Beiträge zum IT-Compliance Management

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 Thorben Sandner

geboren am 7. Juni 1977 in Hannover

2011

Betreuer und Gutachten:	Professor Dr. Michael H. Breitner
Gutachten:	Jun.-Professor Dr. Hans-Jörg von Mettenheim
Tag der Promotion:	23. Juni 2011

Summary

This cumulative dissertation deals with the research area IT compliance management, as well as the research area IT risk management. Based on real life problems and literature reviews, the following research objectives have been defined:

I. Design of artifacts for the automated rule-based monitoring of system controls in IT-systems to support business processes and an appropriate target group oriented reporting of control exceptions.

II. Design of an artefact to include the factors of the "Fraud Triangle" in IT risk management in consideration of the available IT-Infrastructure.

In order to achieve these research objectives, design science is used as the research method. The research results are summarized in four research papers regarding IT compliance and research objective I and one research paper regarding IT risk management and research objective II.

Key words: IT compliance management, IT risk management, Internal Control

Abstract

Die vorliegende kumulative Dissertation setzt sich mit den Forschungsgebieten IT-Compliance Management sowie IT-Risikomanagement auseinander. Ausgehend von Problemstellungen aus der Praxis und Literaturrecherchen wurden folgende Forschungsziele definiert:

I. Gestaltung von Artefakten zur automatisierten regelbasierten Überwachung maschineller Kontrollen in IT-Systemen zur Unterstützung von Geschäftsprozessen und zur zielgruppen-gerechten Berichterstattung von Kontrollausnahmen.

II. Gestaltung eines Artefakts zur Einbeziehung der Faktoren des „Fraud Triangle“ im IT-Risikomanagement unter Berücksichtigung der vorliegenden IT-Infrastruktur.

Zur Umsetzung dieser Forschungsziele wird Design Science (DS) als Forschungsmethode eingesetzt. Die Forschungsergebnisse wurden in vier Forschungsbeiträgen zu IT-Compliance Management und Forschungsziel I sowie einem Forschungsbeitrag zum IT-Risikomanage-ment und Forschungsziel II zusammengefasst.

Schlagworte: IT-Compliance Management, IT-Risikomanagement, Interne Kontrollen

Kurzzusammenfassung

Einleitung und Problemstellung

Die Informationstechnologie (IT) hat in den letzten Jahrzehnten erheblich an Bedeutung gewonnen. Eine Ursache dafür ist, dass die Geschäftsabwicklung und die Geschäftsprozesse vieler Unternehmen und Organisationen stark abhängig von dem Einsatz der IT bzw. der Unterstützung durch die IT sind. Ohne eine gut strukturierte IT bzw. an den Bedürfnissen des Unternehmens ausgerichtete IT-Dienstleistungen sind für viele Unternehmen ein Marktbestehen oder gar ein wirtschaftlicher Erfolg nicht mehr zu erreichen. Das wirtschaftliche Handeln muss dabei fortwährend mit Gesetzen und Normen in Einklang gebracht werden.

Bekannt gewordene Verstöße wie z. B. auf internationaler Ebene Enron und Worldcom oder auf nationaler Ebene Flowtex haben u. a. dafür gesorgt, dass in den letzten Jahren vielfältige staatliche und nichtstaatliche Vorgaben erlassen worden sind. Diese oft verpflichtenden Vorgaben (zur Vermeidung von Verstößen) lassen sich unter den Begriffen Compliance und Governance subsummieren. Compliance bezieht sich auf gesetzliche oder regulatorische Anforderungen. Governance hingegen bezieht sich auf die von der Unternehmensführung erlassenen Auflagen.[1] Bedingt durch den hohen Automatisierungs- und Durchdringungsgrad der IT wird eine Vielzahl von Geschäftsprozessen direkt in den IT-Systemen der Unternehmen implementiert.[2] In diesen IT-Systemen lassen sich deshalb häufig Verletzungen der Auflagen und Vorgaben identifizieren. Es gilt daher, neben dem oft vorherrschenden Fokus der Ausrichtung der IT an betriebswirtschaftlichen Prozessen und Zielen auch Kontrollziele in IT-Systeme, festzulegen, Risikobewertungen vorzunehmen und Kontrollen durch Audits zu überwachen.

Aktuelle Regularien wie z. B. Sarbanes-Oxley Act (SOX), Solvabilität II oder Basel II legen die Vorgaben und Anforderungen fest. Die operative Umsetzung dieser Anforderungen hingegen obliegt den Unternehmen. Die Überprüfung der technischen Implementierungen und die Einhaltung der IT-Compliance-Vorschriften erfordern meist einen hohen manuellen Aufwand. Um den finanziellen, zeitlichen und personellen Aufwand zu strukturieren, werden oft Rahmenwerke wie z. B. Control Objectives for Information and related Technology (COBIT) oder

[1] Vgl. Müller und Terzidis 2008, S. 341.
[2] Vgl. ebd., S. 341.

Information Technology Infrastructure Library (ITIL) hinzugezogen. In diesem vielschichtigen Kontext, oft erschwert durch die Heterogenität und Komplexität der IT-Systeme, werden nun Anwendungsprogramme eingesetzt, die umfangreiche Audits regelmäßig und zeitnah ermöglichen bzw. erleichtern sollen. Der Einsatzzeitpunkt der Anwendungsprogramme lässt sich grob in „vor dem Ereignis“ (ex ante) und „nach dem Ereignis“ (ex post) unterscheiden. Beim ex ante Ansatz wird schon im Entwurf eine Identifikation von Problemen und Schwachstellen angestrebt. Beim ex post Ansatz werden die bereits durchgeführten Geschäftsvorfälle im Nachhinein auf Verletzungen der Compliance geprüft. Aktuelle Audit-Programme arbeiten meist ex post.[3] Sie können somit Aussagen zur Compliance nur nachträglich bezogen auf den jeweiligen Zeitpunkt tätigen, sich aber nicht auf aktuelle Geschäftsvorfälle beziehen.

Die zeitnahe Berichterstattung eventueller Kontrollausnahmen und die zügige Veranlassung von Gegenmaßnahmen sind Erfolgsfaktoren für ein funktionierendes internes Kontrollsystem (IKS). Die prüfenden und informierenden Anwendungssysteme sind also essentielle Bestandteile eines IT-Compliance Managements. Daher beschäftigen sich die Forschungsbeiträge der vorliegenden Dissertation mit dieser Art von Anwendungssystem. Innerhalb der Forschungsbeiträge werden Verfahren, Modelle und Implementierungen zur automatisierten Überwachung von Kontrollen in IT-Systemen vorgestellt.

Bei der Prüfung in den IT-Systemen werden vorzugsweise technisch leicht abbildbare Aspekte untersucht wie z. B. Berechtigungsvorgaben oder Buchungsbelege. Der Faktor Mensch als qualitative Komponente wird nicht umfangreich in die Prüfung integriert. Nach der „Global Fraud Study“ der Association of Certified Fraud Examiners (ACFE) werden jedoch 80% der Betrugsfälle (fraud) in den eigenen Unternehmensreihen, insbesondere durch Mitarbeiter in den Bereichen Rechnungswesen, Vertrieb, Einkauf, Kundenservice oder höheres Management begangen.[4] Im Normalfall werden in diesen Bereichen Enterprise Resource Planning (ERP)-Systeme eingesetzt, die bisher auch vorrangig im Fokus der technisch orientierten Prüfungen standen. Trotz einer Vielzahl technischer Verbesserungen in diesem Gebiet, dauert es nach der Studie der ACFE im Durchschnitt bis zu 18 Monate, um einen Betrugsfall aufzudecken. Dies lässt darauf schließen, dass die

[3] Vgl. Müller und Terzidis 2008, S. 341.
[4] Vgl. ACFE 2010, S. 5.

Informationen, die derzeit mit den gängigen Techniken geliefert werden, nicht unbedingt für eine zeitnahe Betrugsaufdeckung ausreichen. In einem Forschungsbeitrag dieser Dissertation wird daher ein generisches Architekturmodell vorgestellt. Es ermöglicht, den „Fraud Triangle"-Faktoren - Gelegenheit, Motiv und Innere Rechtfertigung - Rechnung zu tragen, so dass es abschließend zu einer Risikoklassifikation eines Unternehmensangehörigen kommt. Die Berücksichtigung dieser Faktoren bietet insofern einen Mehrwert, als die von einem Auditor zu untersuchenden Geschäftstransaktionen besser differenziert und priorisiert werden können. Durch die Einbeziehung des menschlichen Verhaltens ist es möglich, Geschäftstransaktionen zu entdecken, die einem bisher noch nicht bekannten Muster unterliegen und mit herkömmlichen Mitteln unentdeckt geblieben wären.

Forschungsziele und Forschungsmethode

Die vorliegende kumulative Dissertation beschäftigt sich mit den Forschungsgebieten IT-Compliance Management und IT-Risikomanagement. Ausgehend von Problemstellungen aus der Praxis und Literaturrecherchen sind folgende Forschungsziele definiert worden:

I. Gestaltung von Artefakten zur automatisierten regelbasierten Überwachung maschineller Kontrollen in IT-Systemen zur Unterstützung von Geschäftsprozessen und zur zielgruppengerechten Berichterstattung von Kontrollausnahmen.

II. Gestaltung eines Artefakts zur Einbeziehung der Faktoren des „Fraud Triangle" im IT-Risikomanagement unter Zuhilfenahme der vorliegenden IT-Infrastruktur.

Zur Umsetzung dieser Forschungsziele wird Design Science (DS) als Forschungsmethode eingesetzt (s. Abbildung I). Die Forschungsergebnisse wurden in vier Forschungsbeiträgen zu IT-Compliance Management und Forschungsziel I sowie einem Forschungsbeitrag zum IT-Risikomanagement und Forschungsziel II zusammengefasst.

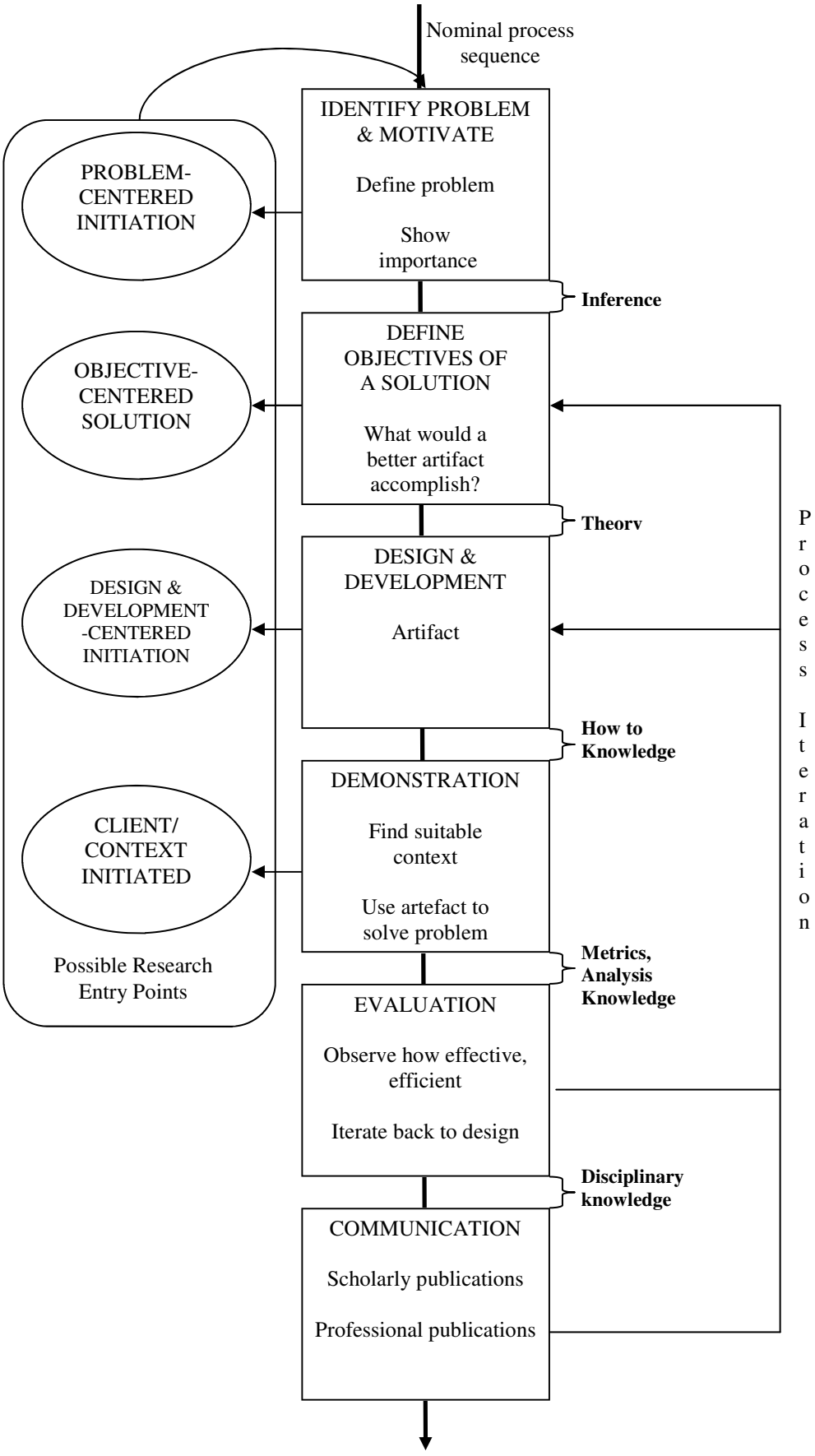

Abbildung I: Design Science Research Methode (DSRM).

Quelle: Peffers et al. (2007), S. 11.

Forschungsstand

Bei der Erstellung der Forschungsbeiträge ist jeweils eine intensive Literaturrecherche in den einschlägigen Internetdatenbanken der Verlage und Verbände betrieben worden. Die Recherchen erstreckten sich somit auf die relevanten Konferenzen, Zeitschriften und Bücher. Die Ergebnisse sind in den jeweiligen Forschungsbeiträgen eingearbeitet worden. Die Publikationszahlen im Bereich der IT-Compliance steigen seit ca. Anfang 2000 kontinuierlich an. Im Bereich der Einbeziehung von Persönlichkeitsfaktoren in die IT-Sicherheit oder IT-Risikomanagement gibt es bis auf Einzelpublikationen zu Teilaspekten weder ein weit verbreitetes Forschungsforum noch eine Forschungsagenda.

Eigene Forschungsbeiträge und Forschungsergebnisse

Die vorliegende Dissertation enthält vier Forschungsbeiträge zum Forschungsgebiet IT-Compliance Management und Forschungsziel I sowie einen Forschungsbeitrag zum Forschungsgebiet IT-Risikomanagement und Forschungsziel II. Innerhalb des Forschungsgebietes und –zieles I bauen die einzelnen Forschungsbeiträge aufeinander auf.

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

- Entwicklung eines Prototypen mit einer Service-Orientierten Architektur bestehend aus einem integrierten Modell und funktionsorientierten Webservices zur Überwachung von Zugriffskontrollen in IT-Systemen, veröffentlicht bei der Hawaii International Conference on System Sciences (HICSS) 2010,
- Ergänzung des Prototypen um eine automatische Transformation von Zugriffskontrolldaten aus dem proprietären SAP-Modell in ein Standard-Modell und Weiterentwicklungen an der Architektur und den Webservices, veröffentlicht bei der European Conference on Information Systems (ECIS) 2010,
- Analyse der Anforderungen und der unterschiedlichen Informationsbedürfnisse verschiedener Anspruchsgruppen mit Bezugnahme auf unter-

schiedliche Einsatz- und Auswirkungsszenarien des Prototypen, veröffentlicht bei der International Conference on Availability, Reliability and Security (ARES) 2010,

- ❖ Darstellung von compliancerelevanten Informationen mit Hilfe eines Dashboards auf Basis der vom Prototyp bereitgestellten Daten, veröffentlicht beim International Workshop on Visualization and Information Security Management (VISM) 2010.

Innerhalb des Forschungsgebiets IT-Risikomanagement und des Forschungsziels II ist folgender Beitrag erstellt worden:

- ❖ Entwurf eines Ansatzes für ein Modell zur Berücksichtigung der Faktoren des „Fraud Triangle“ im IT-Risikomanagement unter Zuhilfenahme der bestehenden IT-Infrastruktur eines Unternehmens, ursprünglich bei der ECIS 2011 eingereicht, aktuell in der Überarbeitung für eine Neueinreichung.

Kritische Würdigung und Ausblick

Zur Erreichung der Forschungsziele ist die Forschungsmethode Design Science angewendet worden und entsprechende DS-Artefakte wurden geschaffen. Die Vorgehensweise bei der Erstellung der Forschungsbeiträge entspricht dem Design Science Prinzip bzw. der gestaltungsorientierten Wirtschaftsinformatik. Die Forschungsergebnisse entsprechen den Forschungszielen, so dass die Forschungsziele als umgesetzt angesehen werden können. Dennoch gibt es Aspekte, die einer kritischen Reflexion lohnen sowie weitere zukünftige Forschungsmöglichkeiten aufzeigen.

Kritische Würdigung

Nachfolgende Punkte sind einer kritischen Würdigung unterzogen worden:

- **Bei der Nutzung von IT-Compliance Management Anwendungen kann es zu einer einseitigen Sicht der Beurteilung von (Kontroll-) Problemen kommen.** Dann gibt es für die Nutzer dieser Anwendungen vorrangig nur noch das Szenario der Kontrollverletzung (Schwarz) oder Nichtverletzung (Weiß). Andere Überlegungen (Grau) werden nicht zugelassen bzw. in Betracht gezogen. Werden Ziele der Unternehmensführung, wie langfristige

Unternehmensexistenzsicherung und Ertragsorientierung berücksichtigt, ergibt sich oft ein etwas differenzierteres Bild. Das Eingehen eines abgeschätzten Risikos u. a. durch die Akzeptanz eines Restrisikos durch die Unternehmensführung kann betriebswirtschaftlich sinnvoll sein, wenn z. B. nur eine geringe Schadenshöhe, aber hohe Kontrollkosten erwartet werden. So ist eine „graue“ Sichtweise in einem Unternehmen unter Umständen gewünscht und muss im IT-Compliance Management entsprechend berücksichtigt werden.

- **Uneingeschränktes oder zu mindestens großes Vertrauen in die selbstkonfigurierten Kontrollen/Regeln der IT-Compliance Management Anwendung könnte bei den Verantwortlichen zu einer ungeprüften Akzeptanz der Ergebnisse führen.** So könnten die Prozesseigner bzw. Prozessverantwortlichen, die als Zielpersonen für eine eigenständige Konfiguration identifiziert wurden, ggf. der Fehleinschätzung unterliegen, dass durch die vorliegende Prozesskenntnis und selbstdefinierter Kontrollen kein unbeobachtetes Abweichen mehr möglich ist. Hier gilt es, den Anwender bzw. die Verantwortlichen durch Schulungen etc. zu sensibilisieren.
- **Abwägung von Kosten und Nutzen bei der Implementierung und beim Einsatz des Prototypen.** Vor dem Hintergrund einer Kosten-Nutzen-Diskussion und der Berücksichtigung der oft gegebenen heterogenen IT-Infrastruktur eignen sich u. a. die Eigenschaften des Prototypen für eine Zentralisierung von IT-Compliance Management Lösungen (Synergieeffekte) und für eine einfache Anbindung verschiedener IT-Systeme.
- **Überlegungen zur Einsatzfähigkeit der Ermittlung von Persönlichkeitsfaktoren unter Berücksichtigung gesetzlicher Rahmenbedingungen (z. B. BDSG).** Die rechtliche Situation in Deutschland erlaubt z. B. nicht den Einsatz von Anwendungen, die kontinuierlich eine Prüfung der Mitarbeiteraktivitäten in IT-Systemen vornehmen. Auf eine mögliche Lösung dieser Problematik mit Hilfe der Pseudonymisierung wird detaillierter eingegangen.

Ausblick

Folgende Punkte wurden für einen weiteren Forschungsbedarf identifiziert:

- **Prüfung der Akzeptanz und der Nutzung einer IT-Compliance Management Lösung mit Hilfe des Technology Acceptance Model (TAM).** Zielgruppe einer solchen Prüfung wären interne Fachkräfte eines Unternehmens und Mitarbeiter von Wirtschaftsprüfungsgesellschaften, die externe Prüfungen durchführen. Die ermittelten Faktoren würden Rückschlüsse auf die wahrgenommene Nützlichkeit und Einfachheit (usability) zulassen. Hieraus können dann Ideen oder Handlungsempfehlungen zur Umgestaltung bzw. zum Neudesign der IT-Compliance-Management-Software abgeleitet werden, um den Akzeptanz- und Nutzungslevel bei den Anwendern zu erhöhen.
- **Entwicklung verbesserter Methoden und Techniken, die die Anzahl der Falschmeldungen reduzieren.** Vorstellbar wäre der Einsatz Künstlicher Intelligenz bzw. Neuronaler Netze oder mathematischer Modelle zur differenzierten Analyse.
- **Verfügbarkeit aktueller Prozesssichten durch vom IT-System selbstgenerierte Prozessmodelle.** Dazu müssten diese um IT-Compliance Informationen angereicherte Prozessmodelle über eine Rückkopplung automatisiert in das IT-System übertragen werden und sich somit direkt auf die Prozesse auswirken können. So könnte das Verständnis der Prozesseigner für die Hinterlegung von Kontrollen in ihren Prozessen und den zu erwartenden Auswirkungen leichter geschaffen bzw. „live“ demonstriert werden.
- **Einbindung eines Knowledge Management Systems bei der Analyse von ermittelten IT-Compliance Informationen.** Die Verknüpfung von regulatorischen, gesetzlichen oder selbstgestellten Anforderungen mit strukturierten Daten aus dem betrieblichen oder organisationalen Kontext mit Hilfe eines Knowledge Management Systems könnte die Anwendbarkeit und das Verständnis der Analyse vereinfachen. Insgesamt ließe sich das Potenzial dieser Analysemöglichkeit erhöhen.

- **Abgleich der bisher berücksichtigten und umgesetzten Erkenntnisse mit den Anforderungsprofilen und –kriterien von Softwareauswahl-Frameworks im Bereich des Compliance.** Hier könnten sich weitere Ansatzpunkte zur Verbesserung oder Weiterentwicklung des Prototypen ergeben.
- **Unterstützung der Extensible Business Reporting Language (XBRL).** Mit der Unterstützung bzw. Implementierung von XBRL könnten Daten leichter mit anderen IT-Compliance Lösungen ausgetauscht oder aus unterstützenden Quellsystemen kontextbezogen exportiert werden.
- **Prüfung der Implementierungstauglichkeit für Echtzeitanalysen in IT-Systemen.** Ein Ansatzpunkt wäre die Nutzung eines alternativen Policy Decision Points (PDP). Dafür wäre eine Evaluation möglicher PDPs zur Prüfung der Einsatzfähigkeit in diesem Arbeitsgebiet notwendig. Die anschließenden Performancemessungen der in Frage kommenden PDPs würden Hinweise auf die Implementierungstauglichkeit für eine Echtzeit-analyse geben.
- **Identifizierung weiterer Persönlichkeitsmerkmale, die in Verbindung mit IT-Sicherheit, Betrugsaufdeckung oder IT-Compliance in Zusammen-hang gebracht werden können.** Denkbar wäre die Anwendung bzw. der Einsatz von Modellen aus der Psychologie z. B. das „Big Five"- oder Fünf-Faktoren-Modell (FFM). Bei der Berücksichtigung der ermittelten Faktoren besteht für die konkrete operative Ausgestaltung und Würdigung noch Forschungsbedarf.
- **Ermöglichung zeitnaher Risikoabschätzungen durch Anreicherung des PDPs**. So könnte der PDP (z. B. direkt implementiert in Prüfungsanwen-dungen) schon im Entscheidungsprozess eigenständig entsprechende Entscheidungen fällen oder Warnungen ausgeben. Die Risikoabschätzungen würden dazu um die Mitarbeitereinstufungen respektive durch den ermittelten potential threat classification (PTC) Faktor ergänzt werden.

Für Beatrice und meine Eltern.

Inhaltsverzeichnis

Seite

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACFE	Association of Certified Fraud Examiners
ACM	Association for Computing Machinery
AIS	Association for 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
BPMN	Business Process Modeling Notation
BSR	Behavioural Science Research
BWL	Betriebswirtschaftslehre
COBIT	Control Objectives for Information and related Technology
DEXA	International Conference on Database and Expert Systems Applications
DS	Design Science
DSR	Design Science Research
DV	Datenverarbeitung
DW	Data Warehouse
ECIS	European Conference on Information Systems
EMEA	Europa, Mittlerer Osten und Afrika
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 DV-gestützter Buchführungssysteme
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
IKS	Internes Kontrollsystem
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library
IS	Information Science
ISACA	Information Systems Audit and Control Association
IuK	Informations- und Kommunikationssystem
KMS	Knowledge Management System
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
NBA	Network Behavior Analysis
PDP	Policy Decision Point
PTC	Potential Threat Classification
SOA	Service-Orientierte Architektur
Solvabilität II	Solvabilitätsvorschriften für die Eigenmittelausstattung von Versicherungsunternehmen
SOX	Sarbanes-Oxley Act
TAM	Technology Acceptance Model
VHB	Verband der Hochschullehrer für Betriebswirtschaft
VISM	International Workshop on Visualization and Information Security Management
WI	Wirtschaftsinformatik
WKWI	Wissenschaftlichen Kommission Wirtschaftsinformatik
XACML	Extensible Access Control Markup Language

1 Einleitung

Die Informationstechnologie (IT) hat in den letzten Jahrzehnten erheblich an Bedeutung gewonnen. Eine Ursache dafür ist, dass die Geschäftsabwicklung und die Geschäftsprozesse vieler Unternehmen und Organisationen stark abhängig von dem Einsatz der IT bzw. der Unterstützung durch die IT sind. Ohne eine gut strukturierte IT bzw. an den Bedürfnissen des Unternehmens ausgerichtete IT-Dienstleistungen sind für viele Unternehmen ein Marktbestehen oder gar ein wirtschaftlicher Erfolg nicht mehr zu erreichen.[5] Das wirtschaftliche Handeln muss dabei fortwährend mit Gesetzen und Normen in Einklang gebracht werden.

Bekannt gewordene Verstöße wie z. B. auf internationaler Ebene Enron und Worldcom oder auf nationaler Ebene Flowtex haben u. a. dafür gesorgt, dass in den letzten Jahren vielfältige staatliche und nichtstaatliche Vorgaben erlassen worden sind. Diese oft verpflichtenden Vorgaben (zur Vermeidung von Verstößen) lassen sich unter den Begriffen Compliance und Governance subsummieren. Compliance bezieht sich auf gesetzliche oder regulatorische Anforderungen. Governance hingegen bezieht sich auf die von der Unternehmensführung erlassenen Auflagen.[6] Bedingt durch den hohen Automatisierungs- und Durchdringungsgrad der IT wird eine Vielzahl von Geschäftsprozessen direkt in den IT-Systemen der Unternehmen implementiert.[7] In diesen IT-Systemen lassen sich deshalb häufig Verletzungen der Auflagen und Vorgaben identifizieren. Es gilt daher, neben dem oft vorherrschenden Fokus der Ausrichtung der IT an betriebswirtschaftlichen Prozessen und Zielen, auch Kontrollziele in IT-Systeme festzulegen, Risikobewertungen vorzunehmen und Kontrollen durch Audits zu überwachen. Die Einhaltung von gesetzlichen Regularien durch IT-Systeme wird auch als IT-Compliance bezeichnet.

Aktuelle Regularien wie z. B. Sarbanes-Oxley Act (SOX), Solvabilität II oder Basel II legen die Vorgaben und Anforderungen fest. Die operative Umsetzung dieser Anforderungen hingegen obliegt den Unternehmen. Die Überprüfung der technischen Implementierungen und die Einhaltung der IT-Compliance-Vorschriften bedürfen meist eines hohen manuellen Aufwands. Um den finanziellen, zeitlichen und personellen Aufwand zu strukturieren, werden oft Rahmenwerke wie z. B. Control Objectives for Information and related Technology (COBIT) oder

[5] Vgl. Disterer 2009, S. 530.
[6] Vgl. Müller und Terzidis 2008, S. 341.
[7] Vgl. ebd., S. 341.

Information Technology Infrastructure Library (ITIL) hinzugezogen. In diesem vielschichtigen Kontext, oft erschwert durch die Heterogenität und Komplexität der IT-Systeme, werden nun Anwendungsprogramme eingesetzt, die umfangreiche Audits regelmäßig und zeitnah ermöglichen bzw. erleichtern sollen. Der Einsatzzeitpunkt der Anwendungsprogramme lässt sich grob in „vor dem Ereignis“ (ex ante) und „nach dem Ereignis“ (ex post) unterscheiden. Beim ex ante Ansatz wird schon im Entwurf eine Identifikation von Problemen und Schwachstellen angestrebt. Beim ex post Ansatz werden die bereits durchgeführten Geschäftsvorfälle im Nachhinein auf Verletzungen der Compliance geprüft. Aktuelle Audit-Programme arbeiten meist ex post.[8] Sie können somit Aussagen zur Compliance nur nachträglich bezogen auf den jeweiligen Zeitpunkt tätigen, sich aber nicht auf aktuelle Geschäftsvorfälle beziehen.

Ungeachtet dessen ist die zeitnahe Berichterstattung eventueller Kontrollausnahmen und die zügige Veranlassung von Gegenmaßnahmen ein Erfolgsfaktor für ein funktionierendes IKS. Die prüfenden und informierenden Anwendungssysteme sind essentielle Bestandteile eines IT-Compliance Managements. Daher beschäftigen sich die Forschungsbeiträge der vorliegenden Dissertation mit dieser Art von Anwendungssystem. Innerhalb der Forschungsbeiträge werden Verfahren, Modelle und Implementierungen zur automatisierten Überwachung von Kontrollen in IT-Systemen vorgestellt. Die Kontrollziele werden mit Hilfe von Monitoren überwacht, und durch ein anpassbares Regelwerk können Geschäftsvorfälle untersucht werden. Eine zielgruppengerechte Kommunikation der Ergebnisse erfolgt anhand der Einbindung eines Business Intelligence (BI)-Systems.

Bei der Prüfung in den IT-Systemen werden vorzugsweise technisch leicht abbildbare Anhaltspunkte untersucht wie z. B. Berechtigungsvorgaben oder Buchungsbelege. Der Faktor Mensch als qualitative Komponente wird nicht umfangreich in die Prüfung integriert. Nach der „Global Fraud Study“ der Association of Certified Fraud Examiners (ACFE) werden jedoch 80% der Betrugsfälle (fraud) in den eigenen Unternehmensreihen, insbesondere durch Mitarbeiter in den Bereichen Rechnungswesen, Vertrieb, Einkauf, Kundenservice oder höheres Management begangen.[9] Im Normalfall werden in diesen Bereichen Enterprise Resource Planning (ERP)-Systeme eingesetzt, die bisher auch vorrangig im Fokus der technisch

[8] Vgl. Müller und Terzidis 2008, S. 341.
[9] Vgl. ACFE 2010, S. 5.

orientierten Prüfungen standen. Trotz einer Vielzahl technischer Verbesserungen in diesem Gebiet, dauert es nach der Studie der ACFE im Durchschnitt bis zu 18 Monate, um einen Betrugsfall aufzudecken. Dies lässt darauf schließen, dass die Informationen, die derzeit mit den gängigen Techniken geliefert werden, nicht unbedingt für eine zeitnahe Betrugsaufdeckung ausreichen. In einem Forschungsbeitrag dieser Dissertation (s. Abschnitt 5.5) wird daher ein generisches Architekturmodell vorgestellt. Es ermöglicht, den „Fraud Triangle"-Faktoren - Gelegenheit, Motiv und Innere Rechtfertigung - Rechnung zu tragen, so dass es abschließend zu einer Risikoklassifikation eines Unternehmensangehörigen kommt. Die Berücksichtigung dieser Faktoren bietet insofern einen Mehrwert, als die von einem Auditor zu untersuchenden Geschäftstransaktionen besser differenziert und priorisiert werden können. Durch die Einbeziehung des menschlichen Verhaltens ist es möglich, Geschäftstransaktionen zu entdecken, die einem bisher noch nicht bekannten Muster unterliegen und mit herkömmlichen Mitteln unentdeckt geblieben wären.

Zwischen den Forschungsgebieten IT-Compliance Management und IT-Risikomanagement zeigt sich ein enger thematischer Zusammenhang. Beide Themen haben eine Reihe von Schnittpunkten, die sich bei der Nutzung von IT-gestützten Werkzeugen, mit einem hohen Automatisierungsgrad zur Anlage, Anreicherung, Überwachung und Berichterstattung von Kontrollen darstellen lassen.

Die vorliegende kumulative Dissertation enthält fünf verschiedene Forschungsbeiträge. Vier der Forschungsbeiträge wurden bereits veröffentlicht. Einer befindet sich noch in der Überarbeitung für eine Neueinreichung. Die veröffentlichten Beiträge wurden alle bei renommierten internationalen Konferenzen eingereicht und haben dabei immer ein blindes Begutachtungsverfahren mit mindestens zwei bzw. drei Gutachtern erfolgreich durchlaufen.

Nachfolgend ist die Arbeit in folgende Kapitel aufgeteilt: die für die vorgestellten Forschungsbeiträge wichtigen Grundlagen werden getrennt nach dem Forschungsgebiet IT-Compliance Management und dem Forschungsgebiet IT-Risikomanagement in Kapitel 2 vorgestellt. Eine Übersicht über den aktuellen Forschungsstand zu dem Forschungsgebiet IT-Risikomanagement, wird anhand einer umfangreichen Literaturrecherche in Kapitel 3 gegeben. Für das Forschungsgebiet IT-Compliance Management werden dafür wichtige ausgewählte Beiträge herangezogen. In Kapitel 4 wird erst auf wissenschaftstheoretische Grundlagen sowie auf die wissen-

schaftstheoretische Fundierung der Wirtschaftsinformatik eingegangen. Darauf aufbauend werden die gesetzten Forschungsziele und eingesetzten Forschungsmethoden erläutert. Die selbstverfassten Forschungsbeiträge werden in Kapitel 5 gewürdigt. Dabei werden ergänzend die charakterisierenden Eckdaten der Forschungsbeiträge wie Einstufung in den Rankinglisten, Konferenzbeschreibung und Aufgabenteilung der Autoren beschrieben. Abschließend werden in Kapitel 6 die Forschungsbeiträge einer kritischen Reflexion unterzogen und mögliche Schritte für zukünftige Ansätze werden dargelegt. Im Anhang werden die ungekürzten Forschungsbeiträge aufgeführt.

2 Grundlagen

Um die Forschungsbeiträge in den Forschungsgebieten IT-Compliance Management und IT-Risikomanagement verorten zu können, werden in den folgenden Abschnitten Grundlagen für eine Einführung in diesen Themengebieten gegeben.

2.1 Governance und Compliance

In der Literatur wird oft nicht trennscharf zwischen den Begriffen Governance und Compliance unterschieden bzw. die beiden Begriffe werden häufig fast synonym im Kontext des Governance, Risk und Compliance (GRC) verwendet.[10] Die einzelnen Teilbereiche des GRC lassen sich wie folgt charakterisieren:

- „Corporate Governance: Rahmenwerk von Regeln und Richtlinien, nach denen ein Unternehmen geführt und kontrolliert werden soll
- Risk Management: strukturierter Prozess des einheitlichen und pro-aktiven Umgangs mit Risiken und Chancen
- Compliance Management: effektive und effiziente Erfüllung sämtlicher verbindlichen Richtlinien und Vorgaben.“ [11]

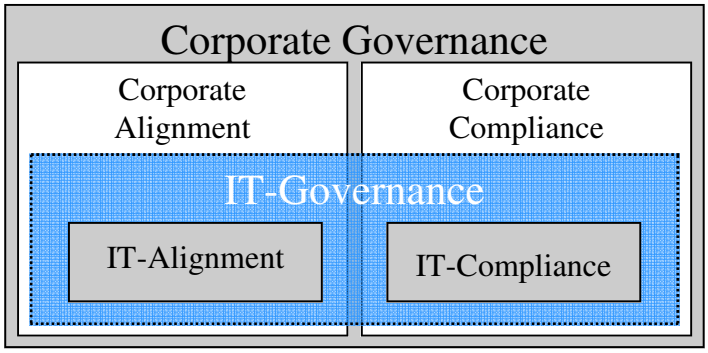

Abbildung 1: Verortung von Governance, IT-Alignment und IT-Compliance.
Quelle: Gull 2010, S. I-2.

Die Abbildung 1 zeigt, wie sich die Teilbereiche der IT-Governance und IT-Compliance in die strategische Unternehmensausrichtung der Corporate Governance und Corporate Compliance einfügen. Das Corporate Alignment bzw. das IT-Alignment[12] wird im Folgenden nicht näher beschrieben, da sich die erstellten

[10] Vgl. Bassen und Zöllner 2009; Teubner und Feller 2008, S. 400.
[11] Goll und Haupt 2008, S. 150.
[12] IT-Alignment ist die Ausrichtung der IT auf die Geschäftsziele. Vgl. Kozlova 2008, S. 418.

Forschungsbeiträge nicht in diesen Teilgebieten bewegen. Zur genaueren Begriffsbestimmung wird in den nächsten Abschnitten von der allgemeinen Bedeutung der Begriffe hin zum speziellen Einsatz im IT gestützten Kontext Bezug genommen.

2.1.1 Corporate Governance und Corporate Compliance

Die Corporate Governance ist ein Teilgebiet der Unternehmensführung.[13] Sie ist, unter Einbezug bzw. Interessensausgleich der Stake- und Shareholder, für die Ausrichtung der Unternehmensleitung und -überwachung auf eine langfristige und verantwortliche Unternehmensführung zuständig.[14] Die Ausrichtung erfolgt unter Rückgriff auf marktliche Regelungen und Gesetze wie z. B. den Deutschen Corporate Governance Kodex[15], die internationalen Principles of Corporate Governance, veröffentlicht durch die Organisation for Economic Co-operation and Development (OECD)[16], das „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ (KonTraG)[17] oder den Sarbanes-Oxley Act (SOX)[18].

Für den Begriff der Corporate Compliance gibt es in der Literatur und der Praxis sowie im gesetzlichen Umfeld keine einheitliche Bestimmung.[19] In dieser Arbeit wird auf die Begriffsbestimmung von Junc (2010, S. 9) zurückgegriffen, der die herrschende Meinung wie folgt zusammenfasst:

> *„Unter Corporate Compliance wird die unternehmensweite Organisation aller Maßnahmen zur Sicherstellung normenkonformen Verhaltens der Mitarbeiter und Organe eines Unternehmens verstanden.“*

Der Begriff Compliance wird vom englischen Ausdruck „to comply with“ (erfüllen, einhalten) abgeleitet und bezieht sich auf die Einhaltung von Vorgaben.[20] Der Terminus wurde im US-amerikanischen Bankenumfeld geprägt und bezieht sich auf die systematisierte Sicherstellung der Einhaltung von Vorgaben in den klassischen Risikobereichen der Finanzdienstleister.[21] Mit Beginn der 1990er Jahre fand dieses Thema in Europa und auch in Deutschland im Bereich des Banken- und Kapital-

[13] Vgl. Rosen 2001.
[14] Vgl. a. a. O.; Vgl. Teubner und Feller 2008, S. 400f.
[15] DCGK 2010.
[16] OECD 2004.
[17] KONTRAG 1998.
[18] SOX 2002.
[19] Vgl. Wolf 2006, S. 1995.
[20] Vgl. Roth 2009, S. 5.
[21] Vgl. Fleischer 2008, S. 1ff.

markts Widerhall.[22] In den folgenden Jahren wurden durch eine zunehmende Regulierungsdichte die Anwendungsfelder z. B. um Datenschutz-, Umwelt- und Steuerrecht erweitert.[23] Das führte zu einer branchenunabhängigen Verwendung, die inzwischen verschiedenste (unternehmerische) Vorgaben berücksichtigen muss.[24] Der Zusatz Corporate in der Corporate Compliance hebt somit die unternehmensweite Sicherstellung der Einhaltung hervor und bezieht sich auf alle Bereiche und Mitarbeiter eines Unternehmens.

2.1.2 IT-Governance

Innerhalb der Corporate Compliance stellt die IT-Governance ein Framework dar, das ein Entscheidungs- und ein Organisationskonzept vereint.[25] Mit dem Begriff IT-Governance wird dabei in der Literatur und in der Praxis eine Vielzahl von Aufgaben, Zielen und Institutionen verbunden.[26]

Es werden in diesem Zusammenhang oft zwei Ansätze postuliert. Ein in der Literatur sehr häufig zitierter Ansatz ist der von Weill und Ross (2004).[27] Sie verstehen IT-Governance als:

> *„[…] specifying the decision rights and accountability framework to encourage desirable behavior in using IT.“*[28]

und stellen damit das Problem der Etablierung von Entscheidungsrechten und Verantwortlichkeiten im Umgang mit der IT in den Mittelpunkt. Weill und Ross (2004) heben dabei die Bedeutung eines Ordnungsrahmens für die IT hervor und vertreten damit einen engen IT-Governance Begriff mit nach außen gerichteter Sichtweise.[29]

Beim zweiten Ansatz liegt ein weiteres Verständnis des IT-Governance Begriffs vor und eine nach innen gerichtete Sichtweise steht im Vordergrund.[30] Ein Vertreter

[22] Vgl. Lösler 2003, S. 15ff.
[23] Vgl. Junc 2010, S. 7f.
[24] Vgl. Campos Nave und Bonenberger 2008, S. 734.
[25] Vgl. Teubner und Feller 2008, S. 403ff.
[26] Vgl. Strecker 2009, S. i.
[27] Vgl. Kozlova 2008, S. 418.
[28] Weill und Ross 2004, S. 2.
[29] Vgl. Strecker 2009, S. 3.
[30] Vgl. a. a. O., S. 4.

dieser Sichtweise ist das IT Governance Institut[31]. Für das IT Governance Institut ist IT-Governance:

> *"[…] the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives."*[32]

Dieser Ansatz beinhaltet Elemente, die oft in die Bereiche Informations- und IT-Management verortet werden. So wird die konkrete, operative Umsetzung der IT-Governance im Zusammenhang mit sicheren, risikominimierten IT-Prozessen und Prüfungsansätzen in den Vordergrund gerückt.[33]
Die Verknüpfung beider Ansätze kann somit die operative, ausführende Ebene und die Managementebene sinnvoll zusammenführen.

2.1.3 IT-Compliance

Der in Abschnitt 2.1.2 eingeführte Begriff der IT-Governance soll als Teil der Corporate Compliance die Einhaltung von Regelungen mit IT Bezug sicherstellen. Als Teilbereich der IT Governance fügt sich die IT-Compliance somit in die Corporate Compliance ein. Die IT-Compliance widmet sich im speziellen den IT-nahen Bestimmungen und prüft deren Einhaltung. Beispiele für diese IT-nahen Bestimmungen sind SOX, die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)[34], das Bundesdatenschutzgesetz (BDSG)[35] oder die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)[36]. Allerdings kann sich auch Handlungsbedarf aus Bestimmungen ergeben, die nicht direkt einen IT-Bezug aufweisen. So können z. B. Vorgaben aus dem Handels- und Steuerrecht zu abgeleiteten Maßnahmen in der IT führen. Grundlegend dazu ist u. a. die Abgabenordnung (AO), die die Grundsätze ordnungsmäßiger Buchführung (GoB) anführt. Für DV-gestützte Buchführungssysteme wird die AO durch die GoBS konkretisiert. Zur Einhaltung der Vorschriften ist nach der GoBS die Etablierung eines IKS vorgesehen.[37] Die eingerichteten Kontrollen eines IKS sollen dabei

[31] Vgl. ITGI 2010.
[32] ITGI 2007, S. 5.
[33] Vgl. Kozlova 2008, S. 420.
[34] Vgl. GOBS 1995.
[35] Vgl. BDSG 2003.
[36] Vgl. GDPdU 2001.
[37] Vgl. Strohmeier 2008, S. 51.

vorrangig die Unternehmensprozesse überwachen und präventiv gegen kriminelles Handeln wirken bzw. dieses aufdecken.[38] Hinsichtlich der DV-gestützten Systeme erfordert dies manuelle oder maschinelle Kontrollen. Letztere können u. a. in die Programmabfolge oder auf Ebene der Anwendungsprogramme integriert werden.[39]

Für die Integration und Durchführung der Kontrollen bieten sich IT-Compliance-Management-Anwendungen an, die hinsichtlich Installationstiefe und -umfang sehr unterschiedlich sein können.

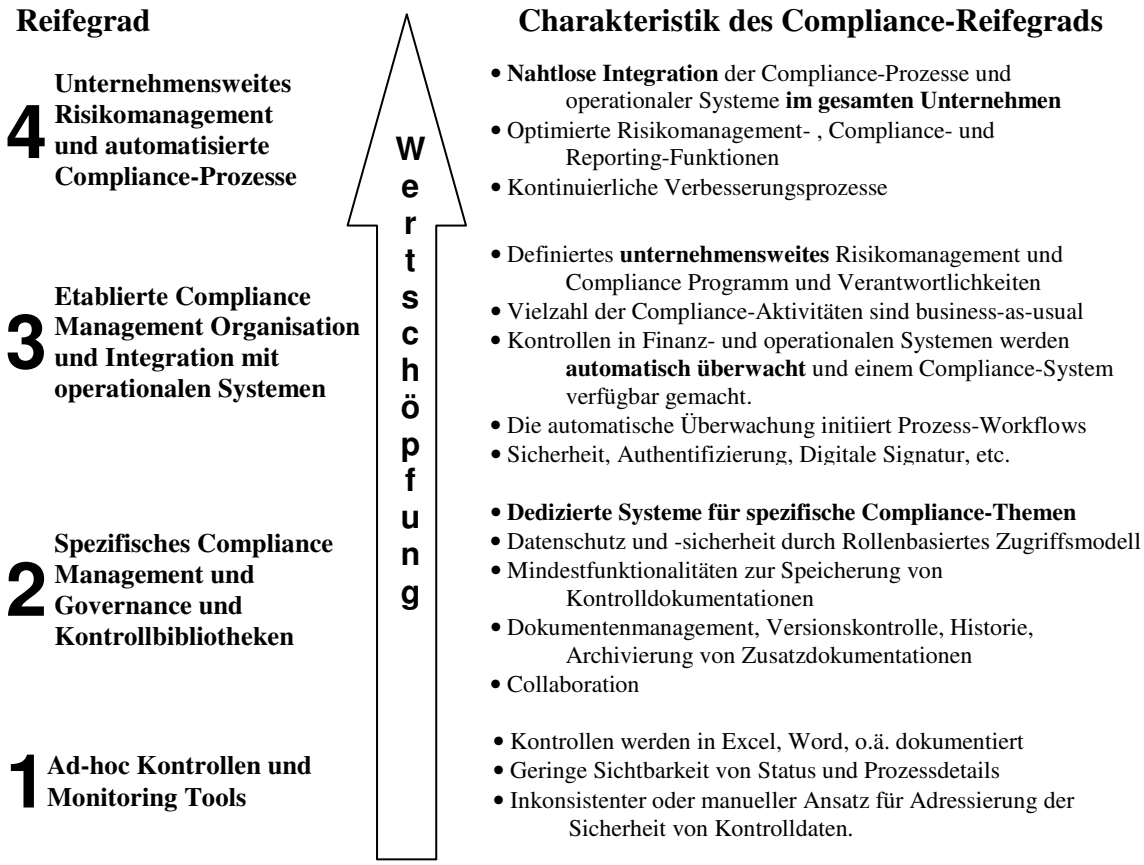

Abbildung 2: Reifegradmodell für Governance, Risiko und Compliance-Management.

Quelle: Standke (2010), S. 272.

Der Grad der Unterstützung durch IT-Compliance-Management-Anwendungen spiegelt sich auch bei dem Reifegrad des GRC-Managements eines Unternehmens wieder (s. Abbildung 2). So ist der Reifegrad 3 für diese Arbeit von Interesse, da in diesem Reifegrad die automatische Überwachung von operationalen Systemen durch Kontrollen und die automatische Bereitstellung der Ergebnisse in einem Compliance-System verortet wird. Eine ähnliche Charakteristik wird in den Forschungsbeiträgen zum Forschungsgebiet I beschrieben.

[38] Vgl. Birkental 2011, S. 178.
[39] Vgl. GOBS 1995, 4.4, a, d.

2.2 Fraud Vermeidung

2.2.1 Bestimmung des Begriffs Fraud

Da der Begriff Fraud ursprünglich im US-amerikanischen Raum geprägt wurde, wird erst auf das Begriffsverständnis im US-amerikanischen Raum und anschließend auf die Verwendung im deutschen Sprachraum eingegangen.[40] Der englischen Übersetzung zur Folge wird „Fraud“ nur anspruchslos mit „Betrug“ oder „Schwindel“ übersetzt werden.[41] Diese Übersetzung greift aufgrund der umfangreichen, vielschichtigen Bedeutung im Englischen zu kurz. Der Bedeutungsumfang von Fraud oder die Sammelbegriffsfunktion kann im Deutschen eher mit dem Begriff „Wirtschaftskriminalität“ eingefangen werden.[42] Da der Begriff in der Literatur vielseitig verwendet wird und auch zum Teil auch unterschiedlich besetzt ist, wird eine einheitliche Begriffsdefinition schwierig.[43] So werden für eine genauere Begriffsbestimmung das juristische, das soziologische und das prüferische Verständnis herangezogen:

- Im juristischen Sinne beinhaltet Fraud alle vorstellbaren Möglichkeiten, die nötig sind unberechtigter Weise gegenüber einem Dritten in Vorteil zu gelangen. Der Vorteil, der bei diesem Hintergehen gewonnen wird, kann sich u. a. auf Vermögenswerte oder Geld beziehen (bank fraud, bankruptcy fraud).[44]
- Das soziologische Verständnis zielt auf täterbezogene Merkmale ab und beinhaltet Straftaten, die oft unter Ausnutzung des Status innerhalb der Berufstätigkeit begangen werden.[45]
- Das prüferische Verständnis nach Wells (2007, S. 1) wird z. B. von der ACFE genutzt[46] und definiert Fraud als

  > *„[…] the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.“*

[40] Vgl. Thomann und Hlavica 2011, S. 84.
[41] Vgl. Pons 1991.
[42] Vgl. Thomann und Hlavica 2011, S. 90f.
[43] Vgl. Singleton und Singleton 2010, S. 40f.
[44] Vgl. Thomann und Hlavica 2011, S. 86.
[45] Vgl. ebd., S. 86.
[46] Vgl. ACFE 2010, S. 6.

Hiernach kann eine Person ihre Befugnisse nutzen, um unrechtmäßig Geschäftsprozesse so zu gestalten, dass sie persönliche Vorteile daraus ziehen kann (occupational fraud).

Letzteres Verständnis ist für die vorliegende Arbeit maßgeblich.

2.2.2 Entstehungsgründe für Fraud

Bei der Vermeidung von Wirtschaftskriminalität oder Fraud sollte bei den Ursachen angesetzt werden. Für die Ursachen des Fehlverhaltens einzelner Personen lassen sich in der Literatur viele Erklärungsmodelle verschiedener Disziplinen finden.[47] Mit dem Fokus dieser Arbeit auf dem „Occupational Fraud“ (Bereicherung während der beruflichen Tätigkeit zu Lasten des Unternehmens) wird auf den prüferischen Ansatz Bezug genommen.[48]

Ein verbreitetes Modell dazu basiert auf den Forschungsergebnissen von Cressey.[49] Es wurde unter dem Begriff „Fraud Triangle“ bekannt und beschäftigt sich mit der Entstehung von Fraud in Unternehmen (s. Abbildung 3).[50]

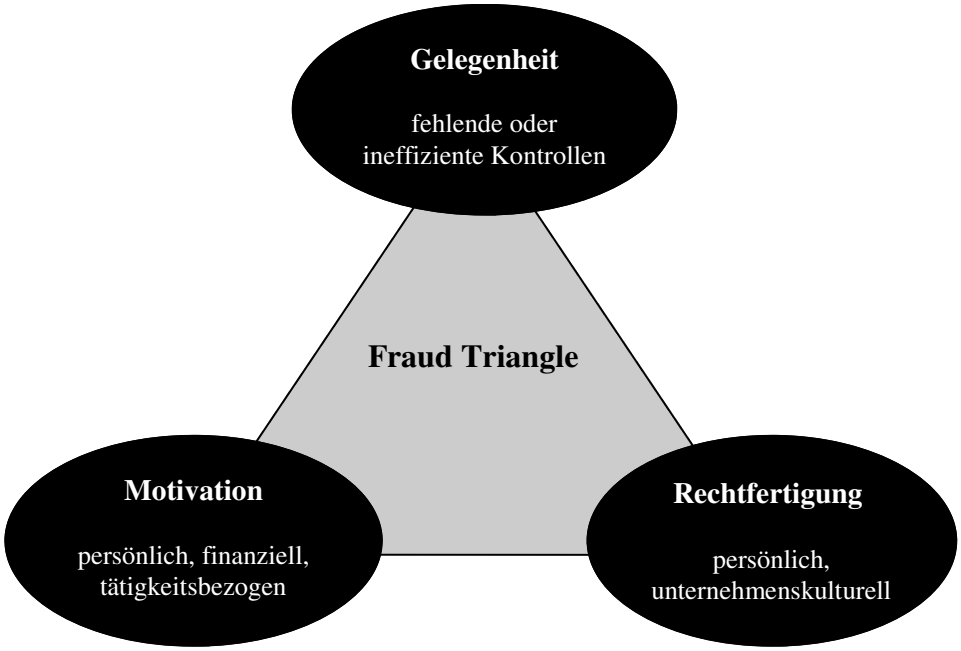

Abbildung 3: Aufbau des Fraud Triangle.

Quelle: Thomann und Hlavica 2011, S. 98.

[47] Vgl. Martenstein 2011, S. 96.
[48] Vgl. Thomann 2011, S. 87.
[49] Vgl. Cressey 1973, S. 30 nach Thomann 2011, S. 186.
[50] Vgl. Ramos 2003; Dieses Modell ist u. a. Element des internationalen Prüfungsstandards ISA 240 bzw. auch des IDW PS 210.

Entstehungsgründe für Fraud sind demnach das gleichzeitige Auftreten der drei Faktoren Gelegenheit, Motivation und Rechtfertigung bei einer Person:[51]

- Bei dem Faktor Gelegenheit wird einer Person der Freiraum zum Fehlverhalten im Unternehmen durch mangelnde oder fehlende Kontrollen eingeräumt.
- Der Faktor Motivation kann verschiedenartig begründet sein. Häufig sind persönliche finanzielle Probleme unterschiedlichster Art die Ursache für die Entwendung monetärer Mittel. Es können aber auch Faktoren der Persönlichkeit sein, die Anreize zum Fehlverhalten geben, wie z. B. Rache, Habgier, Langeweile oder der Wunsch nach Luxus. Die Tätigkeit selbst kann auch Anlass zum Fehlverhalten bieten. Um dem Faktor Leistungsdruck durch zu hohe Anforderungen, Erwartungen oder Zeitknappheit zu begegnen, wird eine Kompensationsstrategie mit Fehlverhalten gewählt.
- Der Faktor innere Rechtfertigung muss es einer Person erlauben, sich vor sich selbst für das eigene Fehlverhalten zu rechtfertigen. Dieser Aspekt wird sehr stark durch den Charakter und die soziale Umgebung geprägt, die Einfluss auf die moralischen und ethischen Vorstellungen zur eigenen Rechtfertigung haben.

Srivastava et al. (2003) unterstreichen, dass der Beziehung zwischen den drei Faktoren Gelegenheit, Motivation und Rechtfertigung eine besondere Bedeutung zukommt. Demnach steigt das Risiko für Fraud stark an, wenn die Stärke des Wirkungsgefüges zwischen den Faktoren zunimmt.[52]

Für Außenstehende oder Kontrollinstanzen sind die Zusammenhänge oder das Ausmaß einzelner Faktoren bei einer Person i. d. R. nur schwer erkennbar bzw. abschätzbar. Da die Faktoren Motivation und Rechtfertigung stark subjektiv geprägt sind, ist eine objektive Einschätzung sowie eine Veränderung der Ausgangslage durch Dritte nur sehr aufwendig zu realisieren. Bei dem Faktor Gelegenheit hingegen sind die ursächlichen Anlässe auf Unternehmensseite begründet und können daher vom Unternehmen oft eigenständig behoben werden.

[51] Vgl. Martenstein 2011, S. 97ff.
[52] Vgl. Srivastava et al. 2003, S. 26.

2.2.3 Prävention und Erkennung von Fraud

Grundsätzlich sollte es das Ziel eines Unternehmens sein, möglichst keinen Fraud zuzulassen. Da ein komplettes Ausschließen vermutlich nicht erreichbar ist, gilt es im Unternehmen, die präventiven Maßnahmen zu maximieren und gleichzeitig eine möglichst frühe Erkennung von Fraud zu fördern.[53]

Bei der Einleitung präventiver Maßnahmen stellt das „Fraud Triangle" Modell für ein Unternehmen einen bedeutenden Ansatz dar. Die Minderung der im „Fraud Triangle" Modell angeführten Faktoren bzw. der Ihnen zugeordneten Umstände führt zur Minderung des Risikos von Fraud im Unternehmen.[54] So kann ein Unternehmen den psychologischen Faktoren Motivation und Rechtfertigung selten direkt oder zeitnah entgegenwirken. Dies Bedarf eher eines langfristigen Konzepts, das auf breiter Basis im Unternehmen wirkt. Es können dazu verschiedene Maßnahmen getroffen werden, die unter Umständen auch weitgehende Auswirkungen auf die Organisation des Unternehmens haben. Die Konzeption sollte daher unternehmens-spezifische Besonderheiten berücksichtigen.

Elemente dieses Präventionskonzeptes oder Fraud Risiko Managements können Unternehmensleitfäden, Verhaltenskodexe, Schaffung eines positiven Arbeitsklimas oder eine Stärkung der Identifikation mit dem Unternehmen sein.[55] Dies soll die innere Rechtfertigungsmöglichkeit oder die Motivation der Mitarbeiter zum Fehlverhalten senken. Dabei sind die Erläuterungen der zu erwartenden Konsequenzen bei Fehlverhalten, der Inhalte der Kontrollen sowie die Vermittlung richtigen Verhaltens bedeutsam. Unter der Annahme, dass bis zu 60% der Mitarbeiter je nach Kontrollstärke zwischen Ehrlichkeit und Unehrlichkeit schwanken, könnte durch diese Maßnahmen ein Großteil des möglichen Fraudrisikos im Unternehmen gesenkt werden.[56]

Die Einschränkung des Faktors Gelegenheit ist für ein Unternehmen leichter zu realisieren und sollte ein erster Ansatzpunkt sein. Eine Möglichkeit der Umsetzung ist der Betrieb eines IKS mit effektiven und effizienten Kontrollen, die den Freiraum für Gelegenheiten erheblich einschränken können.

[53] Vgl. Thomann 2011, S. 185.
[54] Vgl. a. a. O., S. 187.
[55] Vgl. Birkental 2011, S. 181.
[56] Vgl. Jung 2005, S. 45.

3 Stand der Forschung und Literaturübersicht

Da in der zeitnahen Arbeit[57] von Matthias Kehlenbeck eine umfassende Aufstellung der Literatur bzw. des Forschungstandes zum Forschungsgebiet I nach Suchbegriffen, deren Häufigkeit und kumulierten Veröffentlichungsorten gegeben wird, wird in dieser Arbeit auf eine entsprechende Übersicht zu diesem Thema verzichtet. Sie gibt daher eine Übersicht zum Forschungsgebiet II mit Bezug zum IT-Risikomanagement und zur Aufdeckung von Fraud. Die Erstellung der Übersicht bzw. des Literaturreviews richtet sich in Grundzügen nach dem Leitfaden von Vom Brocke et al. (2009) und Ngai et al. (2011). Ziel dieser Autoren ist die Sicherstellung der Nachvollziehbarkeit bzw. der Ermöglichung der nachgelagerten Nutzung des Literaturreviews. Im Weiteren werden die charakterisierenden Faktoren der Literatursuche beschrieben, die Anzahl der Ergebnisse eingeordnet und einige ausgewählte Forschungsbeiträge verortet.

In der Literatur zum Thema Fraud werden, ähnlich wie bei der IT-Sicherheit, zwei Probleme in der Forschung angesprochen.[58] Das Eine ist die grundsätzliche Verfügbarkeit von Daten zu diesem Thema. So werden Fraudvorfälle meist nicht veröffentlicht bzw. bewusst verschwiegen. Eine Beschaffung und Analyse der Daten ist somit für Forscher meist schwierig. Die zweite Problematik betrifft die Forschungen in der Praxis. Sie veröffentlicht bewusst keine Ergebnisse wie z. B. bei der Entwicklung von Fraud-Gegenmaßnahmen. Hiermit soll verhindert werden, dass durch Kenntnis der Gegenmaßnahmen diese zukünftig umgangen werden.

Dennoch gibt es eine Reihe von Forschungsbeiträgen zum Thema Fraud Erkennung und Entdeckung. Diese betreffen überwiegend die fachspezifischen Anwendungen in der Finanzbranche.[59] Daher ist die Finanzbranche auch ein Forschungsgebiet mit einer recht großen Publikationsdichte.[60] Im Gegensatz dazu ist das für diese Arbeit bedeutsame „occupational fraud“ mit dem Bezugsmodell „Fraud Triangle“ in der Literatur weniger vertreten.

Für eine strukturierte Übersicht sind drei Phasen durchlaufen worden:[61] Zieldefinition, Methodenauswahl und Auswertung. In der ersten Phase ist als

[57] Vgl. Kehlenbeck 2011.
[58] Vgl. Allan und Zhan 2010.
[59] Vgl. a. a. O.
[60] Eine aktuelle Übersicht zu dem Thema „financial fraud detection“ gibt Ngai et al. 2011.
[61] Vgl. Ngai et al. 2011, S. 560f.

Forschungsziel die Entdeckung von internem Fraud unter der Nutzung der Faktoren des „Fraud Triangles“ definiert (s. Forschungsziel II) worden. Für den Forschungsbereich ist der Fokus auf akademische Literatur gelegt, der zeitliche Rahmen aber nicht eingeschränkt worden. Da das Thema „Entdeckung von Fraud“ vielseitig (psychologisch, technisch oder mathematisch) bearbeitet werden kann, ist in der zweiten Phase eine fachunspezifische Suche favorisiert worden. Es sind dazu fünf bekannte Literaturdatenbanken aus der IS-Disziplin ausgewählt worden:

- ACM Digital Library[62]
- AIS Library[63]
- IEEE Xplore Digital Library[64]
- Sciencedirect[65]
- Springerlink[66]

Diese Datenbanken beinhalten u. a. die wichtigsten Journals und Konferenzen und können mit einer Volltextsuche abgefragt werden. Für die Volltextsuche sind die Begriffe (i) *„fraud triangle“* und (ii) *"internal fraud" AND (prediction OR prevention OR detection)* gewählt worden. Der Begriff (i) ist insgesamt 65 und der Begriff (ii) 116 Mal in den Beiträgen gefunden worden. Als Grundlage der Prüfung auf den thematischen Zusammenhang dienten bei den selektierten Beiträgen der Titel und die Kurzzusammenfassung. In der letzten Phase wird auf Beiträge, die in dieser Prüfung eine starke Relevanz zum Forschungsziel II gezeigt haben, eingegangen.

Greitzer et al. (2011) diskutieren soziale und ethische Aspekte vor dem Hintergrund der vorhersagenden, internen Bedrohungsüberwachung (basierend auf dem „Fraud Triangle“). Zur Ermittlung der Vorhersagbarkeit von Bedrohungen durch interne Mitarbeiter bestimmen die Autoren dabei mögliche Informationsquellen und bewerten sie unter der zulässigen Einbeziehbarkeit nach US-amerikanischen Gesetz. Die ermittelten Indikatoren dienen als Grundlage für ein Vorhersagbarkeitsmodell. Ethische und moralische Aspekte des Modells werden diskutiert. Eine praktische Umsetzung erfolgt nicht.

[62] ACM 2011.
[63] AIS 2011b.
[64] IEEE 2011.
[65] Elsevier 2011.
[66] Springer 2011.

Die Art der in den Unternehmen verwendeten Kontrollen untersuchen Goode und Lacey (2011). Sie stellen fest, dass eine Reihe von technischen und sozio-technische Kontrollen verwendet werden. In dem von ihnen untersuchten Unternehmen wären nur ein Drittel der Fraud-Fälle mit rein technischen Kontrollen entdeckt worden. Die Autoren plädieren daher auf eine multidimensionale Betrachtung der Fraud-Kontrollen.

Murphy und Dacin (2011) beschreiben ein Rahmenwerk, das zur erhöhten Fraud Vermeidung beitragen soll. Dazu wird detaillierter auf die einzelnen Faktoren des „Fraud Triangle“ eingegangen und es werden die ursächlichen Auslöser untersucht.

Die Identifikation und Einstufung von potentiell Fraud verdächtigen Personen ist ein Kernelement in dem „Insider Threat Prediction Model“ von Kandias et al. (2010). Die Autoren nutzen dafür Daten aus der IT Infrastruktur (z. B. Intrusion Detection System), um einen Überblick über den Nutzer zu bekommen. Der Fokus liegt dabei auf der Einstufung einer Person, eine weitere Verknüpfung der Ergebnisse findet nicht statt. Eine praktische Umsetzung in einen Prototyp erfolgt nicht.

Die Entwicklung eines Rahmenwerks zur Verknüpfung von „klassischen“ Daten der IT-Sicherheit mit psychologischen Daten beschreiben Greitzer und Frincke (2010). Die Autoren sehen in diesem Ansatz den Entwicklungsschritt von der Entdeckung zur Vorhersage. Bei der Beschreibung des Ansatzes wird auf die Herausforderungen, die Umsetzungsmöglichkeiten und den Entscheidungsansatz eingegangen. Mit Hilfe einer Simulation wird das Rahmenwerk bzw. der „Status Indikator“ über das Risiko eines Mitarbeiters einem Validierungstest unterzogen.

Jans et al. (2010) nutzen einen „descriptive data mining“-Ansatz um das Risiko des internen Fraud zu reduzieren. Die Autoren sehen ihren Ansatz der Risikoreduktion mithilfe multivariaten Clustering im Vorteil gegenüber einer einfachen Risikoklassifikation. Sie plädieren für eine Kombination aus Fraud-Erkennung und -Verhinderung.

Die Präsentation und Evaluation eines Modells, das kriminologische, psychologische und IT-Informationen zur Reduktion von IT-Missbrauch verknüpft, steht bei D’Arcy et al. (2009) im Vordergrund. Die Autoren kommen zu dem Schluss, dass die wahrgenommene Schwere der Sanktionen entscheidend ist. Eine praktische Umsetzung erfolgt nicht.

Eine Übersicht über verschiedene Analysemöglichkeiten zum Erkennen von Bedrohungen durch Insider geben Salem et al. (2008). Das Verhalten von Nutzern wird mit Hilfe von verschiedenen Methoden untersucht. Die Autoren kommen zu dem Schluss, dass noch erheblicher Forschungsbedarf besteht und eine Evaluation und Bewährung in der Praxis noch aussteht.

Auf Basis der Spieltheorie entwerfen Liu et al. (2008) ein Modell, mit dem die Aktionen der kriminell Handelnden vorhergesagt und die passende Gegenreaktion identifiziert wird. Im Fokus stehen dabei technische Aspekte der Berechtigungsvergabe bzw. des Berechtigungsentzugs.

Ray und Bradford (2007) beschreiben einen Machbarkeitsnachweis zur Erkennung von internen Bedrohungen. Die Autoren konzentrieren sich dabei auf die Beobachtung des Arbeitsplatzes unter Microsoft Windows und die Speicherung der ermittelten Daten. Eine weitere Verknüpfung der Daten findet nicht statt.

In einem Großteil der Forschungsbeiträge wird bei kriminellen Handlungen von einer bewussten Intention des Handelnden ausgegangen. Taylor (2006) setzt sich hingegen mit unabsichtlichen Handelnden und deren Einfluss auf die IT-Sicherheitsrisiken auseinander. Der Autor kommt zu dem Schluss, dass auf der Ebene des Managements ein größeres Bewusstsein für diese Art von Risiken geschaffen werden muss.

Theoharidou et al. (2005) stellen verschiedene Theorien zur Erklärung von kriminellen Handlungen in Unternehmen der ISO/IEC 17799[67] gegenüber. Diese Norm ist, in Verbindung mit der oft geforderten ISO/IEC 27001[68] Zertifizierung, ein Leitfaden für ein Informationssicherheitsmanagementsystem in einem Unternehmen. Die Autoren finden die Erkenntnisse aus den Theorien in der Norm nur schwach abgebildet und kommen zu dem Schluss, dass noch geeignete Kontrollen bzw. Maßnahmen zu diesem Thema fehlen.

Symonenko et al. (2004) verknüpfen in ihrem Ansatz verschiedene Datenquellen zu einer Risikoanalyse. Die Autoren nutzen dafür Daten einer sozialen Netzwerk Analyse, Berichte über Zugriffsrechte und semantische Analysen der Kommunikation mit Hilfe der Computerlinguistik. Der Schwerpunkt liegt auf der Weiterentwicklung einer Computerlinguistikanwendung.

[67] Seit dem 1.7.2007 ist es die ISO/IEC 27002.
[68] ISO 2005.

4 Forschungsdesign

In diesem Kapitel werden Forschungsgrundlagen und –methoden vorgestellt, welche für die Forschungsbeiträge genutzt worden sind, die dieser Dissertation zu Grunde liegen. Um das Vorgehen, die Wahl der Forschungsmethoden und die gesetzten Forschungsziele besser nachvollziehen zu können, werden zunächst Grundlagen zum wissenschaftlichen Vorgehen in der Wirtschaftsinformatik (WI) erläutert. Die dazu notwendigen Begriffe aus der Wissenschaftstheorie, die die Grundlagen für ein Verständnis der Forschung in der Wirtschaftsinformatik legen, werden daher im Weiteren kurz definiert. Darauf aufbauend wird auf die Forschungsmethodik der Wirtschaftsinformatik eingegangen, die sich nicht nur in der Methodik sondern auch im Selbstverständnis von der internationalen Information Science (IS) unterscheidet. Da die Forschungsbeiträge auf internationalen IS-Konferenzen vorgestellt worden sind und auch internationale IS-Forscher im Fokus haben, soll das Spannungsfeld von WI zu IS und dessen Auswirkungen hier näher beleuchtet werden. Abschließend wird die in den Forschungsbeiträgen eingesetzte Forschungsmethodik Design Science (DS) gegliedert nach Aufbau, Vorgehen und Evaluation vorgestellt.

4.1 Wissenschaftstheorie

Die Wissenschaftstheorie ist nicht nur für die Grundlagendarstellung relevant, sondern stellt auch ein aktuell diskutiertes Thema dar. Das zeigt sich u. a. darin, dass die WI sich vermehrt der Internationalisierung ihres Forschungsgebietes und den damit einhergehenden Herausforderungen bezüglich der Positionierung in den wissenschaftstheoretischen und forschungsmethodischen Grundlagen stellen muss.[69]

Der Forschungsgegenstand der Wissenschaftstheorie ist die Wissenschaft selbst. Aufgabe der Wissenschaftstheorie ist es, ein theoretisches Fundament für den Forschungsprozess zu erstellen und kontinuierlich kritisch zu hinterfragen. In der WI kann sich das u. a. auf Forschen nach Voraussetzungen, Zielen, Theorien, Methoden, Ergebnissen oder Entwicklungen der WI beziehen.[70]

[69] Vgl. WIRTSCHAFTSINFORMATIK 2011 mit auf diese Thematik ausgerichteter Rubrik, die eine Übersicht über ausgewählte Beiträge bietet.
[70] Vgl. Becker et al. 2009; Frank 2006; Heinrich 2005; Frank 2003.

4.2 Einordnung der Wirtschaftsinformatik

Zunächst werden die Inhalte und Charakteristika der WI als Forschungsdisziplin dargestellt. Eine Ausprägung dieser Disziplin ist die gestaltungsorientierte WI. Für einen Literaturüberblick, der den aktuellen Stand der gestaltungsorientierten WI repräsentiert, werden einflussreiche Veröffentlichungen zu diesem Thema vorgestellt. Diese Veröffentlichungen dienen in den späteren Kapiteln als Grundlage zur thematischen Vertiefung. Die eigentlichen Erkenntnisziele der gestaltungsorientierten WI werden untersucht. Anschließend wird die WI zu ihrer Schwesterdisziplin der IS abgegrenzt und das Spannungsfeld zwischen der WI und der IS beleuchtet.

4.2.1 Darstellung der Wirtschaftsinformatik

Die WI lässt sich grob als verbindende Disziplin[71] zwischen den Wirtschaftswissenschaften und der Informatik verorten und ist eine anerkannte eigenständige wissenschaftliche Disziplin.[72] Die WI lässt sich an drei Charakteristika der Forschungsdisziplin darstellen:

- dem behandelten Gegenstand,
- der Ziele,
- der gewählten Methoden und Verfahren.

So „teilt“ sich die WI den Betrachtungsgegenstand mit der Betriebswirtschaftslehre (BWL). Beide „bewegen“ sich im erweiterten Kontext der Unternehmen, Verwaltungen und privaten Haushalte. Die Ziele der BWL und der WI hingegen unterscheiden sich. Während sich die BWL auf das ökonomische Handeln fokussiert, stützt sich die WI auf die Informationsverarbeitung in IT-basierten Informations- und Kommunikationssystemen (IuK). Bei den Methoden und Verfahren „bedient“ sich die WI gleichermaßen sowohl bei den Wirtschaftswissenschaften als auch bei der Informatik. Aber auch andere Forschungsdisziplinen wie z. B. die Mathematik oder die Psychologie werden zur Betrachtung herangezogen. Letztere ist z. B. bei der Analyse von IuK hilfreich, da diese oft als soziotechnische Systeme aufgefasst werden, die eine Verknüpfung bzw. Kooperation personeller und maschineller

[71] Vgl. Kurbel 2008, S. 85; Winter et al. 2009, S. 223; Jarke 2009, S. 83.
[72] Vgl. Heinrich et al. 2007, S. 13.

Aufgaben umfasst.[73] Die WI ist somit, bezogen auf die betrieblichen IuKs querschnittsbezogen und aus Sicht der Wissenschaftsdisziplinen, interdisziplinär. So werden Methoden und Verfahren bei der Informatik für die Arbeit mit den technischen Informationssystemen entliehen. Nach einer Untersuchung von Wilde und Hess (2007) werden folgende Forschungsmethoden im großen Umfang eingesetzt:

- **Argumentativ-deduktiv:** deduktives Schließen rein sprachlich bzw. argumentativ.
- **Quantitativ-empirisch:** Erhebungen mit Hilfe von quantitativen Methoden lassen Rückschlüsse auf eine Grundgesamtheit zu.
- **Fallstudie:** Analyse von Problemen im natürlichen Kontext. Sie ist eine Unterform der qualitativ-empirischen Methode und bezieht sich nur auf wenige Merkmalsträger.
- **Prototyping:** Entwicklung und Evaluierung eines nicht vollumfänglichen IT-Systems.

Da die Wahl der Methoden und Verfahren einer Disziplin angemessen und zielgerichtet sein soll, ist sie für die Abgrenzung einer Disziplin nicht entscheidend.[74] Die WI unterscheidet sich deutlich von den Wirtschaftswissenschaften und der Informatik in Bezug auf Gegenstand und Ziele. Somit kann eine Eigenständigkeit der WI begründet werden. Zentrales Themenfeld in der WI sind die IT-basierten Informationssysteme und mit speziellen Schwerpunkten auf Ihre Entwicklung, inhaltliche Ausgestaltung und Betrieb.[75] Die konkrete inhaltliche Ausgestaltung erfolgt in Hinblick auf die spezifischen Anwendungsfelder. In der Verfolgung dieser Ziele, Themen- und Forschungsfelder in der Grundlagenforschung weist die WI in den letzten Jahrzehnten eine große Konstanz auf.[76] Gleichwohl zeigen mehrere Untersuchungen, dass sich die WI aktuellen Entwicklungen konsequent zuwendet und am „Puls der Zeit“ ist.[77] Das wird, in einer oft von technischen Entwicklungen „getriebenen“ Forschungsdisziplin, als hohe Praxisnähe oder hohe Praxisrelevanz gewertet. Dieses Selbstverständnis der WI ist somit ein Baustein in der „rigor versus relevance“ Diskussion (s. Abschnitt. 4.3).

[73] Vgl. Steininger et al. 2009, S. 478.
[74] Vgl. Heinrich et al. 2007, S. 13.
[75] Vgl. Hess 2010, S. 9.
[76] Vgl. Heinzl et al. 2001, S. 6f.
[77] Vgl. Steininger et al. 2009, S. 493; Mertens 2006.

4.2.2 Gestaltungsorientierte Wirtschaftsinformatik

Die gestaltungsorientierte WI hat in Europa und besonders im deutschsprachigen Raum eine lange Tradition und ist in diesen Ländern auch das vorherrschende Forschungsparadigma der WI.[78] Frühe grundlegende Arbeiten[79] für die gestaltungsorientierte WI finden sich u. a. in den Beiträgen von Nunamaker et al. (1991) und Walls et al. (1992) (s. Abschnitt 4.3.2). Drei Jahre später stellten March und Smith (1995) einen Rahmen für die gestaltungsorientierte Wirtschaftsinformatikforschung vor. Vielbeachtete Richtlinien[80] für eine gestaltungsorientierte WI präsentierten Hevner et al. (2004). Diese Arbeiten dienten u. a. als Grundlage für die Entwicklung von Standards, Vorgehensweisen[81] oder Konzepten[82] in diesem Bereich. Mit der nun notwendigen Durchführung von Evaluationen der entstandenen Ergebnisse setzten sich z. B. Bucher et al. (2008), March und Storey (2008) und Winter (2008) auseinander.

Im Mittelpunkt der gestaltungsorientierten WI steht die Lösung von Konstruktionsproblemen bzw. die Konstruktion betrieblicher Informationssysteme.[83] Dabei gilt es das Untersuchungsgebiet so zu strukturieren und zu abstrahieren, dass Prozesse entworfen und Informationssysteme gestaltet werden können. Die dabei anhand von anerkannten Methoden (Abschnitt 4.3.2) herzuleitenden Abstraktionen werden Artefakte genannt. Hevner et al. (2004, S. 77) konstatiert:

> *„IT artifacts are broadly defined as constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems)".*

Ein Erkenntnisprozess zur Entwicklung eines Artefaktes sowie entsprechender Prinzipien der gestaltungsorientierten WI werden hier unter Bezugnahme auf Österle et al. (2010) und Becker (2010) vorgestellt.

[78] Vgl. Winter 2008, S. 470.
[79] Vgl. Österle und Otto 2010, S. 274; Offermann et al. 2010, S. 287f.
[80] Vgl. Piirainen et al. 2010, S. 96; Zelewski 2007, S. 71.
[81] Vgl. Peffers et al. 2007.
[82] Vgl. Rossi und Sein 2003, S. 12ff.
[83] Vgl. Sinz 2010, S. 27f.

Dieser Prozess setzt sich aus folgenden Phasen zusammen:

- Analyse,
- Entwurf,
- Evaluation,
- Diffusion.

Die Analysephase beinhaltet die Konkretisierung der Problemstellung, der Beschreibung der Forschungsziele, der Feststellung des aktuellen Forschungsstandes und der Lösungsansätze sowie die Selektion der adäquaten Forschungsmethode. In der Entwurfsphase sind die Artefakte methodisch herzuleiten und zu erstellen. Eine dazu begleitend erstellte detaillierte Begründung muss das Artefakt von anderen bereits existierenden Lösungen abgrenzen. Die Evaluationsphase dient der Überprüfung des geschaffenen Artefaktes unter Berücksichtigung der formulierten Forschungsziele. Das wird häufig durch das Reviewverfahren beim Veröffentlichungsprozess umgesetzt. In der abschließenden Diffusionsphase sollen die Ergebnisse der Artefaktkonstruktion im größtmöglichen Umfang an die Anspruchsgruppen kommuniziert werden.

Die Prinzipien der gestaltungsorientierten WI beziehen sich auf die Abstraktion, die Originalität, die Begründung und den Nutzen des Artefaktes. Das Artefakt muss dabei allgemeingültig auf eine Klasse von Problemen anwendbar sein. Das gestaltete Artefakt muss auch eine schöpferische Höhe haben, welches einen innovativen Beitrag zum bisherigen Stand der Forschung darstellt. Die Herbeiführung des Artefaktes muss für Dritte nachvollziehbar und validierbar sein. Für die Anspruchsgruppen muss ein Nutzen generiert werden.

In der gestaltungsorientierten bzw. in der allgemeinen WI ist in den letzten Jahren eine Tendenz zur Internationalisierung zu bemerken.[84] Dies führt dazu, dass sich die Forschungsdisziplin WI hinsichtlich der Methoden und Erkenntniszielen vermehrt an der IS ausrichtet.[85] Im nächsten Abschnitt wird auf diese aktuelle Entwicklung sowie auf die Forschungsmethode DS eingegangen, die in den vorgestellten Forschungsbeiträgen verwendet worden ist.

[84] Vgl. Frank 2003, S. 4f.
[85] Vgl. Steininger et al. 2009, S. 480; Frank 2008, S. 42f.

4.3 Einordnung des Design Science Research

4.3.1 Abgrenzung von Design Science zu Behavioural Science

Die Gestaltungsorientierung als Ausprägung einer eigenen wissenschaftlichen Disziplin erfährt vermehrt internationale (bzw. angelsächsische) Aufmerksamkeit.[86] Sie ist in der IS, der internationalen Schwesterdisziplin der WI, unter dem Begriff Design Science Research (DSR) bekannt.[87] Dass DSR erst seit den frühen 1990er Jahren ein gesteigertes Interesse[88] zukommt, liegt u. a. an einer starken Präferierung der Behavioural Science Research (BSR) in der IS Forschung. Bei der BSR steht die Verhaltensorientierung im Fokus, während bei der DSR die Gestaltungsorientierung im Mittelpunkt steht (s. Tabelle 1).

Tabelle 1: Behavioural vs. Design Science Research.

	Behavioural Science Research (BSR)	**Design Science Research (DSR)**
Origin	natural science	engineering, sciences of the artificial
paradigm	problem understanding paradigm	problem solving paradigm
objective	to develop and justify theories which explain or predict organizational human phenomena surrounding the analysis, design, implementation, management, and use of information systems	to create innovations that define ideas, practices, technical capabilities, and product through the analysis, design, implementation, management, and use of information systems
Object	Human-Computer-Interaction	IT artefact design

Quelle: Niehaves und Stahl (2006), S. 4.

BSR versucht vorrangig, menschliches Verhalten bei der Entwicklung und Nutzung von IuKs zu begründen. Sie hat sich als Ziel gesetzt, erklärende, vorhersagende oder kausale Zusammenhänge zu ermitteln und zu validieren. Vorherrschend sind die Nutzung quantitativer Methoden[89] wie z. B. Befragungen oder Experimente, aber auch qualitative Methoden[90] wie action research sind vertreten. DSR hingegen beschäftigt sich mit der Entwicklung und Evaluation neuer, nutzenstiftender und

[86] Vgl. Fischer et al. 2010, S. 383.
[87] Vgl. Stahl 2009, S. 117f.
[88] Akzeptanz von Einreichungen mit „alternativen" Forschungsansätzen in 1993 durch MISQ (vgl. Chen und Hirschheim 2004, S. 199).
[89] Vgl. Chen und Hirschheim 2004, S. 207f.
[90] Vgl. Davison et al. 2004, S. 65ff.

generischer Lösungen (Artefakte) für Informationssysteme. Es werden dabei vornehmlich deduktive Methoden, Fallstudien und Prototyping verwendet.[91]

Die Unterschiedlichkeit der Ansätze WI und BSR spiegelt sich auch in den jeweiligen Selbstverständnissen wieder.[92] DSR wird dabei eher eine hohe Praxisrelevanz (relevance) zugesprochen. BSR hingegen betont eine hohe Stringenz der verwendeten Forschungsmethoden (rigor). Diese Punkte äußern sich u. a. in der „rigor versus relevance" Diskussion.[93]

Die Auswirkungen dieser verschiedenen Selbstverständnisse lassen sich auch in der Literatur nachweisen. So sprechen Chen und Hirschheim (2004, S. 223) gar von einer „strong ´home grown´ perspective". Ihren Untersuchungen nach dominiert BSR die US-amerikanischen und DSR die europäischen Journale. Auch hätte der Aufruf zum Methodenpluralismus durch das Management Information Systems Quarterly (MISQ)-Journal 1993 nicht den gewünschten Effekt gehabt. Vor dem Hintergrund, dass Beurteilungen der Forschungsleistung oft anhand von Veröffentlichungen in BSR geprägten, hochrangigen Zeitschriften erfolgen, stellt sich für nach DSR vorgehende Forscher die Frage nach der internationalen Wettbewerbsfähigkeit ihres Ansatzes.[94] So wird häufig angeführt, dass in der IS quantitativ-empirische Analysen bevorzugt und konstruktive Arbeiten (Konstruktion von Software-Prototypen) sowie die Evaluation (Vor- und Nachteile in der Nutzung in den IuKs) wenige Chancen auf internationale Publikation haben.[95] Hevner und Winter (2009) betonen, dass sich in jüngerer Zeit international vermehrt mit dem Thema DSR beschäftigt wird. Diese Aussage spiegelt sich in der Zunahme von Schwerpunktheften, entsprechenden Tracks auf renommierten Konferenzen wie z. B. der International Conference on Information Systems[96] (ICIS) sowie in Schwerpunktkonferenzen wie der International Conference on Design Science Research in Information Systems and Technology[97] (DESRIST) wider.

[91] Vgl. Wilde und Hess 2007, S. 284.
[92] Vgl. Steininger et al. 2009, S. 480ff.
[93] Vgl. Hevner und Winter 2009, S. 149f.
[94] Vgl. Loos et al. 2010.
[95] Vgl. Winter et al. 2009, S. 227; WKWI und GI-FB WI 2008; Hevner und Chatterjee 2010.
[96] Vgl. AIS 2011a.
[97] Vgl. Universität St. Gallen 2011.

4.3.2 Entwicklungsprozess im Design Science Research

Ziel des Entwicklungsprozesses ist das Design von Konstrukten, Methoden, Modellen und Instanzen. Die Phasen des Entwicklungsprozesses lassen sich aus einflussreichen und Grundlagen legenden Publikationen (s. Abschnitt 4.2.2) extrahieren. Obwohl die Publikationen unterschiedlich sind, ergeben sich doch übereinstimmend die Prozessschritte Problemidentifikation, Anforderungsanalyse, Design, Evaluation und Kommunikation der Ergebnisse (s. Tabelle 2). Takeda et al. (1990) präsentieren einen Designzyklus, Nunamaker et al. (1991) stellen ein Abstraktmodell vor, Walls et al. (1992) beschäftigen sich mit der Design Theorie selbst, Rossi und Sein (2003) sowie Cole et al. (2005) integrieren action research und DSR und Hevner et al. (2004) stellen ihre weit beachteten Richtlinien für DSR vor.

Tabelle 2: Prozesselemente des Design Science.

Common design process elements	**Takeda et al. 1990**	**Nunamaker et al. 1991**	**Walls et al. 1992**	**Rossi und Sein 2003; Cole et al. 2005**	**Hevner et al. 2004**
1. Problem identification and motivation	Problem enumeration	Construct a conceptual framework	Meta-requirements	Identify a need	Important and relevant problems
2. Objectives of a solution			Kernel theories		Implicit in "relevance"
3. Design and development	Suggestion Development	Develop a system architecture Analyze and design the system. Build the system	Design method Meta design	Build	Iterative search process Artifact
4. Demonstration		Experiment, observe, and evaluate the system			
5. Evaluation	Confirmatory evaluation		Testable design process/product hypotheses	Evaluate	Evaluate
6. Communication					Communication

Quelle: Modifizierte Tabelle aus Peffers et al. 2007.

Die in der Tabelle 2 angeführten Publikationen geben bei der Entwicklung von DSR-Artefakten, unter der Berücksichtigung verschiedener Blickwinkel, einzelne Hinweise bzw. Vorgehensmöglichkeiten. Einen strukturierten, umfassenden[98] und zusammenführenden Ansatz für die einzelnen DSR-Prozessschritte stellen Peffers et

[98] Vgl. Österle und Otto 2010, S. 274.

al. (2007) vor. Das entwickelte DSR-Rahmenwerk beschreibt Methoden für die Konstruktion und Präsentation eines Artefaktes und kann als ein Referenzprozess für die DSR-Artefaktkonstruktion gesehen werden.[99] Das von Peffers et al. (2007) entwickelte Rahmenwerk wird in Abbildung 4 dargestellt. Es ist ein iterativer Prozess, der in sechs Aktivitäten aufgeteilt ist[100]:

- **Problemidentifikation und Motivation:** Das eigentliche Forschungsproblem und der mögliche Wert einer Lösung wird definiert. Basierend auf den Ergebnissen der Problemidentifikation werden Entscheidungen für das zu entwickelnde Artefakt getroffen. Diese Entscheidungen beinhalten die Wahl des Artefakttyps und den genauen Fokus des Artefaktes.
- **Definition der Ziele der Lösung:** Die Ziele (bzw. Metriken zur Messung der Ziele) sollten von der Problemspezifikation abgeleitet werden und können qualitativer oder quantitativer Art sein.
- **Design und Entwicklung:** Die angestrebten Ziele müssen beim Design der Funktionalität und der Architektur des Artefakts berücksichtigt werden. Darauf aufsetzend erfolgt die Entwicklung des konkreten Artefakts.
- **Durchführung:** Die Anwendbarkeit des Artefakts bei der Problemlösung muss demonstriert werden. Zur Durchführung können Simulationen, Experimente oder Fallstudien herangezogen werden.
- **Evaluation des Artefakts:** Der Nutzen des Artefakts muss anhand der definierten Ziele bzw. Metriken evaluiert werden.[101] Dabei können auch Vergleiche zu bereits existierenden Lösungen gezogen werden. Am Ende dieser Phase muss geprüft werden, ob eine Design-Iteration notwendig ist und zur Phase „Design und Entwicklung“ zurückgegangen werden muss. Dieser Fall tritt z. B. ein, wenn die Ergebnisse des Artefakts nicht im gewünschten Maße erreicht werden.

[99] Vgl. Cleven et al. 2009, S. 5.
[100] Vgl. Peffers et al. 2007, S. 12ff.
[101] Vgl. Riege et al. 2009, S. 75.

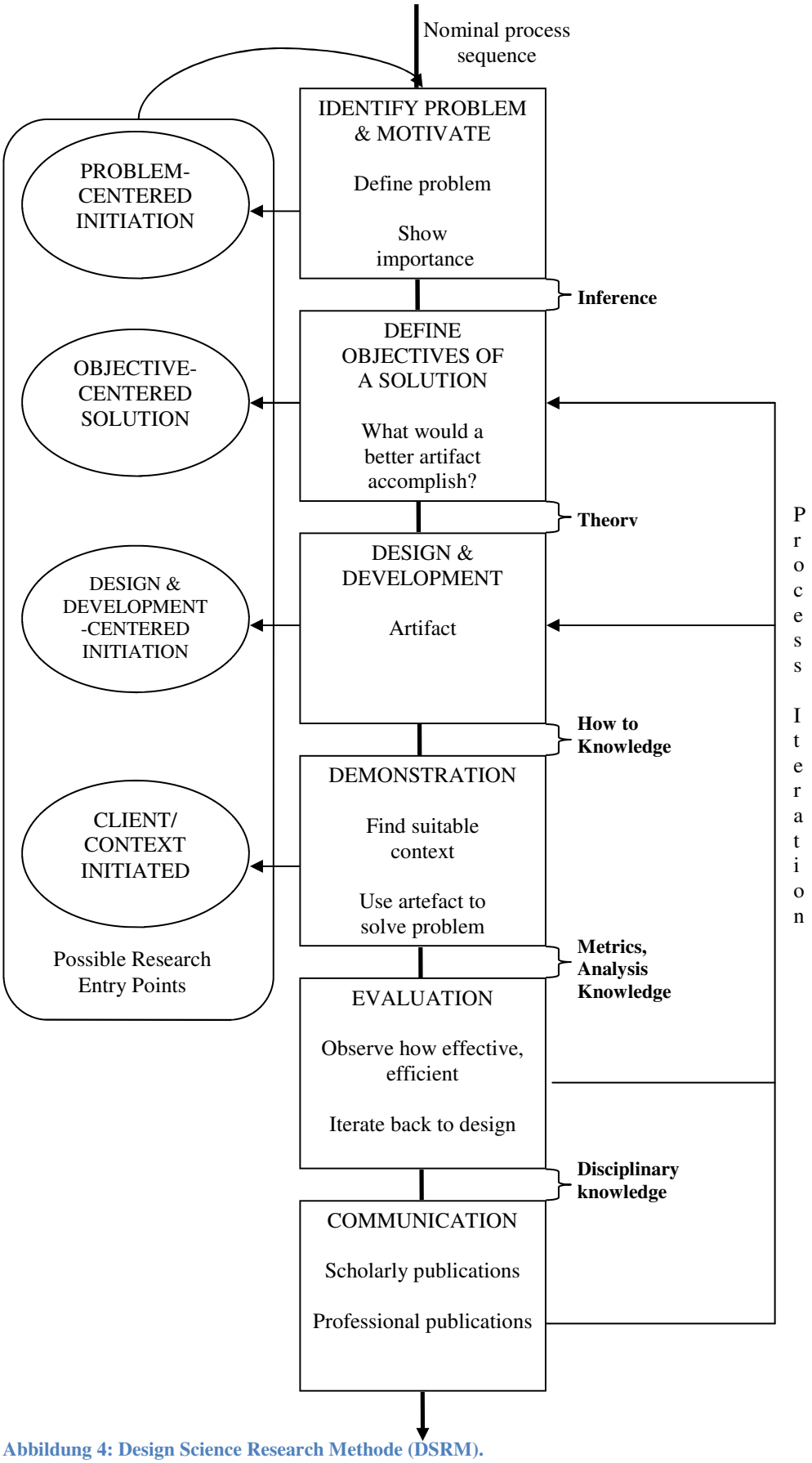

Abbildung 4: Design Science Research Methode (DSRM).

Quelle: Peffers et al. (2007), S. 11.

- **Kommunikation der Ergebnisse:** Eine detaillierte Beschreibung des Artefakts, der zu erwartende Nutzen, die eingesetzten Forschungsmethoden, das verwendete Forschungsdesign sowie die durchgeführte Evaluation (Aufbau, Analyse, Ergebnis) soll den relevanten Anspruchsgruppen wie Wissenschaftlern oder Praktikern vorgestellt werden.

Obwohl der Prozess sequentiell angelegt ist, weisen Peffers et al. 2007 explizit darauf hin, dass der Prozess nicht unbedingt nur von der ersten Aktivität bis zur letzten Aktivität schrittweise durchlaufen werden muss. Vielmehr kann es verschiedene Forschungseinstiegspunkte geben, die vom jeweiligen Forschungsziel abhängig sind (s. Abbildung 4). Ein problemorientierter Ansatz würde bei der ersten Aktivität starten, ein Ansatz mit einer Zielvorgabe z. B. durch Anforderungen aus Forschung oder Praxis in der zweiten Phase und ein Ansatz, in dem die Entwicklung im Vordergrund steht, in der dritten Phase.

4.4 Forschungsziele

Im Vorfeld dieser Arbeit beschäftigte sich der Autor intensiv mit dem Thema „Rollenengineering“. Neben der systematischen und geordneten Vergabe von Berechtigungen, die in Rollen gebündelt sind, stand dabei auch die Prüfung und Kontrolle der Berechtigungsvergabe in IT-Systemen im Vordergrund. Praktische Erfahrungen in diesem Bereich konnten in der täglichen Arbeit als SAP-Anwendungsbetreuer mit Basisaufgaben für mehrere SAP-Systeme gewonnen werden. In diesem Zusammenhang zeigte sich, dass der Abgleich von vergebenen Berechtigungen in IT-Systemen mit den zu erfüllenden fachlichen Anforderungen oft eines erheblichen zeitlichen Aufwandes bedurfte. Diese Beobachtungen und Erfahrungen sind eingebracht worden.

Die Prüfung der korrekten Implementierung und der Funktionsfähigkeit von maschinellen Kontrollen, als Teil eines IKS, können aufgrund der Heterogenität und Komplexität einer IT-Systemlandschaft ebenfalls einen beträchtlichen zeitlichen Aufwand verursachen. Dem steht die zentrale Anforderung nach zeitnaher Berichterstattung von Kontrollausnahmen entgegen. Zum Zwecke der regelmäßigen Überprüfung der Kontrollen werden oft spezielle Softwarelösungen eingesetzt.

Für die Ausarbeitung eines Promotionsthemas setzte sich der Autor der vorliegenden Arbeit intensiv mit verschiedenen Aspekten der IT-Sicherheit auseinander. So wird

in diesem Gebiet häufig postuliert, dass der Mensch das schwächste Glied in der Sicherheitskette sei und ihm daher besondere Aufmerksamkeit zu widmen ist. Um diese angemerkte Aufmerksamkeit abbilden zu können, muss der Fokus mehr auf dem Einbezug und der Berücksichtigung des jeweiligen Menschen liegen. Daher setzte sich der Autor mit den Möglichkeiten des Einbezugs bzw. der Berücksichtigung der Persönlichkeit eines Menschen in Verbindung mit seinem Einsatz in IT-Systemen auseinander.

Ausgehend von diesen Problemstellungen aus der Praxis und auf Basis entsprechend durchgeführter Literaturrecherchen wurden Forschungslücken identifiziert. Darauf aufbauend sind folgende Forschungsziele definiert worden:

I. Gestaltung von Artefakten zur automatisierten regelbasierten Überwachung maschineller Kontrollen in IT-Systemen zur Unterstützung von Geschäftsprozessen und zur zielgruppengerechten Berichterstattung von Kontrollausnahmen.

II. Gestaltung eines Artefakts zur Einbeziehung der Faktoren des „Fraud Triangle“ im IT-Risikomanagement unter Zuhilfenahme der vorliegenden IT-Infrastruktur.

Zur Umsetzung dieser Forschungsziele wurde DSR als Forschungsmethode eingesetzt.

5 Eingereichte Beiträge

Die vorliegende Dissertation enthält vier Forschungsbeiträge zum Forschungsgebiet IT-Compliance und Forschungsziel I sowie einen Forschungsbeitrag zum Forschungsgebiet IT-Risikomanagement und Forschungsziel II. Innerhalb des Forschungsgebietes I bauen die einzelnen Forschungsbeiträge aufeinander auf. Die einzelnen Forschungsbeiträge werden in den folgenden Unterabschnitten erläutert. Dies erfolgt in der Reihenfolge, in der die Forschungsbeiträge erschienen sind. Dabei wird kurz auf die Konferenz, den Inhalt und die Aufgabenteilung unter den Autoren eingegangen. Die Angaben zur Veröffentlichung bzw. zur Konferenz enthalten auch Informationen zur Kategorisierung anhand entsprechender Ranglisten.

Die Kategorisierung der Veröffentlichungen werden anhand des JOURQUAL 2.1 Ranking für betriebswirtschaftlich relevante Zeitschriften des Verbandes der Hochschullehrer für Betriebswirtschaft (VHB)[102], der Ranked Conference List der Excellence in Research for Australia (ERA)[103] und der WI-Orientierungslisten der wissenschaftlichen Kommission Wirtschaftsinformatik im Verband der Hochschullehrer für Betriebswirtschaft e.V. (WKWI) bzw. des Fachbereichs Wirtschaftsinformatik der Gesellschaft für Informatik (GI-FB WI)[104] vorgenommen.

5.1 HICSS 2010

Im Februar 2009 besuchten Matthias Kehlenbeck und der Autor der vorliegenden Dissertation die Internationale Tagung Wirtschaftsinformatik 2009 (WI 2009) in Wien. Die besuchten Vorträge aus den Bereichen der IT-Compliance und IT-Sicherheit gaben den Impuls, gemeinsam einen Beitrag zur Überwachung von Zugriffskontrollen in IT-Systemen auszuarbeiten.

5.1.1 Konferenz

Die Hawaii International Conference on System Sciences (HICSS) ist eine der ältesten und renommiertesten Information System Konferenzen der Welt.[105] Das spiegelt sich auch in den WI-Orientierungslisten und der ERA-Zeitschriftenliste

[102] Vgl. Hennig-Thurau und Sattler 2011.
[103] Vgl. ARC 2010.
[104] Vgl. WKWI und GI-FB WI 2008.
[105] Vgl. Universität Hawaii 2011.

wider, die die in diesem Gebiet führenden Zeitschriften auflisten.[106] So steht in einem Artikel[107] in der Zeitschrift „Communications of the ACM“ die HICSS auf dem zweiten von elf Plätzen unter den betrachteten IS-Konferenzen und in einem Artikel[108] in der Zeitschrift „Information & Management“ auf dem dritten von dreizehn Plätzen unter den betrachteten Management-Information-Systems Konferenzen. Auch spiegeln sich die internationale Beachtung und das Renommee der HICSS in einer Zitierungsuntersuchung der Beiträge der renommierten ICIS[109] wider. Die HICSS wird, nach der ICIS selbst, auf Platz 2 der meist zitierten IS-Konferenzen geführt.[110] Im VHB-JOURQUAL 2.1 Ranking sind die Proceedings der HICSS der Kategorie C, in den WI-Orientierungslisten der Kategorie B und in der ERA Ranked Conference List der Kategorie A zugeordnet.

Der Forschungsbeitrag wurde bei der HICSS 2010 in anonymisierter Form eingereicht. Die drei Reviewer gaben eine sehr positive Rückmeldung. Der von einem Reviewer vorgeschlagenen stärkeren Betonung von organisatorischen Aspekten wurde bei der Überarbeitung Rechnung getragen. Der überarbeitete Beitrag wurde in der „IEEE Digital Library“ der „IEEE Computer Society“ des „Institute of Electrical and Electronics Engineers“ (IEEE) veröffentlicht.

5.1.2 Inhalt

Der Forschungsbeitrag beschreibt die verschiedenen Anforderungen und Herausforderungen an Organisationen hinsichtlich der Umsetzung eines Risiko-managements. Die erfolgreiche Umsetzung und der Nachweis der Funktionalität ist für Organisationen umso wichtiger geworden, da viele Gesetze wie z. B. Sarbanes-Oxley Act (SOX), EuroSOX oder Basel II dies zwingend voraussetzen. Zur Umsetzung des Risikomanagements werden in den Geschäftsprozessen bzw. in den zugrunde liegenden IT-Systemen der Organisation interne Kontrollen implementiert. Für den Erfolg des Risikomanagements sind dabei die Einführung, Weiter-entwicklung und Überwachung dieser internen Kontrollen oder auch die zeitnahe Weitergabe von Kontrollverletzungen unerlässliche Grundbedingungen. Der Forschungsbeitrag legt den thematischen Schwerpunkt auf diese Aspekte und präsentiert einen im Hinblick auf diese Anforderungen entwickelten Prototyp.

[106] Vgl. ARC 2011.
[107] Vgl. Hardgrave und Walstrom 1997, S. 123.
[108] Vgl. Walstrom und Hardgrave 2001, S. 121.
[109] Vgl. AIS 2011a.
[110] Vgl. Hock et al. 2006, S. 1268ff.

Als Grundlage für den Prototypen werden ein Modell für Zugriffskontrollen, die Extensible Access Control Markup Language (XACML), ein Modell für Geschäftsprozesse, die Business Process Modeling Notation (BPMN) und ein Modell für interne Kontrollsysteme, das Internal Control – Integrated Framework bzw. das Enterprise Risk Management – Integrated Framework (COSO) zu einem integrierten Gesamtmodell, der Business Risk Description Language (XBRDL) verknüpft.
Die Modellierung der Zugriffskontrollen und der Geschäftsprozesse basieren auf bereits formal beschriebenen und standardisierten Modellen. Im Gegensatz dazu sind für die IKS keine formal beschriebenen und standardisierten Modelle verfügbar. Es ist daher ein etabliertes Modell formal beschrieben worden. Um eine gute Widerverwendbarkeit und Austauschbarkeit zu gewährleisten, ist für den Forschungsbeitrag eine Service-Orientierte Architektur (SOA) gewählt worden. Die unterschiedlichen Aufgaben konnten so modular in verschiedene Services aufgeteilt werden. Die beschriebene Architektur sieht einen Überwachungsdienst, einen Zugriffskontrollentscheidungsdienst, einen Schlussfolgerungsdienst, Webservices und einen Data Warehouse (DW)-Dienst vor.
Abschließend wird die Funktionsweise des Prototyps anhand eines Fallbeispiels erläutert. Es wird dabei ein typisches Szenario aus dem Finanzbereich vorgestellt, in dem in einem ERP-System (SAP) eine Vorerfassung und eine Buchung eines betriebswirtschaftlichen Vorganges durch unterschiedliche Personen durchgeführt werden muss.

5.1.3 Aufgabenteilung

Der Autor der vorliegenden Dissertation war bereits vor der Arbeit an dem Forschungsbeitrag umfassend in die Themen IT-Sicherheit und Zugriffskontrolle (XACML) eingearbeitet. Er leistete den überwiegenden Teil der Literaturarbeit. Matthias Kehlenbeck entwarf das integrierte Gesamtmodell, die Architektur und entwickelte den Prototyp. Die Einarbeitung in das verwendete Zugriffskontroll-modell und die entsprechende Softwarekomponente erfolgte zu gleichen Teilen.

5.2 ARES 2010

5.2.1 Konferenz

Die seit 2006 jährlich stattfindende International Conference on Availability, Reliability and Security (ARES) beschäftigt sich schwerpunktmäßig mit der

Stabilität von Systemen sowie den Wirkungsbeziehungen zwischen deren Verfügbarkeit, Zuverlässigkeit und Sicherheit. Sie zeichnet sich durch oft hochkarätige Keynote-Sprecher[111] wie z. B. Ross Anderson und Elisa Bertino sowie niedrige Annahmequoten (z. B. ARES 2010 unter 25%[112]) aus. In der ERA Ranked Conference List ist die Konferenz der Kategorie B zugeordnet.

Der Forschungsbeitrag wurde beim First Workshop on Economics of Compliance Control and Automation (ECCA 2010) der ARES 2010 eingereicht. Die geringe Anzahl geeigneter Beiträge führte zu der Absage des ECCA-Workshops. Der eingereichte Forschungsbeitrag wurde allerdings als interessant eingestuft und nach einem Review durch zwei Gutachter für den Second International Workshop on Organizational Security Aspects (OSA) angenommen. Die Reviewer hoben die Relevanz und die Aktualität hervor und wünschten sich nur eine etwas klarere Ausdifferenzierung der ökonomischen Implikationen. Der überarbeitete Forschungsbeitrag ist in der IEEE Digital Library veröffentlicht worden.

5.2.2 Inhalt

Dieser Forschungsbeitrag geht vorrangig auf die Anwendung des prototypisch implementierten automatisierten Compliance-Management- und Berichtssystems aus HICSS 2010 ein. Es werden allgemein die ökonomischen Auswirkungen unter Berücksichtigung verschiedener Geschäftsanforderungen und –informationen in vier Szenarien beleuchtet. Dazu werden die im Geschäftsumfeld auftretenden Anspruchs- bzw. Personengruppen oder Organisationseigenschaften identifiziert und charakterisiert. Die jeweiligen unterschiedlichen Verantwortlichkeiten und Informationsbedürfnisse der Anspruchsgruppen werden detailliert beschrieben. Die Eigenschaften der Organisation sind gerade bei der Überwachung des IKS hinsichtlich des Umfangs der Prozessdokumentation und der Heterogenität der Systemlandschaft ausschlaggebend. So kann eine Vier-Felder-Matrix, die die unterschiedlichen Szenarien widerspiegelt, aufgebaut werden. Für jedes Szenario ergeben sich dabei unterschiedliche Geschäftsanforderungen und -voraussetzungen. Aus dieser Divergenz leitet sich auch entsprechend ein unterschiedlicher Zielerreichungsgrad des Prototypen ab, da die verschiedenen Geschäftsanforderungen und Informationsbedürfnisse nur abhängig von der Ausgangssituation befriedigt werden können.

[111] Vgl. Secure Business Austria 2011a.
[112] Vgl. Secure Business Austria 2011b.

Um der organisationalen und ökonomischen Zielrichtung des OSA-Workshops gerecht zu werden, wird dem zugrundeliegenden Prototypen nur eine kurze Betrachtung eingeräumt. Dabei werden die notwendigen Entwicklungen und Evaluationen unterteilt nach Modell, Architektur und Implementierung vorgestellt. Den Hauptteil bildet eine differenzierte Auseinandersetzung mit den in der Literatur beschriebenen kritischen Erfolgsfaktoren zu IT-Compliance. Dazu wird auf die unterschiedlichen Einsatzphasen entsprechender IT-Compliance Management Software eingegangen. Eckpunkte der abschließenden Diskussion bilden die vorgestellte Anwendung des Prototypen unter der Berücksichtigung der jeweiligen Einsatzphase mit Ihren Geschäftsanforderungen, Informationsbedürfnissen und kritischen Erfolgsfaktoren.

5.2.3 Aufgabenteilung

Der Autor der vorliegenden Dissertation leistete den grundlegenden Teil der Literaturarbeit. Insbesondere hat er die kritischen Erfolgsfaktoren und die Einsatzphasen identifiziert und erläutert. Weiterhin beschäftigte er sich intensiv mit den entwickelten Szenarien und arbeitete sie detailliert aus. Matthias Kehlenbeck übernahm die methodische Einordnung, charakterisierte die verschiedenen Personenkreise und erstellte die Abbildungen. An der Diskussion zur Anwendung des Prototyps und der entsprechenden Auswirkungen wurde zu gleichen Teilen gearbeitet.

5.3 ECIS 2010

5.3.1 Konferenz

Die European Conference on Information Systems (ECIS) ist die größte und prestigeträchtigste Konferenz für Wirtschaftsinformatik in Europa.[113] Die ECIS ist die Regionalkonferenz der Association for Information Systems (AIS)[114] für Europa, den Mittleren Osten und Afrika (EMEA). In den WI-Orientierungslisten und in der ERA Ranked Conference List wird die Konferenz in der Kategorie A eingestuft. Im VHB-JOURQUAL 2.1 Ranking sind die Proceedings der ECIS der Kategorie B zugeordnet.

Der Forschungsbeitrag wurde bei der ECIS 2010 in anonymisierter Form eingereicht und nach einem Review durch drei Gutachter angenommen. Die Gutachter hoben

[113] Vgl. Universität Pretoria 2011.
[114] Vgl. AIS 2011.

besonders die hohe Relevanz, den klaren Argumentationsfluss und die transparente Methodologie hervor. Es wurde lediglich eine stärkere Abgrenzung zu den bereits in SAP eingebauten Überwachungsmöglichkeiten empfohlen, die dann in der Überarbeitung stärker betont und herausgearbeitet wurde. Der angenommene Forschungsbeitrag wurde durch die AIS veröffentlicht.

5.3.2 Inhalt

Der Forschungsbeitrag für die ECIS 2010 setzte sich speziell mit der automatisierten Konvertierung von Zugriffsdaten aus einem ERP-System (SAP) auseinander. Dazu wurden das Modell und die Architektur aus dem Forschungsbeitrag für die HICSS 2010 weiterentwickelt. Bereits im Forschungsbeitrag für die HICSS 2010 wurde darauf hingewiesen, dass der Erfolg eines Compliance Managements in einer Organisation positiv mit der Überwachungs- und Berichtshäufigkeit korreliert ist. Diese Häufigkeiten werden oft negativ durch eine Vielzahl von komplexen und zeitraubenden manuellen Arbeitsschritten beeinflusst. Die für diesen Zweck von den Organisationen genutzten Softwarelösungen müssen sich nahtlos in eine meist heterogene Systemlandschaft integrieren und an verschiedenste IT-Systeme ankoppeln lassen.

Um diesen Herausforderungen gerecht zu werden, konnte aufgrund der eingesetzten Service Orientierten Architektur (SOA), der Prototyp des Forschungsbeitrages für die HICSS 2010 um einen Konvertierungswebservice ergänzt und der Schlussfolgerungswebservice trotz Modifikation ohne Aufwand integriert werden. Der Schlussfolgerungswebservice verwendet nun eine andere quelloffene Softwarekomponente, die das Erstellen von Definitionen für Kontrollausnahmen deutlich vereinfacht. So können nun Anfragen an den Schlussfolgerungswebservice in einer Standardsprache formuliert werden. Der neu hinzugekommene Konvertierungswebservice exportiert und konvertiert SAP-Zugriffskontrolldaten. Der Export kann über einen Webservice, eine Datenbankschnittstelle oder direkt über die grafische SAP-Benutzeroberfläche erfolgen. Die Konvertierungskomponente leitet die exportierten Daten vollautomatisch aus dem SAP-Zugriffskontrollmodell in das Standardzugriffskontrollmodell über.

Abschließend wurde der Prototyp mit Hilfe eines produktiven SAP ERP-Systems evaluiert. Die Evaluation zeigt, dass die Anzahl der durch den Konvertierungswebservice zu konvertierenden Objekte deutlich über einer manuell zu

überblickenden oder zu bearbeitenden Grenze liegt. Dies lässt die Notwendigkeit einer automatischen Konvertierung als notwendig bzw. sehr hilfreich erscheinen.

5.3.3 Aufgabenteilung

Der Autor der vorliegenden Dissertation hat den überwiegenden Teil der Literaturarbeit geleistet und hat die Motivation sowie die Vorzüge des erstellten Prototyps herausgearbeitet. Die Weiterentwicklung des Prototyps und die Erstellung der Abbildungen hat Matthias Kehlenbeck übernommen.

5.4 VISM 2010

In den Forschungsbeiträgen für die HICSS 2010 und die ECIS 2010 steht die Informationsextraktion und -gewinnung im Vordergrund. Eine Präsentations-möglichkeit der Compliance-Daten wird in den Forschungsbeiträgen zwar beschrieben, aber nicht näher beleuchtet. Die Präsentationsschicht stellt bei einem solchen Prototyp einen wichtigen Faktor bei der Gewinnung der „Management Attention“ dar. Letztere wiederum ist essentiell für den Erfolg einer solchen Softwarelösung. Folglich wurde im nächsten Schritt die Visualisierung von managementrelevanten Compliance-Informationen untersucht.

5.4.1 Konferenz

Die International Conference on Database and Expert Systems Applications (DEXA), die 2010 das 21. Mal durchgeführt wurde, ist in den WI-Orientierungslisten der Kategorie C und in der ERA Ranked Conference List der Kategorie B zugeordnet.

Der Forschungsbeitrag ist beim „First International Workshop on Visualization and Information Security Management“ (VISM 2010) der DEXA 2010 eingereicht worden. Der VISM-Workshop thematisiert schwerpunktmäßig die Visualisierung sicherheits-relevanter Informationen. Nach einem Review durch drei Gutachter, die besonders positiv die Originalität und die Relevanz des Beitrages hervorhoben, ist der Forschungsbeitrag angenommen worden. Der Beitrag ist in den Proceedings der „Workshops on Database and Expert Systems Applications“ und der IEEE Digital Library veröffentlicht worden.

5.4.2 Inhalt

Grundlage für den Forschungsbeitrag ist die tiefergehende Auseinandersetzung mit den Themen „Visualisierung der IT-Sicherheit“ und „Entwicklung bzw. Umsetzung von Informationsmanagement-Dashboards“. Die Visualisierung von Informationen im Bereich der IT-Sicherheit soll die Mustererkennung und die Informationsgewinnung erleichtern. Für eine schnellere und leichtere Informationsgewinnung wird für die Zielgruppe „Management“ oft ein Dashboard-Ansatz gewählt. Ein Dashboard enthält auf einem einzigen Bildschirm die wichtigsten Informationen in konsolidierter Form. Die Auswahl der angezeigten Informationen erfolgt zielgenau und erleichtert die Überwachung der Zielerreichung für das Management. Für den Forschungsbeitrag wurde in der Literatur ein passendes Vorgehensmodell für die Entwicklung und die Umsetzung des Dashboards identifiziert.

Da in diesem Forschungsbeitrag die Umsetzung der Visualisierung von IT-Compliance Informationen im Vordergrund steht, wird der datenliefernde Prototyp nur kurz beschrieben. Um ein Verständnis für die Funktionsweise des Gesamtkonzepts herzustellen, wird vorwiegend die Informationsbereitstellung durch den Prototypen erläutert. Die durch den Prototyp bereitgestellten Informationen bilden die Grundlage für die Erstellung eines Dashboards zur Unterstützung des Compliance Managements auf Basis des Vorgehensmodells. Die Erstellung und Evaluation des Dashboards erfolgte in Abstimmung mit Interessenvertretern und bezog sich jeweils auf die aktuelle Version des Dashboards.

5.4.3 Aufgabenteilung

Der Autor der vorliegenden Dissertation übernahm die Einarbeitung in das Thema der Informationsvisualisierung und die Konsolidierung der Inhalte anhand von Leitfäden. Matthias Kehlenbeck arbeitete die Beschreibung der Informationsbereitstellung und die Umsetzung des Dashboards heraus.

5.5 ECIS 2011

Inspiriert durch verschiedene Vorträge beim Besuch der DEXA 2010 Konferenz in Bilbao im Bereich IT-Sicherheit und IT-Risikomanagement, skizzierte der Autor der vorliegenden Dissertation einen Ansatz für ein Modell zur Berücksichtigung der Faktoren des „Fraud Triangle“ im IT-Risikomanagement unter Zuhilfenahme der IT-

Infrastruktur. In Zusammenarbeit mit Halyna Zakhariya und Stefan Hoyer wurde der Ansatz im November 2010 detaillierter ausgearbeitet.

5.5.1 Konferenz

Der Forschungsbeitrag ist bei der „19th European Conference on Information Systems“ (ECIS) 2011 in anonymisierter Form eingereicht worden. Die ECIS 2011 ist eine Weiterführung der ECIS 2010, so dass die Konferenzinformationen aus Abschnitt 5.3.1 herangezogen werden können. Der Forschungsbeitrag wurde nicht angenommen, jedoch hoben die Gutachter das vielversprechende Thema hervor, lobten das insgesamt gute Konzept und empfahlen eine Weiterarbeit an diesem Thema. Bemängelt wurden Schwächen in der Ausführung u. a. in der Präsentation der DSR-Komponenten. Der Forschungsbeitrag wird anhand der Gutachter-vorschläge überarbeitet und erneut eingereicht.

5.5.2 Inhalt

In diesem Forschungsbeitrag wird ein generisches Architekturmodell vorgestellt, das die Berücksichtigung der „Fraud Triangle“-Faktoren Gelegenheit, Motiv und innere Rechtfertigung ermöglicht. Die Berücksichtigung der „Fraud Triangle“-Faktoren bietet insofern einen Mehrwert, als dass die von einem Prüfer zu untersuchenden Geschäftstransaktionen besser differenziert und priorisiert werden können.

Bei vielen Prüfungen hingegen wird der Faktor Mensch als eigenständige qualitative Komponente meist nicht umfangreich in Prüfungen integriert. In der Regel finden eher technisch orientierte Analysen der Geschäftstransaktionen statt. Durch die Einbeziehung des menschlichen Verhaltens (Risikoklassifikation des Unternehmens-angehörigen: kritisch oder nicht kritisch) soll es ermöglicht werden, den Fokus auf Geschäftstransaktionen zu legen, die einem bisher noch nicht bekannten Muster unterliegen und mit herkömmlichen Mitteln unentdeckt geblieben wären.

In der entwickelten Architektur werden unterschiedliche Informationsquellen für die verschiedene Auswertungsziele vorgeschlagen. Ein wichtiger Eckpfeiler sind dabei die IT-Systeme, in denen die einzelnen Geschäftsprozesse abgebildet sind. In diesen IT-Systemen erfolgt die Prüfung von Buchungsbelegen oder es werden Berechtigungsanalysen z. B. auf die Einhaltung des 4-Augen-Prinzips durchgeführt. Die nun zusätzlich hinzugefügten Informationssysteme wie z. B. E-Mail-Server und Netzwerkkomponenten gehören in der Regel in jedem Unternehmen zur vorhandenen Infrastruktur. Beschaffenheit und Verfügbarkeit dieser Systeme bieten

den Vorteil, dass sie organisationsweit einen Rückschluss auf auffällige (potenziell Fraud-verdächtige) Nutzer zulassen. Ein Beispiel ist die Untersuchung des Netzwerkverkehrs. Hierbei wird eine permanente Network Behavior Analysis (NBA) durchgeführt, um Abweichungen vom Normverhalten eines Unternehmens-angehörigen im Netzwerk aufzudecken. Dieses dient der Berücksichtigung des Fraud-Faktors Gelegenheit. Aus den ermittelten Einzelergebnissen wird unter Berücksichtigung von Gewichtungsfaktoren eine potential threat classification (PTC) ermittelt. Die PTC wird dann zur Gesamteinschätzung der Geschäftstransaktionen hinzugezogen. Im zweiten Schritt werden im Forschungsbeitrag bereits am Markt existierende Softwarelösungen auf Ihre Einsetzbarkeit untersucht und beispielhaft zusammengeführt.

Die Diskussion der möglichen Anwendung der beispielhaften Zusammenführung ist durch die Überlegungen zur Berücksichtigung des Datenschutzes, der realistischen Aussagefähigkeit der Faktoren des „Fraud Triangle“ sowie zur Erstellung der Risikoklassifikation geprägt.

5.5.3 Aufgabenteilung

Der Autor der vorliegenden Dissertation skizzierte den Ansatz des Modells zur Berücksichtigung der Faktoren des „Fraud Triangle“ im IT-Risikomanagement unter Zuhilfenahme der in einem Unternehmen vorhandenen IT-Infrastruktur. Er identifizierte dabei aus der Literatur mögliche Infrastrukturkomponenten und prüfte beispielhaft die praktische Verwendung von am Markt existierenden Software-lösungen. Stefan Hoyer beschäftigte sich eingehend mit dem Vorgehen bei der Analyse von E-Mails. Halyna Zakhariya untersuchte intensiv die Einsatz-möglichkeiten neuronaler Netze im Zusammenhang mit der Risikoabschätzung von Unternehmensmitgliedern. An der eigentlichen operativen Erstellung des Forschungsbeitrages, am Design des generischen Modells, an der Zusammenstellung der beispielhaften Zusammenführung, an der Diskussion zur Anwendung der beispielhaften Zusammenführung und an der Analyse der entsprechenden Aus-wirkungen wurde zu gleichen Teilen gearbeitet.

6 Kritische Würdigung und Ausblick

Die in dieser Dissertation vorgestellten Forschungsbeiträge sollen in diesem Kapitel zusammenhängend in einem Kontext gesetzt einer kritischen Reflexion unterzogen werden. Dies erfolgt in drei Schritten. Im ersten Schritt findet eine Einordnung der Forschungsbeiträge mit dem in Abschnitt 4.2.2 vorgestellten Prozess der gestaltungsorientierten Wirtschaftsinformatik statt. Diese Reflexion wird noch um einen Bezug auf das Design Science Framework zur Würdigung der Vorgehensweise ergänzt. Die in Abschnitt 4.3.2 angeführten Prinzipien der gestaltungsorientierten Wirtschaftsinformatik werden für die Würdigung der Forschungsergebnisse herangezogen. Anschließend wird auf die Ergebnisveröffentlichung gesondert eingegangen. Im dritten Schritt werden einzelne Punkte einer kritischen Reflexion unterzogen. Abschließend wird auf weiterführenden Forschungsbedarf eingegangen.

6.1 Einordnung und Würdigung der Vorgehensweise

Die Vorgehensweise bei der Erstellung der Forschungsbeiträge kann an den in Abschnitt 4.2.2 aufgeführten Phasen der Analyse, des Entwurfs, der Evaluation und der Diffusion aufgezeigt werden.

Am Anfang der **Analysephase** wurde in Kombination mit einem Problemanstoß und konkreten Erfahrungen aus der Praxis, die Analyse zur Problemstellung und Forschungslücke in der Wissenschaft vorgenommen. Die Problemstellung wurde in den einzelnen Forschungsbeiträgen jeweils detailliert erläutert und ist auch in dieser Arbeit in konsolidierter Form in der Einleitung (Kapitel 1) dargelegt. Auf dieser Problemstellung aufbauend wurden die Forschungsziele beschrieben (Abschnitt 4.4). Eine Erhebung des aktuellen Forschungsstandes und eine Übersicht über bisherige Lösungsansätze wurden jeweils aktuell in den Forschungsbeiträgen gegeben. Eine kurze Übersicht des Forschungsstandes wurde in dieser Arbeit in Kapitel 3 gegeben. Die sich aus der Problemstellung und der Forschungslücke ergebene Wahl der Forschungsmethode wurde in Kapitel 4 beschrieben.

Die **Entwurfsphase** begann mit dem Entwurf eines Artefakts. Dies geschah anhand argumentativ-deduktiver Gestaltung von Konstrukten, Modellen und Methoden, die dann mehrfach durch Prototyping instanziert worden sind. Ein wichtiger Faktor dabei war die Integration und Verwendung bereits bestehender und verfügbarer Elemente. Die Auswahl dieser Elemente aus der Wissenschaft oder Praxis wurde in den

Forschungsbeiträgen begründet. Somit konnte auch eine detaillierte Abgrenzung des entworfenen Prototyps zu bereits bestehenden Beiträgen und Lösungen aus der Wissenschaft und Praxis vorgenommen werden.

Die **Evaluationsphase** wurde auf zwei Ebenen durchgeführt. Eine Ebene war die Prüfung der Instanzierung der Konstrukte, Modelle und Methoden in Prototypen auf ihre Eignung zur Umsetzung der Forschungsziele. Auf die konkrete Anwendbarkeit wurde in Fallbeispielen mit Daten aus produktiven IT-Systemen eingegangen. Auf der zweiten Ebene erfolgte eine externe Evaluation durch mehrere Begutachtungen durch Experten im Rahmen von Reviews bei Konferenzeinreichungen. Die Annahme kann als eine positive Evaluation gewertet werden.

Die Präsentation der Ergebnisse auf internationalen Konferenzen und die anschließende Veröffentlichung können als Teil der **Diffusionsphase** angesehen werden. Die Kommunikation der Ergebnisse an die Anspruchsgruppen erfolgte über die Konferenzbände und verfügte somit über eine hohe Sichtbarkeit (Abschnitt 6.2).

Das Vorgehen bei der Erstellung der Forschungsbeiträge und zur Umsetzung der Forschungsziele kann insgesamt als in Übereinstimmung mit den Phasen des Prozess der gestaltungsorientierten Wirtschaftsinformatik gewertet werden.

Vor dem Hintergrund des DSR-Rahmenwerks aus Abschnitt 4.3.2 wird für die Erstellung und Präsentation der Artefakte in den Forschungsbeiträgen Bezug auf die einzelnen DSR-Prozessschritte genommen.

Das DSR-Rahmenwerk schreibt nicht den ausschließlichen Einstieg in der ersten Phase vor. Abhängig von der Zielorientierung oder dem Initiierungsgedanken kann an einer späteren Phase eingesetzt werden.

Bei den vorliegenden Forschungsbeiträgen war die **Problemidentifikation** der Einstiegspunkt in das DSR-Rahmenwerk. Aufbauend auf den Ergebnissen der Problemidentifikation wurden Entscheidungen für das zu entwickelnde Artefakt getroffen. Diese Entscheidungen beinhalteten die Wahl des Artefakttyps und den genauen Fokus des Artefaktes.

Die **Definition der Ziele** wurden von der Problemspezifikation abgeleitet. Die Ziele bezogen sich auf die Machbarkeit, die Einsetzbarkeit in heterogenen Systemlandschaften, die zeitnahe Erzeugung von Ergebnissen, die Erfüllung von

Anforderungen der Anspruchsgruppen und zielgruppenorientierte Präsentation der Ergebnisse.

Bei dem **Design und der Entwicklung** wurden die angestrebten Ziele beim Design der Funktionalität und der Architektur des Artefakts berücksichtigt, z. B. die Nutzung von Standards für eine größere Interoperabilität. Darauf aufsetzend erfolgte die Entwicklung des konkreten Artefakts.

Die Anwendbarkeit des Artefakts wurde anhand von Fallstudien geprüft. Die konkrete **Durchführung** erfolgte durch die Anbindung an ein SAP-System. Anhand der Verarbeitung von produktiven Daten konnte die erfolgreiche Problemlösung demonstriert werden.

Die **Evaluation des Artefakts** machte deutlich, dass die manuelle Übernahme von Daten aus IT-Systemen aufgrund der Komplexität und des Umfangs in einem angemessenen Zeitrahmen kaum zu Ergebnissen führen kann. So wurde beschlossen, dass eine Design-Iteration notwendig war und zur Phase „Design und Entwicklung“ zurück gegangen werden musste. Die Weiterentwicklung des HICSS 2010-Beitrags um eine automatisierte Konvertierung von Zugangsdaten begann iterativ in der dritten Phase „Design und Entwicklung“ und führte zu einem neuen Forschungsbeitrag.

Die Forschungsbeiträge wurden auf verschiedenen Konferenzen vor den relevanten Anspruchsgruppen wie Wissenschaftlern oder Praktikern präsentiert. Somit fand eine **Kommunikation der Ergebnisse** statt. Sie beinhaltete dabei eine Beschreibung des Artefakts, eine Vorstellung des zu erwartenden Nutzen und der eingesetzten Forschungsmethoden sowie die durchgeführten Evaluationen.

Zusammenfassend kann die Erstellung der Forschungsbeiträge und die Umsetzung der Forschungsziele als in Übereinstimmung mit den Phasen des DSR-Rahmenwerkes gewertet werden.

6.2 Ergebnisveröffentlichung

Die ersten Recherchen zu einem möglichen Promotionsthema begannen Anfang 2007 und wurden in Hinblick auf die Veröffentlichung einer Monographie getätigt. Der Autor wählte verschiedene Oberthemen aus und priorisierte anhand einer Nutzwertanalyse die Themenwahl. Diese favorisierten Themen und Fragestellungen, die aus einem jeweiligen aktuellen Anlass in Betracht kamen, wurden im Jahr 2008

aufbereitet. Die Ausarbeitung der Forschungsbeiträge in dieser Dissertation begann in 2009.

Mit den Veröffentlichungen bei der HICSS 2010 und ECIS 2010 konnten Konferenzen mit sehr guten Einstufungen erreicht werden. Diese Konferenzen sind auch wegen ihrer allgemein hohen Sichtbarkeit in der Wirtschaftsinformatik sehr gut für die Ergebnisveröffentlichung geeignet. Der zweite und vierte Konferenzbeitrag richtete sich speziell an Fachkonferenzen mit guten Ranglisteneinstufungen. Bei diesen Konferenzen konnten, vor besonders fachkundigen Konferenzteilnehmern, die Beiträge vorgestellt, diskutiert und weitere Anregungen gesammelt werden.

Die Besuche der Konferenz gaben jedes Mal eine Vielzahl von Impulsen sich weiter und intensiver mit dem gewählten Thema zu beschäftigen. Dieser „Effekt“ hätte, durch frühzeitige Veröffentlichungen beim Einstieg in das Thema (z. B. mit einem Literaturreview) vielleicht noch eher beginnen können. Dieser Umstand ist auch auf den Wechsel von der Monographie zur kumulativen Dissertation zurückzuführen.

6.3 Forschungsergebnisse

Zur Einordnung der Forschungsergebnisse eignen sich die Prinzipien der gestaltungsorientierten Wirtschaftsinformatik (Abschnitt 4.2.2) mit den Prinzipien Abstraktion, Originalität, Begründung und Nutzen.

Bei der Erstellung des Artefaktes war die **Abstraktion** ein wesentliches Ziel. Das erstellte Artefakt nutzt u. a. etablierte Standards, um eine hohe Interkonnektivität und Einsatzfähigkeit in heterogenen Systemlandschaften gewährleisten zu können. Diese Unabhängigkeit zu einem konkreten IT-System wurde nur durch die Erfordernisse der Evaluation eingeschränkt. Hier wurde ein SAP-System gewählt, damit ein Einsatz mit produktiven Daten durchgeführt werden konnte.

In jedem Forschungsbeitrag wurde auf den jeweils neuen Anteil eines innovativen Beitrags (**Originalität**) zum Stand der Forschung geachtet. Dies wurde auch in den Reviews zu den Forschungsbeiträgen, die auf der HICSS 2010, ARES 2010 und VISM 2010 eingereicht wurden, positiv hervorgehoben.

Die Herbeiführung des Artefaktes muss für Dritte nachvollziehbar und validierbar sein. Die **Begründung** für den Entwurf und die Auswahl der einzelnen Elemente des Artefakts wurde in den Forschungsbeiträgen ausführlich dargelegt. Die Experten der einzelnen Begutachtungsverfahren konnten diese Begründungen durchweg

nachvollziehen. Die konkrete Nachvollziehbar- und Validierbarkeit der Forschungsergebnisse sind durch die Rekonstruktion der Artefakte möglich. Die dafür notwendige Tiefe der technischen Details ist in den Forschungsbeiträgen gegeben.

Die Generierung von **Nutzen** für die Anspruchsgruppen lässt sich durch die von den begutachtenden Experten bestätigte Relevanz ablesen. Relevant sind u. a. Forschungsbeiträge, die eine Lösung zu einem real existierenden Problem bieten. Die Relevanz wurde von den Experten sehr positiv bewertet und lässt damit auf eine gute Lösung der Problemstellung hindeuten.

Insgesamt lässt sich feststellen, dass die Forschung den Prinzipien der gestaltungsorientierten Wirtschaftsinformatik entspricht.

6.4 Kritische Würdigung

Ein mögliches Problem im Bereich des IT-Compliance Managements besteht unter Umständen in der Versuchung in eine vereinfachende dichotome Schwarz-/Weißsicht bei der Beurteilung von (Kontroll-) Problemen zu verfallen. Dies wird durch die Nutzung von IT-Compliance Management Anwendungen (z. B. dem vorgestellten Prototyp), die oft über ein von den Nutzern selbst zu pflegendes Regelwerk verfügen, begünstigt. Für die Nutzer dieser Anwendungen gibt es vorrangig nur noch das Szenario der Kontrollverletzung (Schwarz) oder nicht Verletzung (Weiß). Andere Überlegungen (Grau) werden nicht zugelassen bzw. in Betracht gezogen.
In der Praxis kann diese reine Schwarz-/Weißsicht zu kurz greifen. Werden Ziele der Unternehmensführung wie langfristige Unternehmensexistenzsicherung und Ertragsorientierung berücksichtigt, ergibt sich oft ein etwas differenzierteres Bild. Die Ertragsorientierung hat z. B. auch einen Einfluss auf das Risikomanagement, das effizient und effektiv durchgeführt werden soll. Hier gilt es, durch die Unternehmensführung bzw. das obere Managements abzuwägen, inwieweit ein Risiko eingegangen werden kann. Das Eingehen eines abgeschätzten Risikos u. a. durch die Akzeptanz eines Restrisikos durch die Unternehmensführung kann betriebswirtschaftlich sinnvoll sein, wenn z. B. nur eine geringe Schadenshöhe, aber hohe Kontrollkosten erwartet werden. So ist eine „graue Sichtweise“ in einem Unternehmen unter Umständen gewünscht und muss im IT-Compliance Management entsprechend berücksichtigt werden. Diesen Umständen sollte in der Definition der Kontrollen oder bei den abschließenden Auswertungen Rechnung getragen werden.

Eine weitere zu berücksichtigende Herausforderung bei der Nutzung von IT-Compliance-Management-Anwendungen kann der Umgang mit den Ergebnissen sein. Uneingeschränktes oder zu mindestens großes Vertrauen in die selbstkonfigurierten Kontrollen/Regeln der IT-Compliance Management Anwendung könnte bei den Verantwortlichen zu einer ungeprüften Akzeptanz der Ergebnisse führen. In den vorgestellten Forschungspapieren wurden gerade die Prozesseigner bzw. Prozessverantwortlichen als Zielpersonen für eine eigenständige Konfiguration identifiziert. Dieser Personenkreis, der naturgemäß sehr gut mit den zu prüfenden Prozessen vertraut ist, könnte ggf. der Fehleinschätzung unterliegen, dass durch die vorliegende Prozesskenntnis und selbst definierter Kontrollen ein unbeobachtetes Abweichen nicht mehr möglich ist. Sollte nun eine IT-Compliance-Management-Anwendung keine Kontrollverletzungen signalisieren, könnte die Gefahr bestehen, dass das Ergebnis bzw. der Prozess ungeprüft akzeptiert wird. Das könnte zu deutlich verminderten manuellen Prüfungsaktivitäten führen oder gar in einer praktischen Untätigkeit der Verantwortlichen gipfeln. Hier gilt es den Anwender bzw. die Verantwortlichen durch Schulungen etc. zu sensibilisieren, um nicht den direkten Blick auf den Prozess unabhängig von der Prüfsoftware zu verlieren.
Das Vertrauen in die eigenen Kontrollen muss auch vor dem Hintergrund der Entdeckungswahrscheinlichkeit von Fehlverhalten hinterfragt werden. So ist nach einer aktuellen Umfrage der ACFE[115] der häufigste Entdeckungsgrund der Hinweis aus den eigenen Mitarbeiterreihen (40,2%). Management Reviews (15,4%) oder interne Audits (13,9%) sind trotz Platz zwei und drei schon erheblich seltener vertreten. Hier kann noch Potential in der intensiveren Auseinandersetzung (Review) oder in einer (pro)aktiven Arbeit (Audit) gesehen werden. Obwohl die Entdeckungswahrscheinlichkeit durch interne Kontrollen in dieser Umfrage als gering eingestuft wurde, sollte die einschränkende Wirkung auf den Faktor Gelegenheit des „Fraud Triangles“ nicht unterschätzt werden.[116]

Auch im Bereich des IT-Compliance Managements gilt die Abwägung von Kosten und Nutzen. So wird in diesem Zusammenhang oft die Frage gestellt, ob IT-Compliance auch einen Nutzen oder Fortschritt bei der Umsetzung der IT-Sicherheit bringt. Dahinter steht i. d. R. die Annahme, dass nur eine Budgetverlagerung von der

[115] Vgl. ACFE 2010, S. 16f.
[116] Vgl. Birkental 2011, S. 180.

IT-Sicherheit hin zur IT-Compliance geschieht.[117] Vor diesem Hintergrund bieten die Eigenschaften des Prototyps mögliche Synergieeffekte und Einsparpotenziale (s. Abschnitte 5.1.2, 5.2.2, 5.3.2). Einer der wichtigsten Kosteneinspareffekte ist die mögliche Zentralisierung und Vereinheitlichung der IT-Compliance-Management-Software. Dies ist, hinsichtlich der meist vorherrschenden heterogenen Systemlandschaften, ein relativ leicht zu realisierender Beitrag zur monetären Entlastung.

Ein nicht unerheblicher Posten in der Kostendiskussion beim IT-Compliance Management ist die IT-Compliance-Management-Software. Auf dem Markt bieten oft Wirtschaftsprüfungsgesellschaften IT-Compliance-Management-Softwarepakete zur Installation oder ergänzend dazu mit personeller Betreuung an. Daraus kann ein nicht unerheblicher und kontinuierlicher Kostenblock erwachsen. Trotz der eigenständigen Implementierung, der selbstständigen Durchführung des operativen Einsatzes und der Ermöglichung der selbstbestimmten Pflege der Konfiguration, Kontrollen und Regeln, unterliegt auch der Prototyp mit den vorgenannten kostensparenden Eigenschaften noch externen Kostenfaktoren. So muss eine IT-Compliance Management Software in der Regel noch von einem Wirtschaftsprüfer (z. B. Prüfung der Kontrollen auf ihre Funktionsfähigkeit) abgenommen werden. Unter Umständen führt das zu erheblichen periodischen Kosten. Allerdings beinhalten die vorgenannten Angebote der Wirtschaftsprüfungsgesellschaften oft erheblichen Personalaufwand. Bei der Umsetzung nach dem Konzept des Prototyps hingegen erfolgt ein Rückgriff auf eigene Mitarbeiter. Das hat neben den daraus resultierenden Kosten den Vorteil, dass Wissen im Unternehmen verbleibt bzw. aufgebaut wird und auch zukünftig flexibler gehandhabt werden kann.

Die schon in den ersten beiden Forschungsbeiträgen priorisierten umfangreichen Extraktions- und Austauschfähigkeiten des Prototypen wurden als wichtiger Erfolgsfaktor für die Arbeit in heterogen Systemlandschaften identifiziert. Hierbei wurde auf zeitgemäße Modelle und Standards zur Datenbeschreibung und -verwaltung gesetzt. Es ist insofern angebracht, als dass in einem aktuellen Fachartikel des Berufsverbandes der IT-Revisoren des Information Systems Audit and Control Association (ISACA)[118] noch u. a. eine Vereinheitlichung des Austausches von Daten mit dem anachronistischen Comma-Separated-Values (CSV)-Format

[117] Vgl. Hulme 2008.
[118] Die ISACA ist u. a. verantwortlich für die Certified Information Systems Auditor (CISA) Zertifizierung; ISACA 2011.

beschrieben wird.[119] Weitere Entwicklungsmöglichkeiten zur Weitergabe der Daten werden im Ausblick erläutert.

Generell wird der Einsatz eines Prototyps als Werkzeug der Evaluation gegen eine Forschungslücke als gut geeignet angesehen.[120] Im Rahmen der Evaluation der einzelnen Forschungsbeiträge wurde ebenso eine Analyse im Hinblick auf die Usability sowie Anforderungen der Anwender und Performance durchgeführt. Der Umfang dieser Evaluationen könnte noch erweitert werden. In den Forschungsarbeiten musste jedoch den beschränkten Ressourcen Rechnung getragen werden. Ähnliches trifft auf die Einschränkungen des betrachteten Themenkreises zu. Hier wurde der Fokus auf ein Themengebiet gelegt, das im Rahmen der vorliegenden IT-Infrastruktur abbildbar (Einsatzszenario, Test, Evaluation) war.

Die Verfahren und Methoden der Ermittlung und Einbeziehung der Persönlichkeitsfaktoren in eine Risikoabschätzung und der Umfang der ermittelten Daten unterliegen verschiedenen Einschränkungen. Diese Einschränkungen, die rechtlicher oder selbsteinschränkender Natur (z. B. Regelungen mit der Arbeitnehmervertretung) sein können, lassen möglicherweise die Umsetzung als nicht realisierbar erscheinen. Hierbei spielen allerdings die unterschiedlichen rechtlichen Ausgangssituationen in den Ländern eine wesentliche Rolle. So weisen die rechtlichen Rahmenbedingen bezüglich Datenschutz bzw. der informellen Selbstbestimmung oder der Ermittlung und Weiterverarbeitung von persönlichen Daten (z. B. Krankheitsdaten oder psychologische Daten) erhebliche Unterschiede auf.[121]

Stellvertretend sei hier als Indikator das BDSG[122] genannt, das in § 6a Abs. 1 auf automatisierte Entscheidungen eingeht, die auf personenbezogenen Daten zur Bewertung einzelner Persönlichkeitsmerkmale, basieren. Wenn bei solchen Entscheidungen rechtliche Auswirkungen oder erhebliche Beeinträchtigungen zu erwarten sind, dürfen diese nicht ausschließlich automatisiert getroffen werden, sondern bedürfen zusätzlich einer Bewertung und Entscheidung durch eine natürliche Person. Dies soll Entscheidungen verhindern, die ausschließlich auf Grundlage von automatisiert erstellten Persönlichkeitsprofilen beruhen.[123] Allerdings kann dieses

[119] Vgl. Singleton 2010.
[120] Vgl. Riege et al. 2009, S. 81.
[121] Vgl. Flegel 2011, S. 194f.
[122] Vgl. BDSG 2003.
[123] Vgl. Bizer 2006, S. 572 nach Strohmeier 2008, S. 45.

Verfahren durch Zustimmung des Betroffenen oder durch Vertragsverhältnisse zulässig sein.[124]

Die Durchführung von kontinuierlichen Prüfungen (continuous auditing) mit Mitarbeiterbezug in IT-Systemen ist, ähnlich wie eine ständige Videoüberwachung von Mitarbeitern, nach deutschem Recht nicht zulässig.[125] Solche Prüfungen dürfen nur anlassbezogen durchgeführt werden. Nach einer Entscheidung des Bundesverfassungsgerichts ist z. B. ein möglicher Lösungsweg bei Massendatenanalysen, dass die Prüfungsergebnisse möglichst wenig Daten beinhalten, die Personen konkret identifizierbar machen und somit Nichtbetroffene anonym bleiben können.[126] Ein weiterer Lösungsweg wäre die kontinuierlich erhobenen Auditdaten einer Pseudonymisierung zu unterziehen.[127] Falls sich bei der Analyse der pseudonymisierten Auditdaten ein konkreter Verdachtsmoment ergibt, ist eine Rückwandlung zur Zuordbarkeit und Untersuchung der Daten erlaubt.[128]

Im US-amerikanischen Recht sind die Hürden für eine Verarbeitung betrieblicher personenbezogener Daten niedriger. So können z. B. Daten aus Überprüfungen eines „Background Checks“, Arbeitszeiten, Disziplinar- oder Fertigkeitenaufstellungen des Mitarbeiters ohne rechtliche Bedenken für eine interne Bedrohungsanalyse genutzt werden.[129]

6.5 Ausblick

Bei der Bereitstellung von IT-Compliance-Management-Software soll, neben der in den Forschungsbeiträgen 1 und 3 dargestellten Überwindung technischer Probleme durch die heterogenen komplexen Systemlandschaften, auch die spätere Nutzung bzw. der Anwender betrachtet werden. Das wurde in den Forschungsbeiträgen 2 und 4 mit der Ermittlung der Informationsanforderungen und der Bedürfnisse bei der abschließenden visualisierten Informationsbereitstellung berücksichtigt.

Ein nächster Schritt wäre, die Akzeptanz und die Nutzung eines solchen Anwendungssystems konkret bei den Anwendern zu prüfen. Zielgruppen einer solchen Prüfung wären interne Fachkräfte eines Unternehmens und Mitarbeiter von

[124] Vgl. Bizer 2006, S. 572 nach Strohmeier 2008, S. 45.
[125] Vgl. Flegel 2011, S. 194f. Zur Wahrung der Revisionsfähigkeit ist ein Logging möglich. Berücksichtigt werden muss dabei das Datenschutzthema Leistungs- und Verhaltenskontrolle.
[126] Vgl. BVerfG 2009.
[127] Diese Problematik ist auch im Revisionsumfeld ein Thema. Vgl. Leitfaden für Datenauswertungen und personenbezogene Datenanalysen: DIIR und GDD 2009.
[128] Vgl. Flegel 2011, S. 199.
[129] Vgl. Greitzer et al. 2011, S. 148.

Wirtschaftsprüfungsgesellschaften. Mit Hilfe des Technology Acceptance Model (TAM) können Faktoren bestimmt werden, die die Akzeptanz und Nutzung des IT-Systems beeinflussen. So lassen u. a. die Faktoren „wahrgenommene Nützlichkeit“ (perceived usefulness) und „wahrgenommene Benutzerfreundlichkeit“ (perceived ease-of-use) Rückschlüsse auf die empfundene Nützlichkeit und Einfachheit zu. Hieraus können dann ggf. Ideen oder Handlungsempfehlungen zur Umgestaltung bzw. zum Neudesign der IT-Compliance-Management-Software abgeleitet werden, um den Akzeptanz- und Nutzungslevel bei den Anwendern weiter zu erhöhen.

Bei dem Design des Artefakts wurde zwei Aspekten ein hohes Maß an Bedeutung eingeräumt. Der erste Aspekt betrifft die einfache Anpassbarkeit durch den Anwender. Der zweite Aspekt ist die Berücksichtigung der Problematik, dass fachliche Anwender und IT-Fachpersonal oft Probleme haben, eine gemeinsame Verständnisebene zu finden. Diese Grundannahmen waren aus Praxiserfahrungen von Matthias Kehlenbeck und dem Autor der Dissertation im Vorfeld abgeleitet worden. Die umfangreiche Anpassbarkeit eines einfach zu pflegenden Regelwerks wurde mit Hilfe einer Oberflächenunterstützung umgesetzt. Um eine gemeinsame Verständnisebene von nicht technisch versierten Anwendern von Fachabteilungen und IT-Fachpersonal zu schaffen, wurde die BPMN zur Prozessbeschreibung gewählt. Die BPMN-gestützte „Kommunikation“ zwischen dem Anwender und dem IT-Fachpersonal liefert die Grundlagen für den Aufbau eines gemeinsamen Verständnisses über die Prozesse. Dies soll es dem Anwender ermöglichen seine Kernkompetenzen, d. h. sein fachliches Prozesswissen zielführender einzubringen.
Dennoch gibt es hier noch weiteren Forschungsbedarf. In der Praxis wurde bei IT-Compliance-Management-Softwarelösungen häufiger beobachtet, dass sie eine regelrechte „Alarmflut" auslösen können (je nach Aussteuerung des Regelwerks oder Kontrollen).[130] Ob diese fehlerhaft sei oder nicht, muss oft zeitaufwendig nachgeprüft werden. In diesem Zusammenhang gilt es, verbesserte Methoden und Techniken zu entwickeln, die die Datenauswahl mit Hilfe von differenzierten Analysen sinnvoll treffen (Bsp. für einen Ansatz ist der Forschungsbeitrag in Abschnitt 5.5), um so die Anzahl der Falschmeldungen zu reduzieren. Vorstellbar wäre der Einsatz künstlicher Intelligenz bzw. Neuronaler Netze oder anderer mathematischer Lösungen. Im Bereich der Verständnisebene gibt es z. B. im Umfeld der ERP-Systeme noch erhebliches Verbesserungspotenzial. So könnten vom ERP-

[130] Vgl. Kuhn und Sutton 2010, S. 99.

System selbstgenerierte Prozessmodelle für eine stets aktuelle Übersicht über die Prozesse sorgen. Zur Generierung eines Mehrwertes hinsichtlich des IT-Compliance-Managements müssten diese Prozessmodelle um IT-Compliance-Informationen anreicherbar und anpassbar sein. Diese angepassten Prozessmodelle müssten über eine Rückkopplung automatisiert in das ERP-System übertragen werden und sich somit direkt auf die Prozesse auswirken können. Das Verständnis der Prozesseigner für die Hinterlegung von Kontrollen in ihren Prozessen und den zu erwartenden Auswirkungen könnte so leichter geschaffen bzw. „live" im ERP-System demonstriert werden.

Bei der Erstellung der Prototypen wurde von Anfang an an eine sinnvolle, zielführende und vor allem innerhalb seines natürlichen Arbeitskontextes bleibende Kommunikation zum Anwender gedacht. Dies wurde durch die Nutzung eines DW und der Verknüpfung mit BI-Anwendungen umgesetzt. Auf dieser Auswertungsmöglichkeit aufsetzend, wurde die Informationsbereitstellung in einem späteren Forschungsbeitrag (s. Abschnitt 5.4) mit Hilfe eines Dashboards noch visuell verfeinert. Der Anwender wird somit in die Lage versetzt auf Grundlage der generierten Informationen, adäquate zeitnahe Entscheidungen treffen zu können.
Hinsichtlich der Einbindung der vorliegenden Informationen gibt es noch weiteren Forschungsbedarf. Damit die durch die IT-Compliance-Management-Software generierten Informationen ihr Potenzial für Analysemöglichkeiten noch besser entfalten können, müssten sie in einen betrieblichen oder organisationalen Kontext eingeordnet und um Hintergrundinformationen zu den Regularien ergänzt werden. Hierzu bietet sich ein Knowledge Management System (KMS) an. Dieses IT-Compliance-KMS müsste, für eine einfache Anwendbarkeit, transparent in die IT-Compliance Management Software bzw. in die IT-Compliance Management Prozesse integriert sein. Bei Erstellung einer Kontrolle, der Pflege des Regelwerks, der Analyse von Prozessmodellen, der Anbindung an das DW oder der Anreicherung des Anwender Dashboards könnten Verknüpfungen zum IT-Compliance-KMS sinnvoll für ein leichteres Verständnis der Entscheider sein.

Die Anforderungen an eine IT-Compliance Management Lösung wurden u. a. anhand umfangreicher Literaturanalysen, Berücksichtigung der identifizierten Erfolgsfaktoren, Erfahrungen aus der Praxis und Erhebung der Anwenderbedürfnisse gewonnen.

Ein weiterer Schritt könnte nun ein ergänzender Abgleich der gewonnen Erkenntnisse mit den Anforderungsprofilen und –kriterien von Softwareauswahl-Frameworks im Bereich der Compliance sein. Hier könnten sich weitere Ansatzpunkte zur Verbesserung oder Weiterentwicklung ergeben. Allerdings stehen diese Art von Frameworks noch am Anfang der Entwicklung. Stellvertretend seien hier Singh und Lija (2010) genannt, die im ISACA Journal Kriterien und Methoden für die Auswahl von GRC-Lösungen vorstellen.

Da die IT-Compliance Management Software im betrieblichen Kontext häufig in einem heterogenen Systemumfeld eingesetzt wird, ist die Anbindungs-, Extraktions- und Austauschfähigkeit einer solchen Software essenziell. Schon bei dem Design des Artefakts (HICSS-Beitrag) und bei der späteren Überarbeitung zur Automatisierung (ECIS-Beitrag) wurden diese Anforderungen berücksichtigt. Sinnvoll wäre in einem weiteren Schritt, die Extensible Business Reporting Language (XBRL) zu unterstützen. Diese auf XML basierende Sprache dient der Markierung bzw. Anreicherung von Daten und erlaubt somit eine vereinfachte standardisierte Übergabe, Veröffentlichung und Analyse von Daten. Mit der Unterstützung bzw. Implementierung von XBRL könnten Daten leichter mit anderen IT-Compliance Lösungen ausgetauscht oder aus unterstützenden Quellsystemen kontextbezogener exportiert werden.

Die zeitnahe Extraktion und Analyse der Daten aus dem Quellsystem ist ein wichtiger Erfolgsfaktor für eine IT-Compliance Softwarelösung. In den hier vorgestellten Forschungsbeiträgen wurde erfolgreich die Extraktion der Daten und die anschließende Analyse mit Hilfe eines XACML Policy Decision Point (PDP) im SAP ERP Umfeld durchgeführt.
Um eine zeitnahere oder sogar eine Echtzeitanalyse zu ermöglichen, müsste in mehreren Bereichen noch Forschungsarbeit geleistet werden. Ein Ansatzpunkt wäre die Nutzung eines alternativen PDPs. Dafür wäre eine Evaluation möglicher PDPs zur Prüfung der Einsatzfähigkeit in diesem Arbeitsgebiet notwendig. Die anschließenden Performancemessungen der in Frage kommenden PDPs würden Hinweise auf die Implementierungstauglichkeit für eine Echtzeitanalyse geben. Die Implementierung müsste in einem Echtsystem getestet werden, um z. B. negative Effekte auf die Systemgeschwindigkeit auszuschließen.

Der Forschungsbeitrag im Bereich des IT-Risikomanagements (s. Abschnitt 5.5) stellt einen Ansatz zur Berücksichtigung von beobachtbaren Persönlichkeitsmerkmalen eines Unternehmensangehörigen vor. Es wurden die Persönlichkeitsmerkmale herangezogen, die - in Verbindung mit dem „Fraud Triangle“ - ein Indiz für potentiellen Betrug (Fraud) darstellen können.
Hier gilt es weitere Persönlichkeitsmerkmale zu identifizieren, die in Verbindung mit IT-Sicherheit, Betrugsaufdeckung oder IT-Compliance gebracht werden können. Denkbar wären Modelle aus der Psychologie, z. B. das „Big Five“- oder Fünf-Faktoren-Modell (FFM), welche die Hauptdimensionen einer Persönlichkeit erfassen können. Bei der Berücksichtigung dieser ermittelten Faktoren innerhalb der IT-Compliance, der Prüfung oder der Berechtigungsvergabe, besteht für die konkrete Ausgestaltung und Würdigung noch Forschungsbedarf. So müsste der Einfluss dieser Faktoren auf einzelne Themengebiete noch detaillierter untersucht werden.

Die Ermittlung einer Gesamteinschätzung PTC (mit Bezug auf die „Fraud Triangle“ Faktoren) einer möglichen Risikobedrohung wurde im Forschungsbeitrag zum IT-Risikomanagement skizziert. Der PTC wird bei späteren Auswertungen im Dashboard oder für Selektionen der zu untersuchenden Transaktionen eingesetzt.
Um Risikoabschätzungen zeitnah zu ermöglichen, wäre daher eine direkte Implementierung im IT-System oder in Anwendungen, welche Kontrollen durchführen, sinnvoll. In diesem Zusammenhang wäre die Anreicherung des PDPs um Risikoabschätzungen des PTC eine Möglichkeit. So könnte der PDP eigenständig im Entscheidungsprozess entsprechende Entscheidungen treffen oder Warnungen ausgeben.

Literaturverzeichnis

ACFE 2010: Association of Certified Fraud Examiners: Report to the Nations on Occupational Fraud and Abuse. 2010 Global Fraud Study. URI: http://www.acfe.com/rttn/rttn-2010.pdf. Abrufdatum: 26. Januar 2011.

ACM 2011: Association For Computer Machinery (ACM): ACM Guide to Computing Literature. URI: http://portal.acm.org/guide.cfm. Abrufdatum: 26. Januar 2011.

AIS 2011: Association for Information Systems (AIS): About the Association for Information Systems. URI: http://home.aisnet.org/displaycommon.cfm?an=3. Abrufdatum: 26. Januar 2011.

AIS 2011a: Association of Information Systems (AIS): International Conference on Information Systems (ICIS 2010). URI: http://icis2010.aisnet.org/. Abrufdatum: 26. Januar 2011.

AIS 2011b: Association for Information Systems (AIS): AIS Electronic Library (AISeL). URI: http://aisel.aisnet.org/. Abrufdatum: 26. Januar 2011.

ALLAN UND ZHAN 2010: Allan, T.; Zhan, J.: Towards Fraud Detection Methodologies. In: 5th International Conference on Future Information Technology (FutureTech).

ARC 2010: Australian Research Council (ARC): The Excellence in Research for Australia (ERA) Ranked Outlets, URI: http://www.arc.gov.au/era/era_journal_list.htm. Abrufdatum: 19. Januar 2011.

BASSEN UND ZÖLLNER 2009: Bassen, A; Zöllner, C.: Erhöht gute Corporate Governance den Unternehmenswert? In: Wagenhofer, A. (Hrsg.), Controlling und Corporate Governance-Anforderungen, Konzepte, Maßnahmen, Umsetzung. Berlin. S. 43–58.

BDSG 2003: Bundesdatenschutzgesetz (BDSG). In: Bundesgesetzblatt, Teil I, S. 66.

BECKER ET AL. 2009: Becker, J.; Krcmar, H.; Niehaves, B.: Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik, Springer, DOI 10.1007/978-3-7908-2336-3.

BECKER 2010: Becker, J: Prozess der gestaltungsorientierten Wirtschaftsinformatik. In: Österle, H. (Hrsg.); Winter, R. (Hrsg.); Brenner, W. (Hrsg.):

Gestaltungsorientierte Wirtschaftsinformatik: Ein Plädoyer für Rigor und Relevanz. Infowerk. ISBN 978-3-00-030310-4.

BIRKENTAL 2011: Birkental, R.: Fraud: Aufdeckung und Prävention durch Forensic Accounting. In: Hlavica, C. (Hrsg.); Klapproth, U. (Hrsg.); Hülsberg, F. M. (Hrsg.): Tax Fraud & Forensic Accounting - Umgang mit Wirtschaftskriminalität. Gabler, Wiesbaden.

BIZER 2006: Bizer, J.: Kommentar zu § 6a Automatisierte Einzelentscheidung. In: Simitis, S. (Hrsg.) Bundesdatenschutzgesetz, 6. Aufl., Baden-Baden. Nomos, S. 558-570.

BUCHER ET AL. 2008: Bucher, T., Riege, C., Saat, J.: Evaluation in der gestaltungsorientierten Wirtschaftsinformatik – Systematisierung nach Erkenntnisziel und Gestaltungsziel. In: Becker, J., Krcmar, H., Niehaves, B. (Hrsg). Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik. Arbeitsbericht Nr. 120 des Instituts für Wirtschaftsinformatik, Universität Münster, S. 69–86, ISSN 1438-3985.

BVERFG 2009: Bundesverfassungsgericht (BVerfG): 2 BvR 1372/07 vom 17.2.2009, Absatz-Nr. (1 - 35). URI: http://www.bverfg.de/entscheidungen/rk20090217_2bvr137207.html. Abrufdatum: 27. März 2011.

CAMPOS NAVE UND BONENBERGER 2008: Campos Nave, J. A.; Bonenberger, S.: Korruptionsaffären, Corporate Compliance und Sofortmaßnahmen für den Krisenfall. In: Betriebs-Berater, 63, S. 734–741.

CHEN UND HIRSCHHEIM 2004: Chen, W.; Hirschheim, R.: A paradigmatic and methodological examination of information systems research from 1991 to 2001. In: Information Systems Journal, 4 (3), S. 97–235.

CLEVEN ET AL. 2009: Cleven, A.; Gubler, P.; Hüner, K.: Design Alternatives for the Evaluation of Design Science Research Artifacts. In: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology (DESRIST 2009), Malvern.

COLE ET AL. 2005: Cole, R.; Purao, S.; Rossi, M.; Sein, M.: Being Proactive: Where Action Research Meets Design Research. In: Proceedings of the International Conference on Information Systems (ICIS 2005).

CRESSEY 1973: Cressey, D. R.: Other People's Money: A Study in the Social Psychology of Embezzlement. New York, Free Press.

D'ARCY ET AL. 2009: D'Arcy, J.; Hovav, A.; Galletta, D.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. In: Information Systems Research. 20 (1), 2009, S. 79–98.

DAVISON ET AL. 2004: Davison, R.M.; Martinsons, M.G.; Kock, N.: Principles of canonical action research. In: Information Systems Journal, 14, S. 65-86.

DCGK 2010: Deutscher Corporate Governance Kodex. URI: http://www.corporate-governance-code.de/ger/download/kodex_2010/D_CorGov_Endfassung_Mai_2010.pdf. Abrufdatum: 13. Februar 2011.

DIIR UND GDD 2009: DIIR – Deutsches Institut für Interne Revision e.V. und der GDD - Gesellschaft für Datenschutz und Datensicherheit: Datenauswertung und personenbezogene Datenanalyse: Beispiele für den praktischen Umgang im Revisionsumfeld. URI: https://www.gdd.de/nachrichten/arbeitshilfen/DIIR-Datenanalyse_091209.pdf. Abrufdatum: 27. März 2011.

DISTERER 2009: Disterer, G.: Zertifizierung der IT nach ISO 20000. In: Wirtschaftsinformatik, 51 (6), S. 530-534.

ELSEVIER 2011: Elsevier: ScienceDirect. URI: http://www.sciencedirect.com. Abrufdatum: 26. Januar 2011.

FLEGEL 2007: Flegel, U.: Privacy-Respecting Intrusion Detection. In: Advances in Information Security, 2007 (35), Part I, S. 77-87. Springer Science+Business Media, New York.

FLEGEL 2011: Flegel, U.: Privacy Compliant Internal Fraud Screening. In: ISSE 2010 Securing Electronic Business Processes 2011, Part 5, S. 191-199.

FLEISCHER 2008: Fleischer, H.: Corporate Compliance im aktienrechtlichen Unternehmensverbund. In: Corporate Compliance Zeitschrift, 1; S. 1–6.

FISCHER ET AL. 2010: Fischer, C.; Winter, R.; Wortmann, F.: Gestaltungstheorie. In: Wirtschaftsinformatik, 52 (6), S. 383-386.

FRANK 2003: Frank, U.: Einige Gründe für die Wiederbelebung der Wissenschaftstheorie. Die Betriebswirtschaftslehre, 63 (3), S. 278-292.

FRANK 2006: Frank, U.: Towards a Pluralistic Conception of Research Methods in Information Systems Research. ICB-Research Report Nr. 7. Universität Duisburg-Essen. ISSN 1860-2770.

FRANK 2008: Frank, U.: Herausforderungen der Wirtschaftsinformatik in Zeiten des Wandels. In: Jung, R. (Hrsg); Myrach, T. (Hrsg): Quo vadis Wirtschaftsinformatik. Festschrift für Prof. Gerhard F. Knolmayer zum 60. Geburtstag. Gabler, Wiesbaden, S. 37–56.

GDPdU 2001: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU). In: BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01.

GOBS 1995: Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS). In: Bundessteuerblatt, Teil I, IV A 8 – S 0316 – 52/95, S. 738.

GOLL UND HAUPT 2008: Goll, L.; Haupt, S.: Corporate Governance, Risk- and Compliance Management in der Beschaffung. In: BME Bundesverband Materialwirtschaft Einkauf Und Logistik e.V. (Hrsg.): Best Practice in Einkauf und Logistik, 2. Auflg., Wiesbaden. S. 149–168.

GOODE UND LACEY 2011: Goode, S.; Lacey, D.: Detecting complex account fraud in the enterprise: The role of technical and non-technical controls. In: Decision Support Systems. 50 (2011), S. 702–714.

GREITZER UND FRINCKE 2010: Greitzer, F. L.; Frincke, D. A.: Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation. In: Probst, C.W.; Hunker, J.; Gollmann, D.; Bishop, M. (Eds.): Insider Threats in Cyber Security Advances in Information Security, 2010 (49). Springer, New York, S. 85-113.

GREITZER ET AL. 2011: Greitzer, F. L.; Frincke, D. A.; Zabriskie, M.: Social/Ethical Issues in Predictive Insider Threat Monitoring. In: Dark, M. J. (Ed.): Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives. Information Science Reference, Hershey, New York.

GULL 2010: Gull, D.: Beiträge zur Unterstützung von IT-Sourcing-Entscheidungen. Dissertation. URI: http://opus.bibliothek.uni-augsburg.de/volltexte/2010/1590/pdf/Dissertation_Daniel_Gull.pdf. Abrufdatum: 12. Februar 2011.

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

HENNIG-THURAU UND SCHRADER 2011: Hennig-Thurau, T.; Sattler, H.: VHB-JOURQUAL2.1. URI: http://vhbonline.org/service/jourqual/vhb-jourqual-21-2011/jq21/ Abrufdatum: 30. März 2011.

HEINRICH 2005: Heinrich, L. J.: Forschungsmethodik einer Integrationsdisziplin: Ein Beitrag zur Geschichte der Wirtschaftsinformatik. NTM International Journal of History and Ethics of Natural Sciences, Technology and Medicine, 13 (2), S. 104-117.

HEINRICH ET AL. 2007: Heinrich, L. J.; Heinzl, A.; Roithmayr, F.: Wirtschaftsinformatik: Einführung und Grundlegung, 3. Aufl. Oldenbourg, München.

HEINZL ET AL. 2001: Heinzl, A.; König, W.; Hack, J.: Erkenntnisziele der Wirtschaftsinformatik in den nächsten drei und zehn Jahren. In: Wirtschaftsinformatik, 43 (3), S. 223–233.

HESS 2010: Hess, T.: Erkenntnisgegenstand der (gestaltungsorientierten) Wirtschaftsinformatik. In: Österle, H. (Hrsg.); Winter, R. (Hrsg.); Brenner, W. (Hrsg.): Gestaltungsorientierte Wirtschaftsinformatik: Ein Plädoyer für Rigor und Relevanz. Infowerk. ISBN 978-3-00-030310-4.

HEVNER ET AL. 2004: Hevner, A.R.; March, S.T.; Park, J.; Ram, S.: Design science in information system research. In: MIS Quarterly, 28 (1), S. 75–105.

HEVNER UND WINTER 2009: Hevner, A.R.; Winter, R.: Interview mit Alan R. Hevner zum Thema „Design Science“. In: Wirtschaftsinformatik, 51 (1), S. 148-151.

HEVNER UND CHATTERJEE 2010: Hevner, A. R. (Hrsg.); Chatterjee, S. (Hrsg.): Design Research in Information Systems. Berlin, Springer, 2010.

HOCK ET AL. 2006: Hock C.; Hee-Woong K.; Weai Chee, T.: Information System Citation Patterns from ICIS Articles. In: Journal of the American Society for Information Science and Technology, 57 (9), S. 1263-1274.

HULME 2008: Hulme, G. V.: Gesetzliche Vorgaben gehen oft zu Lasten der IT-Sicherheit Balanceakt Compliance – IT-Security oder ein zufriedener Prüfer? URI: http://www.searchsecurity.de/themenbereiche/sicherheits-management/compliance/articles/111884/. Abrufdatum: 21. Februar 2011.

IEEE 2011: Institute Of Electrical And Electronics Engineers (IEEE): IEEE Xplore. URI: http://ieeexplore.ieee.org/Xplore/dynhome.jsp. Abrufdatum: 26. Januar 2011.

ISACA 2011: Information Systems Audit and Control Association (ISACA). URI: https://www.isaca.org. Abrufdatum: 21. Februar 2011.

ISO 2005: International Organization for Standardization: ISO/IEC 27001:2005. URI: http://www.iso.org/iso/catalogue_detail?csnumber=42103. Abrufdatum: 21. Februar 2011.

ITGI 2007: IT Governance Institute (ITGI) (Hrsg.): CobiT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models. IT Governance Institute. Rolling Meadows.

ITGI 2010: IT Governance Institute (ITGI). URI: http://www.itgi.org/template_ITGI923a.html?Section=About_ITGI&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=57434. Abrufdatum: 15. Februar 2011.

JANS ET AL. 2010: Jans, M.; Lybaert, N.; Vanhoof, K.: Internal fraud risk reduction: Results of a data mining case study. In: International Journal of Accounting Information Systems, 2010 (11), S. 17–41.

JARKE 2009: Jarke, M.: Perspektiven der Wirtschaftsinformatik aus Sicht der Informatik. In: Wirtschaftsinformatik, 51 (1), S. 82-87.

JUNC 2010: Junc, L.: Corporate-Compliance-Berichterstattung in Deutschland - Eine theoretische und empirische Analyse. Gabler. Wiesbaden.

JUNG 2005: Jung, C. G.: Präventionskonzept zum Schutz vor Wirtschaftskriminalität. In: Schweizer Treuhänder, 1-2 (05). URI: http://www.hslu.ch/iwi_publikation_wirtschaftskriminalitaet_praeventionskonzept.pdf. Abrufdatum: 27. Februar 2011.

KANDIAS ET AL. 2010: Kandias, M; Mylonas, A.; Virvilis, N.; Theoharidou, M.; Gritzalis, D.: An Insider Threat Prediction Model. In: Trust, Privacy and Security in Digital Business, Lecture Notes in Computer Science, 6264/2010, S. 26-37.

KEHLENBECK 2011: Kehlenbeck, M.: Beiträge zu Business Intelligence und IT-Compliance. Dissertation. (noch unveröffentlicht).

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

KOZLOVA 2008: Kozlova, E.: WI – Vergleichende Literaturstudie - IT-Governance. In: Wirtschaftsinformatik, 50 (5), S. 418-424.

KUHN UND SUTTON 2010: Kuhn, J. R.; Sutton, S. G.: Continuous Auditing in ERP System Environments: The Current State and Future Directions. In: Journal of Information Systems, 24 (1), S. 91-112.

KURBEL 2008: Kurbel, K.: Internationalisierung der Wirtschaftsinformatik. Weiter auf der Erfolgsspur – oder in die Sackgasse?. In: Jung, R. (Hrsg); Myrach, T. (Hrsg): Quo vadis Wirtschaftsinformatik. Festschrift für Prof. Gerhard F. Knolmayer zum 60. Geburtstag. Gabler, Wiesbaden, S. 83–94.

LIU ET AL. 2008: Liu, D.; Wang, X.; Camp, J.: Game-theoretic modeling and analysis of insider threats. In: International Journal of Critical Infrastructure Protection, 2008 (1), S. 75-80.

LOOS ET AL. 2010: Loos, P.; König, W.; Österle, H.; De Marco, M.; Pastor, J. A.; Rowe, F.: Nationale Forschung und internationale Wettbewerbsfähigkeit – ein Widerspruch?. In: Wirtschaftsinformatik, 52 (4), S. 243-253.

LÖSLER 2003: Lösler, T.: Compliance im Wertpapierdienstleistungskonzern. De Gruyter Recht. Berlin.

MARCH UND SMITH 1995: March, S.T.; Smith, G.F.: Design and natural science research on information technology. In: Decision Support Systems, 15, S. 251-266.

MARCH UND STOREY 2008: March, S.T.; Storey, V.C.: Design science in the information systems discipline: an introduction to the special issue on design science research. In: MIS Quarterly, 32 (4), S. 725–730.

MARTENSTEIN 2011: Martenstein, I.: Grundlagen zum Phänomen Wirtschaftskriminalität. In: Hlavica, C. (Hrsg.); Klapproth, U. (Hrsg.); Hülsberg, F. M. (Hrsg.): Tax Fraud & Forensic Accounting - Umgang mit Wirtschaftskriminalität. Gabler, Wiesbaden.

MERTENS 2006: Mertens, P.: Moden und Nachhaltigkeit in der Wirtschaftsinformatik. In: HMD - Praxis der Wirtschaftsinformatik, 250, S. 109-118.

MEYER ET AL. 2003: Meyer, M.; Zarnekow, R.; Kolbe, L.M.: IT-Governance - Begriff, Status quo und Bedeutung. In: Wirtschaftsinformatik, 45 (4), S. 445–448.

MURPHY UND DACIN 2011: Murphy, P., R.; Dacin, M.T.: Psychological Pathways to Fraud: Understanding and Preventing Fraud in Organizations. In: Journal of Business Ethics. DOI 10.1007/s10551-011-0741-0.

MÜLLER UND TERZIDIS 2008: Müller, G.; Terzidis, O.: IT-Compliance und IT-Governance. . In: Wirtschaftsinformatik, 50 (5), S. 341–342.

NGAI ET AL. 2011: Ngai, E. W. T.; Hu, Y.; Wong, Y H.; Chen, Y.; Sun, X.: The application of data mining techniques in financial fraud detection: A classificationframework and an academic review of literature. In: Decision Support Systems, 50, S. 559-569.

NIEHAVES UND STAHL 2006: Niehaves, B.; Stahl, B. C.: Criticality, Epistemology, and Behaviour vs. Design - IS Research across different sets of paradigms. In Proceedings of the 14th European Conference on Information Systems (ECIS 2006).

NUNAMAKER ET AL. 1991: Nunamaker, J.F.; Chen, M.; Purdin, T.D.M.: Systems-development in information systems research. Journal of Management Information Systems, 7 (3), S. 89–106.

OECD 2004: Organisation for Economic Co-operation and Development (OECD): OECD Principles of Corporate Governance. URI: http://www.oecd.org/dataoecd/32/18/31557724.pdf. Abrufdatum: 13. Februar 2011.

OFFERMANN ET AL. 2010: Offermann, P.; Blom, S.; Bub, U.; Levina, O.: Vorschlag für Komponenten von Methodendesigntheorien - Steigerung der

Nutzbarkeit von Methodendesignartefakten. In: Wirtschaftsinformatik, 52 (5), S. 287-297.

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. Infowerk. ISBN 978-3-00-030310-4.

ÖSTERLE UND OTTO 2010: Österle, H.; Otto, B.: Konsortialforschung - Eine Methode für die Zusammenarbeit von Forschung und Praxis in der gestaltungsorientierten Wirtschaftsinformatikforschung. In: Wirtschaftsinformatik, 52 (5), S. 273-285.

PEFFERS ET AL. 2007: Peffers, K.; Tuunanen, T.; Rothenberger, M.A.; Chatterjee, S.: A design science research methodology for information systems research. In: Journal of Management Information Systems, 24 (3), S. 45–77.

PIIRAINEN ET AL. 2010: Piirainen, K.; Gonzalez, R. A.; Kolfschoten, G.: Quo Vadis, Design Science? – A Survey of Literature. In: Global Perspectives on Design Science Research. Lecture Notes in Computer Science, 6105/2010, S. 93-108.

PONS 1991: Pons Kompaktwörterbuch Englisch-Deutsch. 2. Auflg. , Klett Verlag, 1991.

RAMOS 2003: Ramos, M.: Auditor's responsibility for fraud detection. In: Journal of Accountancy, 195 (1), 28.

RATH UND SPONHOLZ 2009: Rath, M.; Sponholz, R.: IT-Compliance : Erfolgreiches Management regulatorischer Anforderungen. Berlin. Schmidt. 2009.

RAY UND BRADFORD 2007: Ray, D.; Bradford, P.: An Integrated System for Insider Threat Detection. In: Craiger, P.; Shenoi, S. (Eds.): Advances in Digital Forensics III. IFIP International Federation for Information Processing, 2007, 242/2007, S. 75-86.

RIEGE ET AL. 2009: Riege, C.; Saat, J.; Bucher, T.: Systematisierung von Evaluationsmethoden in der gestaltungsorientierten Wirtschaftsinformatik. In: Becker, J.; Krcmar, H.; Niehaves, B.: Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik, Springer, S. 69-86.

ROSEN 2001: Rosen, R. v.: Corporate Governance: Eine Bilanz. In: Die Bank, 2001 (4), S. 283–287.

ROSSI UND SEIN 2003: Rossi, M.; Sein, M.K.: Design research workshop: a proactive research approach. In: Design research workshop within the IRIS26.

ROTH 2009: Roth, M.: Compliance – Konzept und Umsetzung. In: Zeitschrift Risk, Fraud & Compliance, 2009 (1). S. 5–10.

SALEM ET AL. 2008: Salem, M. B.; Hershkop, S.; Stolfo, S.: A Survey of Insider Attack Detection Research. In: Stolfo, S. J.; Bellovin, S. M.; Hershkop, S.; Keromytis, A. D.; Sinclair, S.; Smith, S. W. (Eds.): Insider Attack and Cyber Security. Advances in Information Security, 2008 (39), S. 69-90.

SECURE BUSINESS AUSTRIA 2011a: Secure Business Austria: International Conference on Availability, Reliability and Security (ARES) Conference, URI: http://www.ares-conference.eu/conf/index.php/index.php?option=com_content&view=article&id=26&Itemid=47. Abrufdatum: 19. Januar 2011.

SECURE BUSINESS AUSTRIA 2011b: Secure Business Austria: International Conference on Availability, Reliability and Security (ARES) Conference. URI: http://www.ares-conference.eu/conf/index.php/index.php?option=com_content&view=article&id=10&Itemid=6. Abrufdatum: 19. Januar 2011.

SINGH UND LIJA 2010: Singh, A.; Lija, D.J.: Criteria and Methodology for GRC Platform Selection. In: ISACA Journal, 2010 (1). URI: http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Pages/Criteria-and-Methodology-for-GRC-Platform-Selection1.aspx. Abrufdatum: 21. Februar 2011.

SINGLETON 2010: Singleton, T. W.: Data Extraction, A Hindrance to Using CAATs. In: ISACA Journal, 2010 (6). URI: http://www.isaca.org/Journal/Past-Issues/2010/Volume-6/Pages/Data-Extraction-A-Hindrance-to-Using-CAATs.aspx. Abrufdatum: 21. Februar 2011.

SINGLETON UND SINGLETON 2010: Singleton, T. A.; Singleton, A. J.: Fraud Auditing and Forensic Accounting. 4. Auflage, New Jersey, J. Wiley & Sons.

SINZ 2010: Sinz, E. J.: Konstruktionsforschung in der Wirtschaftsinformatik: Was sind die Erkenntnisziele der gestaltungsorientierter Wirtschaftsinformatik-Forschung?. In: Österle, H. (Hrsg.); Winter, R. (Hrsg.); Brenner, W. (Hrsg.): Gestaltungsorientierte Wirtschaftsinformatik: Ein Plädoyer für Rigor und Relevanz. Infowerk. ISBN 978-3-00-030310-4.

SPRINGER 2011: Springer Science+Business Media (SPRINGER): SpringerLink. URI: http://www.springerlink.de. Abrufdatum: 26. Januar 2011.

SRIVASTAVA ET AL. 2003: Srivastava, R. P.; Mock, T. J.; Turner, J. L.: The Effects of Integrity, Opportunity, Incentives, Mitigating Factors and Forensic Audit Procedures on Fraud Risk.

STAHL 2009: Stahl, C. B.: The Ideology of Design: A Critical Appreciation of the Design Science Discourse in Information Systems and Wirtschaftsinformatik. In: Becker, J.; Krcmar, H.; Niehaves, B.: Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik, Springer, S. 111-131.

STANDKE 2010: Standke, F.: Unternehmensweiter Ansatz einer Governance-, Risk- und Compliance-Lösung. In: Keuper, F. (Hrsg); Neumann, F. (Hrsg): Corporate Governance, Risk Management und Compliance. Wiesbaden, Gabler.

STEININGER ET AL. 2009: Steininger, K.; Riedl, R.; Roithmayr, F.; Mertens, P.: Moden und Trends in Wirtschaftsinformatik und Information Systems – Eine vergleichende Literaturanalyse. In: Wirtschaftsinformatik, 51 (6), S. 478-495.

STRECKER 2009: Strecker, S.: Ein Kommentar zur Diskussion um Begriff und Verständnis der IT-Governance - Anregungen zu einer kritischen Reflexion. ICB-Research Report Nr. 36. Universität Duisburg-Essen. ISSN 1860-2770.

STROHMEIER 2008: Strohmeier, S.: Informationssysteme im Personalmanagement. Vieweg+Teubner Verlag. Wiesbaden.

SYMONENKO ET AL. 2004: Symonenko, S.; Liddy, E. D.; Yilmazel, O.; Del Zoppo, R.; Brown, E.; Downey, M.: Semantic Analysis for Monitoring Insider

Threats. Intelligence and Security Informatics. Lecture Notes in Computer Science. 2004, 3073/2004, S. 492-500.

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

TAKEDA ET AL. 1990: Takeda, H.; Veerkamp, P.; Tomiyama, T.; Yoshikawa, H.: Modeling Design Processes. In: AI Magazine, 11 (4), S. 37-48.

TAYLOR 2006: Taylor, R.: Management Perception of Unintentional Information Security Risks. In: Proceedings of the International Conference on Information Systems (ICIS 2006).

THEOHARIDOU ET AL. 2005: Theoharidou, M.; Kokolakis, S.; Karyda, M.; Kiountouzis, E.: The insider threat to information systems and the effectiveness of ISO17799. In: Computers & Security, 2005 (24), S. 472-484.

THOMANN 2011: Thomann, D: Risikofaktoren und Indikatoren für dolose Handlungen. In: Hlavica, C. (Hrsg.); Klapproth, U. (Hrsg.); Hülsberg, F. M. (Hrsg.): Tax Fraud & Forensic Accounting - Umgang mit Wirtschaftskriminalität. Gabler, Wiesbaden.

THOMANN UND HLAVICA 2011: Thomann, D.; Hlavica, C.: Grundlagen zum Phänomen Wirtschaftskriminalität. In: Hlavica, C. (Hrsg.); Klapproth, U. (Hrsg.); Hülsberg, F. M. (Hrsg.): Tax Fraud & Forensic Accounting - Umgang mit Wirtschaftskriminalität. Gabler, Wiesbaden.

TEUBNER UND FELLER 2008: Teubner, A.; Feller, T.: Informationstechnologie, Governance und Compliance. In: Wirtschaftsinformatik, 50 (5), S. 400-407.

UNIVERSITÄT HAWAII 2011: University of Hawai'i at Manoa: Hawaii International Conference on System Sciences (HICSS). URI: http://www.hicss.hawaii.edu. Abrufdatum: 19. Januar 2011.

UNIVERSITÄT PRETORIA 2011: University of Pretoria: 18th European Conference on Information Systems (ECIS 2010). URI: http://web.up.ac.za /default.asp?ipkCategoryID=8136. Abrufdatum: 26. Januar 2011.

UNIVERSITÄT ST. GALLEN 2011: Universität St. Gallen: 5th International Conference on Design Science Research in Information Systems and Technology (DESRIST 2010). URI: http://desrist2010.iwi.unisg.ch. Abrufdatum: 26. Januar 2011.

VOM BROCKE ET AL. 2009: Vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Plattfaut, R.; Cleven, A.: reconstructing the giant: on the importance of rigour in documenting the literature search process. In: Proceedings of the 17th European Conference on Information Systems (ECIS 2009).

VON MAUR 2009: von Maur, E.: Konstruktivismus und Wirtschaftsinformatik – Begriffsver(w)irrungen. In: Becker, J.; Krcmar, H.; Niehaves, B.: Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik, Springer, S. 133-159.

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

WALLS ET AL. 1992: Walls, J.G.; Widmeyer, G.R.; El Sawy, O.A.: Building an information system design theory for vigilant EIS. In: Information Systems Research, 3 (1), S. 36–59.

WEILL UND ROSS 2004: Weill, P.; Ross, J.W.: IT governance: how top performers manage IT decision rights for superior results. Harvard Business School Press. Boston, Massachusetts.

WELLS 2007: Wells, J. T.: Corporate Fraud Handbook: Prevention and Detection. 2. Auflage, John Wiley & Sons, New Jersey.

WILDE UND HESS 2007: Wilde, T.; Hess, T.: Forschungsmethoden der Wirtschaftsinformatik – Eine empirische Untersuchung. In: Wirtschaftsinformatik, 49 (4), S. 280–287.

WINTER 2008: Winter, R.: Design science research in Europe. European Journal of Information Systems, 17, S. 470–475, DOI 10.1057/ejis.2008.44.

WINTER ET AL. 2009: Winter, R.; Krcmar, H.; Sinz, E. J.; Zelewski, S.; Hevner, A. R.: Was ist eigentlich Grundlagenforschung in der Wirtschaftsinformatik?. In: Wirtschaftsinformatik, 51 (2), S. 223-231.

WIRTSCHAFTSINFORMATIK 2011: Wissenschaftstheorie und Forschungsmethodik. URI: http://www.wirtschaftsinformatik.de/index.php;do=co_fo/site=wi/sid=17545978254d32f3e9a9. Abrufdatum: 16. Januar 2011.

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

WOLF 2006: Wolf, K. W.: Corporate Compliance - ein neues Schlagwort? Ansatzpunkte zur Umsetzung der Compliance in der Finanzberichterstattung. In: Deutsches Steuerrecht, 2006 (44), S. 1995-2000.

ZELEWSKI 2007: Zelewski, S.: Kann Wissenschaftstheorie behilflich für die Publikationspraxis sein? Eine kritische Auseinandersetzung mit den „Guidelines“ von Hevner et al. In: Lehner, F. (Hrsg.); Zelewski, S. (Hrsg.): Wissenschaftstheoretische Fundierung und wissenschaftliche Orientierung der Wirtschaftsinformatik, Berlin, GITO, S. 71-120.

Anhang

Seite

a) HICCS 2010

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], it is important that control exceptions are timely communicated to the right decision-makers. This timeliness provides the decision-makers with the necessary lati-

DOI: 10.1109/HICSS.2010.262

tude 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. 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

DOI: 10.1109/HICSS.2010.262

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.

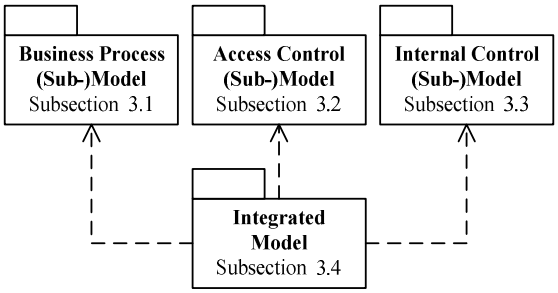

Figure 1: Overview of the proposed model and its sub-models as a UML package diagram

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

DOI: 10.1109/HICSS.2010.262

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.

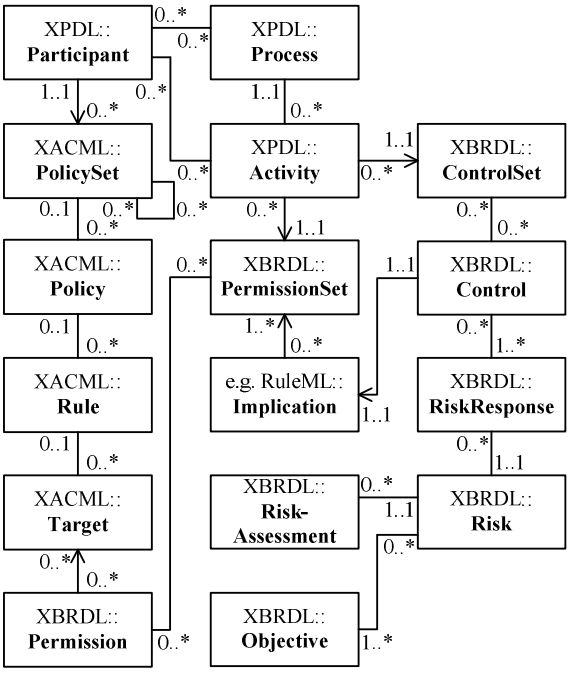

Figure 2: Overview of the proposed model as a UML class diagram. The defined internal control model (XBRDL) and the relevant parts of the adopted business process model (XPDL), access control model (XACML) and rule model (e.g. RuleML) are integrated with each other.

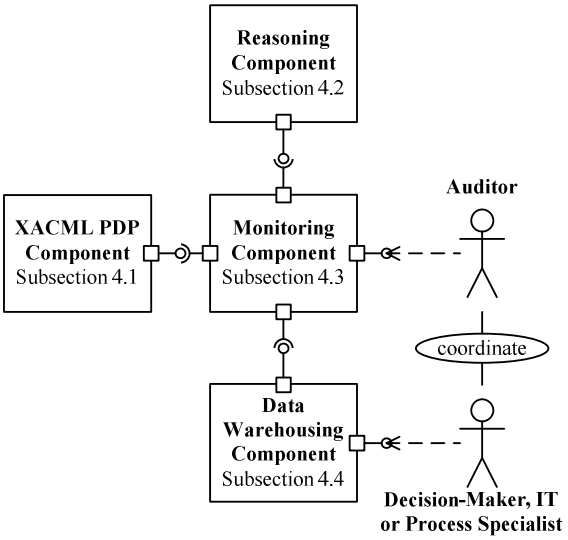

Figure 3: Overview of the proposed Service Oriented Architecture as a combined UML component and use case diagram

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.

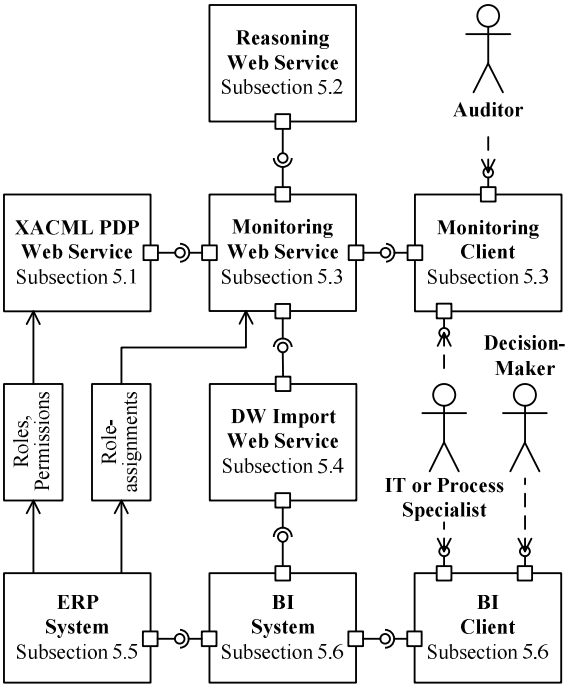

Figure 4: Overview of the implemented prototype as a combined UML component and use case diagram

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 (SUN-XACML) [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

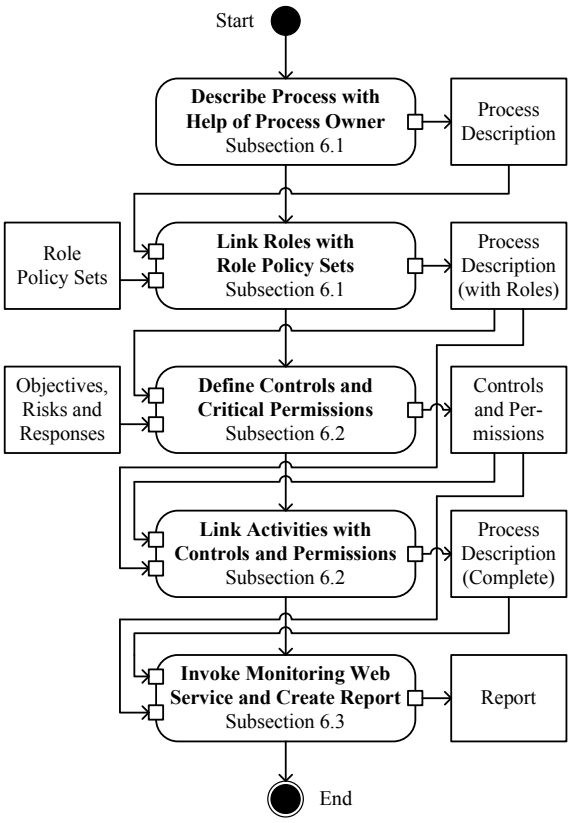

Figure 5: Overview of the conducted case study as a UML activity diagram.

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.

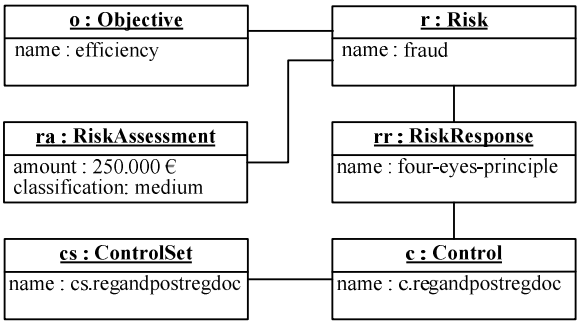

Figure 6: Example XBRDL control as a UML object diagram

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

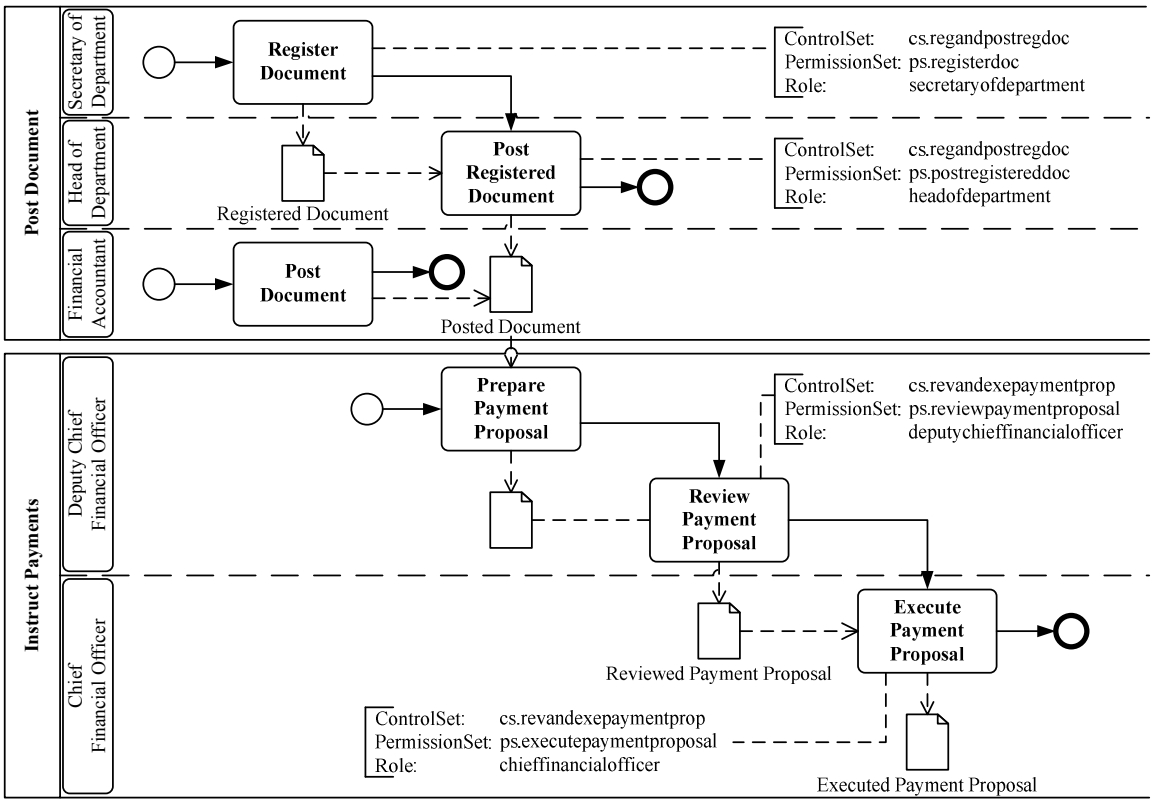

Figure 7: Example process in Business Process Modeling Notation

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 commu-

DOI: 10.1109/HICSS.2010.262

nication and deep analysis of thereby detected control exceptions using business intelligence (BI) is proposed.

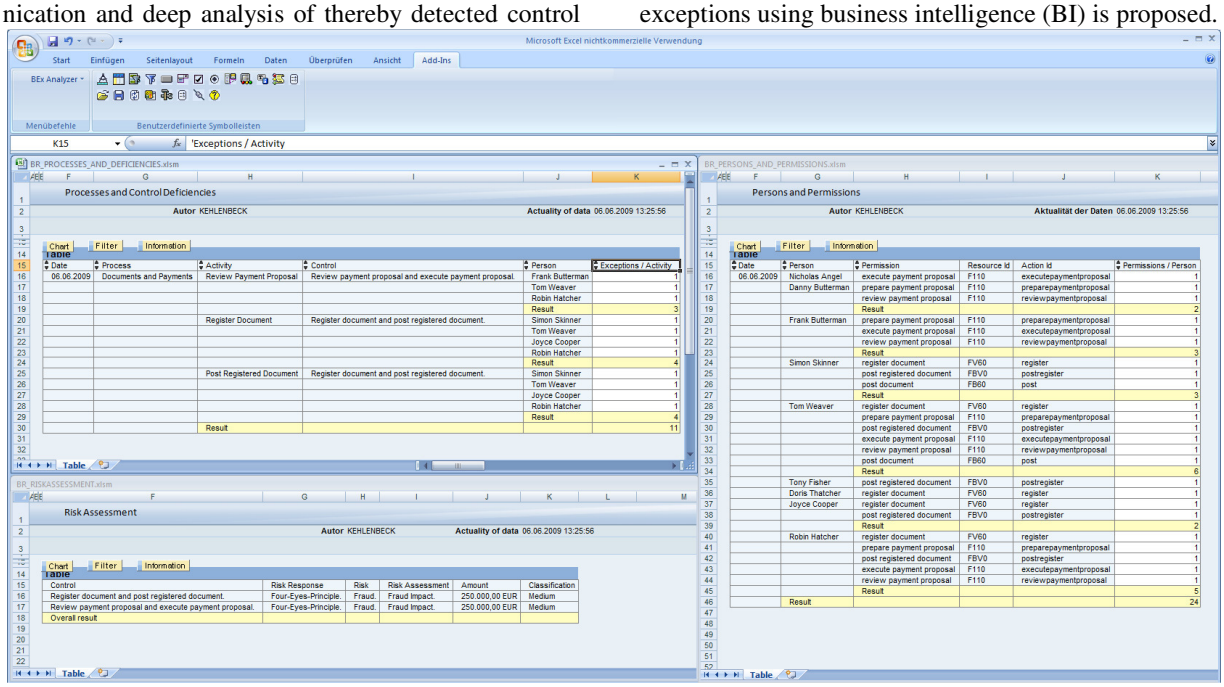

Figure 8: Example queries regarding business processes, internal control, control exceptions and permissions created using the implemented prototype and the SAP Business Explorer Analyzer.

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 Con-

DOI: 10.1109/HICSS.2010.262

trols Using Database Technology", Proceedings of the 22nd 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. zur Muehlen, M. Rosemann, "Integrating Risks in Business Process", *ACIS 2005 Proceedings,* 2005.
[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. 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.
[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

b) ARES 2010

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 that is 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 has been 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

Legal requirements considerably increased during the last years and entailed high investment costs [1]. Compliance management can be defined as the use of frameworks, standards and software to ensure compliance with these legal requirements [2]. This compliance may be achieved by embedding control activities into business processes. The maintenance and monitoring of these control activities 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. Table I characterizes typical participants by means of their responsibilities and information needs. This information needs considerably differ in their focus and granularity. For example, decision-makers prefer highly aggregated information regarding effects, while IT specialists require detailed information regarding causes.

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

DOI: 10.1109/ARES.2010.88

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:

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. The relevance of the presented prototype arises from its ability to meet business requirements and information needs for a given scenario.

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 research arises from the effective use of scientific knowledge for the design and evaluation process.

III. DESIGN AND EVALUATION PROCESS

The design of the prototype has 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.

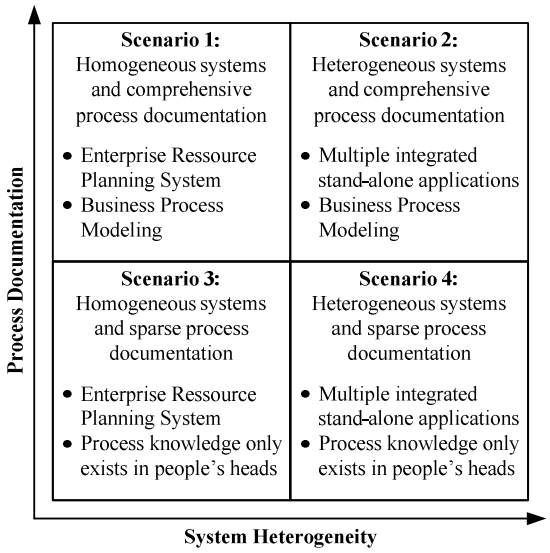

Figure 1. Process Documentation, System Hereogeneity and Scenarios

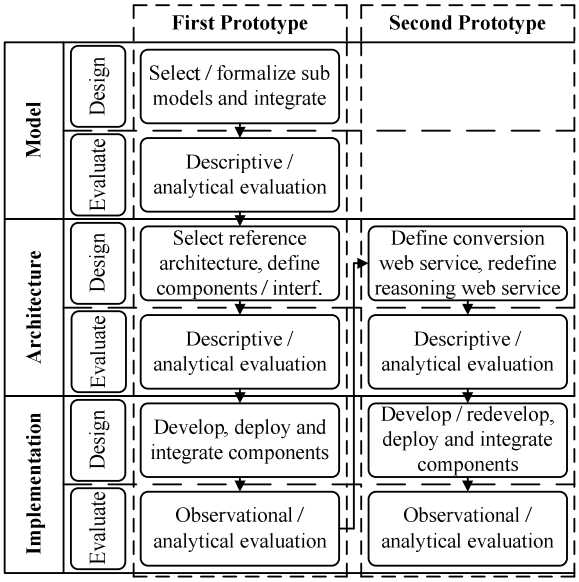

Figure 2. Design and Evaluation Process for the Prototypes

A. *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) [13] has been developed to ease this understanding for participants. The XML Process Definition Language (XPDL) [14] 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) [15] is used to store access control data.

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 [16] respectively the Enterprise Risk Management – Integrated Framework [17] (COSO). The core concepts of the COSO model have been formalized and supplemented with definitions of control exceptions. Control exceptions may be defined using any Extensible Markup Language (XML) [18] based rule language, e.g. RuleML [19] or SWRL [20].

Business process, access control and internal control models have been integrated. An overview of the integrated model is presented in Fig. 3. This model has been evaluated as semantically rich but yet not too complex. 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.

DOI: 10.1109/ARES.2010.88

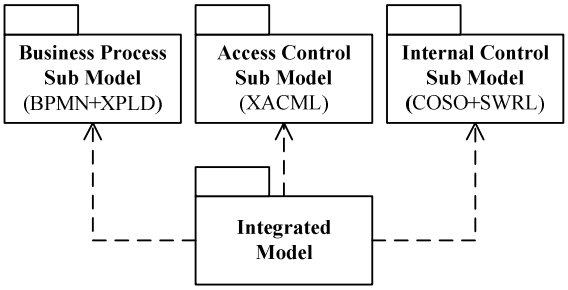

Figure 3. Business Process, Access Control and Internal Control Model

B. *Architecture*

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

- The XACML 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.
- 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 an optionally other systems and provides analysis and reporting services to the participants.

The architecture has been assessed as suitable for many system landscapes. It reduces dependencies between components and enables their independent development. Moreover, the use of a BI system as a presentation layer allows the coherent 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.

C. *Implementation*

The XACML PDP WS is currently based on the XACML PDP implementation of Sun (SUNXACML) [21], the reasoning WS on the Jena framework [22] and the Pellet reasoner [23]. The other web services have been implemented from scratch. Large parts of the Java source code have been generated using the Eclipse Modeling Framework (EMF) [24] and the Apache CXF (CXF) [25] services framework.

The first prototype did not contain a conversion WS and used a RuleML based reasoning WS. In a case study (scenario 1), the manual transformation of access control data from the proprietary SAP model to XACML turned out as impractical, even for single areas. 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) [26] 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 analyse and report detected control exceptions. The generated XACML policies and the detected control exceptions have been 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 critical factors for the success of compliance management as well as business requirements and information needs with respect to compliance monitoring and reporting.

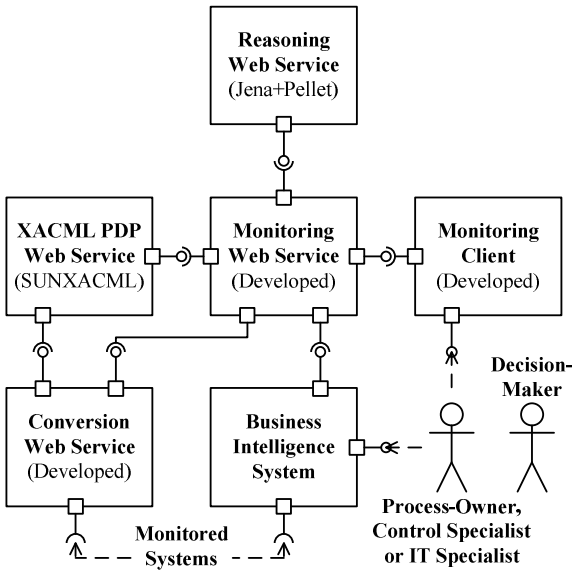

Figure 4. Individual Components and Interfaces of the Architecture

DOI: 10.1109/ARES.2010.88

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 [27]. Moreover, dynamic business environments require continuously changing processes and systems although these have to comply with legal requirements. Chatterjee et al. [28] 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 supports such a central approach.

Compliance solutions can generally be divided by their employment phase: “before-the-fact” or “after-the-fact“ [29]. 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 implemented prototype represents a synthesis between (ii) and (iv). It enables the automated detection of control exceptions both “before-the-fact” and “after-the-fact”. 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. Moreover, the responsibilities with respect to the definition and monitoring of controls can be rearranged. Such rearrangements may have a significant impact on recurrent compliance costs. After the prototype has been initially configured, checked and accepted by auditors, lower expenses for the following years can be expected, as unchanged processes and their embedded controls may be monitored at any time without external assistance. Additionally, internal participants may easily define their own controls. Internal control is not limited to compliance objectives and their process knowledge is a valuable asset for the achievement of other business objectives. This possibility may contribute to the decentralization, quality and timeliness of decisions and strengthen the effectiveness of operational management.

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 background of the organizations systems. The prototype can be used for 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 [30]. However, the legal requirements or the risk environment may suggest a reasonable trade off.

B. *Business Requirements and Information Needs*

The adaptability of a compliance management solution to a specific organization significantly influences its usefulness for the participants. The following paragraphs discuss different scenarios, as described in Fig. 1.

In scenario 1, comprehensive process documentation facilitates the definition of internal control on a functional level. The impact of changes to both access control and business processes on internal control can be examined proactively before-the-fact and reactively after-the-fact. The homogeneous system landscape renders the integration of application systems easy.

Scenario 2 refers to comprehensive process documentation, as well. However, the heterogeneous system landscape requires the definition of access control in different proprietary models. Access control model differences are overcome for subsequent processing by the transformation of access control data to XACML. The numerous XACML functions render the development of corresponding transformations comparatively easy.

In scenario 3, the lack of process documentation prevents the definition of internal control on a functional level and enforces its concentration on a technical level. Although the impact of changes to access control on internal control can still be examined before-the-fact and after-the-fact, business process are left unconsidered. Information needs can only be met, if at least some process documentation is prepared. However, the homogeneous system landscape renders the integration of application systems easy.

Scenario 4 refers to incomprehensive process documentation, as well. As in scenario 3, information needs can only be met, if at least some process documentation is prepared. However, XACML serves as an abstract layer for the homogeneous processing of access control data from heterogeneous systems.

DOI: 10.1109/ARES.2010.88

As the developed prototype accounts for business process documentation, the negative impact of missing documentation on the fulfillment of information needs is not characteristic to it.

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, harmful 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 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. Additionally, harmful 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. [29] 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. For 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. However, academia either focuses on exploratory problem-identifying or neglects actual information needs. Consequently, business demand and academic supply diverge.

In order to counter this divergence, the present paper has presented an innovative prototypical implementation of an automated compliance monitoring and reporting system. This system is oriented to business requirements and information needs, and based on established standards and existing technologies. The development of the prototype has been aligned with common design-science research guidelines and consequently followed a corresponding design and evaluation cycle.

Critical success factors for the application of the developed prototype to specific organizations as well as corresponding economic implications 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.

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 benefits. 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.

DOI: 10.1109/ARES.2010.88

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] 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[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.

DOI: 10.1109/ARES.2010.88

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

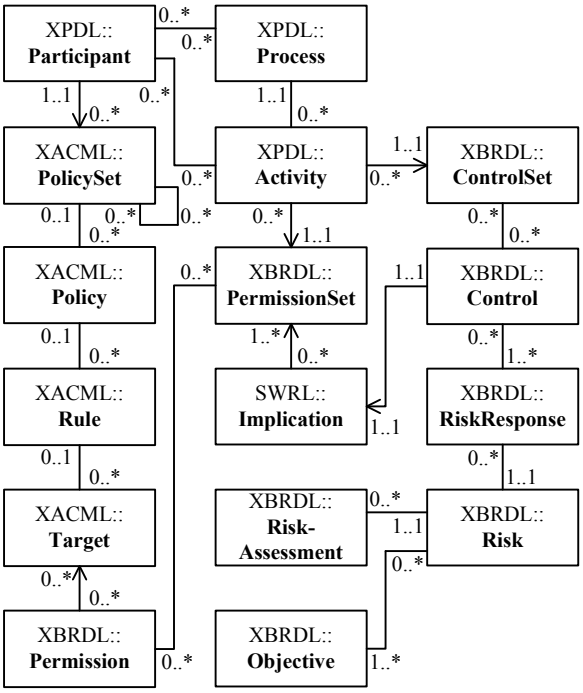

Figure 1. Used model as a UML diagram.

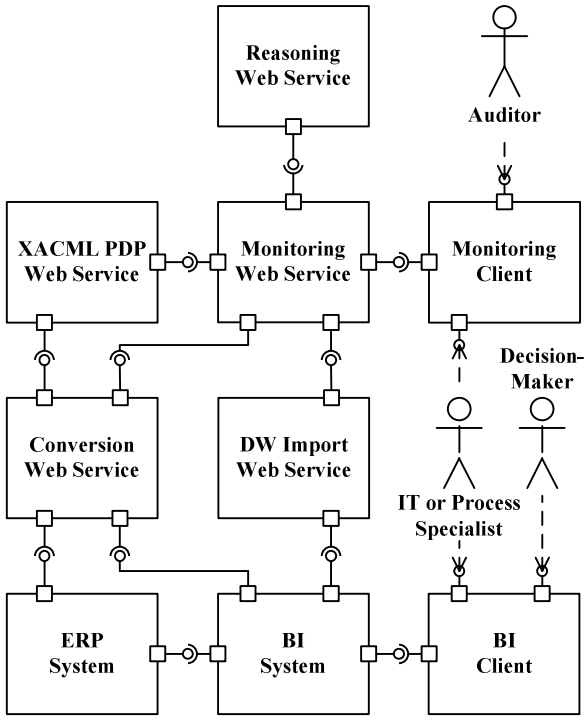

Figure 2. Used architecture as a UML diagram.

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.

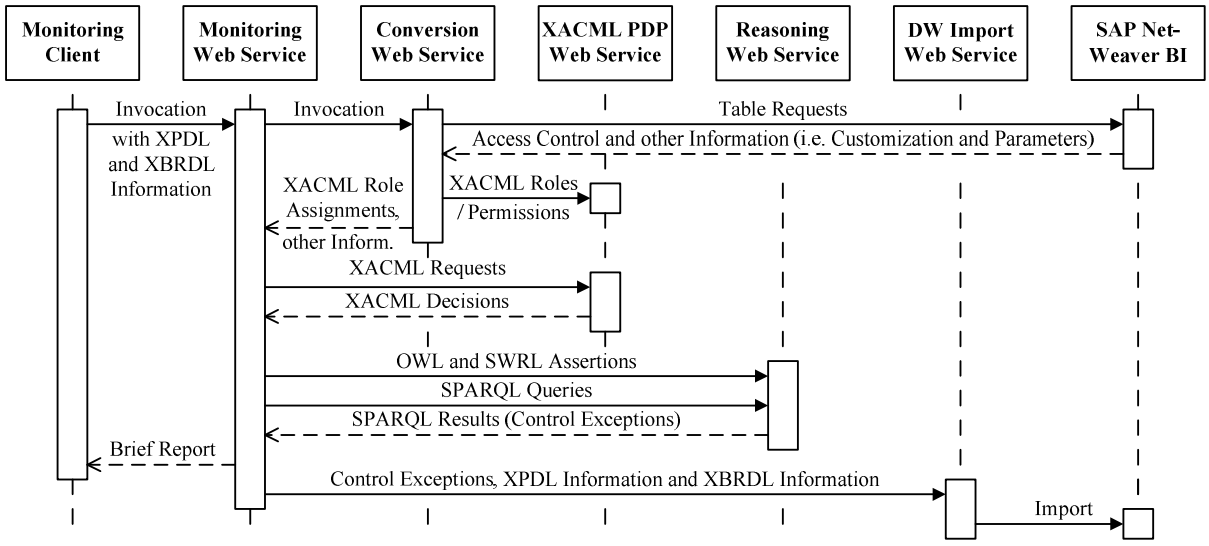

Figure 3. Interaction of the individual prototype components as a UML diagram. SAP BI and SAP ERP share the same access control model. The illustration therefore omits SAP ERP.

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.

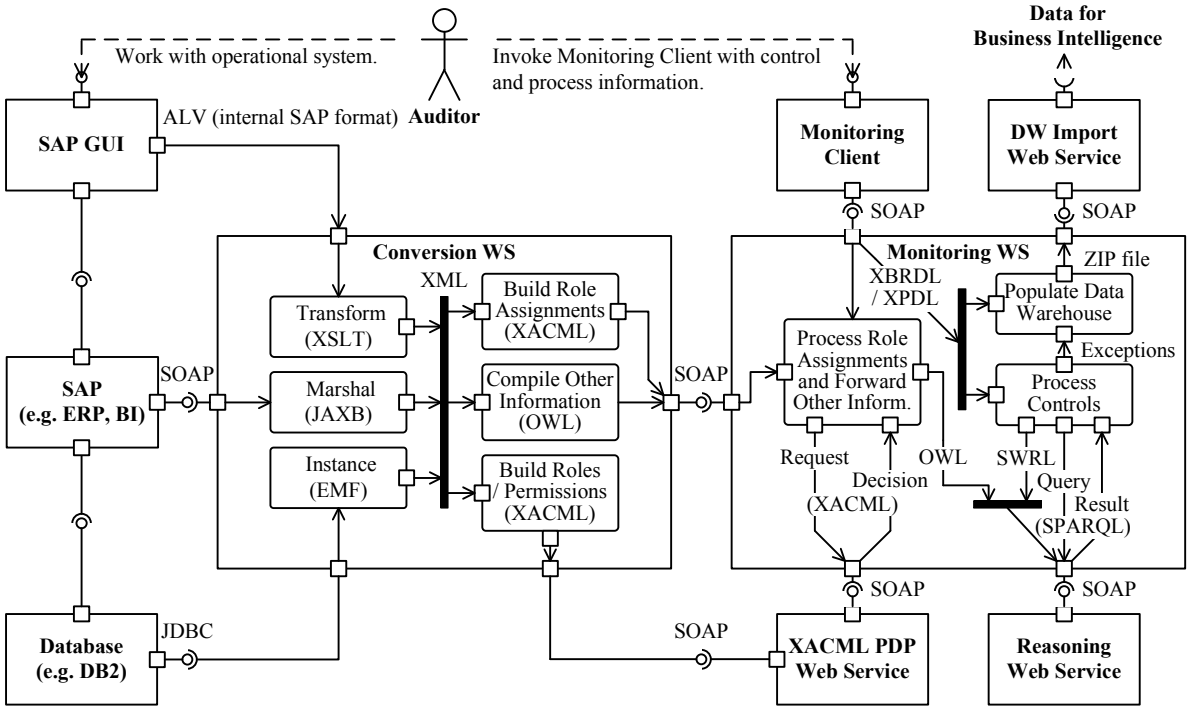

Figure 4. Conversion and monitoring web service as a UML diagram.

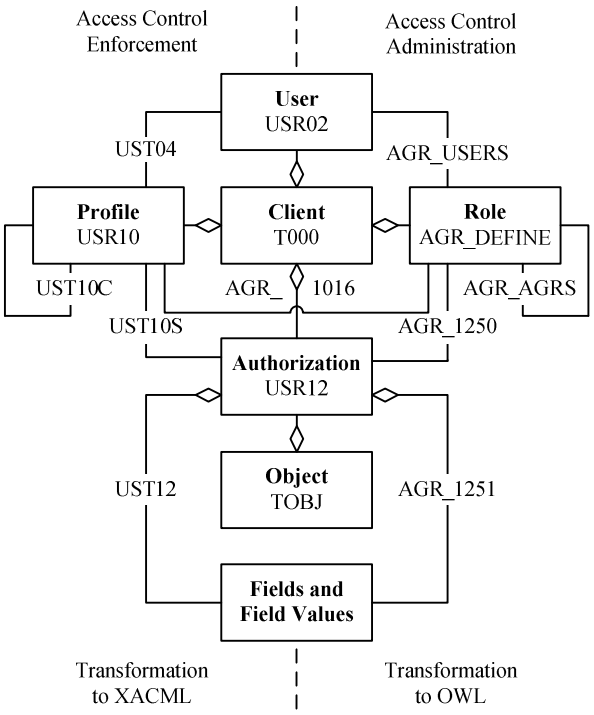

Figure 5. SAP access control model as a UML diagram.

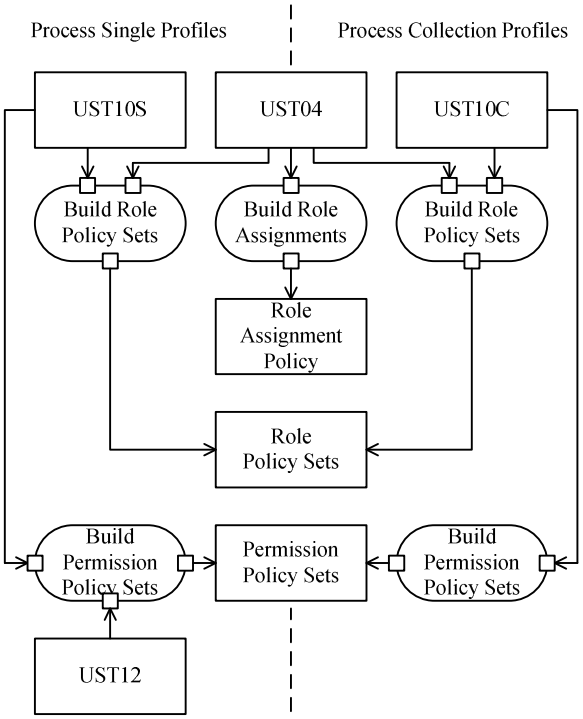

Figure. 6. Transformation from SAP to XACML as a UML diagram.

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.

d) VISM 2010

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 responsible 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.

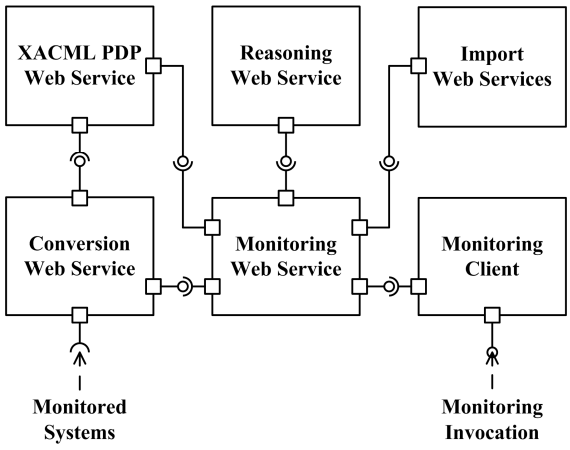

Figure 1. Core components and interfaces of the architecture

DOI: 10.1109/DEXA.2010.77

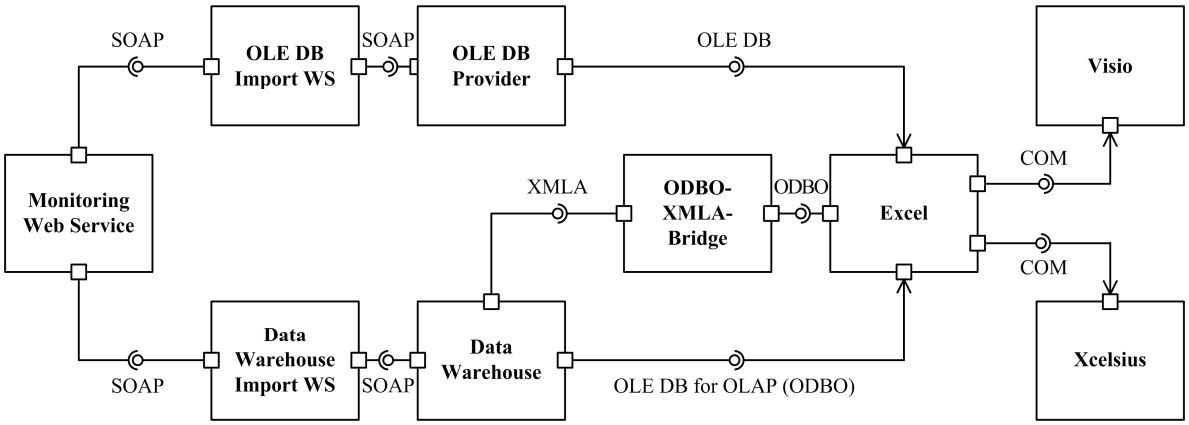

Figure 2. Components for the provision of compliance monitoring data to visualization tools

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 a 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

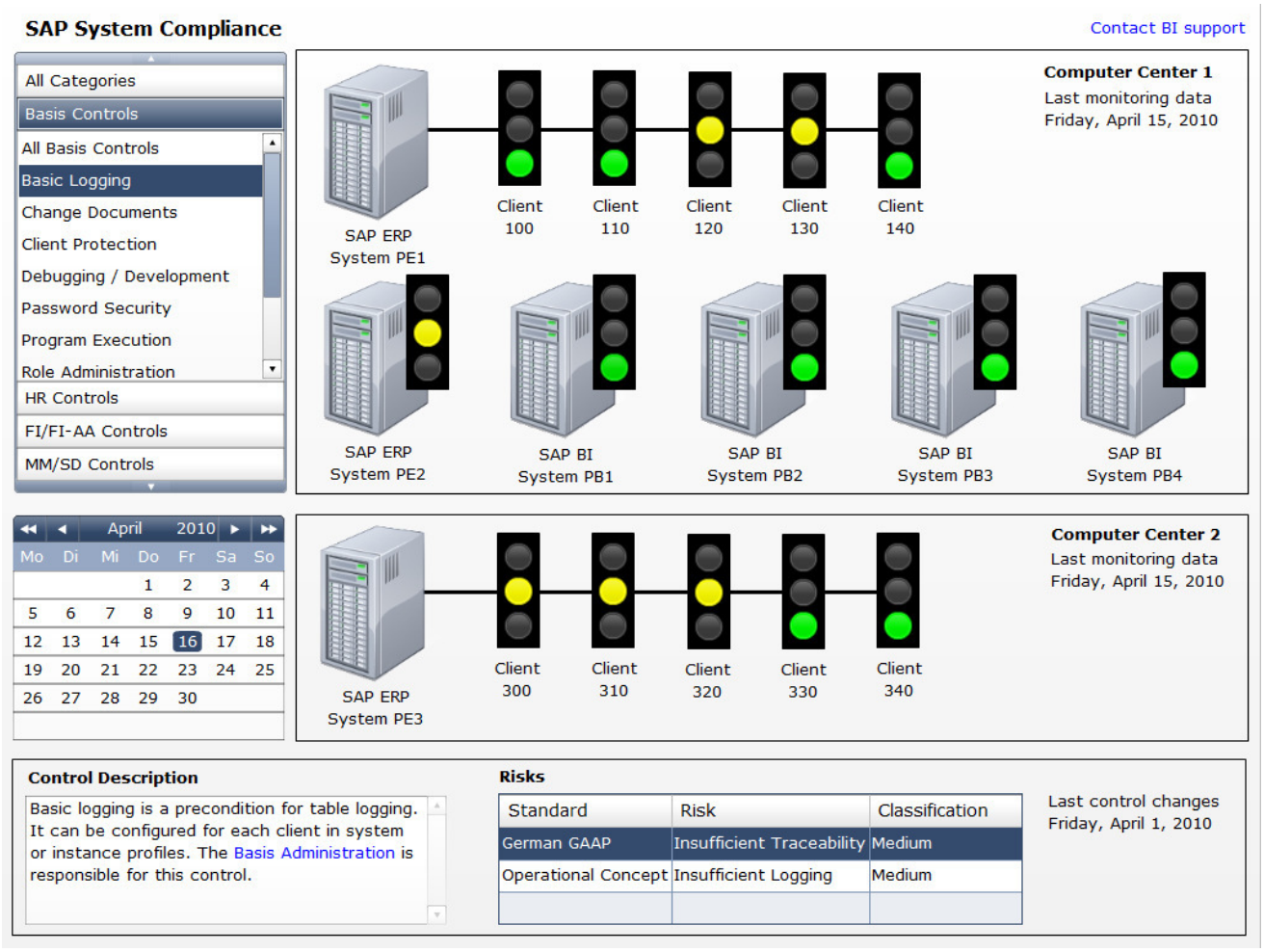

Figure 3. Screenshot of the designed dashboard. It is devoted to the monitoring of compliance for several SAP systems in two different data centers.

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

AUTOMATIC CONTINUOUS AUDITING: PROCESSES, SOFTWARE, AND HUMAN BEHAVIOR

Abstract

Every year, fraud causes billions in damage worldwide. In this paper, we introduce a generic architectural model that makes sufficient allowance for the fraud triangle factors. In this way, in addition to the classic quantitative analysis of business transactions that are already being applied as part of the fraud audit, the human factor is extensively integrated into the audit as a qualitative component. This provides added value because the transactions examined by the auditor can be better differentiated and prioritized. By taking critical and non-critical human behavior into account, it is possible to uncover transactions that are part of a pattern that is not yet known and that would have been left undiscovered using normal means. An example of an architecture is implemented using a prototype and is applied to a SAP ERP system.

Keywords: fraud audit, continuous auditing, ERP system, human behavior, software prototype.

1 Introduction

A current study from the Association of Certified Fraud Examiners (ACFE) demonstrates that fraud is a big problem in organizations (ACFE 2010). The ACFE estimates that fraud causes a mean loss of 5% of the annual turnover of a company. The average fraud case runs at $160,000 in damages. A global study by PricewaterhouseCoopers (PwC 2009) showed that such cases are quite widespread. They found that 30% of the companies they surveyed had already dealt with fraud. Eighty percent of fraud is committed within the company's own ranks, especially in accounting, operations, sales, executive/upper management, customer service or purchasing (ACFE 2010). The processes of the departments listed above are core elements of an accounting information system (AIS), which is of special importance for a fraud audit. Due to the high number of fraud cases, in this paper we are especially focusing on internal fraud audits.

Various methods and techniques for fighting fraud have been developed. In the past few decades, the focus was on developing technical instruments to examine information systems (Alles et al. 2004). Only in the past few years were processes taken into account (Phua et al. 2005). Audit techniques have developed over time into continuous audit and real-time audit approaches. Despite these technical improvements, it takes an average of up to eighteen months to uncover a case of fraud (ACFE 2010). From this we can conclude that the information provided by the current techniques is not necessarily sufficient to uncover a fraud case in a timely manner. As noted by Jans et al. (2010): “Most important of all for auditing, there are anomalies or frauds that cannot be captured by analyzing input data alone”. When referring to the triangle of people, process, and technology, the human factor appears to have been neglected. When taking the development of fraud into account, including human behavior in the context of business processes has high potential. When we look at behavior, we can draw conclusions based on the three factors of the fraud triangle: incentives, opportunities und rationalizations (Wells 2008).

In this paper, we are introducing a generic architectural model that attempts to adequately take the fraud triangle factors into account. In this way, in addition to the classic quantitative analysis of business transactions that are already being applied as part of the fraud audit, the human factor is extensively integrated into the audit as a qualitative component. This is clear when we look at the Enron financial scandal, which led to legal changes and tightening of legal regulations, such as the Sarbanes-Oxley Act (SOX). In the Enron employee e-mails published by the Federal Energy Regulatory Commission, there is evidence of inappropriate employee behavior (Gray and Debreceny 2007, Davis et al. 2007). Holton (2009) introduced a process that uses automatic e-mail text mining to detect similar circumstances.

Taking the human factor into account provides added value because the transactions examined by the auditor can be better differentiated and prioritized. By distinguishing between types of behavior (critical and non-critical), it is possible to uncover transactions that are part of a pattern that is not yet known and that would have been left undiscovered if using normal means. Because fraud takes place using both known and unknown patterns, it is necessary to analyze the entire database during an investigation. Especially during a continuous audit, the focus of these types of audit can be determined and the circumstances that appear to be the most relevant can be prioritized.

In information systems (IS), there are two basic research approaches: behavioral science and design science (Hevner et al. 2004, Hevner and Chatterjee 2010). In this paper, we are using design science methods. We are following the design science research process (DSRP) model from Peffers et al. (2006 & 2007). An artifact in the form of a generic architectural model was developed in a solution-oriented way. This artifact was implemented as a prototype within a test environment of a SAP enterprise resource planning system (SAP ERP). Iterations back to design were performed using the review feedback of two certified information systems auditors (CISA).

The remainder of the paper is structured as follows. Section 2 gives an overview of related work. In section 3 and section 4 short basics of fraud, the well known fraud triangle and continuous auditing are given. Section 5 gives a risk oriented determination of the data population. Our generic architectural model, presented in section 6, is processed by an implementation of a prototype in section 7. We proceed with a discussion in section 8 and conclude with future work in section 9.

2 Related Work

There are papers in the literature that deal with the topic of recognizing the circumstances surrounding fraud or identifying people who could be involved in fraud. One of the most extensive overviews of automated fraud detection was done by Phua et al. (2005). They compare and summarize publications over a period of ten years. A briefer but more current overview was provided by Jans et al. (2009) as part of their work. The identification and classification of potential fraud by suspicious people is a core element of the insider threat prediction model from Kandias et al. (2010). Like the approach described here, they use data from the IT infrastructure (e.g. intrusion detection system) to get an overview of users. The focus is on classifying a person, but there is no further linking of results.

Jans et al. (2010) focus on reducing internal fraud risk by a descriptive data mining strategy of procurement data. The evaluation of results is made through assessment of the data mining issues by domain experts. An automated risk rating is not implemented. They explicitly exclude the factors rationalization and incentive of the fraud triangle. The human factor is therefore not integrated directly. It is restricted to the analysis of business transactions.

In the topic of continuous auditing, there was a research focus on examining restrictions, improvements, and feasibility studies of the prevailing technical methods (Kuhn and Sutton 2009). Kogan et al. (2010) analyzed continuous audit used for real-time error correction. They use analytical processes to identify possible business process issues. The human factor and possible fraud-related behavior are not considered.

To our best knowledge there is no paper that takes into account telltale human behavior that raises suspicion of fraud as part of continuous auditing. In this paper, we suggest to unify the classic audit approach with human behavior taking into account the fraud triangle in order to achieve better fraud detection and prevention.

3 The Nature of Fraud

There is no general scientific definition of fraud. In principle, an auditor understands fraud to include all intentional actions of employees or third parties with the objective of attaining unfair advantage over the organization by illegal means. This can be done, for example, through deception and misappropriation of assets and breaking the law. The ACFE (2010) defines fraud as: “The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.”

With the ACFE definition in mind, the objective of our work is “(...) the category of fraud — occupational fraud — in which an employee abuses his or her position within the organization for personal gain” (ACFE 2010). Fraud can be classified into corruption, asset misappropriation, and fraudulent statements (ACFE 2010). Here we look at only the occurrence of fraud in which the ERP/AIS systems are used (business transactions such as accounting, orders or payments). Beyond the focus of this paper are fraud activities (such as physical theft) that leave no traces in the ERP/AIS system (for example in the form of postings or log files).

The fraud triangle is often used to explain fraud (Ramos 2003). The fraud triangle comprises three generally accepted factors: pressures and incentives, opportunities, and attitudes and rationalizations (integrity). According to this model, people act fraudulently when all three factors have been fulfilled.

Incentive is the perceived pressure that "drives" a person to commit fraud (dissatisfaction with the job). Rationalization is the attitude toward fraud and respect for rules and following those rules (internal justification, attitudes). An opportunity includes the danger of being caught. As Srivastava et al. (2003) emphasize, the relationship between the three factors has a special significance. The risk for fraud increases exponentially when there is an increase in the connection between incentives, opportunities and rationalizations (Srivastava et al. 2003).

During a classic fraud audit, the analysis mainly focuses on data from the information system. It checks for conspicuousness in business transactions using, for example, Benford's law (Benford 1938), limit value controls, special receipts and unusual posting times. There are various statistical and mathematical methods that help distinguish between usual and unusual transactions. In this way, analytical procedures can be used to find deviations between forecast and actual business values (Koskivaara 2007). Data mining techniques can be used to analyze larger amounts of data (Yue 2007). Jans et al. (2010a) use a descriptive data mining strategy with a multivariate latent class clustering algorithm to procurement data to assess the risk of internal fraud.

4 The Concept of Continuous Auditing

Internal audits are performed regularly, and more and more often, they include the IT infrastructure. In order to be able to process such large amounts of data in a timely manner, they require "a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a short period after, the occurrence of events underlying the subject matter" (CICA/AICPA 1999). The continuous auditing method can be roughly split into two architecture methods. In the first method, the audit technique is integrated directly into the information system to be looked at as a software module (embedded audit module, or EAM, Debreceny et al. 2003, Chou et al. 2007). In the second method, the audit technique is installed and operated separate from the information system. For the actual audit, a monitoring control layer (MCL) creates a connection to the monitored information system or the database (Yeh and Shen 2010). In the recent past, other methods were developed to complement the two most often used ones, EAM and MCL, such as the interceptor mechanism (Lin et al. 2010), ghosting approach (Kuhn and Sutton 2009) or data-oriented online auditing (DOOA) (Chen et al. 2007). All approaches have their pros and cons, which can lead to problems depending on the existing system landscape. In heterogeneous system landscapes, the use of EAM, which requires a highly system-specific level of implementation, can be quite time consuming and complicated. Implementation requires a high level of technical understanding, exact knowledge of the system and can have a negative effect on system performance (Kuhn and Sutton 2009). The MCL method, on the other hand, only has to be adapted to system-specific data interfaces. This process usually requires much less technical effort and the system is not approached invasively, meaning performance is not affected.

5 Differentiation among Data to be audited

Because fraud takes place using both known and unknown patterns, it is necessary to analyze the entire data pool as part of an investigation. Differentiating among the data before the analysis supports a risk-oriented approach. Especially during a continuous audit, the focus of the audit can be determined and the circumstances that appear to be the most relevant can be prioritized.

From a fraud perspective, transactions can be classified into usual and unusual (Figure 1). During a fraud audit, predefined and known fraud signatures are applied to limit the amount of unusual transactions (chapter 3). By taking critical and non-critical human behavior into account, it is possible to uncover transactions that are part of a pattern (unknown fraud signature) that is not yet known and that would have been left undiscovered if using normal means. Figure 1 shows that the amount of data that should be prioritized increases for case 2 when taking critical behavior of employees into account.

It also enables sophisticated investigation into the unusual transactions because they are classified into case 3 and case 4. We assume that the majority of transactions by employees with non-suspicious behavior are unremarkable (case 1). The usual transactions with suspicious behavior (case 2) and the unusual transactions with non-suspicious behavior (case 3) follow. The lowest, but most critical part consists of unusual transactions and suspicious employee behavior (case 4).

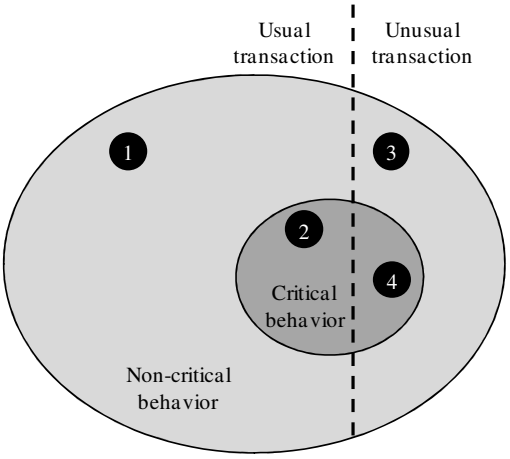

Figure 1: Differentiation among data to be audited

Case	Transaction classification	Employee behavior	Potential threat classification
1	Usual	Non-critical	Low
2	Usual	Critical	Medium
3	Unusual	Non-critical	Medium
4	Unusual	Critical	High

Table 1: Potential threat classification

The data parts shown in Figure 1 are prioritized in Table 1 using the potential threat classification (PTC) low to high, in which case 1 receives the lowest level priority and case 4 the highest. Classification enables us to perform a risk-oriented differentiated analysis.

6 Introducing the Generic Architectural Model

We designed a continuous auditing architecture that makes sufficient allowance for the fraud triangle factors (chapter 3). In this way, in addition the classic quantitative analysis of business transactions that are already being applied as part of the fraud detection audit, the human factor is extensively integrated into the audit as a qualitative component. Sections A I-V of Figure 2 reflect the classic procedure of a continuous auditing application. This approach includes extraction of audit data from the source systems using the MCL technique, processing using the predefined risk characteristics and then visualization of the results. Within the context of the fraud triangle, the opportunities factor hereby is taken into account.

The inclusion of the human factor is focused on the manifestation of various behavior patterns. These behavior patterns can be derived from the analysis of user-related data from one or more information systems. They are derived using the individual factors of the fraud triangle. The information systems selected in sections B-D usually belong to the business infrastructure of every organization. The configuration and availability of this system offers the advantage that they enable us to draw conclusions about unusual and potentially fraudulent users across the organization. Section B sketches an analysis that was made based on the event logs made for AIS/ERP. Both a deviation analysis between actual and reference processes (Jans et al. 2010) and determining the social networks are possible (van der Aalst et al. 2005). Analogous to that, in section C, the network traffic is analyzed. A permanent network behavior analysis (NBA) is performed to find deviations from the normal behavior of an employee in the network. All this takes the opportunities factor into account. For example, otherwise unauthorized access to protected and sensitive areas (e.g. human resources) remains undiscovered. In section D, text mining is performed on all organizational e-mail accounts to evaluate the basic mood of employees. Holton (2009) remarks that "(…) automated ways to find e-mail fraud indicators are very promising for reducing fraud losses." In this way, the fraud triangle is taken into

account because “Organizations' abundant e-mail archives provide a path for detecting fraud incentives and potential for rationalization.” (Holton 2009) The mood of e-mail writers can be determined by analyzing word choice and frequency.

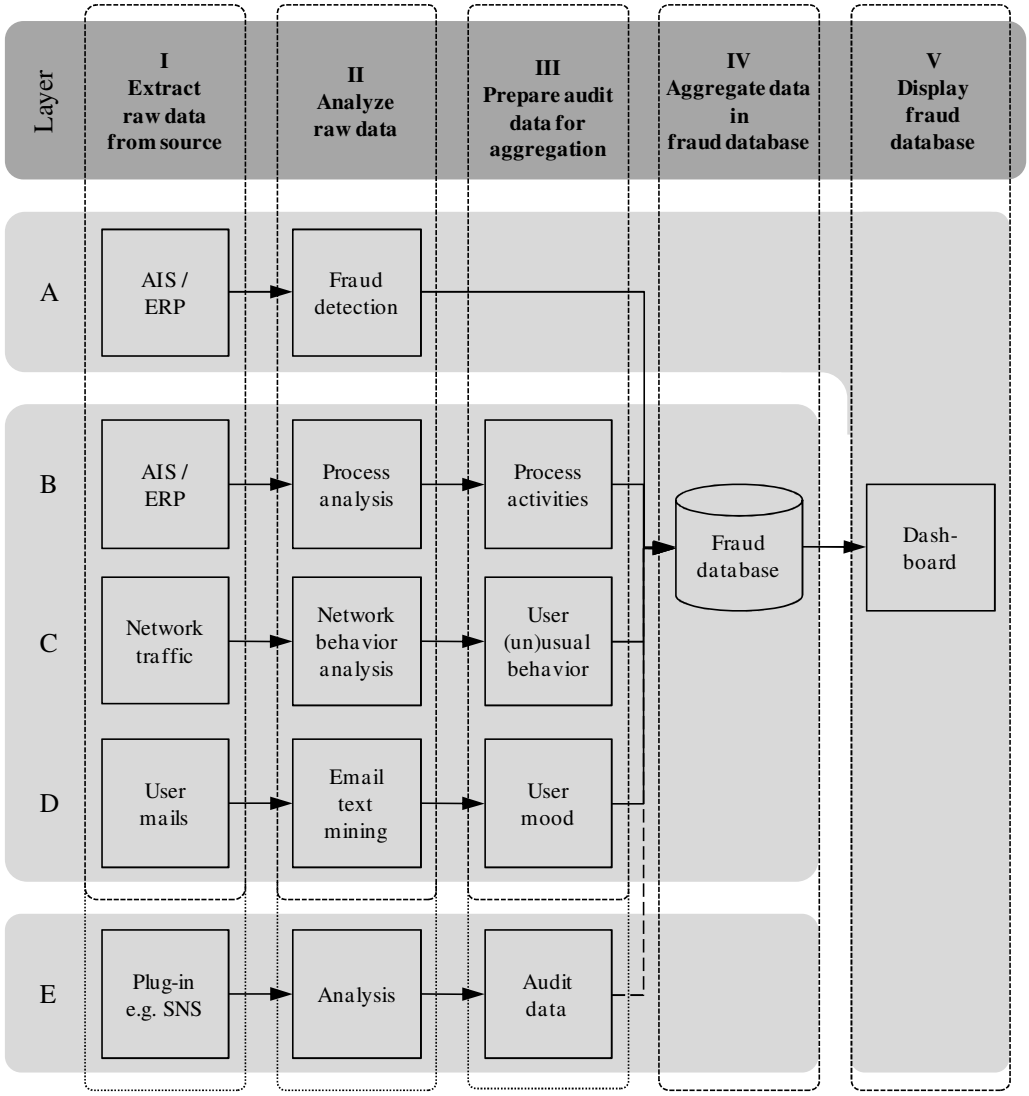

Figure 2: Generic architectural model

The optional section E sketches the connection of plug-ins. Plug-ins can help take the three fraud triangle factors into account in as much detail as possible, making use of additional information. This is conceivable for the factors incentives and rationalizations, in connection with social networking sites (SNS), instant messenger logs or extensive psychological predisposition tests (Rogers 2001).

The individual results of the analyses from sections A-E are summarized in a fraud database (layer IV) on user level (e.g. using a unique user ID). Finally, the results are prepared for auditors and high/level management using a dashboard (layer V). The dashboard enables individual analysis of results via various views. It provides both an overview of risky transactions in connection with behavior analysis of the person who made them and access to detailed data sets per drill down. Critical data sets are specially highlighted, taking into account the partial amounts shown in Figure 1. Prioritizing is done using Table 1, where partial amount 1 has the lowest priority level and partial amount 4 the highest. Case-related best practices are suggested for further examination.

The time it takes to realize the generic architectural model depends on the individual components. A data and process analysis can be implemented much more quickly than components that require a learning phase, such as network components or e-mail text mining.

7 Prototype

Our generic architectural model from chapter 6 is evaluated using the IT infrastructure that follows. A SAP ERP 6.0 test system with multiple clients was available.

Figure 3 illustrates the generic architectural model introduced in chapter 6, in which a concept for practical implementation is introduced using freely available or open source tools where useful. The AIS/ERP shown in section A, Layer I is an SAP ERP 6.0 system. The data required for the fraud analysis was extracted from this system (e.g. the tables BKPF, BSEG, USR02). In the next layer, the data written to a data base is analyzed using Picalo (Picalo 2010). Picalo is data analysis software that, analogous to ACL (ACL 2010) and IDEA (IDEA 2010) focuses on fraud detection. It is used for both simple and more complex script-based analyses. Special analyses, such as Benford or Gap analyses are part of the standard functions. The results of the Picalo analysis are supplemented with results from other analyses (B-D).

Extracted process logs from the SAP ERP 6.0 used in section A are used as input in section B. To compare actual and reference processes, we import the logs for analysis into ProM (ProM 2010, van Dongen et al. 2005) using an intermediate database.

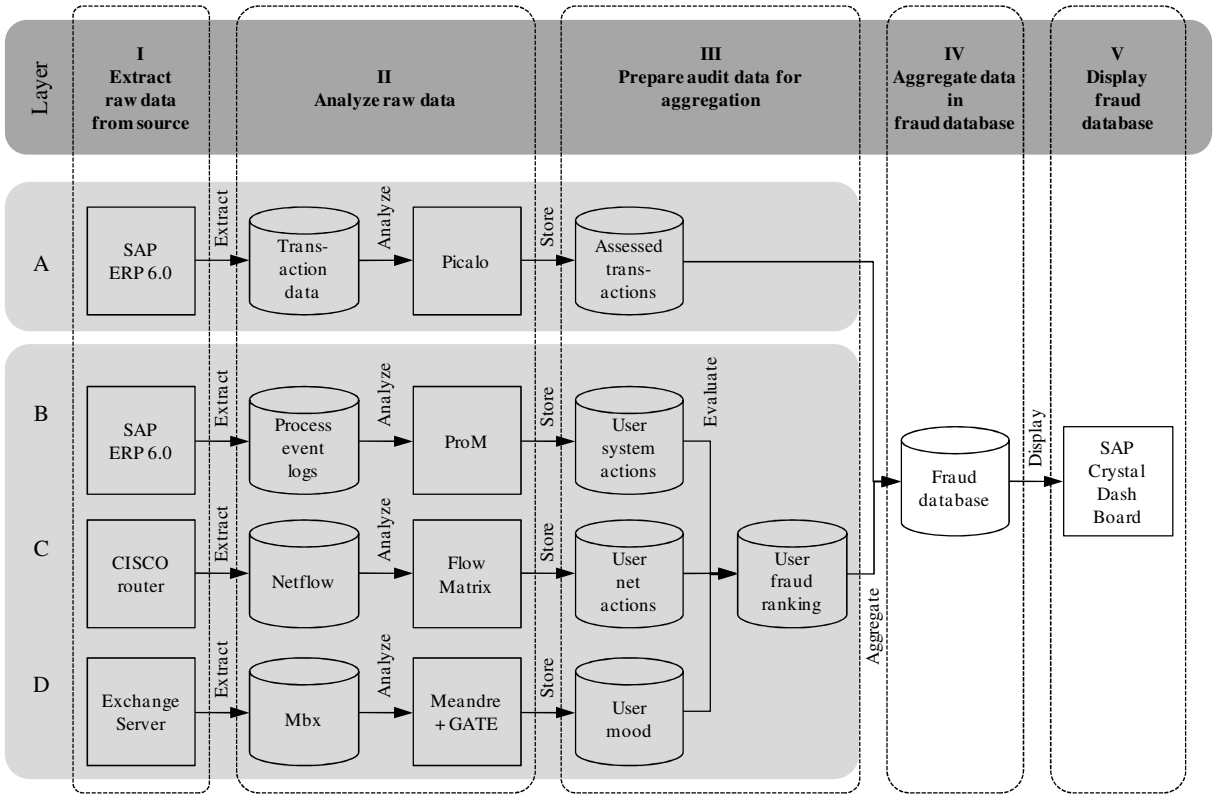

Figure 3: Prototype

A further component of our model is the network component shown in section C. The network data communication of a CISCO router is exported and can be called up by the software FlowMatrix (FlowMatrix 2010) in the NetFlow format. NetFlow is a standardized network protocol for traffic monitoring and includes information on data traffic (IETF 2010). Behavioral changes in employees are

determined with the help of network behavior analysis. Before deviating behavioral patterns, including IP addresses and the associated user names are available, an initial learning period is required. The usual observation period takes 7-14 days.

A Microsoft Exchange Mail Server is used as the data basis for section D. A conversion of the proprietary Microsoft Exchange Mailbox Format into plain text e-mail format mbx is required in order to be able to perform text mining on the e-mails. Text mining is done using general architecture for text engineering (GATE 2010). The GATE components are controlled using Meandre (Meandre 2010), which enables automated text mining in the form of a workflow. The result classifies the general mood of the employees, for example, as disgruntled or non-disgruntled. This procedure was already described and successfully evaluated by Holton (2009).

The results of sections B-D of Layer III are summarized in a user fraud ranking database. A potential threat classification (PTC) is then determined from the individual results, taking the weighting factors into account. For the introductory phase, in our model we used an equal weight distribution. Later, each organization can adjust the weighting of factors individually after the evaluation phase is over, and using the empirical values from that phase.

In order to keep the model practice-oriented and comprehensible, we use the following calculation for the aggregation (PTC) of the individual values:

$$PTC = x_1 B + x_2 C + x_3 D$$

with PTC = potential threat classification; $x_1 = x_2 = x_3 = 1$ – weighting factors; $B, C, D \in \bullet \{0,1\}$ – classification, with 0 – non critical; 1 – critical.

The classification described in chapter 5 was taken into account when we visualized the dashboard. The overall assessment was mapped using traffic lights. The cases (case 1) that were classified in Table 1 as low PTC (transaction usual, employee behavior non-critical) got green light. A yellow light is given when the PTC is not equal to zero or the transactions are considered unusual (medium: case 2 and 3). The highest warning level (high) is output for case 4. The traffic light is red when the transactions are unusual and the PTC was not equal to zero.

The results are visualized using SAP Crystal Dashboard Design (SAP 2010). This front end offers the auditor and/or high-level management the information required for further analysis. The various predefined views can be controlled using a defined authorization concept by target group.

8 Discussion

Many of the concerns discussed in the literature refer to the analysis of personal data and the possible breach of personal privacy of employees. Here the legal and data protection regulations of the particular country must be taken into account (Kaarst-Brown and Kelly 2005). It is absolutely necessary to perform an organization specific check. An example of this is text mining of e-mails, as discussed in Chapter 7. For reasons of privacy, auditors generally do not have access to the e-mails being analyzed. Only in the case of a confirmed suspicion when further investigations have been launched is this type of access permitted. E-mails are important pieces of internal business data for which there is an obligation toward archiving and documentation. In this case, employees only have limited rights to privacy (Kaupins and Minch 2005).

Another point of discussion is the analysis of human behavior and dealing with the results. It must be noted that unusual behavior is not synonymous with the intention of actually committing fraud or with having committed fraud (Holton 2009). Risk indicators can be derived from behavior that raises suspicion of fraud. These indicators must be weighed against principles of professional judgment and can be used as a starting point for further intensive checks. The costs of not discovering the fraud (false negatives) exceed the expected additional expenditure of pursuing false positives. “With total

accuracy clearly out of reach, false positives are preferred to false negatives (…)."(Holton 2009) The exact measure of prevention or combating fraud can be selected specific to the organization. With regard to prevention, awareness-building measures have proven to be helpful among employees (Albrechtsen and Hovden 2010).

Beyond that, the combination of the PTC provides another point of discussion that requires separate evaluation. In Chapter 7, we determined that the selection of weighting factors must be done by each organization. As part of a future case study, we need to check whether modifying the PTC calculation can provide a more precise risk classification of employees. This can, for example, be done based on work from Srivastava et al. (2003) and Turner et al. (2003), who have already done mathematical work on the possible connections between fraud triangle factors.

9 Conclusions and Outlook

In this paper, we introduce a generic architectural model that makes sufficient allowance for the fraud triangle factors. In this way, in addition to the classic quantitative analysis of business transactions that are already being applied as part of the fraud detection audit, the human factor is extensively integrated into the audit as a qualitative component. This provides added value because the transactions examined by the auditor can be better differentiated and prioritized. By taking critical and non-critical human behavior into account, it is possible to uncover transactions that are part of a pattern that is not yet known and that would have been left undiscovered using normal means. The inclusion of the human factor is focused on the manifestation of various behavior patterns. These behavior patterns can be found in user data. E-mails are examined using text mining, a network behavior analysis is performed on network traffic and the ERP/AIS process logs are analyzed. The generic architectural model can be expanded in a modular way by adding plug-ins. The proposed architecture is implemented using a prototype and is applied exemplary to an SAP ERP system. We suggest a selection of established tools for implementation.

Legal regulations may represent the largest obstacle to the practical implementation of the prototype. Beforehand, it is very important to clarify how the respective legal regulations permit unlimited use in an organizational context. The modular structure of the prototype enables step-by-step implementation of the permitted components. It is also necessary that the auditors have the required expertise, and they are well versed in both fraud and the technical operation of the individual components (e.g. scripting). The approach developed in this paper provides support and can relieve the auditor, but it does not replace the required basic experience and knowledge. Because it is important to remember that the indication of suspicious behavior concerning fraud does not mean that fraud has taken place or that there was intent to commit fraud. The generic architectural model presented in this paper is part of a further and more intense research effort.

Our future work will concentrate on evaluating the prototype introduced in this paper using a case study. The interrelation between risk indicators, weighting factors, and the PTC need to be looked at in more detail. Another goal is the implementation as a complete automatic continuous auditing tool for real-time assessments. To this end, the degree of automation of the tools that are linked to one another must be increased and manual intervention in the analysis process must be reduced to an absolute minimum. Another interesting aspect of plug-ins is connecting to social networking sites. In this way, ideally, additional information on the social networks of employees can be extracted, and this information can be useful for fraud analysis. It is conceivable that personality profiles be investigated scientifically in order to better connect the behavior respectively human factor and to make even more precise risk estimations. We can also examine whether investigating personality profiles can lead to more precise predictions during e-mail text mining. Another conceivable approach is using neural networks. These are especially known for their ability to recognize patterns in data. The connections found in this way can be used successfully for prognoses. Detection and prognosis of employee behavior or analysis of business transactions could be promising new areas of application.

References

ACFE (2010). Report to the Nations on Occupational Fraud and Abuse. 2010 Global Fraud Study. http://www.acfe.com/rttn/rttn-2010.pdf.

ACL (2010). http://www.acl.com.

Albrechtsen, E. and Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study Computers & Security, 29 (4), 432-445.

Alles, M.G. and Kogan, A. and Vasarhelyi, M.A. (2004). Restoring auditor credibility: tertiary monitoring and logging of continuous assurance systems. International Journal of Accounting Information Systems, 5 (2), 183-202.

Benford, F. (1938). The Law of Anomalous Numbers. In Proceedings of the American Philosophical Society, 78 (4), 551-572.

Chen, W. and Zhang, J.-C. and Jiang, Y.-Q. (2007). One Continuous Auditing Practice in China: Data-oriented Online Auditing (DOOA). In IFIP International Federation for Information Processing. Volume 252, Integration and Innovation Orient to E-Society, 2, eds. Wang, W., 521-528.

Chou, C. and Du, T. and Lai, V. (2007). Continuous auditing with a multi-agent system. Decision Support Systems, 42 (4), 2274-2292.

CICA/AICPA (1999). Continuous auditing. Research Report, Toronto, Canada: The Canadian Institute of Chartered Accountants.

Davis, J. and Hossain, L. and Murshed, S. (2007). Social Network Analysis and Organizational Disintegration: The Case of Enron Corporation. In Proceedings of ICIS 2007.

Debreceny, R. et al. (2003). The Development of Embedded Audit Modules to Support Continuous Monitoring in the Electronic Commerce Environment. International Journal of Auditing, 7 (2), 169-185.

FlowMatrix (2010). http://www.akmalabs.com/flowmatrix.php.

GATE (2010). http://gate.ac.uk.

Gray, G.L. and Debreceny, R. (2007). Data Mining Of Emails To Support Periodic And Continuous Assurance. Working Paper.

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

Hevner, A.R. and Chatterjee, S. (2010). Design Research in Information Systems. Integrated Series in Information Systems, 22, 9-22.

Holton, C. (2009). Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. Decision Support Systems, 46 (4), 853-864.

IDEA (2010). http://www.caseware.com/products/idea.

IETF (2010). Cisco Systems NetFlow Services Export Version 9. http://tools.ietf.org/html/rfc3954.

Jans, M. and Lybaert, N. and Vanhoof, K. (2009). A framework for Internal Fraud Risk Reduction at IT Integrating Business Processes: The IFR² Framework. The International Journal of Digital Accounting Research, 9 (15), 1-29.

Jans, M. and Alles, J. and Gamini, M. and Vasarhelyi, M.A., (2010). Process Mining of Event Logs in Auditing: Opportunities and Challenges. Working Paper.

Jans, M. and Lybaert, N. and Vanhoof, K. (2010a). Internal fraud risk reduction: Results of a data mining case study. International Journal of Accounting Information Systems, 11 (1), 17-41.

Kaarst-Brown, M.L. and Kelly S. (2005). IT Governance and Sarbanes-Oxley: The latest sales pitch or real challenges for the IT Function?. In Proceedings of the 38th Annual Hawaii International Conference on System Sciences HICSS 2005.

Kandias, M. et al. (2010). An Insider Threat Prediction Model. Trust, Privacy and Security in Digital Business, Lecture Notes in Computer Science, 6264/2010, 26-37.

Kaupins, G. and Minch, R. (2005). Legal and Ethical Implications of Employee Location Monitoring. In Proceedings of the 38th Annual Hawaii International Conference on System Sciences HICSS 2005.

Koskivaara, E. (2007). Integrating Analytical Procedures into the Continuous Audit Environment. Journal of Information Systems and Technology Management, 3 (3), 331-346.
Kuhn, R. and Sutton, S.G. (2003). Continuous Auditing in ERP System Environments: The Current State and Future Directions.
Lin, C. and Lin, F. and Liang, D. (2010). An Analysis of Using State of the Art Technologies to Implement Real-Time Continuous Assurance. 6th World Congress on Services, 415-422.
Meandre (2010). http://seasr.org/meandre.
Peffers, K. et al. (2006). The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. In proceedings of DESRIST 2006, 83-106.
Peffers, K. et al. (2007). A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24(3), 45-77.
Phua, C. et al. (2005). A comprehensive survey of data mining-based fraud detection research.
Picalo (2010). http://www.picalo.org.
ProM (2010). http://prom.sourceforge.net.
PWC (2009). The Global Economic Crime Survey. Economic crime in a downtorn. November 2009. http://www.pwc.com/en_GX/gx/economic-crime-survey/pdf/global-economic-crime-survey-2009.pdf
Ramos, M. (2003). Auditor's responsibility for fraud detection. Journal of Accountancy. 195 (1), 28.
Rogers, M.K. (2001). A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study. Doctoral Dissertation. Department of Psychology, University of Manitoba .
SAP (2010). http://www.sap.com/solutions/sap-crystal-solutions/dashboards-visualization/index.epx.
Srivastava, R.P. and Mock, T.J. and Turner, J.L. (2003). The Effects of Integrity, Opportunity, Incentives, Mitigating Factors and Forensic Audit Procedures on Fraud Risk.
Turner, J.L. and Mock, T.J. and Srivastava, R.P. (2003). An Analysis of the Fraud Triangle. Working Paper.
van der Aalst, W.M.P. and Reijers, H.A. and Song, M. (2005). Discovering Social Networks from Event Logs. Computer Supported Cooperative Work (CSCW), 14 (6), 549-593.
van Dongen, B.F. et al. (2005). The ProM Framework: A New Era in Process Mining Tool Support. Applications and Theory of Petri Nets 2005 Lecture Notes in Computer Science, 3536/2005, 444-454.
Wells J.T. (2008). Principles of Fraud Examination, Wiley, 2nd Edition.
Yeh, C. and Shen, W. (2010). Using continuous auditing life cycle management to ensure continuous assurance. African Journal of Business Management, 4(12), 2554-2570.
Yue, D. et al. (2007). A Review of Data Mining-Based Financial Fraud Detection Research. Wireless Communications, Networking and Mobile Computing 2007, 5519-5522.