are passed to the monitoring WS. Other data (e.g. parameters) may be transformed to assertions which are passed to the reasoning WS via the monitoring WS.
- The monitoring WS accepts incoming process data, control data, role assignments and assertions. Control data and role assignments are combined and send to the XACML PDP WS for access control evaluation. The returned decisions, the assertions received from the conversion WS and the control exception definitions are passed to the reasoning WS. The latter returns the detected control exceptions. Finally, data is passed to the Business Intelligence (BI) system.
- The monitoring client is used to invoke the monitoring WS with a specific configuration, in particular after changes to business processes, access control and / or internal control.
- The BI system receives data from the monitoring WS and optionally other systems. It provides comprehensive analysis and reporting services to the participants.

The architecture was assessed as suitable for many different system landscapes. It reduces the dependencies between its components and enables their independent development.

The automated transformation of access control data from heterogeneous systems to XACML by means of the conversion WS enables their homogeneous processing. This homogeneous processing eases the monitoring of internal control across systems and may take place at a single and central instance. Thus, success factors (1) and (3), central approaches and automated processes are addressed. Moreover, the use of a BI system as a presentation layer allows the coherent and timely presentation of internal control information with other characteristics and facts, enables both aggregated reports and deep analyses, and reduces implementation expenditure.

The conversion WS was incorporated into the architecture after the evaluation of the first prototype implementation. At the same time, the reasoning WS was redesigned. Fig. 4 illustrates the individual components and interfaces of the architecture.

D. Implementation

The XACML PDP WS is currently based on the XACML PDP implementation of Sun (SUNXACML) [25] and the reasoning WS is based on the Jena framework [26] and the Pellet reasoner [27]. The other web services were implemented from scratch. Large parts of the Java source code have been generated using the Eclipse Modeling Framework (EMF) [28] and the Apache CXF (CXF) [29] services framework.

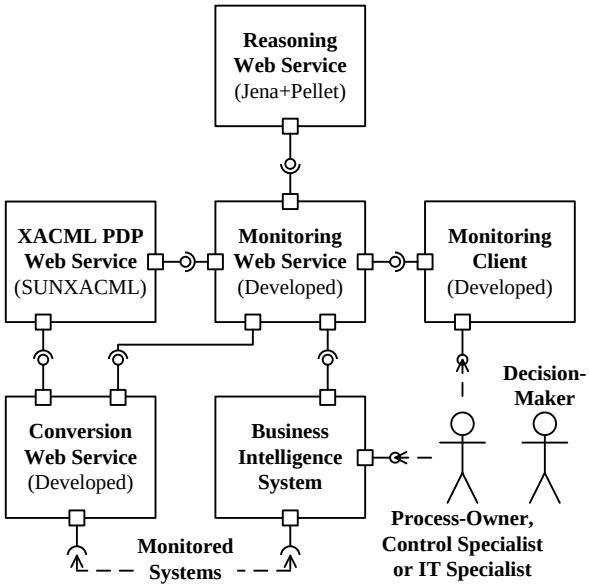

Figure 4. Individual Components and Interfaces of the Architecture

The first prototype did not contain a conversion WS and used a RuleML based reasoning WS. In a case study (close to scenario 1), the manual transformation of access control data from the proprietary SAP model to XACML turned out as impractical, even for single areas. However, the numerous available XACML functions rendered the development of corresponding transformations for the conversion WS easy. Moreover, it was necessary to account for the fact that SAP access control additionally depends on other data (e.g. parameters). It was assessed as more convenient to store this data using the Web Ontology Language (OWL) [30] instead of RuleML. Therefore, the reasoning WS was redeveloped based on SWRL, which combines OWL and RuleML.

The second prototype successfully monitors authorization and segregation of duties controls for a productive client in a SAP Enterprise Resource Planning (ERP) system with currently 586 active users and 1,200 active roles. A SAP BI system is used to analyze and report detected control exceptions.

The generated XACML policies and the detected control exceptions were verified against the source data by random checks.

IV. Application and Economic Implications

The application of the prototype and its economic implications are discussed based on deployment phases, critical success factors, business requirements as well as information needs.

A. Post Design Verification and Automated Detection

The implemented prototype represents a synthesis between post design verification and automated detection. It enables the automated detection of control exceptions both before-the-fact and after-the-fact.

DOI: 10.1109/ARES.2010.88

In the before-the-fact phase, subsequent adjustment costs may be avoided, if new business process, access control and internal control designs are evaluated by means of the prototype before they become productive.

In the after-the-fact phase, recurrent monitoring costs may be decreased. After the prototype has been initially configured, checked and accepted by auditors, lower costs for the following years can be expected, as unchanged processes and their embedded controls may be monitored in an instant without time-consuming manual tasks. The necessary knowledge is captured by the prototype and is thereby in the property of the organization. Thus, decision-makers and process-owners may respond in time (i.e. before periodic audits) to detected control exceptions.

Additionally, other participants than control specialists may easily define their own controls. Their knowledge is a valuable asset for the achievement of business objectives and internal control is not limited to compliance objectives. This possibility may contribute to decentralization, quality and timeliness of decisions and strengthen the effectiveness of operational management.

B. Business Requirements and Critical Success Factors

The following paragraphs discuss different scenarios as described in Fig. 1, incorporate the identified critical success factors and point out the potential economic implications associated to an application of the implemented prototype. The seamless integration in the organizational design, success factor (4), is not discussed, as it is largely independent of the described scenarios and the prototype.

In scenario 1, the homogeneous system landscape and the existing process documentation facilitates success factors (1), (2) and (3). The homogeneous system landscape eases the implementation of a central approach. The prototype requires few different transformations of access control data from proprietary models to XACML in order to enable this central approach. Furthermore, the existing process documentation facilitates the definition of internal control on a functional level. Thus, the impact of changes to both access control and business processes on internal control may be monitored proactively before-the-fact and reactively after-the-fact. The homogeneous system landscape reduces the number of different interfaces, while the existing process documentation prevents comprehension problems associated to the automation of monitoring. This automation may be achieved by means of the prototype.

In scenario 2, the heterogeneous system landscape increases complexity and demands for a more interoperable monitoring system than in scenario 1. The heterogeneous system landscape requires the definition of access control in different proprietary models. The prototype overcomes the differences between these proprietary models by the transformation of access control data to XACML before subsequent processing. The numerous XACML functions render the development of corresponding functions comparatively easy. Thus, the prototype enables a central approach. As in scenario 1, existing process documentation facilitates the definition of internal control on a functional level. However, internal control is distributed among different systems and therefore described using different models. This makes automated processing and proactive responses more difficult. However, the prototype transforms access control data to XACML before processing. Therefore, the impact of changes may be automatically monitored proactively and reactively.

In scenario 3, the homogeneous system landscape facilitates the implementation of a central approach, as in scenario 1. However, the lack of process documentation prevents the definition of internal control on a functional level and enforces its concentration on a technical level. The impact of changes to access control on internal control may still be automatically monitored before-the-fact and after-the-fact by the prototype, but business processes are left unconsidered.

Scenario 4 refers to a heterogeneous system landscape and a lack of process documentation. It combines the challenges of scenario 2 and scenario 3. As in scenario 2, the prototype enables a central approach in spite of access control model differences. As in scenario 3, the impact of changes to access control on internal control may be automatically monitored before-the-fact and after-the-fact by the prototype, but business processes are left unconsidered.

In summary, scenario 1 is most suitable for automated compliance monitoring and reporting. As the prototype overcomes system heterogeneity, a comparable level may be reached in scenario 2. The prototype supports automated proactive and reactive reporting in all scenarios. However, the definition of internal control on a functional level requires at least some existing process documentation. Thus, the full potential of the prototype cannot unfold in scenario 3 and 4.

C. Information Needs

Participants have different needs regarding functionality and information. The following paragraphs discuss different information needs, as described in Table I.

Decision-makers require highly aggregated risk, control and process information that is coherently presented with other strategic information. The use of a BI system as a presentation layer enables cockpits, dashboards and scorecards which link information from the prototype with information from other sources.

Process-owners require detailed process and some risk, control and system information that is coherently presented with other operative information. The prototype links process, control, risk and system information and provides it for combined analyses and reports with other operative information to a BI system. Additionally, problematic changes to processes can be proactively identified and revoked, before they become productive.

Control specialists require detailed control and some risk, process and system information. The prototype provides information that has both the necessary detail for drill-down analyses of internal control and the required

DOI: 10.1109/ARES.2010.88

process and system context for efficient collaboration with other participants. Additionally, automated and homogeneous processing of access control data from heterogeneous systems is enabled.

IT specialists require detailed system and some process, control and risk information. The prototype provides information as needed and thereby facilitates collaboration with other participants. The additional context makes it easier to incorporate controls into systems. Furthermore, problematic changes to roles and role assignments can be proactively identified and revoked before they become productive.

V. Related Work

A crucial point for compliance management and therefore compliance software is the consideration of business processes in conjunction with compliance and security requirements. There is some work on this topic, including a few proposals on architectures or applications. Höhn et al. [31] deal with the monitoring of compliance requirements and security policies. They establish a mapping between Unified Modeling Language (UML) [32] activity diagrams and configuration data for business applications. Limitations are the use of a tightly coupled architecture and proprietary formats for access control and rule data. Through the use of standard access control and rule languages as well as a service-oriented architecture, these limitations do not apply to the present approach.

Wolter et al. [33] present a mapping between BPMN and XACML and use an XSL transformation (XSLT) [34] to convert security constraints into XACML policies. The present approach provides for transformations between different access control models, not between a process model and an access control model. Other works, e.g. [35], [36] and [37] are thematically and technically related. They also focus on the combination of BPMN or UML models with security policies, but do not directly deal with the monitoring of controls.

Pistoia et al. [38] focus on the static policy validation for a Role Based Access Control (RBAC) model. The present approach additionally enables runtime analyses and allows the use of other access control models than RBAC. Sadiq et al. [39] use a proprietary language to define controls and annotate business processes with corresponding tags. However, the present approach includes an access control model, uses an internal control model, which resembles the COSO model more closely and prefers a standard rule language.

Compliance management is increasingly addressed by IS research since about 2001. Julisch [8] even demands a new research discipline to consider security compliance more adequately. In spite of the business needs, about two-thirds of the articles to this subject are case studies or exploratory articles and only few are solution oriented [6].

VI. Conclusion

Business possesses a current need for compliance software to form the technical infrastructure for compliance management. To account for this need, this has paper presented an innovative prototypical implementation of an automated compliance monitoring and reporting system. This system is oriented to business requirements and information needs, and is based on established standards and existing technologies. The development of the prototype was aligned with common design-science research guidelines and consequently follows a corresponding design and evaluation cycle.

Critical success factors for the application of the developed prototype to specific organizations have been concisely discussed with respect to different business requirements and information needs. The developed prototype has been examined against the background of different organization scenarios and assessed as able to fulfill the considered business requirements and information needs as far as possible. However, some information needs can only be met, if at least some process documentation exists.

Potential economic implications have been identified. Automated compliance monitoring may reduce time-consuming manual tasks and increase the timeliness of reporting. It can thereby enable the monitoring of more complex controls and create the necessary leeway for corrective adjustments. Adjustment costs may be avoided by proactive post design verification. Likewise, damage to the organization (e.g. fraud, fines, and loss of reputation) may be prevented. Moreover, development costs may be reduced by the homogeneous processing of access control data from heterogeneous systems and the adherence to established standards and existing technologies. By means of the formal definition of controls and control exceptions, organizations may establish a corresponding knowledge base. This knowledge base may reduce monitoring costs in the following years, as unchanged processes and their embedded controls may still be monitored in an instant.

Future work will be dedicated to the evaluation of the prototype in a field study. This field study shall increase the degree of confirmation with respect to the feasibility and suitability of the prototype and back up the estimated economic implications. Furthermore, the considered critical success factors are to be critically assessed with respect to lessons learned from the field study. Moreover, experiences from the field study may result in other perspectives and additional research questions.

References

[1] M. E. Kharbili, S. Stein, I. Markovic, and E. Pulvermüller, ”Towards a Framework for Semantic Business Process Compliance Management,” Proc. of the 1st International Workshop on Governance, Risk and Compliance: Applications in Information Systems (GRCIS'08), vol. 339, June 2008, pp. 1-15.

[2] M. McGreevy, “AMR Research Finds Spending on Governance, Risk Management, and Compliance Will Exceed $32B in 2008,” http://www.amrresearch.com/Content/View.aspx?pmillid=21310, 2008.

[3] J. Bace, and C. Rozwell, “Understanding the Components of Compliance,” Gartner Report: G00137902, 2006.

DOI: 10.1109/ARES.2010.88

[4] R. Agrawal, C. Johnson, J. Kiernan, and F. Leymann, "Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology," Proc. of the 22nd International Conference on Data Engineering (ICDE'06), IEEE Computer Society, 2006, pp. 92-102, doi:10.1109/ICDE.2006.155.

[5] J. Liebenau, and P. Kärrberg, "International Perspectives on Information Security Practices," London School of Economics and Political Science, McAfee, 2006.

[6] A. Syed, N. H. Syed, M. Indulska, and S. Sadiq, "A Study of Compliance Management in Information Systems Research," Proc. of the 17th European Conference on Information Systems (ECIS), June 2009.

[7] A. Gericke, H.-G. Fill, D. Karagiannis, and R. Winter, "Situational Method Engineering for Governance, Risk and Compliance Information Systems," Proc. of the 4th International Conference on Design Science Research in Information Systems and Technology (DESRIST'09), ACM, May 2009, Article No. 24, doi:10.1145/1555619.1555651.

[8] K. Julisch, "Security compliance: the next frontier in security research," Proc. of the 2008 workshop on New security paradigms, ACM, Sept. 2008, pp. 71-74, doi:10.1145/1595676.1595687.

[9] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," MIS Quarterly, vol. 28, no. 1, March 2004, pp. 75-105.

[10] M. Kehlenbeck, T. Sandner, and M. H. Breitner, "Managing Internal Control in Changing Organizations through Business Process Intelligence – A Service Oriented Architecture for the XACML based Monitoring of Supporting Systems," Proc. of the 43th Hawaii International Conference on System Sciences (HICSS 2010), IEEE Computer Society, in press.

[11] Object Management Group (OMG): Model Driven Architecture, http://www.omg.org/mda/

[12] Organization for the Advancement of Structured Information Standards (OASIS): SOA Reference Model, http://www.oasis-open.org/committees/soa-rm/

[13] P. Pinder, "Preparing Information Security for legal and regulatory compliance (Sarbanes–Oxley and Basel II)," Information Security Technical Report, vol. 11, Issue 1, 2006, pp. 32-38, doi:10.1016/j.istr.2005.12.003.

[14] A. Chatterjee, and D. Milam, "Gaining Competitive Advantage from Compliance and Risk Management," in From Strategy to Execution, D. Pantaleo and N. Pal, Eds. Springer, 2008, pp. 167-183, doi: 10.1007/978-3-540-71880-2_9.

[15] A. Awad, G. Decker, M. Weske, „Efficient Compliance Checking Using BPMN-Q", Business Process Management, Springer, Berlin, 2008, pp. 326-341.

[16] J. Grundel, "Examining the Relationship Between Trust and Control in Organizational Design," in Information and Organization Design Series, vol. 6, R. M. Burton, D. D. Håkonsson, B. Eriksen and C. C. Snow, Eds. Springer, 2006, pp. 43-65, doi:10.1007/0-387-34173-0_3.

[17] Object Management Group (OMG): Business Process Modeling Notation (BPMN), http://www.bpmn.org/

[18] Workflow Management Coalition (WfMC): XML Process Definition Language (XPDL), http://www.wfmc.org/xpdl.html

[19] Organization for the Advancement of Structured Information Standards (OASIS): eXtensible Access Control Markup Language (XACML), http://www.oasis-open.org/committees/xacml/

[20] Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework (1992), http://www.coso.org/guidance.htm

[21] Committee of Sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management - Integrated Framework, 2004, http://www.coso.org/guidance.htm

[22] World Wide Web Consortium (W3C): Extensible Markup Language (XML), http://www.w3.org/XML/

[23] The Rule Markup Initiative: Rule Markup Language (RuleML), http://ruleml.org

[24] World Wide Web Consortium (W3C): SWRL: A Semantic Web Rule Language Combining OWL and RuleML, http://www.w3.org /Submission/SWRL/

[25] Sun's XACML implementation, Version 1.2, http://sourceforge.net /projects/sunxacml, 2004.

[26] Jena – A Semantic Web Framework for Java, http://jena. sourceforge.net/

[27] Clark and Parsia: Pellet: The Open Source OWL Reasoner, http://clarkparsia.com/pellet

[28] The Eclipse Foundation: Eclipse Modeling Framework Project (EMF), http://www.eclipse.org/modeling/emf/

[29] The Apache Software Foundation: Apache CXF: An Open Source Service Framework, http://cxf.apache.org/

[30] World Wide Web Consortium (W3C): OWL Web Ontology Language, http://www.w3.org/TR/2004/REC-owl-features-20040210/

[31] S. Höhn, and J. Jürjens, "Rubacon: automated support for model-based compliance engineering," Proc. of the 30th international conference on Software engineering (ICSE'08), ACM, May 2008, pp. 875-878, doi:10.1145/1368088.1368228.

[32] Object Management Group (OMG): Unified Modeling Language (UML), http://www.uml.org/

[33] C. Wolter, A. Schaad, and C. Meinel, "Deriving XACML Policies from Business," Web Information Systems Engineering – WISE 2007 Workshops, Springer, 2007, pp. 142-153, doi:10.1007/978-3-540-77010-7_15.

[34] World Wide Web Consortium (W3C): XSL Transformations, http://www.w3.org/TR/xslt20/

[35] X. Wang, Y. Zhang, H. Shi, and J. Yang, "BPEL4RBAC: An Authorisation Specification for WS-BPEL," Web Information Systems Engineering - WISE 2008, Springer, 2008, pp. 381-395, doi:10.1007/978-3-540-85481-4_29.

[36] D. Basin, J. Doser, and T. Lodderstedt, "Model Driven Security for Process-Oriented Systems," Proc. of the eighth ACM Symposium on Access Control Models and Technologies (SACMAT'03), ACM, 2003, pp. 100–109, doi:10.1145/775412.775425.

[37] J. Jürjens, "UMLsec: Extending UML for Secure Systems Development," Proc. of the 5th International Conference on The Unified Modeling Language (UML'02), Springer, 2002, pp. 412–425, doi:10.1007/3-540-45800-X_32.

[38] M. Pistoia, S.J. Fink, R.J. Flynn, and E. Yahav, "When Role Models Have Flaws," Proc. of the 29th International Conference on Software Engineering (ICSE'07) , IEEE Computer Society, 2007, pp. 478-488, doi:10.1109/ICSE.2007.98.

[39] S. Sadiq, G. Governatori, and K. Namiri, "Modeling Control Objectives for Business Process Compliance," Proc. of the 5th International Conference on Business Process Management (BPM2007), Springer, 2007, pp. 149-164, doi:10.1007/978-3-540-75183-0_12.

DOI: 10.1109/ARES.2010.88

Visualization of Automated Compliance Monitoring and Reporting

Thorben Sandner, Matthias Kehlenbeck, Michael H. Breitner
Institut für Wirtschaftsinformatik
Leibniz Universität Hannover
Hannover, Germany
{sandner,kehlenbeck,breitner}@iwi.uni-hannover.de

***Abstract*— Compliance management is a critical financial and legal subject for organizations. It is operationally implemented by embedding internal controls into business processes and their supporting IT systems. Challenges arise from the complexity of real-life processes and systems, their continuous monitoring and the timely communication of thereby detected problems. In order to realize effective and efficient monitoring, the responsible persons must be supported by suitable compliance software. This compliance software should enable the responsible persons to get both high-level information regarding the overall compliance status and low-level information regarding possible problems. Furthermore, it should not be limited to passive reporting components for compliance management, but also allow for interactive user interfaces, which facilitate the proactive supervision of tasks. The aim of this work is to encourage the responsible persons to analyze and explore compliance information through their appropriate visualization. Thus, unique and valuable human strengths, such as lateral thinking, can be used aside from the computational strengths of compliance software during control monitoring.**

***Keywords*— IT compliance, IT risk management, IS security, Visualization, Dashboard**

I. INTRODUCTION

Various regulations were introduced in the last years to increase the compliance standards in organizations. The implementation of these regulations, as for example Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA) or EuroSOX, is mandatory for many organizations. The thereby occurred costs are estimated in the U.S. as 32 billion U.S. dollars for the year 2008 [1]. These costs result from the embedding of internal controls into business processes as well as from their ongoing maintenance and monitoring, which is a complex, time-consuming and often manual task [2], [3]. The whole process of compliance management can be defined as the use of frameworks, standards and software to ensure compliance with legal requirements [4].

Especially the timely communication of control exceptions to the right decision-makers is a critical factor for the success of compliance management [5]. This timeliness provides decision-makers with the necessary leeway for corresponding measures. If these measures are not taken, several negative consequences may follow, e.g. fraud, damage to the organizations reputation, fines as well as the decline of the organizations credit rating or market value. Thus, the achievement of the organizations objectives is put at risk.

To enable decision-makers to react timely, they have to be provided with consistent, sound and properly visualized information concerning the occurrence and the implications of control exceptions. Therefore, data concerning different processes and viewpoints must be integrated into a comprehensive view [6].

The design of well-considered dashboards may overcome several obstacles for decision-making. These obstacles are, amongst others, the inadequate organization of potentially decision relevant data, the cross organizational integration of data, as well as personal biases in decision making and information processing [6]. However, the requirements for such dashboards highly depend on the particular information needs of different user groups [7]. Thus, target group aligned information visualization is needed.

The present paper presents ongoing research regarding the visualization of compliance monitoring information, in particular with respect to different information needs. This information is generated by a prototypical implementation of an automated compliance monitoring and reporting system. This system is based on established standards and existing technologies and its development has been aligned with common design-science research guidelines [8]. Detailed information for the construction of the system and its exemplary integration with a major Enterprise Resource Planning (ERP) system has been presented in previous papers [9], [10].

The remainder of this paper is structured as follows. Section II introduces the problem domain and the research approach. The design of the prototype is described in section III. An application of this prototype with respect to information visualization is discussed in section IV. Section V presents an overview of the related work. Finally, section VI concludes and gives an outlook.

II. VISUALIZATION OF COMPLIANCE MONITORING

There is a current need for the appropriate visualization of security issues [11]. The research area dealing with visualization in information systems is referred as ‘information visualization’. Information visualization can be described as the interactive computer based visual representation of abstract data to amplify cognition [12]. ‘Information visualization’ deals primarily with abstract data, such as compliance data, as opposed to ‘scientific visualization’, which deals with physically-based data [12].

DOI: 10.1109/DEXA.2010.77

The research area referred to as 'visualization of computer security' focuses on the provision of information visualization applications to strengthen the human perceptual and cognitive processes in solving computer security problems [13]. Card et. al [12] outline different ways for the amplification of cognition. One way is to enhance the detection of patterns e.g. by using visual schemata for structuring data in time-referenced relationships [14]. Another way is the provision of a manipulatable tool which allows users to explore data with parameter values and ensures user actions. Of particular importance are functions to simplify the search for information. Visualization can represent a lot of information in a small space. An example of this is a dashboard. Few [15] defines a dashboard as "[…] *a visual display of the most important information needed to achieve one or more objectives; consolidated and arranged on a single screen so the information can be monitored at a glance."* Other mentioned features of a dashboard are high-level summaries as well as clearly structured usable and customizable display mechanisms. Regarding the visual design of dashboards, the focus should be on the gain of insight. In particular, discovery, explanation and decision making are of importance and not the presentation of nice graphics [12]. To avoid the mentioned pitfalls, several guidelines for the design of structured dashboards where developed [6, 16]. The graphical implementation of a dashboard can be done with a variety of graphical elements. But not all graphical elements are equally well suited for the performance of analysis and the acquisition of knowledge [17]. The development of a dashboard as a user interface of a compliance monitoring tool should therefore be pursued in close consultation with users and stakeholders [18] and with regard to their information needs.

III. PROTOTYPE

Sensible compliance monitoring is not feasible without an understanding of the underlying business processes, the embedded control definitions and the controls implemented in supporting systems. In a previous paper, a business process model, an internal control model and an access control model were combined into an integrated model [9]. This integrated model enables the examination of changes to processes, controls and systems with respect to compliance issues.

As internal control is embedded into business processes, it can not be understood without them. However, business processes are frequently subject to changes. These changes may be captured by the modeling of business processes. The Business Process Modeling Notation (BPMN) [19] is commonly used for the modeling of business processes. The integrated model uses the XML Process Definition Language (XPDL) [20] to store BPMN processes.

Internal control definitions are commonly based on the Internal Control – Integrated Framework [21] and the Enterprise Risk Management – Integrated Framework [22] (COSO). The core concepts of the COSO model were formalized to an internal control model. This internal control model was formalized to include definitions of control exceptions. Control exceptions can be defined using any Extensible Markup Language (XML) [23] based rule language.

Many controls are implemented into supporting systems by means of access controls. Typically, these access controls are defined in proprietary formats. To enable a homogeneous processing of access control related data from heterogeneous systems, this data is converted to the standardized Extensible Access Control Markup Language (XACML) [24].

Following a service-oriented architecture (SOA), the prototype was separated into distinct components. This increases the flexibility and the reusability of the individual components. The prototype can be invoked by a monitoring client. The monitoring clients connects to the monitoring web service, which uses the conversion web service to convert access control data to XACML, the XACML PDP web service to make access control decisions and the reasoning web service to identify control exceptions. Using one or multiple import web services, these control exceptions are published together with the integrated model to data providers. Figure 1 illustrates these components.

The import web services are used to decouple the monitoring web service from a particular data provider. Currently, a data warehouse server is used as a data provider. However, an OLE DB data provider is in development. While the use of a data warehouse enables the deployment of the prototype in large-scale environments, the OLE DB provider is developed to enable the deployment in small-scale environments. Both allow for the provision of data to Microsoft Excel. Excel in turn allows for the provision of data to visualization tools like Microsoft Visio and SAP Business Objects Xcelsius. Figure 2 illustrates this provision.

IV. APPLICATION TO INFORMATION VISUALIZATION

The different ways for the amplification of cognition introduced in section II have influenced the development of a visualization artifact for compliance monitoring and reporting. In particular, they have led to the decision of developing a dashboard. For this development, the mentioned guidelines have been adopted under the focus of compliance management.

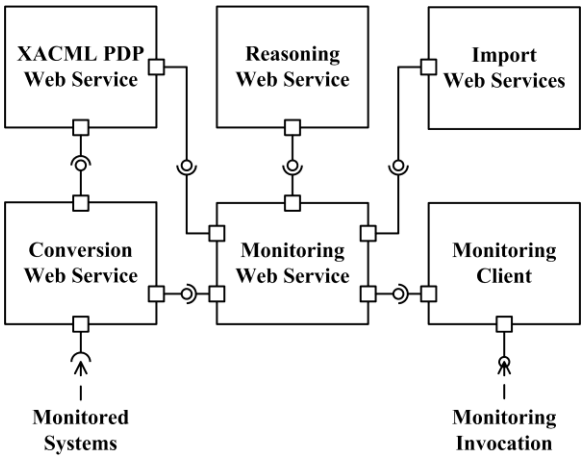

Figure 1. Core components and interfaces of the architecture

DOI: 10.1109/DEXA.2010.77

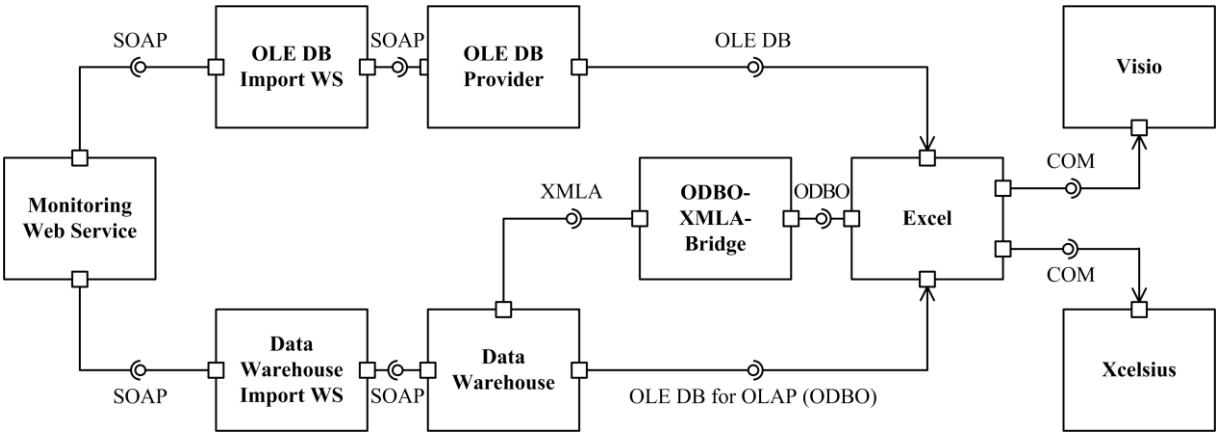

Figure 2. Components for the provision of compliance monitoring data to visualization tools

In a first stage, the scope of the dashboard has been defined in conversations with different stakeholders. The stakeholders have asked for an aggregated view regarding the status of clients, a differentiated choice of controls and a time-referenced based view. The requirements of the users are to be met without overstraining their cognitive abilities [25]. On the contrary, a dashboard has to be clear and comprehensible, as too much complexity regarding interactions and relations make it more difficult and less interpretable. After all, the visual presentation shall increase performance of compliance management task by reducing cognitive workloads [25]. The design of the dashboard was an iterative process involving frequent conversations. Various graphical elements were proposed by the stakeholders. Considering several visualization design guidelines, some graphical elements such as gauges or detailed tree views were deliberately not used [16]. Figure 3 contains a screenshot of the designed dashboard. This dashboard is presented as one possible solution for the visualization of automated compliance monitoring and reporting. It is devoted to the monitoring of several SAP systems in two different data centers. The dashboard was created using Xcelsius.

In a second stage, the dashboard was populated with data. The aforementioned prototype allowed for an easy integration with a SAP system. As Xcelsius embeds Excel, it was also easily possible to integrate semi-automatic as well as manual controls. The controls to incorporate were selected together with the stakeholders. The nature of these controls determines their monitoring frequency.

There are some additional stages described in the literature [6]. However, they are difficult to adapt to compliance management. Furthermore, the project is still in the second stage, as not all of the selected controls are incorporated.

Although the described dashboard was well received, such a dashboard can only be one of many elements which belong to a compliance strategy in an organization. The discussion with the stakeholders showed that a high-level tool like this dashboard can get widely accepted. This acceptance was also increased by the involvement of Excel, which is both available and transparent for the stakeholders.

V. Related Work

Numerous works deal with the visualization for computer and network security. Corresponding systems, e.g. intrusion detection systems, often generate vast amounts of data. Goodall [13] presents an overview of approaches that reduce complexity and thereby improve performance on attack classification and detection tasks. The approaches commonly distinguish between different levels of granularity, e.g. internet, company and packet. The present paper pursues similar objectives but uses different source data and therefore possesses other levels of granularity, i.e. process, system and control.

Several works examine the implications of Unified Modeling Language (UML) [26] models or BPMN models in conjunction with security policies, e.g. Wang et al. [27] and Wolter et al. [28]. Furthermore, an analysis of UML models of business applications and corresponding configuration data in terms of their relevance for security policies and compliance requirements is described by Höhn and Jürjens [29]. However, the main focus of these works does neither lie on control monitoring nor on visualization.

Some works use model checking technology in a compliance management context. For example Awad and Weske [30] use BPMN-Q queries and anti pattern queries to identify violations. However, they want to ensure that business activities are executed in a particular order and do not discuss visualization.

Other works, such as [31] and [32] are technically and thematically related. However, they rather focus on the combination of BPMN or UML models with security policies and do neither directly incorporate the monitoring of controls nor discuss visualization

DOI: 10.1109/DEXA.2010.77

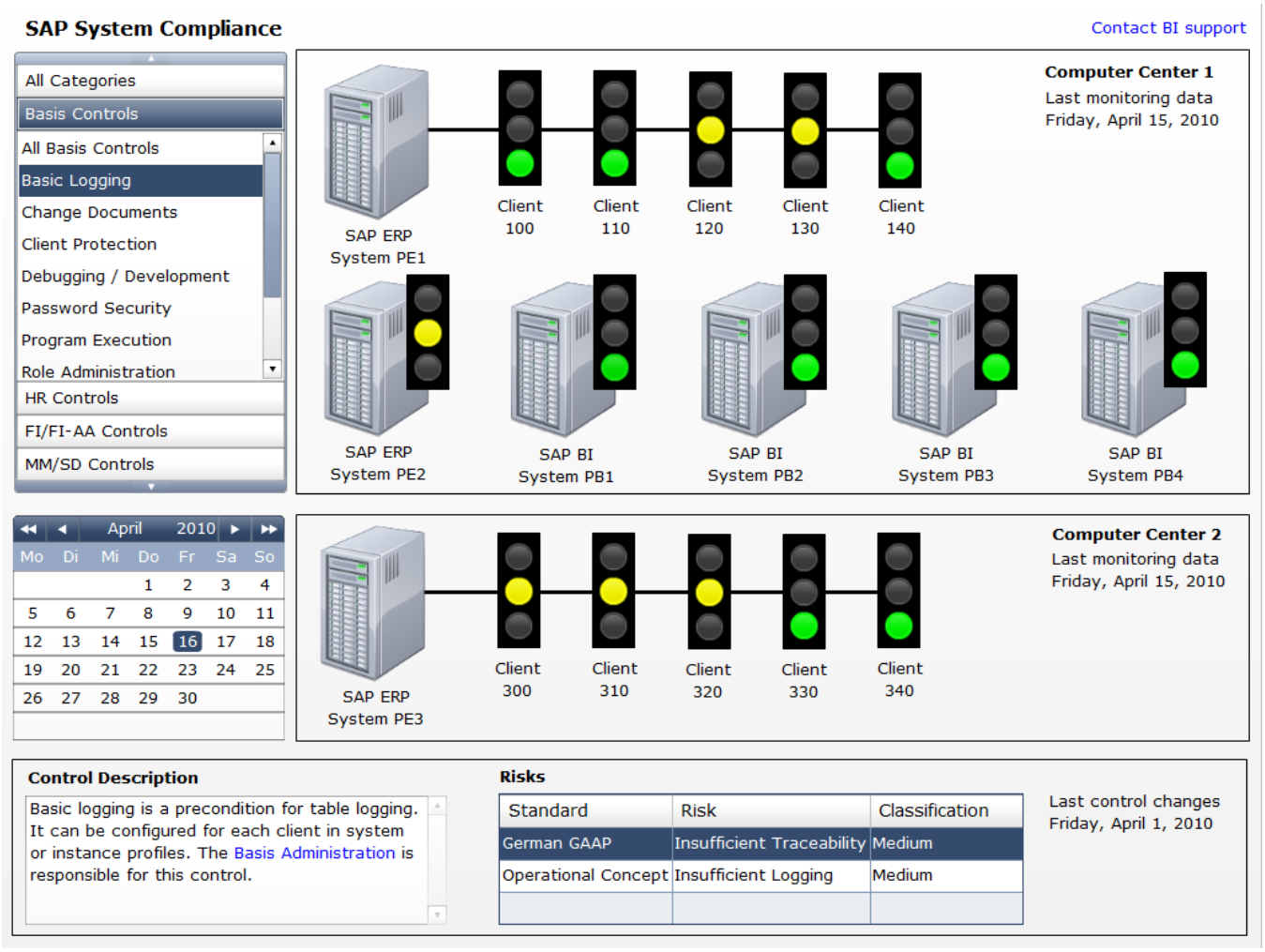

Figure 3. Screenshot of the designed dashboard. It is devoted to the monitoring of compliance for several SAP systems in two different data centers.

Finally, Bellamy, et al. [18] deal with the visualization of compliance processes, in particular regarding the Sarbanes-Oxley Act. However, they do not incorporate an infrastructure for the provision of compliance monitoring data.

VI. Conclusion

The present paper presented ongoing research regarding the visualization of compliance monitoring information. This information is generated by a prototype of an automated compliance monitoring and reporting system and provided to a developed compliance dashboard.

The first phase of dashboard development, the definition of the scope and the basic functionality was successfully completed. The second phase, the population with data, was started with success. This is encouraging, as this second phase turned out to be difficult to realize for many organizations because of their heterogeneous system landscapes [6]. In contrast to this, the prototype allows for a comparatively easy provision of data. In particular, because it solely relies on established standards and existing technologies.

The development and presentation of the compliance dashboard showed that besides the visualization of control exception, the presentation of additional and more detailed information is necessary. Furthermore, the integration of information regarding the financial as well as the legal impacts of control exceptions is an important issue.

Future research will be dedicated to a more sophisticated usability evaluation. Therefore, a corresponding case study will be made. The idea is to evaluate different types of visualization while users accomplishing compliance tasks in real situations.

DOI: 10.1109/DEXA.2010.77

ACKNOWLEDGEMENT

The authors would like to especially thank Dr. Andreas Prieß for the fruitful conversation during the design of the dashboard.

REFERENCES

[1] M. McGreevy, "AMR Research Finds Spending on Governance, Risk Management, and Compliance Will Exceed $32B in 2008," http://www.amrresearch.com/Content/View.aspx?pmillid=21310, 2008.

[2] J. Bace, and C. Rozwell, "Understanding the Components of Compliance," Gartner Report: G00137902, 2006.

[3] R. Agrawal, C. Johnson, J. Kiernan, and F. Leymann, "Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology," Proc. of the 22nd International Conference on Data Engineering (ICDE'06), IEEE Computer Society, 2006, pp. 92-102, doi:10.1109/ICDE.2006.155.

[4] M. E. Kharbili, S. Stein, I. Markovic, and E. Pulvermüller, "Towards a Framework for Semantic Business Process Compliance Management," Proc. of the 1st International Workshop on Governance, Risk and Compliance: Applications in Information Systems (GRCIS'08), vol. 339, June 2008, pp. 1-15.

[5] J. Liebenau, and P. Kärrberg, "International Perspectives on Information Security Practices," London School of Economics and Political Science, McAfee, 2006.

[6] K. Pauwels, T. Ambler, B.Clark, P. LaPointe, D. Reibstein, B. Skiera, B. Wierenga, and T. Wiesel**, "**Dashboards as a Service**,"** Journal of Service Research, vol. 12(2), 2009, pp. 175-189, doi:10.1177/1094670509344213.

[7] M. Kehlenbeck, T. Sandner, and M. H. Breitner, "Application and Economic Implications of an Automated Requirement-Oriented and Standard-Based Compliance Monitoring and Reporting Prototype," Proc. of the 5th International Conference on Availability, Reliability and Security (ARES 2010) , IEEE Computer Society, 2010.

[8] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," MIS Quarterly, vol. 28, no. 1, March 2004, pp. 75-105.

[9] M. Kehlenbeck, T. Sandner, and M. H. Breitner, "Managing Internal Control in Changing Organizations through Business Process Intelligence – A Service Oriented Architecture for the XACML based Monitoring of Supporting Systems," Proc. of the 43th Hawaii International Conference on System Sciences (HICSS 2010), IEEE Computer Society, 2010.

[10] T. Sandner, M. Kehlenbeck, and M. H. Breitner, "An Implementation of a Process-Oriented Cross-System Compliance Monitoring Approach in a SAP ERP and BI Environment," in press.

[11] L. Cranor and S. Garfinkel, "Security and Usability - Designing Secure Systems that People Can Use," O'Reilly Media, August 2005.

[12] S. Card, J. Mackinlay, and B. Shneiderman, "Readings in Information Visualization - Using Vision to Think," Morgan Kaufmann, January 1999.

[13] J. Goodall, "Introduction to Visualization for Computer Security," in Mathematics and Visualization, Springer, 2008, pp.1-17, doi: 10.1007/978-3-540-78243-8.

[14] S. Card, "Information Visualization," in The human-computer interaction handbook, J. Jacko, A. Sears, Eds., Erlbaum, 2003, pp. 544-582.

[15] S. Few, "Dashboard Confusion," March 2004, http://intelligent-enterprise.informationweek.com/showArticle.jhtml?articleID=18300136

[16] S. Few, "Information Dashboard Design - The Effective Visual Communication of Data," O'Reilly, February 2006.

[17] S. Few, "Dashboard Confusion Revisited," March 2007, http://www.perceptualedge.com/articles/visual_business_intelligence/dboard_confusion_revisited.pdf

[18] R. Bellamy, et al., "Seeing is believing: Designing visualizations for managing risk and compliance," IBM Systems Journal, vol. 46(2), 2007, pp. 205-218.

[19] Object Management Group (OMG): Business Process Modeling Notation (BPMN), http://www.bpmn.org/

[20] Workflow Management Coalition (WfMC): XML Process Definition Language (XPDL), http://www.wfmc.org/xpdl.html

[21] Committee of Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework (1992), http://www.coso.org/guidance.htm

[22] Committee of Sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management - Integrated Framework, 2004, http://www.coso.org/guidance.htm

[23] World Wide Web Consortium (W3C): Extensible Markup Language (XML), http://www.w3.org/XML/

[24] Organization for the Advancement of Structured Information Standards (OASIS): eXtensible Access Control Markup Language (XACML), http://www.oasis-open.org/committees/xacml/

[25] R. Swart, "Evaluating Visualization of Security Alerts in Complex Network Environments for Maintenance of Situational Awareness," Proc. Americas Conference on Information Systems (AMCIS 2006), 2006, http://aisel.aisnet.org/amcis2006/519.

[26] OMG: Unified Modeling Language (UML), http://www.uml.org/

[27] X. Wang, Y. Zhang, H. Shi, and J. Yang, "BPEL4RBAC: An Authorisation Specification for WS-BPEL," Web Information Systems Engineering - WISE 2008, Springer, 2008, pp. 381-395, doi:10.1007/978-3-540-85481-4_29.

[28] C. Wolter, A. Schaad, and C. Meinel, "Deriving XACML Policies from Business Process Models," in Proc. WISE 2007 Workshops, LNCS 4832, 2007, pp. 142–153.

[29] S. Höhn and J. Jürjens, "Rubacon: automated support for model-based compliance engineering," in Proc. of the 30th international conference on Software engineering, ACM, NY, 2008, pp. 875-878.

[30] A. Awad and M. Weske, "Visualization of compliance violation using anti-patterns," Business Process Technology Group at Hasso Platter Institute at the University of Potsdam, Tech. Rep. 02-2009, 2009. [Online]. Available: http://bpt.hpi.uni-potsdam.de/pub/Public/BptPublications/VoV.pdf

[31] D. Basin, J. Doser, and T. Lodderstedt, "Model Driven Security for Process-Oriented Systems," Proc. of the eighth ACM Symposium on Access Control Models and Technologies (SACMAT'03), ACM, 2003, pp. 100–109, doi:10.1145/775412.775425.

[32] J. Jürjens, "UMLsec: Extending UML for Secure Systems Development," Proc. of the 5th International Conference on The Unified Modeling Language (UML'02), Springer, 2002, pp. 412–425, doi:10.1007/3-540-45800-X_32.

DOI: 10.1109/DEXA.2010.77

Integrating Knowledge Management and Business Intelligence Using Semantic Middleware and Established Standards

Matthias Kehlenbeck and Michael H. Breitner

Institut für Wirtschaftsinformatik, Leibniz Universität Hannover
{kehlenbeck,breitner}@iwi.uni-hannover.de

Abstract. In order to perform analysis and to create reports, business users often require deep knowledge about the origin and the meaning of data. A significant part of this valuable knowledge is entered into Business Intelligence (BI) applications in the form of definitions and functions as part of the design of queries and reports. But captured knowledge is not made available to Knowledge Management (KM) applications. This paper presents design science research that enables the exchange of this knowledge between different BI and KM applications using established standards as well as its application using a semantic middleware layer. The research contains developed models, procedures and prototypical implementations, all of which have been thoroughly evaluated. **Keywords.** Business Intelligence, Knowledge Management, Semantic Web, OLAP

1 Introduction

Organizations support their employees during decision making by establishing, maintaining and developing applications and processes which enable them to analyze and report on data from various sources. These activities are commonly summarized under the term Business Intelligence (BI). In order to perform sound analyses and to create meaningful reports, business users often require deep knowledge about the origin and the meaning of data. A significant part of this valuable knowledge is entered into BI applications in the form of definitions and functions as part of the design of queries and reports. But captured knowledge is not made available to Knowledge Management (KM) applications. Moreover, knowledge available in KM applications is not directly usable for the design of queries and reports using BI applications. Thus, BI and KM applications are not well integrated with respect to this knowledge.

This paper presents design science research ([1],[2],[3]) concerning the integration of KM and BI using semantic middleware and established standards. It thereby focuses on the knowledge required for the design of queries and reports that can be captured in the form of functions for calculated and/or restricted measures as well as definitions of sets. The research objectives are (1) to enable the exchange of this knowledge between different BI applications using KM and (2) to enable the application of exchanged knowledge. The research results contain developed models, procedures and prototypical implementations, all of which enable:

- The clear separation of business knowledge from implementation details by means of distinct ontologies [Section 3],
- The automatic import of business knowledge from wiki pages into business ontologies [Section 3.1] and the automatic import of implementation details from data warehouse (DW) servers into DW ontologies [Section 3.2],
- The combination of business ontologies and DW ontologies to Online Analytical Processing (OLAP) ontologies by means of mappings and business rules [Section 3.3] as well as semantic reasoning [Section 4],
- The utilization of OLAP ontologies as semantic middleware layers between common DW servers and BI clients by means of a standards-compliant XML for Analysis (XMLA) proxy [Section 5.1],
- Their utilization during the export of business knowledge from BI applications to wiki pages [Section 5.2]).

As business knowledge is clearly separated from implementation details, it may be independently acquired, created, maintained, and transferred. This also increases the independence of queries and reports from DW servers. Differences between DW servers are overcome by the XMLA proxy. This proxy enables the application of exchanged knowledge by establishing a semantic middleware layer.

2 Related Work

This paper can be classified into the research areas BI, KM and Artificial Intelligence (AI). Relations between these research areas have been established in various papers. The following paragraphs outline relevant papers and highlight their similarities and differences.

The integration of BI and KM was discussed by Cody et al. [4]. They argue for a blended BI and KM technology (BIKM) which combines structured data and unstructured text analysis. Nemati et al. discuss the integration of KM, decision support (DS), AI and DW [5]. They argue for a blended KM and DW technology, the knowledge warehouse (KW). Whereas Cody et al. like to enable the same possibilities for text that already exist for structured data, Nemati et al. like to enable them for knowledge. The importance of an integration between BI and KM is stressed by Herschel and Jones [6]. While the papers mentioned above discuss the development of new applications, the present paper improves the integration of already existing BI and KM applications. Because existing BI and KM applications are considered, the paper presents concrete models, procedures and implementations.

An architecture for ontology-based KM was presented by Fensel [7]. This architecture extracts ontologies from text on Web pages. Ontologies are used to capture knowledge. They are a popular research topic of AI and in particular Knowledge Engineering (KE) [8]. A KE approach to KM (KMKE) is presented by Lai [9]. This approach also provides for an inference engine. The present paper does not try to capture knowledge from unstructured text. Knowledge is captured from formal definitions of quantities and objects. However, these structured parts may be contained in otherwise unstructured texts.

BI systems may use information from different sources. Wache et al. present a survey of earlier research regarding the ontology-based integration of information sources [10]. Caires and Cardoso use ontologies to create a virtual view of a set of relational data sources [11]. Users access this virtual view through an XML-based language that is internally converted to SPARQL [12] queries. A similar approach is presented by Spahn et al. [13]. They describe a query designer that uses both a technical ontology and a business ontology to create queries for a set of relational data sources. In contrast to these papers, the present paper provides for the automatic creation of ontologies, focuses on multidimensional data sources and solely relies on standard interfaces and languages. Thus, it requires neither new servers or clients, nor changes to existing ones.
Cao et al. use ontologies to integrate enterprise information systems (EIS), DW systems and reporting systems [14]. They structure knowledge into business ontologies, DW ontologies, and EIS ontologies and map between these ontologies to allow for queries. However, they do provide detail how queries may be created.
A framework that enhances traditional OLAP with semantic functionality was presented by Sell et al. [15]. They distinguish between a domain ontology that contains classes and properties regarding the business domain and a BI ontology that maps these classes and properties to data sources. Business rules and inference are also supported. The client and server tools communicate through an XML-based protocol. However, the present paper also provides for the automatic creation of ontologies, solely relies on standard interfaces and languages and is therefore compatible with existing client and server tools.
Ontologies and inference are also used for the design of extract, transform and load (ETL) processes by Skoutas and Simitsis [16] and the design of DWs by Romero and Abell [17]. Finally, Diamantini and Potena report on the semantic annotation of OLAP cubes [18].
The present paper extensively broadens and deepens research that was previously published as research-in-progress [19]. The research is now considered complete.

3 Ontology Creation

BI systems are fact-based Decision Support Systems (DSS) [20]. Fact-based decision making can be supported and improved using DW systems [21]. Thus, BI systems commonly use data from DW systems. Business and data warehousing are different domains. Insufficient separation between these domains impairs the applicability and exchangeability of information [19]. Therefore, the entities and relations of the business domain and the DW domain are mapped to distinct ontologies. Business entities and their relations are only mapped to the business ontology, and DW entities and their relations are only mapped to the DW ontology. However, the two ontologies are combined by the mapping ontology. The creation of the business ontology, DW ontology, and mapping ontology is continuously supported by a complete tool chain, as illustrated in Fig. 1. The following subsections provide details about both the creation and the corresponding tools.

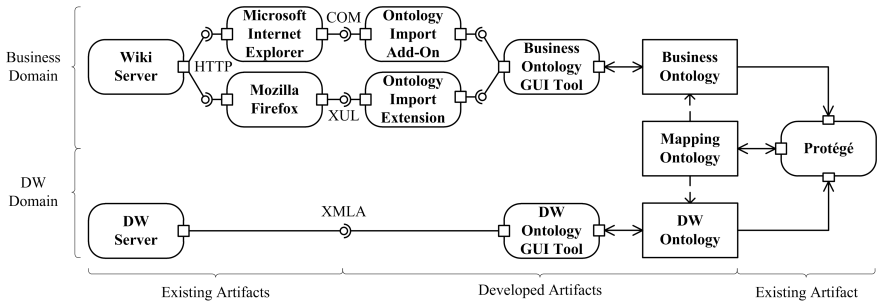

Fig. 1. Complete tool chain for the creation of a business ontology, DW ontology and mapping ontology as a combined UML component and activity diagram.

3.1 Business Ontology

The business ontology is based on the classes *function*, *definition*, *term*, *operator*, *quantity*, *object*, *interval*, *set*, and *constant*. Functions return exactly one quantity, have exactly one calculation term and may have one restriction term that constrains the domain of application. Definitions apply to exactly one object and possess exactly one restriction term. Terms may use one operator. If a term uses an operator, it must have at least one other term as an operand. If a term uses no operator, it is a quantity, object, interval, set, or constant. Intervals possess exactly one constant as their lower bound and exactly one constant as their higher bound. Sets may possess an arbitrary number of constants as their elements. Constants have exactly one type and contain a value. Operators, quantities, objects, intervals, and sets are uniquely identified by their name. Fig. 2 illustrates the classes and properties in the business ontology.

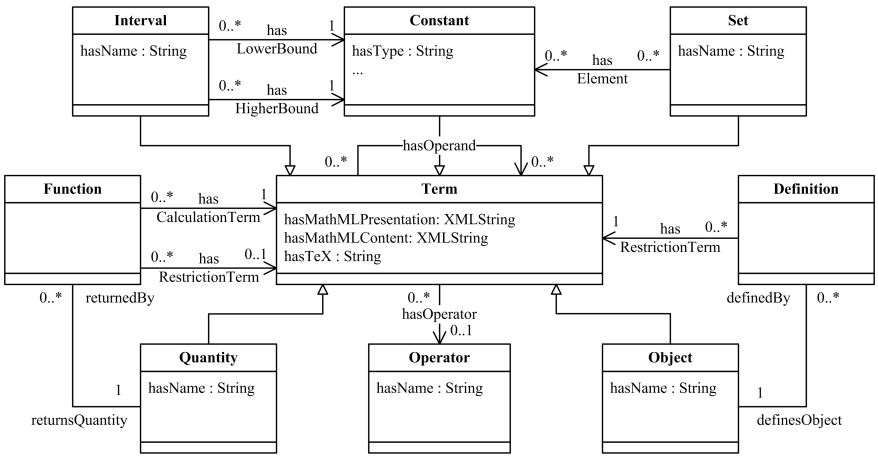

Fig. 2. UML class diagram of the classes and properties in the business ontology.

The classes and properties of the business ontology are described using the Web Ontology Language (OWL) [22]. OWL supports the generalization/specialization of properties and different property types. These features are used to model the roles of operands and terms. In particular, the transitive property *dependsOn* is super property of the properties *hasOperand* and *hasTerm*. The property *hasOperand* is super property of more specialized properties like *hasDividend* or *hasDivisor* and the property *hasTerm* is super property of the properties *hasCalculationTerm* and *hasRestrictionTerm*.

Although OWL is a powerful knowledge representation language, it does not focus on mathematical information. To increase interoperability, terms can also be described using MathML [23] and/or TeX [24] expressions. MathML can be embedded into any Extensible Markup Language (XML) documents, such as office documents or Web pages, and is easy to process for computers. TeX can be embedded into any text documents, and is easy to handle for users.

The creation of the business ontology is supported by the Business Ontology GUI Tool developed by the authors. This tool can be integrated into Microsoft Internet Explorer by the Ontology Import Add-On and integrated into Mozilla Firefox by the Ontology Import Extension, both of which were also developed by the authors. The Business Ontology GUI Tool enables the import of functions and definitions from wiki pages into the business ontology. Wikis facilitate the easy creation of content and its subsequent discussion. They are widely-used for collaborative websites, in corporate intranets, and in KM systems [25]. The Business Ontology GUI Tool allows business users to import functions and definitions that are described directly in the text (plain text content) or inside math tags (TeX content). Both content types are processed by developed parsers. First, plain text content is parsed to TeX, then TeX content is parsed to MathML and finally MathML content is transformed to OWL. Functions and definitions imported from a wiki page refer to terms. These terms may be new to the business ontology or they may already exist there. As content from different sources may vary in its context and underlying concept, business users have to decide, if imported terms share a meaning with existing terms. This knowledge is captured by means of corresponding OWL axioms.

The implementation of the Business Ontology GUI Tool has been developed in Java. It uses the ANTLR [27] parser generator, the JEuclid [28] MathML rendering solution, and the OWL API [29] OWL library. The Ontology Import Add-On has been implemented in C# and the Ontology Import Extension has been implemented in JavaScript. The tool, the add-on and the extension have been successfully evaluated using several manually created wiki pages und using pages with data from two SAP NetWeaver Business Intelligence (SAP BI) [26] systems. These SAP BI systems are used for analysis and reporting by two large organizations. Together, business users defined 183 restricted measures, 1,090 restricted dimensions, 1,080 restricted tuples of dimensions and 11,974 ranges in these systems. Due to the large number of definitions, their exchange would be very time consuming without tool support. Fig. 3 shows a screenshot of the Business Ontology GUI Tool.

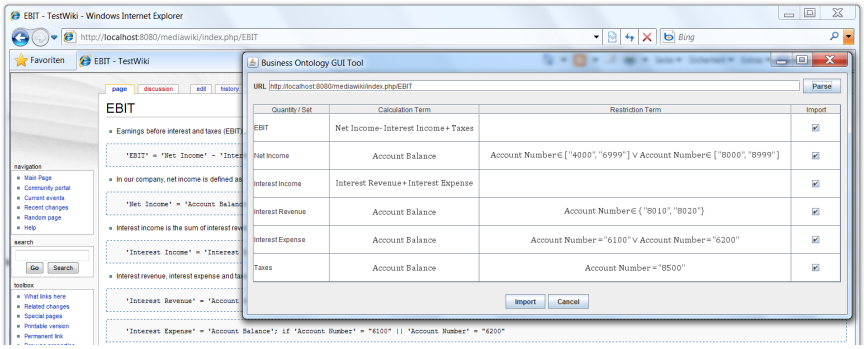

Fig. 3. The Business Ontology GUI Tool, integrated into Microsoft Internet Explorer by an Add-On. The tool imports definitions and functions, in particular from wikis.

The Business Ontology GUI Tool converts the calculation terms of functions into OWL individuals, and the restriction terms of functions and definitions into both OWL individuals and OWL classes. OWL individuals are defined as instances of the model illustrated in Fig. 2, while OWL classes are defined using OWL class expressions. Both representations suit a particular purpose. These purposes are described in the next section.

3.2 Data Warehouse Ontology

The DW ontology is based on the classes *system*, *cube*, *measure*, *dimension*, *hierarchy*, and *level*. Systems possess an XMLA Web service endpoint and an arbitrary number of cubes. Cubes belong to a catalog and a data source, have at least one measure and at least one dimension. Dimensions have an arbitrary number of hierarchies, and hierarchies have an arbitrary number of levels. Individuals are uniquely identified by their identifier. Fig. 4 illustrates the classes and properties in the business ontology.

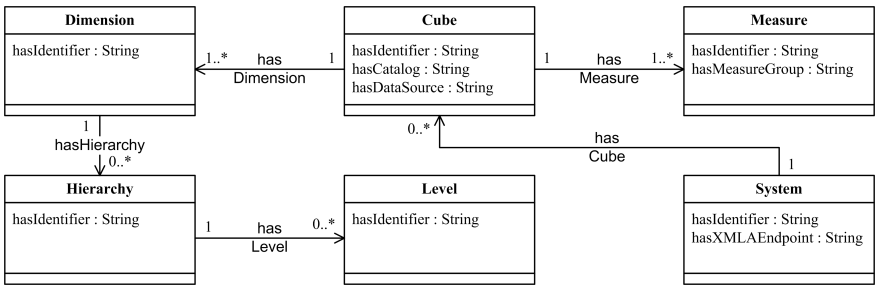

Fig. 4. UML class diagram of the classes and properties in the DW ontology.

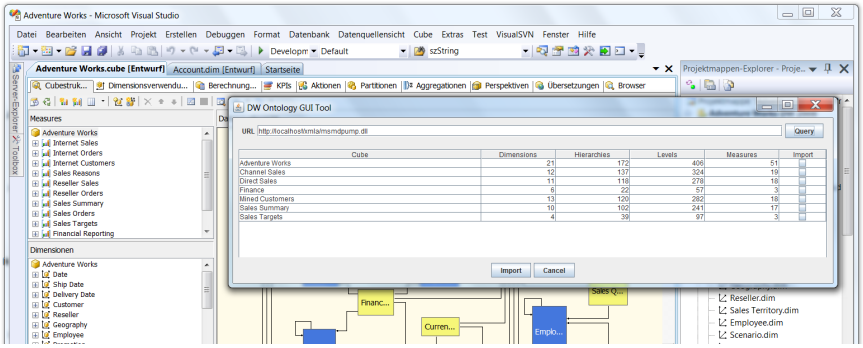

Fig. 5. Screenshot of the DW Ontology GUI Tool, integrated into Microsoft SQL Server BI Development Studio. The tool imports DW metadata from XMLA providers.

The creation of the DW ontology is supported by the developed DW Ontology GUI Tool. This tool enables the import of cubes, hierarchies, levels and measures from XMLA providers like Microsoft Analysis Services [30], Pentaho Analysis Services [31] or SAP BI into the DW ontology. All entities are converted to OWL individuals. The tool can be easily integrated into BI/DW development tools, such as the Microsoft SQL Server BI Development Studio.
The DW Ontology GUI Tool has been implemented in Java and uses the Apache CXF Web services framework [32] and the OWL API. It has been successfully evaluated using data from the two SAP BI systems and data from the Microsoft Analysis Services AdventuerWorks DW sample database. Fig. 5 shows a screenshot of the DW Ontology GUI Tool.

3.3 Mapping Ontology

The mapping ontology combines the business ontology with the DW ontology, thus enabling the use of these ontologies for OLAP. It is based on the symmetric object property $isMappedTo$. This property is used to map quantities to measures and objects to dimensions, hierarchies, or levels. The mappings can either be performed manually, or can be inferred automatically using Semantic Web Rule Language (SWRL) [33] rules. As an example, SAP BI does neither differentiate between quantities and measures nor between objects and dimensions. This behavior may be described by the SWRL rules:

- $Quantity(?q) \wedge hasName(?q, ?u) \wedge Measure(?m) \wedge hasIdentifier(?m, ?i) \wedge substringAfter(?u, ?i, \text{"'Measures'->"'}) \rightarrow isMappedTo(?q, ?m)$
- $Object(?o) \wedge hasName(?o, ?w) \wedge Dimension(?d) \wedge hasIdentifier(?d, ?j) \wedge equal(?w, ?j) \rightarrow isMappedTo(?o, ?d)$

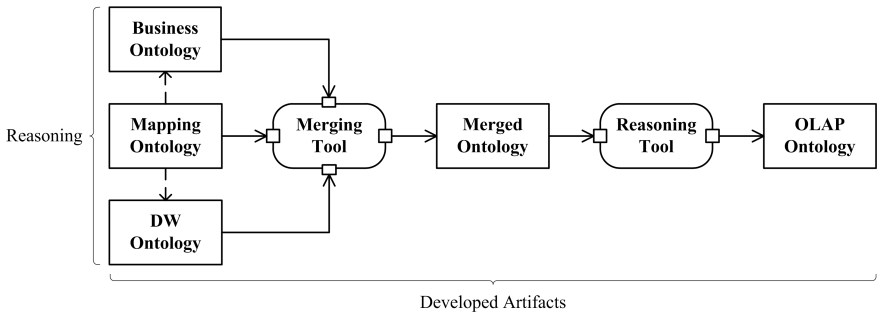

Fig. 6. Complete tool chain for the creation of the merged ontology and the OLAP ontology based on the business ontology, DW ontology and mapping ontology.

SWRL can be used to define much more sophisticated mapping rules. Mapping rules can also link a single business ontology to multiple DW ontologies. Therefore, the same business knowledge may be applied to different DW systems, e.g. systems from different companies, organizations, or departments. This is particularly helpful for corporate groups, consulting companies, or mergers and acquisitions, as it enables consistent analyses and reports from DW systems with different contexts and/or multidimensional models. Moreover, reference ontologies and semantic reasoners may be used to enable this in real time. The Protégé ontology editor [35] can be used to create the mapping ontology.

4 Ontology Inference

OWL ontologies can be used in conjunction with semantic reasoners to infer knowledge that is implicitly contained but not explicitly asserted. To enable this inference, the business ontology, the DW ontology and the mapping ontology are first merged into a single ontology. Afterwards, the merged ontology is passed to a semantic reasoner which then infers the implicitly contained knowledge and stores the inferred axioms together with the asserted axioms in the OLAP ontology. The creation of the merged ontology as well as the OLAP ontology is continuously supported by a complete tool chain as illustrated in Fig. 6. Details on the creation and the corresponding tools are provided in the following.

4.1 Merged Ontology

In order to increase reusability, the business ontology, DW ontology and mapping ontology are each able to import other (sub) ontologies. For example, the business ontology can be structured into department-independent and department-specific parts, or the DW ontology can be structured into system independent and system-specific parts. The knowledge from these ontologies can be merged into a single ontology by the Merging Tool. The Merging Tool was implemented in Java and uses the OWL API. The merged ontology forms the input for the Reasoning Tool, which is described in the next subsection.

4.2 OLAP Ontology

Based on the merged ontology, the Reasoning Tool creates the OLAP ontology. The Reasoning Tool performs three different types of inference, it:

1. Infers the results of the included SWRL rules
2. Infers which cubes are able to provide which quantities and objects by which functions and definitions
3. Infers the hierarchy of restrictions

The results of the included SWRL rules can be directly inferred by a semantic reasoner. However, some additional axioms are required to infer which cubes are able to provide which quantities and objects. The Reasoning Tool:

- Adds the object property $supportsDefinition$ and its inverse $isDefinitionSupportedByCube$
- Adds the object property $supportsFunction$ and its inverse $isFunctionSupportedByCube$
- Adds the object property $isAbleToProvideObject$, its inverse $isObjectAvailableForCube$ and the property chains:
  - $hasDimension \circ isMappedTo \rightarrow isAbleToProvideObject$
  - $supportsDefinition \circ definesObject \rightarrow isAbleToProvideObject$
- Adds the object property $isAbleToProvideQuantity$, its inverse $isQuantityAvailableForCube$ and the property chains:
  - $hasFact \circ isMappedTo \rightarrow isAbleToProvideQuantity$ and
  - $supportsFunction \circ returnsQuantity \rightarrow isAbleToProvideQuantity$
- Adds a new class of definitions `D` and a new class of functions `F` for each cube `C`. Class `D` contains the class of definitions and class `F` contains the class of functions that are supported by the cube `C`.

In Manchester Syntax [34], `D` and `F` can be described as subclasses of `isSupportedByCube value C` and as equivalent to the class expression `Definition and dependsOn only ((not Object) or (isObjectAvailableForCube value C))` respectively `Function and dependsOn only ((not Object and not Quantity) or (isObjectAvailableForCube value C) or (isQuantityAvailableForCube value C))`. As the previous mentioned axioms make use of the universal quantifier (`only`), a semantic reasoner that makes the Open World Assumption (OWA) requires some additional closure axioms. The Reasoning Tool:

- Enumerates all instances of the classes object and quantity
- Complements all instances of class definition with negative object property assertions for all objects that the instances do not depend on
- Complements all instances of class function with negative object property assertions for all objects and quantities that the instances do not depend on.

The hierarchy of restrictions is inferred from restriction term classes. Although the corresponding class expressions can be very complex, there are some simple examples. The function Interest Revenue = Account Balance, if Account Number

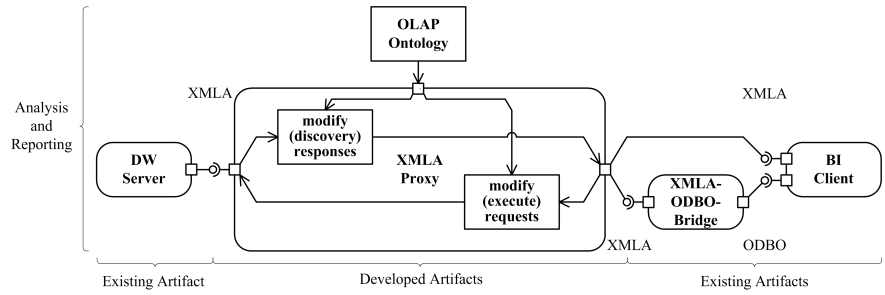

Fig. 7. Utilization of the OLAP ontology by the XMLA Proxy.

$\in$ {"8010","8020"} contains the restriction term Account Number $\in$ {"8010", "8020"}. Using the additional OWL class *Instance* and the additional object property *hasInstance*, the OWL class corresponding to this restriction term can be described as the equivalent of the class expression `RestrictionTerm and restrictsObject some (Object and hasInstance some (Instance and hasValue some string[pattern '8010|8020']) and hasName value 'Account Number')`. Based on such class expressions, a semantic reasoner can infer which classes are different from others, equal to others or sub/super classes of others. The Reasoning Tool has been implemented in Java and uses the OWL API, the Pellet reasoner [36] and the Hermit reasoner [37]. It has been evaluated using data from the two SAP BI systems and successfully infered the corresponding axioms. This inferred knowledge is utilized in the next section.

5 Ontology Utilization

The inferred knowledge in the OLAP ontology can be used for the automatic provision of objects and quantities, and for tool-supported review of definitions, amongst others. The following subsections provide details on this.

5.1 Automatic Provision of Objects and Quantities

The OLAP ontology contains the knowledge as to whether an object or a quantity is available for a cube and how an available object or quantity can be provided. The XMLA Proxy developed here uses the OLAP ontology as a semantic middleware layer and automatically provides these objects and quantities. It is compatible with DW servers and BI clients that support XMLA. However, it can also be used with BI clients that support OLE DB for OLAP (ODBO), as an ODBO to XMLA bridge exists [38]. To achieve a transparent provision, the proxy engages in the communication between DW servers and BI clients. In particular, the responses to XMLA discovery requests and the parameters of XMLA execute requests are modified. Fig. 7 illustrates the utilization of the OLAP ontology by the XMLA Proxy.

XMLA discovery requests possess a request type, a property list, and a restriction list. The responses to these requests contain the corresponding metadata. For certain request types, the XMLA Proxy complements this metadata. This means that the entities from the OLAP ontology are provided additionally to the already existing entities of a cube. To the BI client, these additional entities look like already existing entities.
XMLA execute requests possess a command and a property list. The responses to these requests contain the corresponding data. Among others, commands can be Multidimensional Expressions (MDX) [39] queries. The XMLA Proxy complements MDX queries with definitions and functions for the additionally provided entities. Thereby, additionally provided entities can be used like already existing entities. The MDX for the additionally provided objects and quantities is created as follows:

- Objects mapped to dimensions/hierarchies/levels or defined by supported definitions are converted to named sets.
- Quantities mapped to measures or returned by supported functions are converted to calculated members.

Definitions and functions are used to build corresponding expression trees. Mappings are only required for the leaf nodes of these expressions trees. The trees are traversed in postorder and converted to textual representations. These textual representations are then passed on to a template engine to create MDX. The developed templates provide context-sensitive aggregation of quantities that depend on restriction terms. As an example, a quantity $\mathcal{Q}$ may be returned by a function $\mathcal{F}$ that possesses a calculation term $\mathcal{P}$ and a restriction term $\mathcal{R}$. $\mathcal{R}$ restricts the objects A, B, and C by the expression E. The same restriction is performed by the function *restrict*. Due to $\mathcal{R}$, $\mathcal{F}$ has a domain of application $D = A \times B \times C$, if E also known as $D = restrict(A \times B \times C)$. The current MDX member M influences the aggregation of $\mathcal{Q}$:

- If $M \notin restrict(A \times B \times C)$: $\mathcal{Q}$ can be aggregated over the elements of $restrict(A \times B \times C)$.
- If $M \notin restrict(a \times b)$ and $M \in restrict(c)$ and $a, b, c \in \{A, B, C\}$ and $a \neq b \neq c$: $\mathcal{Q}$ can be aggregated over the elements of $restrict(a \times b)$, but not over the elements of $restrict(c)$. $\mathcal{Q}$ contains an unaggregated value for all elements of $restrict(c)$ that satisfy E.
- If $M \notin restrict(a)$ and $M \in restrict(b \times c)$ and $a, b, c \in \{A, B, C\}$ and $a \neq b \neq c$: $\mathcal{Q}$ can be aggregated over the elements of $restrict(a)$, but not over the elements of $restrict(b \times c)$. $\mathcal{Q}$ contains an unaggregated value for all elements of $restrict(b \times c)$ that satisfy E.
- If $M \in restrict(A \times B \times C)$: $\mathcal{Q}$ cannot be aggregated. $\mathcal{Q}$ contains an unaggregated value for all elements of $restrict(A \times B \times C)$ that satisfy E.

To summarize, the quantity is solely aggregated over the restricted objects that do not contain the current MDX member. This procedure can be easily adapted for less or more than three objects.

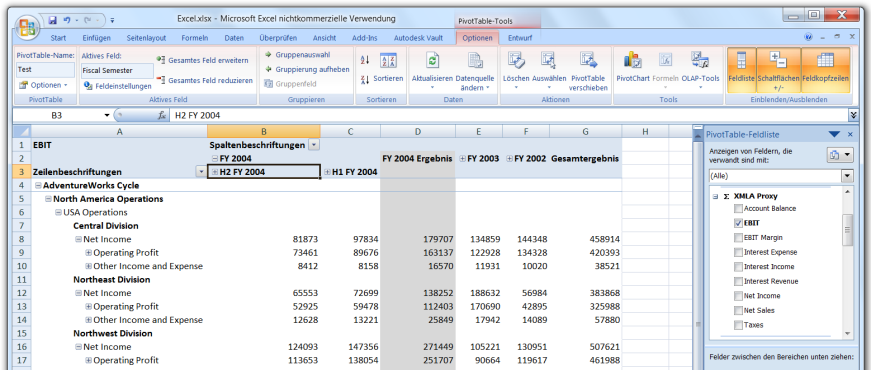

Fig. 8. MS Excel connected to MS Analysis Services through the XMLA Proxy and an ODBO bridge. Additionally provided entities may be used just like original entities.

The XMLA Proxy has been implemented in Java and uses Apache CXF, the OWL API and the StringTemplate template engine [40]. It has been successfully evaluated with the DW servers Microsoft Analysis Services, Pentaho Analysis Services and SAP BI as well as the BI clients IBM DataQuant and Microsoft Excel. Although some additional processing is required, performance differences are barely noticeable. Fig. 8 shows a screenshot of Microsoft Excel connected to Microsoft Analysis Services through the XMLA Proxy and an ODBO bridge.

5.2 Tool-Supported Review of Definitions

In real life environments, business users frequently add new calculated measures and named sets to their systems. These measures and sets are used by other measures and sets, in part by different business users and potentially in entirely different contexts. This harbors a high risk of errors and may lead to a virtually unmanageable network of measures and sets.

As described in the last section, the relationships between different definitions can be inferred by semantic reasoning. In particular, it is possible to discover generalizations/specializations as well as equivalence and non-equivalence relationships. However, it is not very suitable to present the discovered knowledge to business users in the form of OWL axioms. Instead, these axioms have to be transformed into plain speech.

Based on the OLAP ontology, the Definition Tool renders the hierarchy of restriction terms to a wiki page. The tool structures the restriction terms into a sorted tree. Equivalent restriction terms are displayed in the same node and expressions are presented in a readable form. These actions considerably increase comprehensibility and thereby enable business users to efficiently identify inconsistent, redundant or simply false definitions. The chance to efficiently identify these problems also enables regular reviews, which may reduce risk of errors and increase manageability.

The calculation terms contained in the OLAP ontology were exported to a wiki page, as well. However, corresponding equivalence or non-equivalence relationships were not inferred, as this would require symbolic reasoning techniques rather than semantic reasoning techniques. These symbolic reasoning techniques are beyond the scope of this paper.
The Definition Tool has been implemented in Java and uses the OWL API and the OWL2Prefuse [41] graph and tree library. The tool has been successfully evaluated using data from the two SAP BI systems.

6 Conclusion

This paper has presented design science research concerning the integration of KM and BI. It has focused on the exchange of valuable knowledge regarding definitions and functions for objects and quantities which are used for analyses and reports. The research results contain developed models, procedures and prototypical implementations, all of which enable the exchange of this knowledge between different BI and KM applications using established standards as well as its application using a semantic middleware layer.
The exchange is enabled by the clear separation of business knowledge from DW metadata. Both are only combined for OLAP. The developed tools support the import of business knowledge from wiki pages, the import of DW metadata from DW servers as well as the combination of business knowledge with DW metadata. This combination involves mappings and business rules as well as semantic reasoning. Semantic reasoning is also used to support users identifying inconsistent, redundant or simply false definitions.
The application is enabled by the developed XMLA Proxy. The XMLA Proxy engages in the communication between DW servers and BI clients. Based on the exchanged definitions and functions, the proxy automatically provides additional entities. These entities may be used just like original entities. The proxy solely relies on standard interfaces and languages. Thus, it requires neither new servers or clients, nor changes to existing ones.
The developed models and procedures have been detailed. The provided information should be sufficient for the reconstruction of the developed implementations. These implementations have been evaluated. The gathered evidence supports the feasiblity of the approach. This approach is not limited to wiki pages and XMLA. It can be generalized to other document types and interface standards. Moreover, the approach can be extended by symbolic reasoning techniques as well as other metadata types, e.g. variables, queries and permissions.

References

1. Hevner, A. R., March, S. T., Park, J., Ram, S.: Design Science in Information Systems Research, in: MIS Quaterly 28 (2004), 1, 75-106.
2. Vaishnavi, V., Küchler, W.: Design Research in Information Systems, Januar 20, 2004, last updated August 16, 2009. URL `http://desrist.org/design-research-in-information-systems`.

3. Hevner, A., Chatterjee, S.: Design Research in Information Systems, Berlin: Springer, 2010.
4. Cody, W. F., Kreulen, J. T., Krishna, V., Spangler, W. S.: The Integration of Business Intelligence and Knowledge Management, in: IBM Systems Journal 41 (2002), 4, 697-713.
5. Nemati, H. R., Steiger, D. M., Iyer, L. S., Herschel, R. T.: Knowledge Warehouse: An Architectural Integration of Knowledge Management, Decision Support, Artificial Intelligence and Data Warehousing, in: Decision Support Systems 3 (2002), 2, 143-161.
6. Herschel, R. T., Jones, N. E.: Knowledge Management and Business Intelligence: The Importance of Integration, in: Journal of Knowledge Managment 9 (2005), 4, 45-55.
7. Fensel, D.: Ontology-Based Knowledge Management, in: Computer 35 (2002), 11, 56-59.
8. Studer, R., Benjamins, V. R., Dieter, F.: Knowledge Engineering: Principles and Methods, in: Data and Knowledge Engineering 25 (1998), 1-2, 161-197.
9. Lai, L. F.: A Knowledge Engineering Approach to Knowledge Management, in: Information Sciences 177 (2007), 19, 4072-4094.
10. Wache, H., Vgele, T. H., Visser, U., Stuckenschmidt, H., Schuster, G., Neumann, H., Hbner, S.: Ontology-based Integration of Information - A Survey of Existing Approaches, in: Proceedings of the International Joint Conference on Artificial Intelligence 2001 Workshop: Ontologies and Information Sharing, August 4-10, 2001, Seattle, Washington, USA.
11. Caires, B., Cardoso, J.: Using Semantic Web Technologies to Build Adaptable Enterprise Information Systems, in: International Journal of Interoperability in Business Information Systems, 1 (2006), 3, 41-58.
12. World Wide Web Consortium (W3C): SPARQL Query Language for RDF, W3C Recommendation 15 January 2008. URL `http://www.w3.org/TR/rdf-sparql-query`.
13. Spahn, M., Kleb, J., Grimm, S., Schneidl, S.: Supporting Business Intelligence by Providing Ontology-Based End-User Information Self-Service, in: Proceedings of the First International Workshop on Ontology-Supported Business Intelligence, October 26-27, 2008, Karlsruhe, Germany.
14. Cao, L., Zhang, C., Jiming, L.: Ontology-Based Integration of Business Intelligence, in: Web Intelligence and Agent Systems 4 (2006), 3, 313-325.
15. Sell, D., Silva, D. C., Beppler, F. D., Napoli, M., Ghisi, F. B., Pacheco, R. C. S., Todesco, J. L.: SBI: A Semantic Framework to Support Business Intelligence, in: Proceeding of the First International Workshop on Ontology-Supported Business Intelligence, October 26-27, 2008, Karlsruhe, Germany.
16. Skoutas, D., Simitsis, A.: Designing ETL Processes Using Semantic Web Technologies, in: Proceedings of the 9th ACM International Workshop on Data Warehousing and OLAP, November 10, 2006, Arlington, Virginia, USA.
17. Romero, O., Abell, A.: Automating Multidimensional Design from Ontologies, in: Proceedings of the ACM Tenth International Workshop on Data Warehousing and OLAP, November 9, 2007, Lisbon, Portugal.
18. Diamantini, C., Potena, D.: Semantic Enrichment of Strategic Datacubes, in: Proceedings of the ACM 11th International Conference on Data Warehousing and OLAP, October 30, 2008, Napa Valley, California, USA.
19. Kehlenbeck, M., Breitner, M. H.: Ontology-Based Exchange and Immediate Application of Business Calculation Definitions for Online Analytical Processing, In:

Proceedings of the 11th International Conference on Data Warehousing and Knowledge Discovery, August 11 - September 2, Linz, Austria.
20. Power, D. J.: Decision Support Systems: A Historical Overview, in: Burstein, F., Holsaple, C. W. (Eds.): Handbook on Decision Support Systems, Berlin: Springer, 2008.
21. Power, D. J.: Decision Support Systems: Frequently Asked Questions, New York: Universe Inc., 2004.
22. World Wide Web Consortium (W3C): OWL 2 Web Ontology Language Document Overview, W3C Recommendation 27 October 2009. URL http://www.w3.org/TR/owl2-overview/.
23. World Wide Web Consortium (W3C): Mathematical Markup Language (MathML) Version 2.0 (Second Edition), W3C Recommendation 21 October 2003. URL http://www.w3.org/TR/MathML/.
24. Knuth, D. E.: The TEXbook, Reading: Addison-Wesley, 1986.
25. Wikimedia Foundation Inc.: Wiki, accessed April 1, 2010. URL http://en.wikipedia.org/wiki/Wiki.
26. SAP: SAP NetWeaver Business Intelligence, accessed April 1, 2010. URL http://www.sap.com/usa/services/education/catalog/netweaver/bi.epx.
27. Parr, T. J., Quong, R. W.: ANTLR: A Predicated-LL(k) Parser Generator, in: Software - Practice & Experience 25 (1995), 7, 789-810.
28. The JEuclid Project: About JEuclid, accessed April 1, 2010. URL http://jeuclid.sourceforge.net/index.html.
29. Horrdige, M., Bechhofer, S.: The OWL API: A Java API for Working with OWL 2 Ontologies, in: Proceedings of the 5th International Workshop on OWL: Experiences and Directions, October 23-24, 2009, Chantilly, Virginia, USA.
30. Microsoft Corp.: SQL Server 2008: Analysis Services, accessed April 1, 2010. URL http://www.microsoft.com/sqlserver/2008/en/us/analysis-services.aspx.
31. Pentaho Corp: Pentaho Analysis Services (Mondrian), accessed September 22, 2010. URL http://mondrian.pentaho.com.
32. The Apache Software Foundation: Apache CXF: An Open Source Service Framework, accessed April 1, 2010. URL http://cxf.apache.org.
33. World Wide Web Consortium (W3C): A Semantic Web Rule Language Combining OWL and RuleML, W3C Member Submission 21 May 2004. URL http://www.w3.org/Submission/SWRL.
34. World Wide Web Consortium (W3C): OWL 2 Web Ontology Language Manchester Syntax, W3C Working Group Note 27 October 2009. URL http://www.w3.org/TR/owl2-manchester-syntax.
35. Stanford University: The Protégé Ontology Editor and Knowledge Acquisition System, accessed September 22, 2010. URL http://protege.stanford.edu.
36. Clark & Parsia: Pellet, accessed April 1, 2010. URL http://clarkparsia.com/pellet.
37. University of Oxford: Hermit OWL Reasoner, accessed April 1, 2010. URL http://hermit-reasoner.com/.
38. Simba: OLE DB for OLAP (ODBO) to XMLA Adapter Bridge, accessed April 1, 2010. URL http://www.simba.com/odbo-to-xmla.htm.
39. Microsoft Corp.: MDX Query Fundamentals (MDX), accessed April 1, 2010. URL http://msdn.microsoft.com/en-us/library/ms145514%28v=SQL.100%29.aspx.
40. Parr, T.: StringTemplate Template Engine, accessed April 1, 2010. URL http://www.stringtemplate.org.
41. Borsje, J., Jonathan, G.: OWL2Prefuse - An OWL to Prefuse converter, accessed April 1, 2010. URL http://owl2prefuse.sourceforge.net/index.php.

Ein modellunabhängiges und ontologiebasiertes Informationssystem zur Überwachung automatisierter Kontrollen in heterogenen Systemlandschaften

Matthias Kehlenbeck
Leibniz Universität Hannover
kehlenbeck@iwi.uni-hannover.de

Michael H. Breitner
Leibniz Universität Hannover
breitner@iwi.uni-hannover.de

ZUSAMMENFASSUNG

Organisationen betreiben interne Kontrollsysteme, um einen effektiven und effizienten Ressourceneinsatz, eine zuverlässige Finanzberichterstattung und einen gesetzeskonformen Betrieb sicherzustellen. Diese Organisationen haben ein Interesse an Informationssystemen zur Unterstützung des Managements interner Kontrollsysteme. Die Wissenschaft beschäftigt sich bisher wenig mit der Gestaltung entsprechender Informationssysteme. Dabei stellt die Heterogenität der Prozessabläufe, Kontrollumfelder und Systemlandschaften besonders hohe Anforderungen an die Flexibilität entsprechender Software. So kann Software zur Überwachung von Kontrollen in Systemen nur dann allgemein eingesetzt werden, wenn sie flexibel auf unterschiedlichste Modelle und Abläufe eingehen kann.

Der vorliegende Aufsatz präsentiert Verfahren, mit deren Hilfe die Implementierung automatisierter Kontrollen in unterschiedlichen Systemen einheitlich überwacht werden kann. Diese Verfahren wurden als Webservices innerhalb einer Service-Orientierten Architektur implementiert. Für die Evaluation des Prototyps in einer Fallstudie wurde ein produktives SAP-System mit mehreren Mandanten verwendet. Der Prototyp kann jedoch systemunabhängig eingesetzt werden. So kann der vorhandenen Heterogenität in realen Organisationen, System- und Prozesslandschaften Rechnung getragen werden.

Schlüsselwörter

Interne Kontrollsysteme, IT-Compliance, Risikomanagement, Ontologien, Service-Orientierte Architektur

1. EINLEITUNG

Organisationen betreiben interne Kontrollsysteme, um einen effektiven und effizienten Ressourceneinsatz, eine zuverlässige Finanzberichterstattung und einen gesetzeskonformen Betrieb sicherzustellen [1]. Zum Management des internen Kontrollsystems gehören der Entwurf und die Umsetzung von Kontrollverfahren, welche die fortlaufende Durchführung der Kontrollen sowie die zeitgerechte Kommunikation identifizierter Kontrollausnahmen sicherstellen. Zu den Kontrollverfahren gehören die periodische Beurteilung der Kontrollen durch Revisoren, die fortlaufende Überwachung durch entsprechende Software sowie die Analyse mit Hilfe geeigneter Berichte [2]. Die Pflege und Überwachung der Kontrollen ist eine komplexe, zeitaufwendige und häufig manuelle Aufgabe [3][4]. Dennoch ist die zeitgerechte Kommunikation von Kontrollausnahmen wesentlich für den Erfolg eines internen Kontrollsystems [5].

Organisationen haben ein Interesse an Informationssystemen zur Unterstützung des Managements interner Kontrollsysteme. Die Wissenschaft beschäftigt sich bisher wenig mit der Gestaltung entsprechender Informationssysteme [6][7][8]. Dabei stellt die Heterogenität der Prozessabläufe, Kontrollumfelder und Systemlandschaften besonders hohe Anforderungen an die Flexibilität entsprechender Software. So verwenden die zu überwachenden Systeme unterschiedliche

- **Prozessmodelle**, unter anderem die Business Process Modeling Notation (BPMN), die Ereignisgesteuerte Prozesskette (EPK) sowie Unified Modeling Language (UML) Aktivitätsdiagramme
- **Kontrollmodelle**, unter anderem das Modell des Committee of Sponsoring Organizations of the Treadway Commission (COSO) sowie die Control Objectives for Information and Related Technology (CobiT)
- **Zugriffskontrollmodelle**, unter anderem Discretionary Access Control (DAC), Mandatory Access Control (MAC) und Role Based Access Control (RBAC).

Ferner gibt es Unterschiede hinsichtlich der Persistenz von Instanzen dieser und anderer Modelle durch verschiedene

- **Datenmodelle**, unter anderem relationale Datenmodelle (SQL) sowie hierarchische Datenmodelle (XML)
- **Datenschemata**, unter anderem XML Schema Definition (XSD) basierte sowie UML basierte Datenschemata.

Schließlich unterliegen die zu überwachenden Systeme unterschiedlichen internen Verarbeitungsabläufen, welche aufgrund kundenseitiger Anpassungen und Einstellungen vom jeweiligen Auslieferungsstandard abweichen können. Folglich kann ein überwachendes System nur dann allgemein eingesetzt werden, wenn es weder bestimmte Modelle, noch bestimmte Abläufe in den zu überwachenden Systemen voraussetzt. Zur Entwicklungszeit sind diese Modelle und Abläufe nicht bekannt. Vielmehr ist flexibel auf die vorhandene Heterogenität einzugehen.

Der vorliegende Aufsatz präsentiert Verfahren, mit deren Hilfe die Implementierung automatisierter Kontrollen in unterschiedlichen Systemen einheitlich überwacht werden können. Dadurch erübrigt sich deren zeitaufwendige und damit kostenintensive manuelle Überwachung. Die Verfahren wurden als Webservices (WS) innerhalb einer Service-Orientierten Architektur (SOA) implementiert und mit Daten aus einem produktiven SAP-System evaluiert.

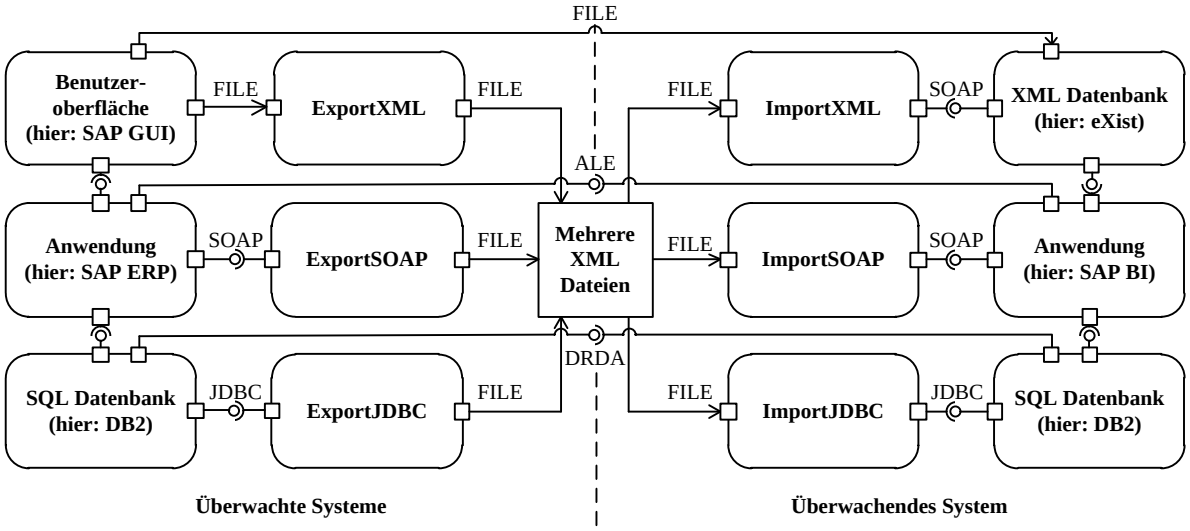

Abbildung 1: Verfahren zum Transfer von Daten aus den überwachten Systemen in das überwachende System als UML-Diagramm. Es unterstützt Standardschnittstellen zum Datenexport und -import auf mehreren softwarearchitektonischen Schichten.

Der übrige Teil des Aufsatzes ist wie folgt gegliedert: Abschnitt 2 präsentiert die relevante Literatur. Abschnitt 3 geht auf den Transfer von Daten aus den überwachten Systemen in das überwachende System ein. Die Konvertierung der transferierten Daten wird in Abschnitt 4 beschrieben. Abschnitt 5 erläutert die Verarbeitung von Daten. Auf den Einsatz und die Evaluation des Prototyps geht Abschnitt 6 ein. Schließlich enthält Abschnitt 7 das Fazit und gibt einen Ausblick.

2. LITERATUR

Syed et al. haben die Veröffentlichungen zum Thema Compliance Management in 13 Wirtschaftsinformatik Zeitschriften zwischen 2001 und 2008 untersucht. Unter den 5633 Beiträgen in diesen Zeitschriften konnten die Autoren 45 zum Thema Compliance Management identifizieren. Etwa dreiviertel der identifizierten Beiträge ist explorativer Natur und bietet keine Lösungen an [6]. Aufgrund des Mangels an Lösungen spricht Julisch von einer Divergenz des Angebotes durch die Wissenschaft und der Nachfrage durch die Wirtschaft [7]. Dabei ist die Nachfrage durch die Wirtschaft dokumentiert. In Bezug auf die fortlaufende Überwachung von Kontrollen gehen Searcy et al. schon früh auf die Motivation, den Nutzen, die Probleme und die Herausforderungen für die vier großen Wirtschaftsprüfungsgesellschaften ein [9].

Accorsi et al. beschäftigen sich mit der Entwicklung eines Frühwarnsystems zur Entdeckung von Verletzungen der Privatsphäre. Die Voraussetzungen für diese Verletzungen werden in einer Richtliniensprache definiert [10]. Eine entsprechende Richtliniensprache präsentieren Sackmann und Kähmer. Obwohl ursprünglich zur Definition von Privacy Richtlinien gedacht, kann diese auch für Compliance Richtlinien verwendet werden. Somit kann sie Teil eines Systems zur Überwachung von Kontrollen sein [11].

Teeter und Brennan unterscheiden zwischen modularer, systemspezifischer und kundenspezifischer Software zur fortlaufenden Überwachung von Kontrollen. Analog zu Alles et al. beschreiben sie eine kundenspezifische Implementierung in einem Unternehmen [11][12].

Eine Komponente zur Identifizierung von Funktionstrennungskonflikten präsentieren Wolf und Gehrke. Sie wurde ursprünglich als systemspezifische Software für SAP Systeme entwickelt und anschließend für weitere ERP Systeme erweitert [14]. Systemeinstellungen können mit ihr nicht geprüft werden. Zur Prüfung von Systemeinstellungen beschreibt Gehrke einen systemspezifischen Prototyp für SAP Systeme [15]. Dieser verwendet eine eigene Regelsyntax.

Hasan und Stiller beschreiben ein generisches Modell und eine generische Architektur zur fortlaufenden Überwachung [16]. Auf Grundlage des Modells und der Architektur wurde ein Prototyp zur fortlaufenden Überwachung von Service Level Agreements implementiert [17].

Schließlich beschreiben Kehlenbeck et al. [18] und Sandner et al. [19] ein Modell, eine Architektur und einen Prototyp zur systemübergreifenden Überwachung von Zugriffskontrollen und Systemeinstellungen. Dabei werden diverse Standardmodelle eingesetzt. Der Prototyp ist aber nicht flexibel hinsichtlich dieser Modelle. Die im Folgenden beschriebenen Verfahren sowie der entwickelte Prototyp zeichnen sich genau durch diese Flexibilität aus.

3. TRANSFERVERFAHREN

Das vorgestellte Verfahren zum Transfer von Daten aus den überwachten Systemen in das überwachende System hat drei wesentliche Eigenschaften:

1. Unterstützung separater Datenbanken für die überwachten Systeme und das überwachende System
2. Unterstützung von Schnittstellen für den Datenexport und -import auf mehreren softwarearchitektonischen Schichten
3. Unterstützung eines einheitlichen Formats zur Sicherstellung der schnittstellenübergreifenden Interoperabilität.

Das Verfahren ist in Abb. 1 illustriert. Auf die Eigenschaften des Verfahrens wird im Folgenden näher eingegangen.

Die Unterstützung separater Datenbanken ermöglicht die Entkopplung der überwachten Systeme vom überwachenden System. Somit können Verarbeitungsprozesse im überwachenden System ablaufen, ohne die Performance der überwachten Systeme zu beeinträchtigen. Ferner ermöglicht dies eine temporale Datenhaltung. Der Prototyp unterstützt sowohl SQL- als auch XML-Datenbanken.

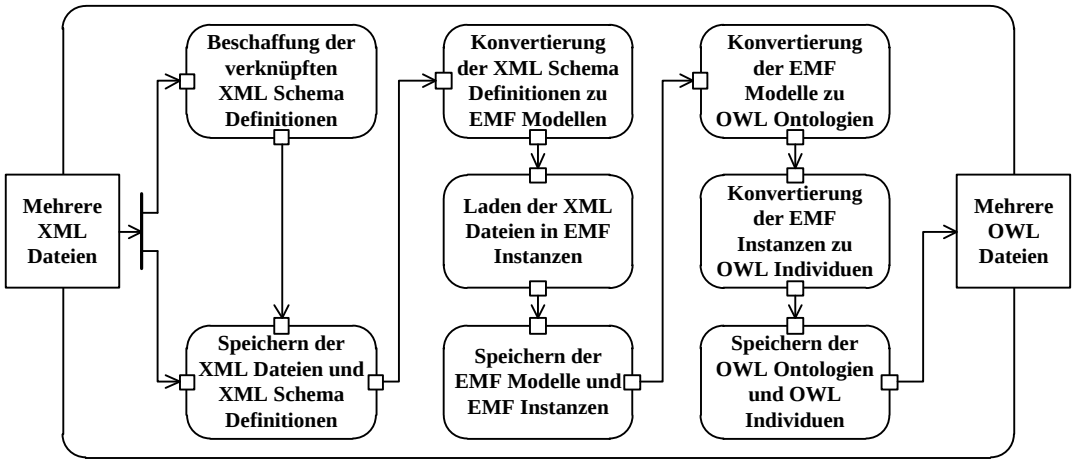

Abbildung 2: Verfahren zum Konvertieren von XML-Daten zu OWL-Ontologien als UML-Diagramm. Es überführt die XML-Daten erst in EMF-Modelle und dann die EMF-Modelle in OWL-Ontologien. Analog kann mit UML-Daten verfahren werden.

Die für den Export und Import von Daten zur Verfügung stehenden Schnittstellen werden durch die Merkmale der zu überwachenden Systeme und den gewährten Zugriff auf diese bestimmt. So unterstützen nicht alle Systeme Datenbank- oder Webserviceschnittstellen. Ferner haben Auditoren teilweise lediglich Zugriff über die Benutzeroberfläche [15]. Gerade der Zugriff über Datenbank- und Webserviceschnittstellen kann jedoch ein höheres Maß an Automatisierung ermöglichen. Der Prototyp unterstützt XML-Dateien, SOAP-Webservices und JDBC-Datenbanken. Zusätzlich können auch die Schnittstellen von Anwendungsservern (z.B. ALE) und Datenbanken (z.B. DRDA) für das überwachende System eingesetzt werden.

Zur Sicherstellung der schnittstellenübergreifenden Interoperabilität verwenden die entwickelten Export- und Importkomponenten ein einheitliches Format. Relationale Daten werden dafür in ein XML-Format überführt. XML-Daten bleiben hingegen unverändert. Auf die Konvertierung von Daten wird im nächsten Abschnitt eingegangen

Das Transferverfahren wird seit etwa neun Monaten produktiv eingesetzt. Die entwickelten Komponenten wurden bereits nach kurzer Zeit auch für andere Projekte verwendet. Unter anderem werden sie für den Export von Stamm- und Bewegungsdaten des Personal- und Rechnungswesen aus verschiedenen produktiven SAP-Systemen eingesetzt.

4. KONVERTIERUNGSVERFAHREN

Kern des vorgestellten Verfahrens zur Konvertierung von transferierten Daten ist eine entwickelte Komponente zur Konvertierung von XML-Daten zu Web Ontology Language (OWL) [20] Ontologien. Der entsprechende Prozess läuft wie folgt ab:

1. Der Prozess nimmt mehrere XML-Dateien als Eingabedaten entgegen. Die Schema Definitionen dieser XML-Dateien sind in referenzierten XSD-Dateien beschrieben. Diese XSD-Dateien werden über das Internet beschafft und zusammen mit den XML-Dateien zwischengespeichert.
2. Die Schema Definitionen in den XSD-Dateien werden mit Hilfe des Eclipse Modeling Frameworks (EMF) [21] zu EMF-Modellen konvertiert. Anschließend werden die Daten in den XML-Dateien in Instanzen dieser Modelle geladen. Die EMF-Modelle werden zusammen mit den EMF-Instanzen zwischengespeichert.
3. Die EMF-Modelle werden zu OWL-Klassen und Properties, die EMF-Instanzen zu OWL-Individuen konvertiert. Dabei wird im Wesentlichen dem Ontology Definition Metamodel (ODM) [20] gefolgt, welches eine solche Konvertierung zwar nicht für EMF, aber für UML beschreibt. Abschließend werden die OWL-Ontologien gespeichert. Sie sind die Ausgabedaten des Prozesses.

Abb. 2 illustriert die Konvertierung von XSD-basierten Daten zu OWL. Da EMF neben XSD auch UML unterstützt, ist der Prozess analog für UML-basierte Daten möglich. Die Fähigkeit zur Konvertierung von XSD- und UML-basierten Daten ist von Bedeutung, weil dies die Standards sind, welche typischerweise von Organisationen wie der Object Management Group (OMG), der Organization for the Advancement of Structured Information Standards (OASIS) oder dem World Wide Web Consortium (W3C) zur Beschreibung von neuen Standardmodellen eingesetzt werden.

Das Verfahren ermöglicht auch die Konvertierung von Daten in zukünftigen Modellen, sofern diese Modelle auf XSD oder UML basieren. In vielen Fällen ist die Konvertierung der Daten zu OWL aber nicht notwendig. Wann genau sich die Konvertierung empfiehlt, wird in den nächsten Abschnitten beschrieben. Zunächst wird noch auf drei Sonderfälle eingegangen.

Viele Kontrollen werden in Systemen auf Grundlage ihrer Zugriffskontrollfunktionen implementiert. Häufig sind dabei Einstellungen in proprietären Zugriffskontrollmodellen vorzunehmen. Daher sind in heterogenen Systemlandschaften viele verschiedene Zugriffskontrollmodelle gleichzeitig im Einsatz. Um die entsprechenden Zugriffskontrolldaten dennoch homogen verarbeiten zu können, werden diese in die XSD-basierte eXtensible Access Control Markup Language (XACML) [23] transformiert. Die hohe Flexibilität und der große Funktionsumfang von XACML ermöglichen selbst die Transformation von Zugriffskontrolldaten aus komplexen Zugriffskontrollmodellen [19]. Darüber hinaus sind freie und quelloffene Komponenten für die Interpretation von XACML verfügbar [24]. Dies erübrigt eigenentwickelte Komponenten.

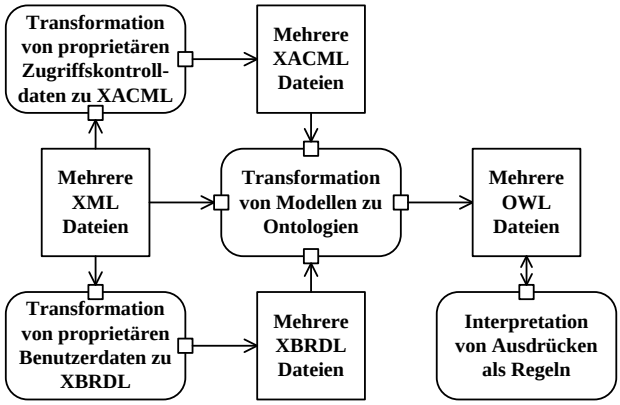

Abbildung 3: Das gesamte Konvertierungsverfahren inklusive der Beachtung von Sonderfällen als UML-Diagramm.

Für die Definition interner Kontrollen im überwachenden System wird ebenso ein Modell benötigt. Gegenwärtig kommt dafür eine erweiterte Version der Extensible Business Risk Description Language (XBRDL) [18] zum Einsatz. Aber auch andere XSD- oder UML-basierte Modelle können verwendet werden. Im Zuge der Evaluation hat es sich als zweckmäßig erwiesen, einzelne Angaben für die Definition interner Kontrollen automatisch zu erstellen. Hierfür werden wenige Daten aus den überwachten Systemen direkt zu XBRDL transformiert.

XACML und XBRDL sind beide XSD-basiert und können daher über den beschriebenen Prozess zu OWL konvertiert werden. Ferner können XBRDL und OWL beide in der Semantic Web Rule Language (SWRL) [25] definierte Regeln einbetten. Über den Prozess werden diese Regeln aber nicht automatisch von XBRDL zu OWL übernommen. Dies regelt eine separate Komponente. Abb. 3 illustriert das gesamte Konvertierungsverfahren.

Das Konvertierungsverfahren wurde mit Hilfe verschiedener Modelle getestet. Die Konvertierung von Modellen zu Ontologien kann auch für andere Zwecke aufschlussreich sein. Ontologien eignen sich als Grundlage für logisches Schlussfolgern. Durch logisches Schlussfolgern können Informationen in Modellen entdeckt werden, die nicht explizit beschrieben, sondern nur implizit enthalten sind.

5. VERARBEITUNGSVERFAHREN

Das vorgestellte Verarbeitungsverfahrens basiert auf einer Erweiterung der in SWRL eingebauten Funktionen. Damit stehen folgende Funktionen zusätzlich für die Definition von SWRL-Regeln zur Verfügung:

1. SQL-Abfragen
2. XQuery-Abfragen
3. XACML-Abfragen

Die Funktionen für SQL- und XQuery-Abfragen ermöglichen einen effizienten Zugriff auf relationale Daten und XML-Daten. Auf eine eigenentwickelte Abfragesprache analog zur Audit Command Language (ACL) [26] und entsprechende Software für deren Editierung und Interpretation wurde bewusst verzichtet. Dies reduziert die erforderlichen Entwicklungs- und Einarbeitungszeiten. Als Eingabeparameter nehmen die Funktionen neben der eigentlichen Abfrage auch eine JDBC-Verbindung bzw. einen XML-Basispfad entgegen. Dies ermöglicht den Zugriff auf mehrere Datenbanken.

Die Funktion für XACML-Abfragen ermöglicht den Zugriff auf XACML Policy Decision Points (PDPs). Auf Grundlage von XACML-Daten entscheidet ein PDP, ob ein bestimmtes Subjekt in Bezug auf eine bestimmte Ressource für eine bestimmte Aktion in einer bestimmten Umgebung zugriffsberechtigt ist. Als Eingabeparameter nimmt die Funktion neben Subjekt, Ressource, Aktion und Umgebung auch die Adresse des PDP entgegen. Dies ermöglicht den Zugriff auf mehrere PDPs.

Die drei aufgeführten Funktionen wurden in einer dedizierten Kontrollkomponente implementiert. Dies isoliert den entsprechenden Programmcode von einer bestimmten Regelevaluationssoftware und erleichtert eine eventuelle spätere Ergänzung um weitere Funktionen. Zur Regelevaluation wird gegenwärtig der Pellet Reasoner [27] eingesetzt. Diese Schlussfolgerungskomponente ist frei und quelloffen verfügbar. Die Integration mit der Kontrollkomponente erforderte daher nur wenige Zeilen Programmcode.

Die OWL-Ontologien bilden eine Wissensdatenbank für die Schlussfolgerungskomponente. Diese OWL-Wissensdatenbank speichert auch die Schlussfolgerungsergebnisse. Gegenwärtig wird hierfür die SPARQL-Datenbank SDB aus dem freien und quelloffenen Jena Framework [28] eingesetzt. SPARQL ist ein Standard, der sowohl ein Protokoll als auch eine Abfragesprache für solche Datenbanken beschreibt [29]. Innerhalb des Jena Frameworks wurde das Protokoll durch die Joseki HTTP Engine und die Abfragesprache durch den ARQ Abfrageprozessor implementiert [30]. Joseki unterstützt auch SDB. Die Komponenten werden gemeinsam als SPARQL-Server eingesetzt.

Auf den SPARQL-Server wird gegenwärtig mit zwei verschiedenen Verfahren zugegriffen: einem Push-Verfahren und einem Pull-Verfahren.

Beim Push-Verfahren stellt die entwickelte Data Warehouse Import Komponente eine Reihe hinterlegter SPARQL-Abfragen an den SPARQL-Server und übermittelt deren Ergebnisse an ein Data Warehouse. Die Ergebnisse können im Data Warehouse temporal gehalten und von dort zu einem beliebigen Zeitpunkt abgefragt werden. Darüber hinaus ist eine Integration mit Informationen aus anderen Quellen möglich.

Beim Pull-Verfahren stellt die entwickelte OLE DB Import Komponente die SPARQL-Abfragen. Die Abfragen müssen erst gestellt werden, wenn die entsprechenden Daten über den entwickelten OLE DB Provider angefordert werden. Folglich wird kein Data Warehouse benötigt. Das Pull-Verfahren hat also geringere Voraussetzungen.

Auf das Data Warehouse und den OLE DB Provider kann über Standardschnittstellen zugegriffen werden. Data Warehouse Server unterstützen in der Regel XML for Analysis (XMLA) [31] und/oder OLE DB for OLAP (ODBO) [32]. Es existiert auch ein Brückentreiber um Clients, die ODBO unterstützen, mit Servern, die XMLA unterstützen, zu verbinden [33]. Der OLE DB Provider unterstützt die Standardschnittstelle Object Linking and Embedding, Database (OLE DB) [34]. Ergänzend können eventuell vorhandene proprietäre Schnittstellen des Data Warehouse Servers verwendet werden.

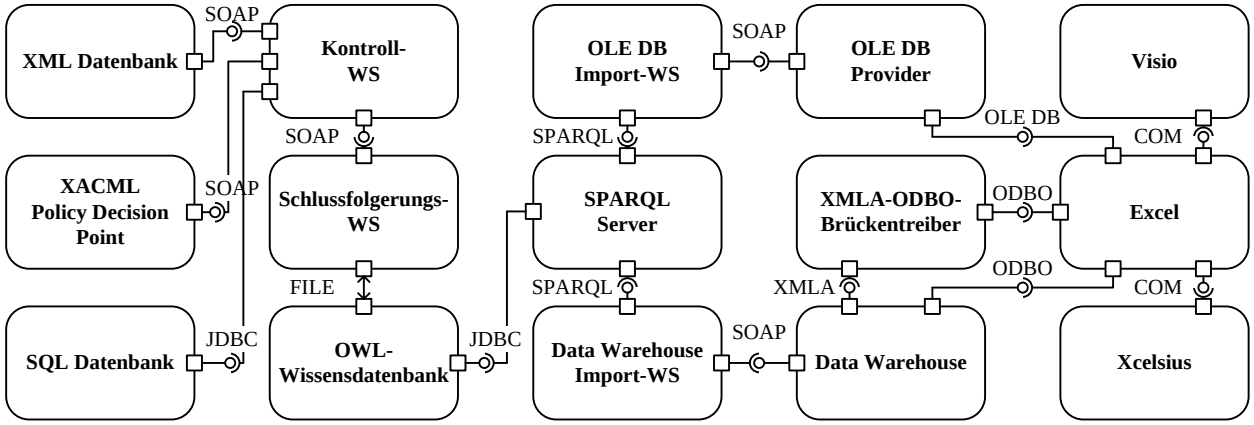

Abbildung 4: Architektur des Verarbeitungsverfahrens für die fortlaufende Überprüfung von Kontrollen als UML-Diagramm. Die Architektur basiert auf Standardschnittstellen. Zur Kontrollanalyse können Werkzeuge wie Excel oder Xcelsius eingesetzt werden.

Als Client wird gegenwärtig Microsoft Excel [35] verwendet. Excel ist ein leistungsfähiges Werkzeug für die Analyse von Daten und unterstützt sowohl OLE DB als auch ODBO. Ergänzend wird für das Erstellen von datenbasierten Grafiken Microsoft Visio [35] und für das Erstellen von Dashboards Business Objects Xcelsius [36] eingesetzt. Sowohl Visio als auch Xcelsius greifen über das Component Object Model (COM) [37] auf Excel zu.

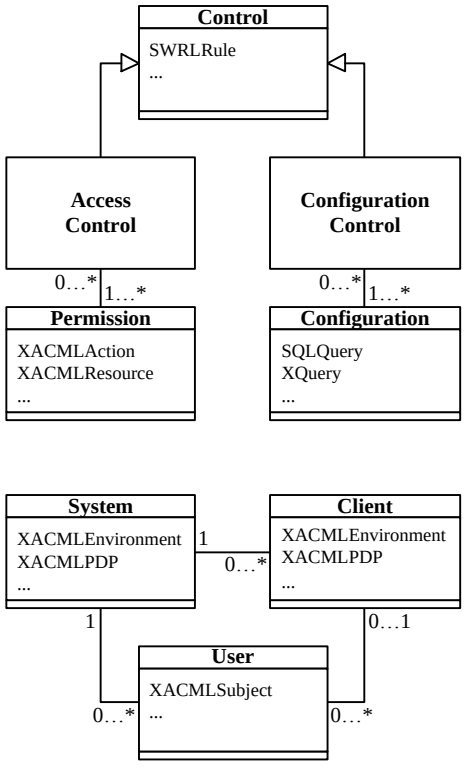

Abbildung 5: Darstellung der Erweiterung des internen Kontrollmodels XBRDL als UML-Diagramm.

An der Überwachung des internen Kontrollsystems sind Personen mit unterschiedlichen Informationsbedürfnissen beteiligt. Beispielsweise benötigen Entscheidungsträger aggregierte Informationen über ganze Systemlandschaften, Anwendungsbetreuer hingegen detaillierte Informationen über einzelne Sachverhalte [38]. Die unterschiedlichen Informationsbedürfnisse verlangen nach unterschiedlichen Werkzeugen. So eignen sich Dashboards für Entscheidungsträger und Analysewerkzeuge für Anwendungsbetreuer [39]. Ein Werkzeug allein kann den Informationsbedürfnisse schwer gerecht werden.

Abb. 4 illustriert die einzelnen Komponenten des Verarbeitungsverfahrens und deren Schnittstellen. Die für den Prototyp entwickelten Komponenten wurden als Webservices implementiert.

6. EINSATZ UND EVALUATION

Der Prototyp wird zur Überwachung von Kontrollen in einem produktiven SAP-System mit mehreren Mandanten eingesetzt. Die Kontrollen können in Konfigurationskontrollen und Zugriffskontrollen untergliedert werden. Konfigurationskontrollen überprüfen, ob das System von einer festgelegten Konfiguration abweicht. Zugriffskontrollen überprüfen, ob die Benutzer über kritische Berechtigungen oder Kombinationen von Berechtigungen verfügen. Um dies abbilden zu können, wurde das interne Kontrollmodell XBRDL um entsprechende Klassen, Attribute und Beziehungen erweitert. Abb. 5 illustriert diese Erweiterung.

Durch die Konvertierung der XBRDL-Daten zu OWL-Ontologien können die XBRDL-Klassen und -Beziehungen in SWRL-Regeln verwendet werden. Dies ermöglicht leicht verständliche Beschreibungen von Kontrollen. Beispielsweise überprüft folgende Regel mittels einer XQuery-Abfrage, ob ein SAP-System eine vorgegebene Passwortlänge erzwingt:

```
Control(?<control>),
System(?<system>),
Configuration(?<config>),
ControlId(?<control>, "urn:control:id:sap:rsparam:login/min_password_lng"),
SystemType (?<system>, "urn:system:type:sap"),
ConfigurationId(?<config>, "urn:configuration:id:sap:rsparam:login/min_password_lng"),
ConfigurationXQuery(?<configuration>, ?<xquery>),
SystemXMLBase(?<system>, ?<xmlbase>),
<control:notFunction>("XQuery",?<xquery>,?<xmlbase>)
```

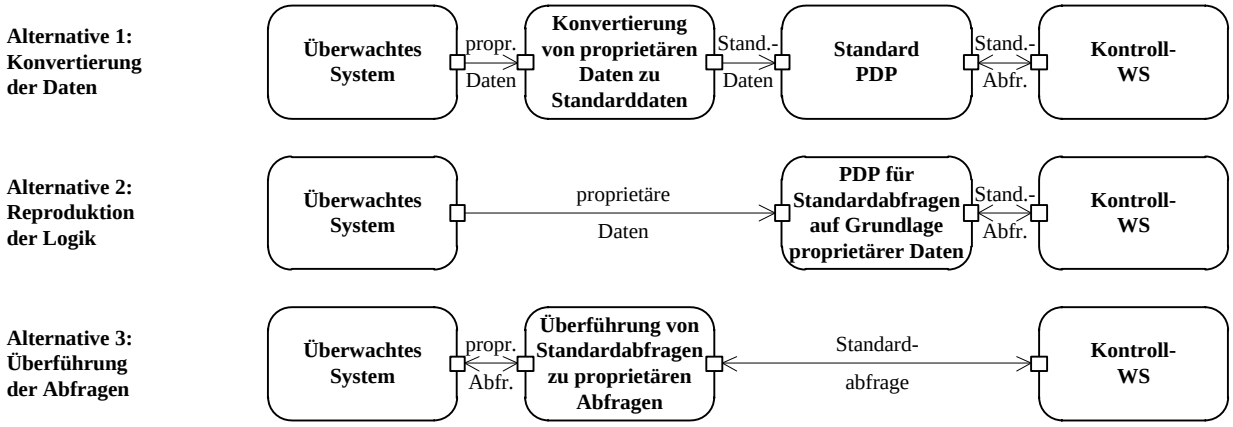

Abbildung 6: Alternative Verfahren zur Nutzung von XACML-Abfragen zusammen mit SAP-Systemen als UML-Diagramm. Die Alternativen 1 und 2 wurden implementiert. Die Alternative 3 wurde auf Grund mangelnder Entkopplung abgelehnt.

Zur Sicherstellung der Skalierbarkeit des Prototyps wird der datenintensive Teil dieser Abfrage, die Verarbeitung einer Menge von XML-Dokumenten (ABAP List Viewer Dateien mit SAP-Profilparametern), mittels des Kontrollwebservices an eine entsprechend optimierte Standardkomponente übergeben.

Als weiteres Beispiel überprüft folgende Regel, ob es Benutzer gibt, die Änderungsbelege in SAP-Systemen löschen können:

```
Control (?<control>),
User (?<user>),
System (?<system>),
Permission (?<permission>),
ControlId(?<control>,"urn:control:id:sap:s_scd0:actvt_06"),
UserSystemId(?<user>,?<systemid>),
UserXACMLSubject(?<user>,?<subject>),
SystemId(?<system>,?<systemid>),
SystemType(?<system>,"urn:system:type:sap"),
SystemXACMLEnvironment(?<system>,?<env>),
SystemXACMLPDP(?<system>,?<pdp>),
PermissionId(?<permission>,"urn:permission:id:sap:s_scd0:actvt_06"),
PermissionXACMLAction(?<permission>, ?<action>),
PermissionXACMLResource(?<permission>, ?<res>),
<control:function>("XACMLRequest",?<pdp>,?<subject>,?<res>,?<action>,?<env>)
```

Auch bei dieser Abfrage wird der datenintensive Teil an eine optimierte Standardkomponente übergeben. Der Schlussfolgerungswebservice verarbeitet lediglich das Ergebnis der Abfrage zur weiteren Evaluation der Regel.

Die Regeln können sehr viel ausgefeilter sein, als in den aufgeführten Beispielen. Beispielsweise können Hierarchien oder Netzwerke von Regeln definiert werden. Ferner müssen sich die Regeln nicht auf einzelne Systeme beschränken. Ebenso wie Geschäftsprozesse können sie sich über mehrere verschiedene Systeme erstrecken. Die Systeme müssen lediglich die genannten Standards unterstützen.

Die Menge der Klassen und Beziehungen sowie die Menge dazugehöriger Daten, welche für die Formulierung von Regeln zur Verfügung stehen, können über den beschriebenen Konvertierungsprozess einfach und ohne Programmänderungen erweitert werden. Beispielsweise können durch die Konvertierung von Daten in der XML Process Definition Language (XPDL) [40] durch die BPMN [39] beschriebene Prozessdaten oder durch die Konvertierung von Daten in der EPC Markup Language (EPML) [42] durch die EPK [43] beschriebene Prozessdaten in die Regeldefinition einbezogen werden.

Die konvertierten Daten und die Ergebnisse der Regelevaluation stehen für SPARQL-Abfragen zur Verfügung. Beispielsweise ermittelt folgende einfache Abfrage, welche Benutzer welche Kontrollen verletzen:

```
SELECT ?user_id ?control_id
WHERE {
        ?user a xbrdl:User;
                xbrdl:UserId ?user_id;
                xbrdl:UserInfringesControl ?control_id;
}
ORDER BY ?user_id
```

Auch in SPARQL-Abfragen stehen also die Klassen und Beziehungen aus konvertierten Modellen zur Verfügung.

Konvertiert werden müssen alle Modelle und dazugehörige Daten, die für die Formulierung oder Evaluation von SWRL-Regeln oder SPARQL-Abfragen benötigt werden. Dies gilt allerdings nicht für Daten, auf die lediglich über SQL-, XQuery- oder XACML-Abfragen zugegriffen wird. Letztere können unkonvertiert in die Datenbanken des überwachenden Systems übernommen werden. Dies hat erhebliche Performancevorteile.

Für die Nutzung von XACML-Abfragen zusammen mit SAP-Systemen wurden drei alternative Verfahren ausgearbeitet:

1. Konvertierung der Zugriffskontrolldaten vom SAP-Modell ins XACML-Modell und Nutzung eines Standard-PDP
2. Entwicklung eines PDP zum Ermöglichen von XACML-Abfragen auf Grundlage von Daten im SAP-Modell
3. Überführung der XACML-Abfragen zu Abfragen auf SAP-Funktionsbausteine zur Zugriffskontrolle.

Abb. 6 illustriert die drei unterschiedlichen Verfahren. Bei jedem dieser Verfahren ist eine Kommunikation mit dem Kontrollwebservice über Standardabfragen möglich. Für den Kontrollwebservice sind die Verfahren somit austauschbar.

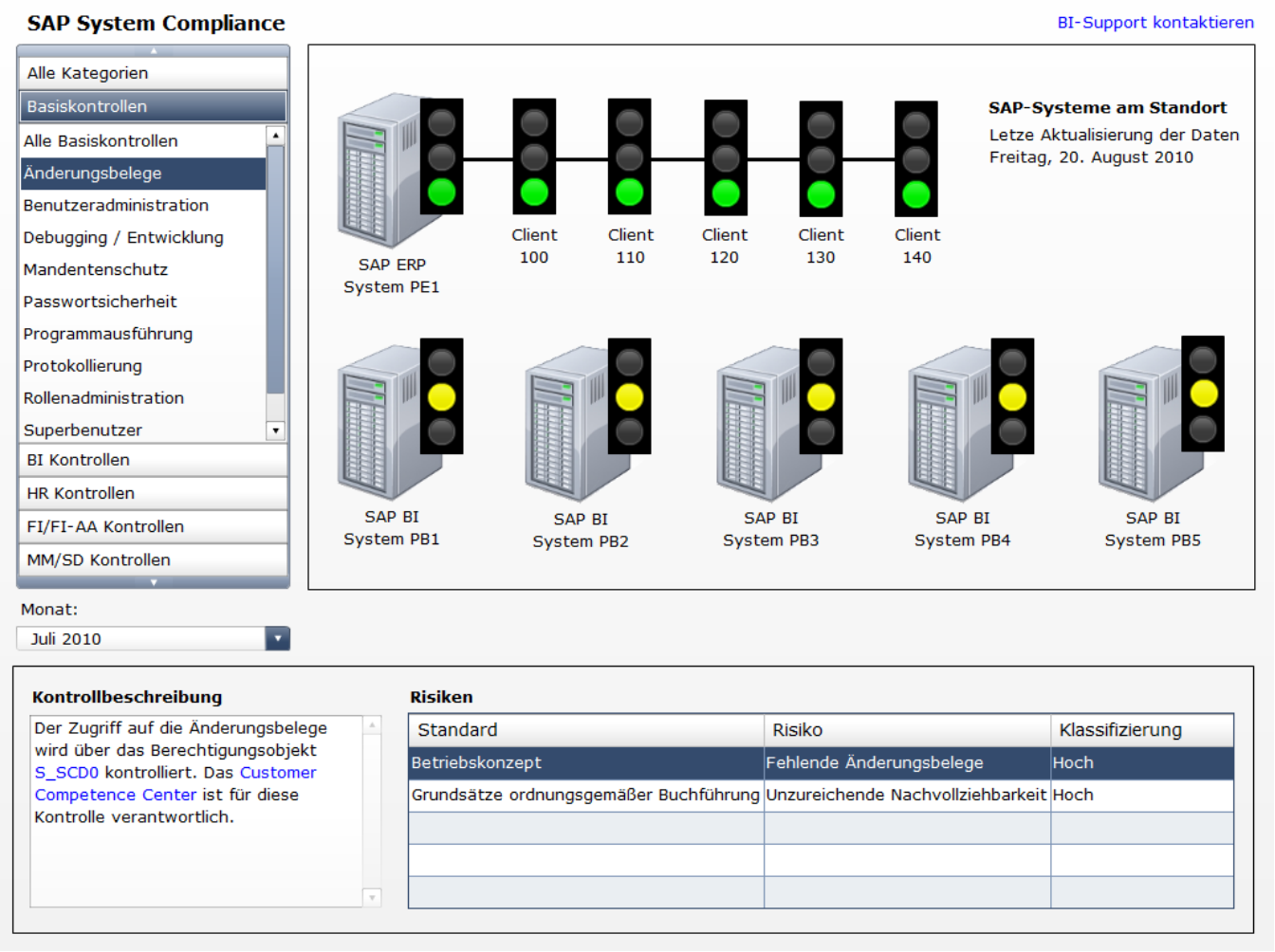

Abbildung 7: Screenshot eines Compliance Dashboards zur Präsentation der durch den Prototyp ermittelten Kontrollergebnisse. Das Dashboard wurde in Zusammenarbeit mit den Benutzern entwickelt und mit Xcelsius erstellt.

Für den Prototyp wurden die Alternativen 1 und 2 implementiert. Alternative 3 wurde durch den Systemverantwortlichen abgelehnt, da sie keine Entkopplung der überwachten Systeme vom überwachenden System bietet. Insbesondere wurden dabei Performanceprobleme im produktiven Betrieb befürchtet.

Für Alternative 1 wurde Sun's XACML Implementierung (SUNXACML) [24] eingesetzt. Sie benötigte um ein Vielfaches länger zur Beantwortung der XACML-Abfragen als die Implementierung zu Alternative 2. Mit Alternative 1 wäre zwar eine regelmäßige aber keine fortlaufende Überwachung von Zugriffskontrollen in SAP-Systemen möglich gewesen. Dafür wären Änderungen am Programmcode von SUNXACML notwendig gewesen. Aufgrund vorliegender Evaluationen wurde auch von anderen XACML Implementierungen keine ausreichende Performance erwartet [44].

In Bezug auf eine vierte Alternative wurde die Möglichkeit einer XACML PDP Implementierung in OWL und SWRL geprüft. Da XACML auf XSD basiert, können XACML-Daten über das beschriebene Verfahren einfach zu OWL-Ontologien konvertiert werden. XACML und OWL verwenden beide die XSD-Datentypen, XACML und SWRL verweisen hinsichtlich der eingebauten Funktionen beide auf XQuery und XPath [45]. Folglich gibt es eine erhebliche gemeinsame Schnittmenge. Nach Versuchen mit verschiedenen Schlussfolgerungskomponenten wurde die Alternative aufgrund von Performanceüberlegungen aber nicht weiter verfolgt. Für eine fortlaufende Überwachung von Kontrollen erwies sich das Volumen von konvertierten SAP-Zugriffskontrolldaten [19] als zu hoch.

Bei der Evaluation des Prototyps wurde festgestellt, dass die eingesetzte Schlussfolgerungskomponente vielfach bereits zuvor gestellte Abfragen über den Kontrollwebservice ausführte. Aus diesem Grund wurde der Kontrollwebservice um einen entsprechenden Abfragecache erweitert. Mit diesem Cache ist der Prototyp schnell genug für die fortlaufende Überwachung von Kontrollen in mehreren Mandanten und Systemen. Gleichwohl werden die Kontrollen im SAP-System gegenwärtig nur einmal im Monat überprüft, da die Analysen und Berichte im vorliegenden Fall durch die Benutzer nicht häufiger benötigt werden.

Abb. 7 enthält einen Screenshot eines erstellten Compliance Dashboards. Das Dashboard wurde in Zusammenarbeit mit den Benutzern zur Präsentation der durch den Prototyp ermittelten Kontrollergebnisse entwickelt [39]. Die Kontrollen in den aufgeführten SAP BI Systemen werden gegenwärtig noch nicht überwacht. Der Produktivstart für diese Systeme steht noch an.

Tabelle 1: Ungesperrte Benutzer, Rollenzuordnungen und Berechtigungszuordnungen im überwachten System.

Anzahl im letzten Monat	Mandanten				
	100	**110**	**120**	**130**	**140**
Ungesperrte Benutzer	36	106	546	57	155
Rollen-zuordnungen	342	1037	5530	923	1454
Berechtigungs-zuordnungen	52045	92784	156543	63619	81713

Durch die Verwendung eines gemeinsamen Referenzmodells haben die einzelnen Mandanten des überwachten Systems eine homogene Konfiguration. Aufgrund unterschiedlicher Aufbau- und Ablauforganisationen gibt es hingegen heterogene Zugriffskontrollen. Tab. 1 enthält eine Übersicht der ungesperrten Benutzer, Rollenzuordnungen und Berechtigungszuordnungen in den Mandaten des überwachten SAP-Systems.

Die Tab. 1 soll verdeutlichen, dass allein für die Überwachung von Zugriffskontrollen in den Mandanten eines produktiven Anwendungssystems erhebliche Datenmengen verarbeitet werden müssen. Gleichwohl reicht dies für eine gewissenhafte Überwachung des Systems noch nicht aus. So sind auch die Zugriffskontrollen auf Datenbank- und Betriebssystemebene zu berücksichtigen. Ferner können die Zugriffskontrollen in vor- und/oder nachgelagerten Systemen von Bedeutung sein. Eine gewissenhafte Überwachung des internen Kontrollsystems erfordert somit die Betrachtung mehrerer heterogener Systeme.

Für die Evaluation des Prototyps wurde ein SAP-System verwendet. Dennoch kann der Prototyp systemunabhängig eingesetzt werden. Beispielsweise kann der Prototyp:

- Andere **ERP-Systeme** überwachen, die ihre Daten in SQL-Datenbank ablegen, wie beispielsweise die aktuellen ERP-Systeme von Oracle, Microsoft oder Sage.
- **Applikationsserver** überwachen, die Konfigurationsdaten in XML-Dateien ablegen, wie beim Sun GlassFish Enterprise Server oder IBM WebSphere Application Server.
- **Datenbanken** überwachen, welche Konfigurations- und Zugriffskontrolldaten in eigene SQL-Tabellen ablegen, wie bei Oracle oder MySQL.
- **Betriebssysteme** überwachen, die Konfigurations- oder Zugriffskontrolldaten in Verzeichnisdiensten ablegen, wie entsprechend konfigurierte Windows oder Linux Systeme.

Das Beispiel der Überwachung von Betriebssystemen verdeutlicht die Flexibilität des Prototyps. Aus Verzeichnisdiensten, wie das Active Directory [46] von Microsoft können über dazugehörige Werkzeuge Daten in der OASIS Directory Services Markup Language (DSML) [47] exportiert werden. DSML ist ein XML-Format und basiert auf XSD. Der Prototyp kann auf unkonvertierte DSML-Daten über XQuery in Regeln zugreifen, oder konvertierte DSML-Daten in der Definition von Regeln verwenden. Neue Modelle können ohne Programmänderungen einbezogen werden.

Der Prototyp ermöglicht die einheitliche Überwachung von Kontrollen in unterschiedlichen Systemen. Somit kann der vorhandenen Heterogenität in realen Organisationen, System- und Prozesslandschaften Rechnung getragen werden.

7. FAZIT UND AUSBLICK

Die Heterogenität der Prozessabläufe, Kontrollumfelder und Systemlandschaften stellt besonders hohe Anforderungen an die Flexibilität von Software zur Unterstützung des Managements interner Kontrollsysteme. So kann Software zur Überwachung von Kontrollen in Systemen nur dann allgemein eingesetzt werden, wenn sie flexibel auf unterschiedlichste Modelle und Abläufe eingehen kann.

Der vorliegende Aufsatz präsentiert Verfahren, mit deren Hilfe die Implementierung automatisierter Kontrollen in unterschiedlichen Systemen einheitlich mit einer Software überwacht werden kann. Diese Verfahren wurden als Webservices innerhalb einer Service-Orientierten Architektur implementiert und mit Daten aus einem produktiven SAP-System in einer Fallstudie evaluiert**.**

Auf die Daten der zu überwachenden Systeme kann der Prototyp über Schnittstellen auf mehreren softwarearchitektonischen Schichten zugreifen. Mit Hilfe eines entwickelten Konvertierungsverfahrens werden Teile dieser Daten zusammen mit den dazugehörigen Modellen in OWL-Ontologien überführt. Die Modelle stehen anschließend als Sprachelemente für die Definition von Kontrollausnahmen zur Verfügung. In den Definitionen können außerdem Abfragen auf den nicht konvertierten Teil der Daten in den vorherrschenden Standards für Zugriffskontroll-, XML- und relationale Daten verwendet werden.

Für die Evaluation des Prototyps wird ein produktives SAP-System mit mehreren Mandanten verwendet. Der Prototyp kann jedoch systemunabhängig eingesetzt werden. Somit kann der vorhandenen Heterogenität in realen Organisationen, System- und Prozesslandschaften Rechnung getragen werden.

Der nächste Schritt ist der Einsatz des Prototyps zur Überwachung von Datenbanken und Betriebssystemen. Hinsichtlich der Überwachung von Datenbanken gibt es eine Transformation von Zugriffskontrolldaten zu XACML [48]. Hinsichtlich der Überwachung von Betriebssystemen wurde bereits auf DSML eingegangen. Ergänzend kann der Kontrollwebservice um eine eingebaute Funktion für DSML-Abfragen ergänzt werden. DSML-Verzeichnisdienste können über Webservices abgefragt werden. Dies erleichtert die Überwachung entfernter Systeme.

8. REFERENZEN

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2004. Enterprise Risk Management - Integrated Framework, Executive Summary. http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf.

[2] Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2009. Guidance on Monitoring Internal Control Systems. http://www.coso.org/guidance.htm.

[3] Bace, J. und Rozwell, C. 2006. Understanding the Components of Compliance. Gartner Report: G00137902.

[4] Agrawal, R., Johnson, C., Kiernan, J. und Leymann, F. 2006. Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology. Proc. of the 22nd International Conference on Data Engineering (ICDE'06), 3.-8. April 2006. IEEE, Atlanta, USA, 92-102. DOI: 10.1109/ICDE.2006.155.

[5] Liebenau, J. und Kärrberg, P. 2006. International Perspectives on Information Security Practices. London School of Economics and Political Science, McAfee.

[6] Syed, A., Syed, N. H., Indulska, M. und Sadiq, S. 2009. A Study of Compliance Management in Information Systems Research, Proc. of the 17th European Conference on Information Systems (ECIS), 8.-10. Juni 2009. Verona, Italien.

[7] Julisch, K. 2008. Security Compliance: The Next Frontier in Security Research. Proc. of the 2008 Workshop on New Security Paradigms, 22.-25. September. ACM, Lake Tahoe, USA, 71-74. DOI: 10.1145/1595676.1595687.

[8] Teubner, A. und Feller, T. 2008. Informationstechnologie, Governance und Compliance. Wirtschaftsinformatik 5, 400-407.

[9] Searcy, D., Woodroof, J. und Behn, B. 2003. Continuous Audit: The Motivations, Benefits, Problems, and Challenges Identified by Partners of a Big 4 Accounting Firm. Proc. of the 36th Hawaii International Conference on System Sciences (HICSS-36), 6.-9. Januar 2003. IEEE, Waikoloa Village, USA.

[10] Accorsi, R., Sato, Y. und Kai, S. 2008. Compliance Monitor for Early Warning Risk Determination. Wirtschaftsinformatik 5, 375-382.

[11] Sackmann, S. und Kähmer, M. 2008. ExPDT: A Policy-based Approach for Automating Compliance. Wirtschaftsinformatik 5, 366-374.

[12] Teeter, R. und Brennan, G. 2008. Aiding the Audit: Using the IT Audit as a Springboard for Continuous Controls Monitoring. Collected Papers of the Seventeenth Annual Research Workshop on Artificial Intelligence and Emerging Technologies in Accounting, Auditing and Tax, 2. August 2008, Anaheim, USA.

[13] Alles, M., Brennan, G., Kogan A. und Vasarhelyi, M. A. 2005. Continuous Monitoring of Business Process Controls: A Pilot Implementation of a Continuous Auditing System at Siemens. International Journal of Accounting Information Systems, Volume 7, Issue 2, 137-161, DOI: 10.1016/j.accinf.2005.10.004.

[14] Wolf, P. und Gehrke, N. 2009. Continuous Compliance Monitoring in ERP Systems - A Method for Identifying Segregation of Duties Conflicts. Proc. der 9. Internationalen Tagung Wirtschaftsinformatik, 25.-27. Februar 2009, Wien, Österreich, 347-356.

[15] Gehrke, N. 2010. The ERP AuditLab – A Prototypical Framework for Evaluating Enterprise Resource Planning System Assurance. Proc. of the 43rd Hawaii International Conference on System Sciences (HICSS-43), 4.-7. Januar 2010, IEEE, Koloa, USA.

[16] Hasan, H. und Stiller, B. 2005. A Generic Model and Architecture for Automated Auditing. 16th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM 2005), 24.-26. Oktober 2005, Barcelona, Spanien, Springer, LNCS 3775, 121-132.

[17] Hasan, H. und Stiller, B. 2007. AURIC: A Scalable and Highly Reusable SLA Compliance Auditing Framework. 18th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM 2007), 29.-31. Oktober 2007, San Jose, USA, Springer, LNCS 4785, 203-215.

[18] Kehlenbeck, M, Sandner, T. und Breitner, M. H.. 2010. Managing Internal Control in Changing Organizations through Business Process Intelligence – A Service Oriented Architecture for the XACML based Monitoring of Supporting Systems. Proc. of the 43th Hawaii International Conference on System Sciences (HICSS-43), 4.-7. Januar 2010, IEEE, Koloa, USA.

[19] Sandner, T., Kehlenbeck, M. und Breitner, M. H. 2010. An Implementation of a Process-Oriented Cross-System Compliance Monitoring Approach in a SAP ERP and BI Environment", Proc. of the 18th European Conference on Information Systems (ECIS 2010), 6.-9. Juni 2010, Pretoria, Südafrika.

[20] World Wide Web Consortium (W3C). 2004. OWL Web Ontology Language Overview - W3C Recommendation February 10, 2004. http://www.w3.org/TR/owl-features.

[21] Eclipse Modeling Framework (EMF) Project. 2010. Eclipse Modeling – EMF – Home. http://www.eclipse.org/modeling/emf/?project=emf.

[22] Object Management Group (OMG). 2009. Ontology Definition Metamodel Version 1.0. http://www.omg.org/spec/ODM/1.0/PDF.

[23] Organization for the Advancement of Structured Information Standards (OASIS). 2005. OASIS eXtensible Access Control Markup Language (XACML) Version 2.0. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.

[24] Sun Microsystems. 2006. Sun's XACML Implementation. http://sunxacml.sourceforge.net.

[25] World Wide Web Consortium (W3C). 2004. SWRL: A Semantic Web Rule Language Combining OWL and RuleML – W3C Member Submission 21 May 2004. http://www.w3.org/Submission/SWRL.

[26] ACL Services Ltd. 2010. ACL Data Analytics and Continuous Monitoring Software Solutions. http://www.acl.com/default.aspx.

[27] Clark & Parsia, LLC. 2010. Pellet: OWL 2 Reasoner for Java. http://clarkparsia.com/pellet.

[28] Jena Semantic Web Framework. 2010. SDB – A SPARQL Database for Jena. http://openjena.org/SDB.

[29] World Wide Web Consortium (W3C). 2008. SPARQL Query Language for RDF – W3C Recommendation, January 15, 2008. http://www.w3.org/TR/rdf-sparql-query.

[30] Jena Semantic Web Framework. 2009. Joseki – A SPARQL Server for Jena. http://www.joseki.org.

[31] Microsoft Corporation und Hyperion Solutions Corporation. 2002. XML for Analysis Specification – Version 1.1. http://www.xmla.org/xmla1.1.doc.

[32] Microsoft Corporation. 2010. OLE DB for OLAP Overview. http://msdn.microsoft.com/en-us/library/ms714903%28VS.85%29.aspx.

[33] Simba Technologies. 2010. Simba O2X 2.5. http://www.simba.com/odbo-to-xmla.htm.

[34] Microsoft Corporation. 2010. Microsoft OLE DB. http://msdn.microsoft.com/en-us/library/ms722784%28VS.85%29.aspx.

[35] Microsoft Corporation. 2010. Microsoft Office. http://office.microsoft.com/de-de.

[36] SAP Deutschland. 2010. Xcelsius - Dashboards und Visualisierungen für bessere Entscheidungen. http://www.sap.com/germany/sme/solutions/businessintelligence/xcelsius/index.epx.

[37] Microsoft Corporation. 2010. COM: Component Object Model Technologies. http://www.microsoft.com/com.

[38] Kehlenbeck, M., Sandner, T. und Breitner, M. H. 2010. Application and Economic Implications of an Automated Requirement-Oriented and Standard-Based Compliance Monitoring and Reporting Prototype. Proc. of the 5th International Conference on Availability, Reliability and Security (ARES 2010), 15.-18. Februar 2010, IEEE, Krakow, Polen.

[39] Sandner, T., Kehlenbeck, M. und Breitner, M. H. 2010. Visualization of Automated Compliance Monitoring and Reporting. Wird erscheinen in Proceedings of the DEXA 2010 Workshops, 30. August – 3. September 2010, IEEE, Bilbao, Spanien.

[40] Workflow Management Coalition. 2010. XPDL Support and Resources. http://www.wfmc.org/xpdl.html.

[41] Object Management Group (OMG). 2009. Business Process Model and Notation (BPMN) – Version 1.2. http://www.omg.org/spec/BPMN/1.2.

[42] Mendling, J. und Nüttgens, M. 2005. EPC Markup Language (EPML): An XML-based Interchange Format for Event-Driven Process Chains (EPC). Information Systems and E-Business Management, Vol. 4, Issue 3, 245-263.

[43] Keller, G., Nüttgens, M., Scheer, A.-W. .1992. Semantische Prozeßmodellierung auf der Grundlage ‚Ereignisgesteuerter Prozeßketten (EPK)‘“, Veröffentlichungen des Instituts für Wirtschaftsinformatik (IWI), Universität des Saarlandes, Heft 89. http://www.iwi.uni-sb.de/Download/iwihefte/heft89.pdf.

[44] Turkmen, F., Crispo, B. 2008. Performance Evaluation of XACML PDP Implementations. Proceedings of the 2008 ACM Workshop on Secure Web Services, 31. Oktober 2008, ACM, Fairfax, USA, 37-44.

[45] World Wide Web Consortium (W3C). 2007. XQuery 1.0 and XPath 2.0 Functions and Operators – W3C Recommendation 23 January 2007. http://www.w3.org/TR/xquery-operators.

[46] Microsoft Corporation. 2010. Active Directory. http://www.microsoft.com/windowsserver2008/en/us/active-directory.aspx.

[47] Organization for the Advancement of Structured Information Standards (OASIS). 2001. Directory Services Markup Language v2.0. http://www.oasis-open.org/committees/dsml/docs/DSMLv2.doc.

[48] Leighton, G. und Barbosa, D. 2010. Access Control Policy Translation and Verification within Heterogeneous Data Federations. Proc. of the 15th ACM Symposium on Access Control Models and Technologies, 9.-11. Juni 2010. ACM, Pittsburgh, USA.