Beiträge zum IT-Compliance Management

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

Doktor der Wirtschaftswissenschaften
- Doctor rerum politicarum -

vorgelegte Dissertation

von

Diplom-Ökonom Thorben Sandner

[redacted]

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.

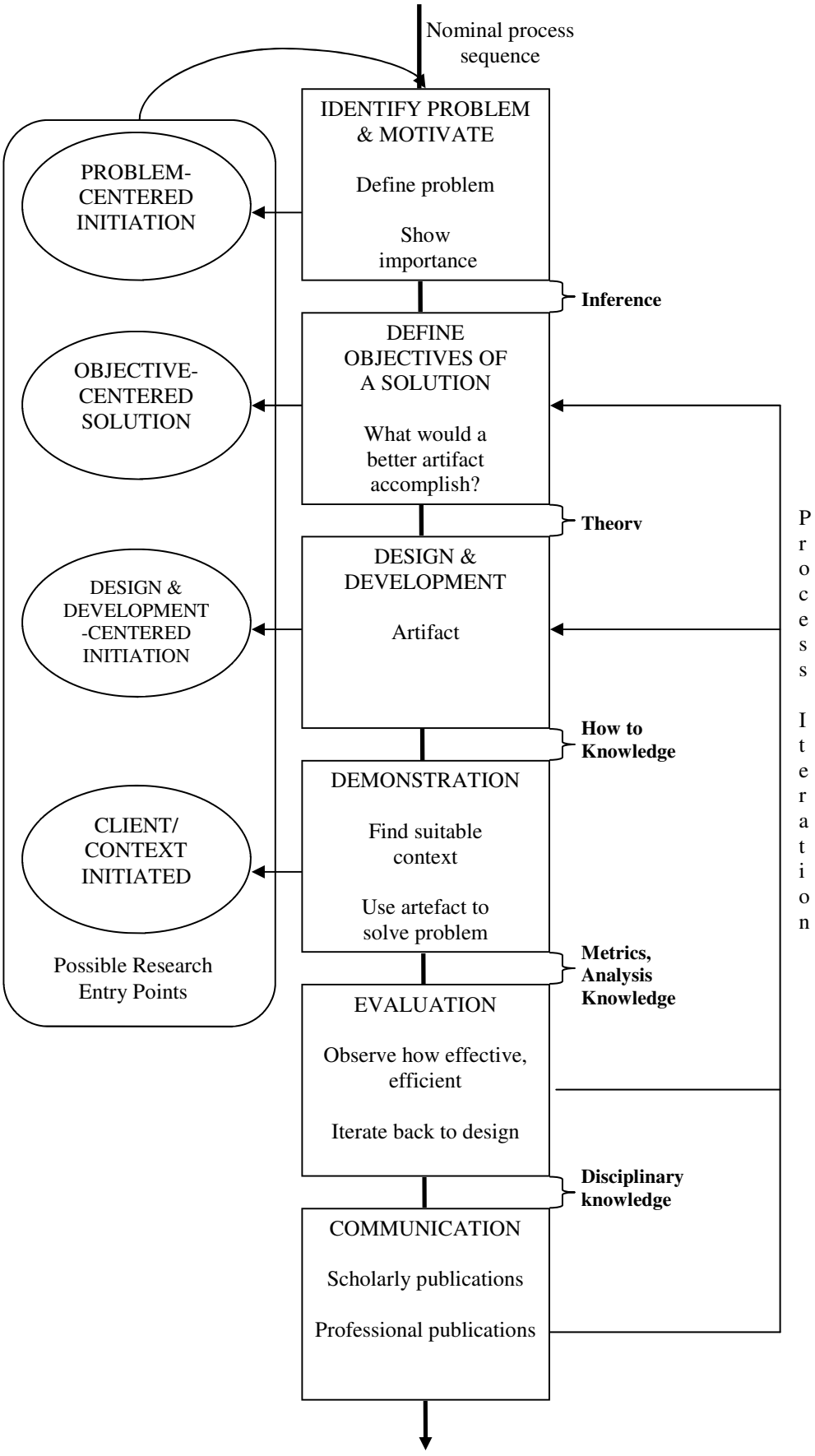

Abbildung I: Design Science Research Methode (DSRM).

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.

Inhaltsverzeichnis

Seite

Abbildungsverzeichnis

Tabellenverzeichnis