Sulk, Ingolf; Hagen, Philipp; Klotz, Michael

Working Paper

Kontrollanforderungen an ein ERP/Cloud-System und Umsetzung in automatisierte Kontrollen

SIMAT Arbeitspapiere, No. 11-19-035

Provided in Cooperation with:
Hochschule Stralsund, Stralsund Information Management Team (SIMAT)

Suggested Citation: Sulk, Ingolf; Hagen, Philipp; Klotz, Michael (2019) : Kontrollanforderungen an ein ERP/Cloud-System und Umsetzung in automatisierte Kontrollen, SIMAT Arbeitspapiere, No. 11-19-035, Hochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund

This Version is available at:
https://hdl.handle.net/10419/204649

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 11-19-035

Kontrollanforderungen an ein ERP/Cloud-System und Umsetzung in automatisierte Kontrollen

Dr. Ingolf Sulk
Philipp Hagen
Prof. Dr. Michael Klotz

Hochschule Stralsund
SIMAT Stralsund Information Management Team

September 2019

ISSN 1868-064X

Sulk, Ingolf; Hagen, Philipp; Klotz, Michael: Kontrollanforderungen an eine ERP/Cloud-System und Umsetzung in automatisierte Kontrollen. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: Hochschule Stralsund, SIMAT Stralsund Information Management Team, 2019 (SIMAT AP, 11 (2019), 35), ISSN 1868-064X

Impressum

Hochschule Stralsund
SIMAT Stralsund Information Management Team
Zur Schwedenschanze 15
18435 Stralsund
www.hochschule-stralsund.de

Herausgeber

Prof. Dr. Michael Klotz
Hochschule Stralsund, Fakultät für Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
E-Mail: michael.klotz@hochschule-stralsund.de

Print

Digitaldruck: www.dokuteam-x.de
Behrndt & Herud GmbH
Anklamer Straße 98
17489 Greifswald

Autoren

Dr. Ingolf Sulk ist langjähriger Lehrbeauftragter an der Hochschule Stralsund. Er arbeitete als leitender wissenschaftlicher Mitarbeiter im Projekt „Integrierte Spezifikation und Umsetzung eines IT-Compliance-Framework für die Interaktion zwischen dem ERP-System und einer Supply Chain Management Service Cloud“ (INSPECTIO).

Philipp Hagen war wissenschaftlicher Mitarbeiter im Projekt INSPECTIO.

Prof. Dr. Michael Klotz lehrt, forscht und publiziert an der Fakultät für Wirtschaft der Hochschule Stralsund auf den Gebieten der Unternehmensorganisation und -überwachung, der IT-Governance und der IT-Compliance. Er war Projektleiter des Projekts INSPECTIO.

Kontrollanforderungen an ein ERP/Cloud-System und Umsetzung in automatisierte Kontrollen

Sulk, Ingolf; Hagen, Philipp; Klotz, Michael[1]

Zusammenfassung: Die in diesem Arbeitspapier enthaltende Darstellung dokumentiert Ergebnisse eines Forschungsprojekts als Forschungs- und Entwicklungsvorhaben im Verbund (FuE-Verbundforschung) im Rahmen der Förderung von Forschung, Entwicklung und Innovation des Landes Mecklenburg-Vorpommern mit Mitteln des „Europäischen Fonds für regionale Entwicklung“ (EFRE) aus den Europäischen Strukturfonds der Europäischen Union in der Förderperiode 2014 bis 2020. Das geförderte Teilprojekt der Hochschule Stralsund trug den Titel „Integrierte Spezifikation und Umsetzung eines IT-Compliance-Framework für die Interaktion zwischen dem ERP-System und einer Supply Chain Management Service Cloud“ (INSPECTIO). Ziel des Projekts war die Entwicklung und technische Umsetzung eines rechnungslegungsbezogenen IT-Compliance-Framework in einer prototypisch zu realisierenden informations- und kommunikationstechnischen Infrastruktur eines ERP/Cloud-Systems. Im Rahmen des Projekts wurde ein „Compliance by Design“-Ansatz verfolgt: Kontrollanforderungen wurden aus verschiedenen gesetzlichen Vorgaben sowie aus Normen und Standards abgeleitet, so dass diese bereits bei der Systementwicklung berücksichtigt werden konnten. Als Grundlage der Ableitung der Anforderungen dienten IDW-Prüfungsstandards und IDW-Stellungnahmen zur Rechnungslegung, DIN- und ISO/IEC-Normen, die GoBD sowie Standards der CSA und der ENISA. Die Umsetzung erfolgte prototypisch am Beispiel einer Kontrolle auf Doppelzahlungen. Für die Realisierung der automatisierten Kontrolle werden die Datenanalysesoftware „IDEA“, das Datenexport-Tool „SmartExporter“ und das CCM-System „CaseWare Monitor“ der Fa. Audicon GmbH verwendet. Die prototypische Umsetzung beinhaltet die Bereitstellung eines sogenannten IDEA-Skripts und den Datenimport aus dem SAP-System „IDES“ mit Hilfe von SmartExporter. Die Verarbeitung der Daten erfolgt in IDEA, die Implementation der automatisierten Kontrolle in CaseWareMonitor als prozessintegrierte Kontrolle.

Gliederung

Vorwort des Herausgebers 5
Abbildungsverzeichnis 6
Tabellenverzeichnis 7
Abkürzungsverzeichnis 8
1 Einleitung 10

[1] Prof. Dr. Michael Klotz, Hochschule Stralsund, Fakultät für Wirtschaft, Zur Schwedenschanze 15, 18435 Stralsund, michael.klotz@hochschule-stralsund.de

2 Kontrollanforderungen gemäß der Grundsätze ordnungsmäßiger Buchführung 11
2.1 IT-Sicherheit 11
2.2 Ordnungsmäßigkeit 13
2.3 IT-Infrastruktur 16
2.3.1 Sicherung der Betriebsbereitschaft 17
2.3.2 IT-Anwendungen 18
2.3.3 IT-gestützte Geschäftsprozesse 18
2.3.4 IT-Umfeld & Organisation 18
2.3.5 Überwachung des IT-Kontrollsystems 19
3 Allgemeine Kontrollanforderungen 19
4 Konzeption und Beschreibung einer automatisierten Kontrolle auf Doppelzahlungen 22
4.1 Risiko der Doppelzahlung 22
4.1.1 Mögliche Ursachen des Risikos 23
4.1.2 Technische Gründe für Doppelzahlungen 23
4.1.3 Identifizierung der relevanten Tabellen sowie Felder in SAP ERP 23
4.1.4 Inhalt der Kontrolle 26
4.1.5 Ergebnis der Kontrolle 26
4.2 Prototypische Umsetzung einer automatisierten Kontrolle auf Doppelzahlungen 26
4.2.1 Export der Daten aus SAP via SmartExporter 27
4.2.2 Umsetzung der Kontrolle in IDEA-Script 31
4.2.3 Implementierung der Kontrolle in CaseWare-Monitor 33
5 IDEA-Skript 43

Schlüsselwörter: Doppelzahlung – Continuous Monitoring – IDEA – Internes Kontrollsystem – Kontrollen – SAP

JEL-Klassifikation: M21, M42

Vorwort des Herausgebers

Die in diesem Arbeitspapier enthaltende Darstellung dokumentiert Ergebnisse eines Forschungsprojekts als Forschungs- und Entwicklungsvorhaben im Verbund (FuE-Verbundforschung) im Rahmen der Förderung von Forschung, Entwicklung und Innovation des Landes Mecklenburg-Vorpommern mit Mitteln des „Europäischen Fonds für regionale Entwicklung“ (EFRE) aus den Europäischen Strukturfonds der Europäischen Union in der Förderperiode 2014 bis 2020. Das geförderte Teilprojekt der Hochschule Stralsund trug den Titel „Integrierte Spezifikation und Umsetzung eines IT-Compliance-Framework für die Interaktion zwischen dem ERP-System und einer Supply Chain Management Service Cloud“ (INSPECTIO). Ziel des Projekts war die Entwicklung und technische Umsetzung eines rechnungslegungsbezogenen IT-Compliance-Framework in einer prototypisch zu realisierenden informations- und kommunikationstechnischen Infrastruktur eines ERP/Cloud-Systems. Hierzu erfolgte eine Konzeption und Umsetzung von in das IT-System integrierter risikobasierter automatisierter Kontrollen im Rahmen eines konzeptionell zu entwickelnden Internen Kontrollsystems. Die Zusammenstellung der inhaltlichen Kontrollanforderungen und ein Beispiel für eine prototypische Umsetzung einer automatisierten Kontrolle unter Nutzung des an der Hochschule eingerichteten Labors für Interne Kontrollsysteme und Datenanalyse sind Inhalt dieses Arbeitspapiers.

Prof. Dr. Michael Klotz

Abbildungsverzeichnis

Abb. 1 Screenshot SmartExporter Datenanforderung zur Kontrolle auf Doppelzahlungen 27

Abb. 2 Screenshot SmartExporter Datenanforderung zur Einführung zur Kontrolle auf Doppelzahlungen..... 27

Abb. 3 Screenshot SmartExporter Tabellenauswahl BSAK zur Kontrolle auf Doppelzahlungen 28

Abb. 4 Screenshot SmartExporter: Daten filtern zur Kontrolle auf Doppelzahlungen 28

Abb. 5 Screenshot SmartExporter: Felder und Filter auswählen zur Kontrolle auf Doppelzahlungen 29

Abb. 6 Screenshot SmartExporter: Join-Definition zur Kontrolle auf Doppelzahlungen 29

Abb. 7 Screenshot SmartExporter: Optionen für Datenanforderung definieren zur Kontrolle auf Doppelzahlungen 30

Abb. 8 Screenshot SmartExporter: Fertigstellung zur Kontrolle auf Doppelzahlungen 31

Abb. 9 Screenshot SmartExporter: Mehrfachbelegung Ermittlung 31

Abb. 10 Screenshot SmartExporter: Mehrfachbelegung Schlüssel definieren 32

Abb. 11 Screenshot SmartExporter: Liste der gefundenen Doppelzahlungen 32

Abb. 12 Screenshot SmartExporter: Paket für Case WareMonitor 33

Abb. 13 Screenshot CaseWare Monitor, Pakete..... 34

Abb. 14 Screenshot CaseWare Monitor, Terminierung erstellen..... 34

Abb. 15 Screenshot CaseWare Monitor, Ausführungsfrequenz..... 35

Abb. 16 Screenshot CaseWare Monitor, Startzeit, -datum 35

Abb. 17 Screenshot CaseWare Monitor, Enddatum 36

Abb. 18 Screenshot CaseWare Monitor, Benutzeranmeldung 36

Abb. 19 Screenshot CaseWare Monitor, Ausführung der Terminierung 37

Abb. 20 Screenshot CaseWare Monitor, Bericht 37
Abb. 21 Screenshot CaseWare Monitor, Berichtdetails 38
Abb. 22 Screenshot CaseWare Monitor, erweiterte Berichtdetails 38
Abb. 23 Screenshot CaseWare Monitor, Risikowert 39
Abb. 24 Screenshot CaseWare Monitor, Benutzerzuweisung 39
Abb. 25 Screenshot CaseWare Monitor, E-Mail Benachrichtgung 40
Abb. 26 Screenshot CaseWare Monitor, SMS-Benachrichtgung 40
Abb. 27 Screenshot CaseWare Monitor, Dashboard 41
Abb. 28 Screenshot CaseWare Monitor, Übersicht der Auffälligkeiten 41
Abb. 29 Screenshot CaseWare Monitor, Überprüfung der Auffälligkeiten 42

Tabellenverzeichnis

Tab. 1 Anforderungen an die IT-Sicherheit 12
1Tab. 2 Anforderungen an die Ordnungsmäßigkeit 14
Tab. 3 Anforderungen an die IT-Infrastruktur 17
Tab. 4 Anforderungen an die Sicherung der Betriebsbereitschaft 17
Tab. 5 Anforderungen an IT-Anwendungen 18
Tab. 6 Anforderungen an IT-gestützte Geschäftsprozesse 18
Tab. 7 Anforderungen an IT-Umfeld & Organisation 18
Tab. 8 Anforderungen an die Überwachung des IT-Kontrollsystems 19
Tab. 9 Allgemeine Anforderungen 19
Tab. 10 Felder aus Tabelle BSAK Nebenbuch Kreditoren – ausgeglichene Posten 24
Tab. 11 Felder aus Tabelle LFB1 Stammdaten Lieferanten (Buchungskreis) 25
Tab. 12 Felder aus Tabelle TBSL Buchungsschlüssel 25

Abkürzungsverzeichnis

AG	Aktiengesellschaft
AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
CC	Cloud Computing
CCM	Continuous Controls Monitoring
CPU	Central Processing Unit
CSA	Cloud Security Alliance
DIN	Deutsche Institut für Normung e. V.
E-Commerce	Electronic Commerce
EFRE	Europäischer Fonds für regionale Entwicklung
E-Mail	Electronic Mail
ENISA	European Union Agency for Cybersecurity
ERP	Enterprise Resource Planning
FAIT	Fachausschuss IT
FI	Finanzwirtschaft
FuE	Forschung und Entwicklung
GoB	Grundsätze ordnungsmäßiger Buchführung
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
HGB	Handelsgesetzbuch
http	Hypertext Transfer Protocol
ID	Identity
IDEA	Interactive Data Extraction and Analysis
IDES	International Demonstration and Education System
IDW	Institut der Wirtschaftsprüfer in Deutschland e. V.
IEC	International Electrotechnical Commission
IKS	Internes Kontrollsystem
INSPECTIO	Integrierte Spezifikation und Umsetzung eines IT-Compliance-Framework für die Interaktion zwischen einem ERP-System und einer Supply Chain Management Service Cloud
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
IT	Informationstechnologie
KMU	Kleine und mittlere Unternehmen

MM	Materialwirtschaft
NPS	Non Press Shop
RAM	Random Access Memory
RS	Stellungnahme zur Rechnungslegung
SAP	Systeme, Anwendungen, Produkte
SCHERPA	Supply Chain-oriented Enterprise Resource Planning Application
SLA	Service Level Agreement
SMS	Short Message Service
SPEC	Specification
SQL	Structured Query Language
SSL	Secure Sockets Layer
TAN	Transaktionsnummer
TCP	Transmission Control Protocol
UStG	Umsatzsteuergesetz
XML	Extensible Markup Language

1. Einleitung

Projektinhalte

Diese Dokumentation beinhaltet Ergebnisse, die im Forschungs- und Entwicklungsprojekt „INSPECTIO“ erzielt wurden und Teile der Arbeitspakete 1 und 3 sind. Im Mittelpunkt des ersten Arbeitspakets stand die Erstellung eines anwendungsspezifischen Compliance-Framework, das die vorgegebenen Kontrollmaßnahmen auflistet. Hierzu wurden folgende Arbeitsschritte ausgeführt: Ist-Aufnahme, Bewertung, Konsolidierung und Dokumentation von Gesetzen, Verordnungen etc. der IT-Compliance für Cloud- und ERP-Systeme. Hieraus wurden Kontrollanforderungen an das im Projekt intendierte ERP-System abgeleitet.

Verwendete Normen und Standards

Als Hauptquellen für die Analyse wurden folgende Standards und Normen verwendet:

- IDW PS 140 – Qualitätskontrollen in der Wirtschaftsprüferpraxis
- IDW PS 261 n. F. – Fehlerrisiken und Reaktionen
- IDW PS 330 – Abschlussprüfung bei Einsatz von IT
- IDW RS FAIT 1 – GoB bei Einsatz von IT
- IDW RS FAIT 2 – GoB bei Einsatz von E-Commerce
- IDW ERS FAIT 5 – GoB bei Einsatz von Cloud Computing (CC)
- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
- ISO/IEC 27017 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- DIN SPEC 66286 – Management von Cloud Computing Lösungen in kleinen und mittleren Unternehmen (KMU)
- ISO/IEC 27002 – Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen
- ENISA Cloud computing security risk assessment
- CSA Security Guidance for Critical Areas of Focus in Cloud Computing

Verwendete Gesetze

Als Gesetze fanden Eingang in die Analyse:

- Handelsgesetzbuch (HGB); § 238 – Buchführungspflicht, § 239 – Führung von Handelsbüchern, § 257 – Aufbewahrung von Unterlagen/Aufbewahrungsfristen; § 261 – Vorlegung von Unterlagen auf Bild-/Dateiträgern
- Bundesdatenschutzgesetz (BDSG): § 9 & Anlage – Berechtigungskontrollen
- Abgabenordnung (AO): § 145 – Allgemeine Anforderungen an Buchführung und Aufzeichnungen; §146 – Ordnungsvorschriften für die Buchführung und für Aufzeichnungen
- Umsatzsteuergesetz (UStG): § 22 – Aufzeichnungspflichten

2. Kontrollanforderungen gemäß der Grundsätze ordnungsmäßiger Buchführung

Die IDW RS FAIT 1 und IDW RS FAIT 2 beschäftigen sich mit den Grundsätzen ordnungsmäßiger Buchführung (GoB) unter Einsatz von Informationstechnologien und E-Commerce. Hierbei konkretisieren Sie die Anforderungen, die sich aus den §§ 238, 239 und 257 des Handelsgesetzbuches (HGB) ergeben. Die FAIT lassen sich hierbei in strukturierte Unterpunkte zusammenfassen, die im Folgenden näher beschrieben werden.

2.1 IT-Sicherheit

Als Anforderungen an die IT-Sicherheit werden gewöhnlich genannt:

- Vertraulichkeit: Vertraulichkeit ist dann gegeben, wenn nur diejenigen Personen, die berechtigt sind, von schützenswerten Daten Kenntnis nehmen können.
- Integrität: Die Integrität beschäftigt sich mit der Kontrolle der Vollständigkeit und Richtigkeit von Daten und Systemen, wobei die Kernpunkte auf der Verhinderung von unbefugten, ungewollten oder fehlerhaften Änderungen liegen.
- Verfügbarkeit: Die Verfügbarkeit beschreibt die Sicherung der Betriebsbereitschaft dergestalt, dass IT-Infrastruktur und IT-Anwendungen zur Verfügung stehen, d. h. zeitgerecht genutzt werden können.

- Autorisierung: Im Rahmen der Autorisierung werden die berechtigten Personen festgelegt, die Daten oder Geschäftsvorfälle bearbeiten und weitergeben dürfen.
- Authentizität: Authentizität ist die eindeutige Zuordnung eines Geschäftsvorfalls zu seinem Verursacher bzw. seinem Ursprung.
- Verbindlichkeit: Verbindlichkeit beschreibt den Vorgang, in dem eine Informationsquelle die Sendung von Informationen nicht abstreiten kann, so dass bindende Rechtsfolgen eintreten.

Diese grundsätzlichen Anforderungen lassen sich wie folgt konkretisieren, s. Tabelle 1:

Tab. 1 Anforderungen an die IT-Sicherheit

Hauptpunkt	Verfahren	
Vertraulichkeit	Verschlüsselung	X
	verschlüsselte Übermittlung	X
	Weitergabebeschränkung	X
	Empfängerverifizierung	X
	Löschfristeneinhaltung	X
Integrität	Testverfahren	X
	Freigabeverfahren	X
	Firewalls	X
	Virenscanner	X
	Zugriffsprotokollierungen	X
	Plausibilitätskontrollen	X
	regelmäßige Auswertung der Einhaltungen	X
	Intrusion-Detection-Systeme	
	Content-Inspektion	X
	Deaktivierung von Programmtransfermöglichkeiten	
	Dokumentation der Abwehrmechanismen/-szenarien	X
Verfügbarkeit	Back-Ups	X
	redundante Systeme	X
	Kapazitätsanalysen bzgl. Übertragungs-/Speichervolumina	X
	Verträge & SLAs bei Leistung Dritter (Outsourcing)	X
Autorisierung	organisatorische Regelungen	X
	Berechtigungsverwaltung	X
	Zugriffsschutz	X
	biometrische Zugriffsgenehmigung	

Authentizität	digitale Signaturen	
	Empfängerbestätigung	
	Pin-Codes/TAN	
	passwortgeschützte Identifikationsverfahren	X
	Prüfsummenverfahren	X
Verbindlichkeit	Verträge	X

Das „X“ in der dritten Spalte der obigen Tabelle (wie auch in den folgenden Tabellen) bezeichnet das Zutreffen der Anforderung im Projekt.

2.2 Ordnungsmäßigkeit

Folgende Anforderungen ergeben sich aus der Ordnungsmäßigkeit:

- Vollständigkeit: Unter Vollständigkeit wird die lückenlose Erfassung aller rechnungslegungsrelevanten Geschäftsvorfälle verstanden.
- Richtigkeit: Die Richtigkeit der Geschäftsvorfälle sagt aus, dass diese inhaltlich zutreffend abzubilden sind.
- Zeitgerechtigkeit: Zeitgerechtigkeit stellt sicher, dass Geschäftsvorfälle möglichst unmittelbar nach Entstehung zu erfassen sind.
- Ordnung: Das Prinzip der Ordnung fordert, dass Buchungen sowohl in zeitlicher als auch in sachlicher Ordnung darstellbar sein müssen.
- Nachvollziehbarkeit: Nachvollziehbarkeit beschreibt, dass sachverständige Dritte in angemessener Zeit in der Lage sein müssen, sich einen Überblick über Geschäftsvorfälle und Unternehmenslage zu verschaffen.
- Unveränderlichkeit: Die Unveränderlichkeit sagt aus, dass Änderungen an Buchungseinträgen nur so durchgeführt werden dürfen, dass der ursprüngliche Inhalt feststellbar bleibt.
- Dokumentation: Die Dokumentation bezieht sich auf die Gewährleistung der Nachvollziehbarkeit des Buchführungsverfahrens; die Verfahrensdokumentation muss daher alle zum Verständnis der Rechnungslegung erforderlichen Bestandteilsbeschreibungen enthalten.
- Aufbewahrung: In der Aufbewahrung werden die Aufbewahrungspflichten für Journale, Konten, Belege, Abschlüsse sowie für die zum Verständnis der Buchführung erforderlichen Unterlagen geregelt.

Diese grundsätzlichen Anforderungen an die Ordnungsmäßigkeit lassen sich wie folgt konkretisieren, s. Tabelle 2:

Tab. 2 Anforderungen an die Ordnungsmäßigkeit

Hauptpunkt	Verfahren	
Vollständigkeit	Client-/Server-Verifizierung der Transaktionen	X
	Absender kann nur vollständige und richtige Transaktionen versenden	X
	Authentizität und Fehlerfreiheit der Daten vor Weiterverarbeitung klären, ansonsten ablehnen	X
	Übergabefehler müssen bei Schnittstellen erkannt werden können	X
	Ausschluss von Doppelverarbeitung	X
	Art der Transaktionsübermittlung klar definieren	
	Daten, die nicht über die definierten Kanäle kommen, sind abzulehnen	X
	vollzählige und lückenlose Aufzeichnung von Geschäftsvorfällen	X
	Erfassungskontrollen	X
	Plausibilitätskontrollen bei Dateieingaben	X
	automatisierte Vergabe von Datensatznummern	X
	Lückenanalyse oder Mehrfachbelegungsanalyse	X
	Aufzeichnungen in maschinell auswertbarer Form	X
	Zulässigkeit von zusammengefassten/verdichteten Aufzeichnungen	X
	Erfassung oder Verarbeitung darf nicht verhindert werden	X
Richtigkeit	automatisierte Autorisierungsverfahren eindeutig festlegen	X
	Dokumentation durch verfahrensmäßige Nachweise	X
	Geschäftsvorfälle inhaltlich zutreffend festhalten	X
	Geschäftsvorfälle bei kontenmäßiger Abbildung zutreffend kontieren	X
Zeitgerechtigkeit	unveränderbarer Zeitstempel für Transaktionen ist festzuhalten und zu dokumentieren	X
	technischer Ort des Eingangs ist zu dokumentieren	X
	Versand und Empfang sind durch Log-Dateien zu dokumentieren	X
	zwischengespeicherte Daten müssen vollständig abrufbar und bis dahin vorgehalten sein	X
	Journalfunktion: Vorgänge grundsätzlich laufend gebucht	X
	Kasseneinnahmen und -ausgaben sind täglich festzuhalten	X
Ordnung	Transaktionsschritte und Zusammenhänge sind nachvollziehbar zu protokollieren und dokumentieren	X

Hauptpunkt	Verfahren	
	getrennte Verbuchung von baren und unbaren Geschäftsvorfällen	X
	steuerbare, steuerfreie und steuerpflichtige Umsätze genügend kennzeichnen	X
	übersichtliche, eindeutige und nachvollziehbare Buchungen	X
	geordnete Darstellung bei doppelter Buchführung	X
	Kontenfunktion: Konten darstellbar als sachliche und einzeln geordnete Buchungen	X
Nachvollziehbarkeit	Geschäftsprozesse sind im Vorhinein zu definieren, wenn in ihrem Rahmen Transaktionsdaten verarbeitet werden	X
	Daten, die nicht über die definierten Strecken und Verfahren übermittelt wurden, müssen abgelehnt werden	X
	nicht abgestimmte Änderungen durch Vertrag mit IPS ausschließen	X
	lückenlose Aufbewahrung der Belege	X
	technische und organisatorische Regelungen zur Unveränderlichkeit der empfangenen Daten	X
	Nachvollziehbarkeit von Buchführungs-, Aufzeichnungsverfahren und Verarbeitung einzelner Geschäftsvorfälle	X
	Aufzeichnungszweck für die Besteuerung muss erfüllt werden	X
	sachverständige Dritte müssen in kurzer Zeit Überblick erhalten können	X
	Entstehung und Abwicklung müssen lückenlos verfolgbar sein	X
	progressive Prüfung muss über Dauer der Aufbewahrungspflicht möglich sein	X
	retrograde Prüfung muss über Dauer der Aufbewahrungspflicht möglich sein	X
	aussagekräftige und vollständige Verfahrensdokumentation	X
Unveränderlichkeit	nach Buchungszeitpunkt dürfen keine Veränderungen vorgenommen werden, so dass der ursprüngliche Inhalt nicht feststellbar ist	X
	bei späteren Eintragungen oder Aufzeichnungen müssen ursprünglicher Inhalt und die Tatsache, dass Veränderungen vorgenommen wurden, erkennbar sein	X
Dokumentation	eingesetzte Hard- und Software	X
	Netzwerkarchitektur, insbesondere ISP-Anbindung	X
	die zur Übertragung verwendeten Protokolle	X
	verwendete Verschlüsselung	X
	eingesetzte Signaturverfahren	X
	Datenflusspläne vom Daten-Eingang im Unternehmen bis	X

Hauptpunkt	Verfahren	
	zu den Rechnungslegungssystemen	
	Schnittstellen sowie darauf bezogene Kontrollen	X
	Autorisierungsverfahren einschließlich der Verfahren zur Generierung automatisierter Buchungen	X
	Rechte und Pflichten von beauftragten Providern	X
	manuelle Nachkorrektur unvollständiger oder nicht format-gerechter Daten	X
	Aufgabenstellung der IT-Anwendung im Kontext der eingesetzten Module	X
	Datenorganisation und Datenstrukturen	X
	veränderbare Tabelleninhalte, die bei der Erzeugung einer Buchung herangezogen werden	X
	programmierte Verarbeitungsregeln einschließlich der implementierten Eingabe- und Verarbeitungskontrollen	X
	programminterne Fehlerbehandlungsverfahren	X
	Schlüsselverzeichnisse	X
	Schnittstellen zu anderen Systemen	X
Auf-bewahrung	Journale, Konten, Belege und Abschlüsse sind für 10 Jahre aufzubewahren	X
	bei Individualsoftware ist der Programm-Quellcode in maschinenlesbarer Form für 10 Jahre aufzubewahren	X
	Systemprotokolle und sonstige technische Aufzeichnungen (Logs etc.) sind für 10 Jahre aufzubewahren	X
	bei Outsourcing muss der Servicegeber vertraglich verpflichtet werden, die Unterlagen aufzubewahren	X

2.3 IT-Infrastruktur

Folgende Anforderungen ergeben sich an die IT-Infrastruktur:

- Physische Sicherheitsmaßnahmen: Unter physischen Sicherheitsmaßnahmen werden physische Maßnahmen zur Sicherstellung der Betriebsbereitschaft oder Eingrenzung von Schäden verstanden.
- Logische Zugriffskontrollen: Logische Zugriffskontrollen dienen der Beschränkung der Zugriffe auf sicherheitsrelevante Anwendungen und Daten.
- Datensicherungs-/Auslagerungsverfahren: Datensicherungs- und Auslagerungsverfahren beziehen sich auf das Vorgehen zur richtigen Sicherung der Betriebsdaten.

- Wiederherstellungsverfahren: Das Wiederherstellungsverfahren bezieht sich auf das Verhalten bei Not- und Katastrophenfall zur Wiederherstellung der Betriebsbereitschaft der Systeme und Anwendungen.

Diese grundsätzlichen allgemeinen Anforderungen an die IT-Infrastruktur lassen sich wie folgt konkretisieren, s. Tabelle 3:

Tab. 3 Anforderungen an die IT-Infrastruktur

Hauptpunkt	Verfahren	
physische Sicherheitsmaßnahmen	bauliche Maßnahmen	
	Zugangskontrollen	
	Feuerschutzmaßnahmen	
	sichere Stromversorgung	
logische Zugriffskontrollen	Benutzer-ID	X
	Passwörter	X
	Berechtigungsverwaltung	X
Datensicherungs- / Auslagerungsverfahren	Tages-, Monats-, Jahressicherung	X
	Inventarisierung der Sicherheitsmedien	X
	Auslagerung der Medien	X
Wiederherstellungsverfahren	Dokumentation von Abläufen	
	organisatorische Regelungen	

Neben diesen allgemeinen Anforderungen an die IT-Infrastruktur lassen sich weitere fünf spezielle Anforderungsbereiche identifizieren.

2.3.1 Sicherung der Betriebsbereitschaft

Die Sicherung der Betriebsbereitschaft umfasst mit Maßnahmen im Soft- und Hardwarebereich, die dafür sorgen, dass die Geschäftsprozesse und Informationsflüsse nicht gestört oder unterbrochen werden, vgl. Tabelle 4.

Tab. 4 Anforderungen an die Sicherung der Betriebsbereitschaft

Hauptpunkt	Verfahren	
kurzfristiger Ersatz	redundante Systemkomponenten	
	fehlertolerante Systeme	
Katastrophenfall-Szenarien	voneinander getrennte Rechenzentren	
	Backup-Rechner/-Server	
	Servicevereinbarungen	
Sicherheitskonzept dokumentieren und an betroffene Mitarbeiter ausgeben		
Training und Test von Fehlerfällen		

2.3.2 IT-Anwendungen

Der Bereich „IT-Anwendungen“ beschäftigt sich mit der Ordnungsmäßigkeit von Anwendungen in Bezug auf die Grundsätze ordnungsgemäßer Buchführung. Hierzu ergeben sich folgende Anforderungen, s. Tabelle 5.

Hauptpunkt	Verfahren	
Generelle Kontrollen in der …	… Entwicklung von Individualsoftware	X
	… Auswahl, Beschaffung, Einführung von Standard-Software	
	… Test-/Freigabeverfahren	
	… Änderung von IT-Anwendungen	
Eingabekontrollen	Datumskontrolle	X
	Muss-/Kann-Felder	X
	Soll-/Habenkombinationen	X
Verarbeitungskontrollen	Kontrollnummern	X
	Recoverymaßnahmen nach Fehlern	X
Ausgabekontrollen	Reports aus Datenbanken oder Schnittstellen	

Tab. 5 Anforderungen an IT-Anwendungen

2.3.3 IT-gestützte Geschäftsprozesse

Es geht in diesem Bereich um die Gestaltung von IT-gestützten Geschäftsprozessen, wobei diese entweder auf Basis einer funktional ausgerichteten oder auf Basis einer geschäftsprozessorientierten Organisation erfolgen kann, s. Tabelle 6

Hauptpunkt	Verfahren	
funktional ausgerichtete Organisation	Transaktionsfreigabeverfahren	X
Geschäftsprozessorientierte Organisation	Transaktionsberechtigungen für Geschäftsprozesse	X

Tab. 6 Anforderungen an IT-gestützte Geschäftsprozesse

2.3.4 IT-Umfeld & Organisation

Beim IT-Umfeld geht es um Anforderungen bzgl. der Eingliederung des Systems in das IT-Umfeld und die Unternehmensorganisation, s. Tabelle 7.

Verfahren	
Problembewusstsein schaffen	X
Überwachung der Umsetzung durch IT-Kontrollsystem	X
Einordnung der IT in die Organisationsstruktur	

Tab. 7 Anforderungen an IT-Umfeld & Organisation

2.3.5 Überwachung des IT-Kontrollsystems

Die Überwachung des IT-Kontrollsystems dient der Sicherstellung der Funktionalität und der Bewertung der Effizienz des eingesetzten Systems. Es ergeben sich folgende Anforderungen, s. Tabelle 8.

Verfahren	
Durchsicht von Fehler-/Ausnahmeberichten	X
Benchmarks	
Beurteilen, ob das IT-Kontrollsystem sowohl angemessen als auch kontinuierlich funktioniert	X
Überprüfung von Dateiinhalten in der Firewall	
Sicherheitskonzept und IT-Kontrollsystem ist in regelmäßigen Abständen auf Angemessenheit und Wirksamkeit hin zu überwachen	X
Programmgestützte Angriffssimulationen (Penetration-Test-Verfahren)	
Einsatz spezieller Programme („Scanner“)	

Tab. 8 Anforderungen an die Überwachung des IT-Kontrollsystems

3. Allgemeine Anforderungen

Allgemeine Anforderungen

Die Stellungnahme IDW RS FAIT 5 sowie die Normen ISO/IEC 27017 und DIN SPEC 66286 beschäftigen sich mit dem ordnungsmäßigen Einsatz von Cloud-Computing-Technologien im Unternehmen. Hierbei werden verschiedenste gesetzliche Aspekte zu IT-Sicherheit, Unternehmensorganisation und den entsprechenden Verantwortlichkeiten beim Einsatz von Cloud Computing angesprochen, woraus sich Anforderungen an das auslagernde Unternehmen ableiten lassen. Die technischen und organisatorischen Anforderungen wirken sich dabei auf die Vorbereitungs-, Aufbau- und Nutzungsphase aus und schließen ebenfalls eine Nutzungsbeendigungsphase mit ein. Es ergeben sich zahlreiche konkrete Anforderungen, s. Tabelle 9.

Hauptpunkt	Verfahren	
Kontrollumfeld und Organisation	Risikobewusstsein schaffen	X
	Überwachung des Austauschs bei Subdienstleistern	
	Sicherstellung der Unveränderbarkeit	X
	Sicherstellung der Nicht-Beendigung des Geschäftsverhältnisses	X
	keine Neubeauftragung von Dienstleistungen ohne Zustimmung	

Tab. 9 Allgemeine Anforderungen

	Aktualität der IKS-Maßnahmen regelmäßig prüfen	X
	Angemessenheit der IKS-Maßnahmen regelmäßig prüfen	X
	Verzögerungsgründe bzgl. vereinbarten Berichten sind zu klären	X
	bei Verzögerung: Ist die IKS-Wirksamkeit beeinträchtigt?	X
	bei Verzögerung: Ist die Ordnungsmäßigkeit der Buchführung beeinträchtigt oder fehlerhaft?	X
	Sicherstellen von Nicht-Vermischung von unternehmensinternen Daten mit Daten anderer Unternehmen	X
	Eskalationsverfahren für Nichterbringung von vertragsgerechten Leistungen	X
	Verfahrensdokumentation und SLAs bzgl. Aufgaben, Tätigkeiten und Verantwortlichkeiten	X
	Koordination von Dienstleistungsänderungen	X
	Wirksamkeit physischer Sicherheitsmaßnahmen ist zu gewährleisten	X
	Zugriffe privilegierter Nutzer sind regelmäßig zu kontrollieren	X
IT-Infrastruktur	Verfahren für Regel- und Notfallbetrieb müssen vollständig und nachvollziehbar dokumentiert und durchgeführt sein	X
	Überblick über IT-Infrastruktur, Schutzmaßnahmen, Sicherheitsvorkehrungen und IT-Prozesse verschaffen	X
	Verzahnung der Maßnahmen für Not-/Katastrophenfall zwischen den Unternehmen	X
	Wirksamkeit der Kontrollen regelmäßig prüfen und beurteilen	X
	logischer Zugriffsschutz bei beiden Unternehmen	X
	Netzwerke trennen	X
	administrative/privilegierte Berechtigungen restriktiv vergeben	X
	Veränderungen der IT-Infrastruktur planen, testen, umsetzen und dokumentieren	X
	vertragsgemäße, vollständige Löschung der Daten	X
	Leistungserbringung regelmäßig kontrollieren	X
	Redundanz bei kritischen Systembestandteilen sicherstellen	X
IT-Anwendungen	Erfüllung der Beleg-, Journal- und Kontenfunktion	X
	Erfüllung der Anforderungen an die Anwendungssicherheit	X
	Anforderungen an die rechnungslegungsrelevanten Verarbeitungsregeln	X
	Überwachungsmaßnahmen und generelle Kontrollen zur Sicherstellung der Ordnungsmäßigkeit	X
	Softwarebescheinigung zu Kontrollen	X
	Eingabe-, Verarbeitungs- und Ausgabekontrollen entsprechend der geforderten fachlichen Konzeption	X

	Projektmanagement praktizieren, das der Projektgröße angemessen ist	
	Einhaltung der geforderten Richtlinien zum Qualitätsmanagement	X
	Verwendung festgelegter Normierungen und Namenskonventionen	
	angemessene Toolunterstützung für Design, Realisierung, Test und Freigabe	X
	angemessenes Change Management	
	nur vom auslagernden Unternehmen autorisierte Anpassungen sind zu genehmigen	
	Integrationstests bei der Übertragung von Daten	
	Kontrolle der Angemessenheit und Wirksamkeit des Berechtigungssystems	X
	systematische Auswertung anwendungsbezogener Verarbeitungsprotokolle	X
	Vollständigkeit, Richtigkeit, Zeitnähe sicherstellen	X
	Überwachung der ausgelagerten Dienstleistungen	X
	Nachweise kritischer Systemberechtigungen und -nutzungen	X
	Vorhandensein von Protokollen über nicht erfolgreiche Systemzugriffe	X
	Vorhandensein von Protokollen über unerwartete Ereignisse	X
	Vorhandensein von Nachweisen über Systemänderungen	X
	Vorhandensein von Nachweisen der vom Dienstleistungsunternehmen vorgenommenen Tests	
	Revisionsberichte der internen Revision des Dienstleistungsunternehmens	
	Freigabe von Anpassungen und Einstellungen freigegeben	X
	angemessene personelle und technische Ressourcen für Tests und Freigaben bei Änderungen	X
	kompensierende Kontrollen bei fehlerhaften Änderungen	X
	Aufbewahrung von Verfahrensdokumentation, Verarbeitungsprotokollen, Kontrollnachweisen, technischen Aufzeichnungen	X
	Dokumentationsaktualisierung bei Änderungen an IT-Anwendung	X
IT-gestützte Geschäftsprozesse	Regelung, welche anwendungsbezogenen und prozessintegrierten Kontrollen bei der Erfassung und Verarbeitung bestehen	X
	Regelung, wie/in welchem Format rechnungslegungsrelevante Daten übergeben werden	X
	Schaffung standardisierter organisatorischer und technischer Prozessschnittstellen	X

	angemessene Verzahnung der ausgelagerten Prozesse mit den unternehmensinternen Prozessen	X
	Einrichtung von Schnittstellenkontrollen	X
	Gewährleistung der Sicherheit und Ordnungsmäßigkeit der rechnungslegungsrelevanten Daten	X
	Umfassendes internes Kontrollsystem, das nicht nur für Teilprozesse oder Teilsysteme implementiert ist	X

4. Konzeption und Beschreibung einer automatisierten Kontrolle auf Doppelzahlungen

Automatisierte Kontrolle auf Doppelzahlung

Im Folgenden soll als Beispiel für eine automatisierte Kontrolle eine Kontrolle auf Doppelzahlungen Von Doppelzahlungen beschreiben werden. Diese Kontrolle stellt die Richtigkeit des Geschäftsvorfalls einer Bezahlung beschaffter Güter oder Dienstleitungen sicher, indem sie kontrolliert, ob diese inhaltlich zutreffend abgebildet ist. Sie erfüllt somit Anforderungen an die Ordnungsmäßigkeit.[2]

Begriff „Doppelzahlung“

Von „Doppelzahlung“ spricht man dann, wenn eine Firma für ein- und dieselbe Lieferung oder Leistung mehr als einmal den vollen Gegenwert bezahlt. Im Sprachgebrauch hat sich „Doppelzahlung“ gegenüber dem eigentlich geeigneteren Begriff (da die Zahlung ja auch öfter als zweimal erfolgen kann) „Mehrfachzahlung“ durchgesetzt. In der Regel geht einer Ausgangsrechnung eine Buchung bzw. genauer die Erfassung einer Verbindlichkeit (Rechnung) voraus. Gemäß dieser Logik muss einer Doppel- bzw. Mehrfachzahlung auch eine Doppel- bzw. Mehrfach(rechnungs-)buchung vorausgehen. Folglich ist nicht die Doppelzahlung der Kern des Problems, sondern die Doppelbuchung der Rechnung.

4.1 Risiko der Doppelzahlung

Risiko der Doppelzahlung

Der Betrag, der über eine Doppelzahlung das Unternehmen verlässt, erhöht die Kosten und mindert den Gewinn um den gleichen Wert. Das Vermögen des Unternehmens verringert sich unnötigerweise, da keine „echte“ Verbindlichkeit gegenübersteht, denn diese wurde mit der Erstzahlung bereits beglichen.

[2] Vgl. die Ausführungen in Abschnitt 2.2, insb. Tabelle 2.

4.1.1 Mögliche Ursachen des Risikos

Risikoursachen

Mögliche Ursachen des Risikos auf Doppelzahlung sind:

- Unzureichende Richtlinien
- Mangelhafte Kontrollen (Buchungskontrollen im Vorfeld der Zahlungen, Zahlungsausgangskontrollen)
- Mangelhafte tochtergesellschaftsübergreifende Kooperation
- Fehlerhafte Stammdatenorganisation

4.1.2 Technische Gründe für Doppelzahlungen

Technische Gründe

Mögliche technische Gründe für Doppelzahlungen sind:

- Eine Eingangsrechnung wird im MM-Modul mit Bestellbezug und zusätzlich direkt in FI ohne Bestellbezug erfasst.
- Eine dem Mahnschreiben beiliegende Rechnung wird erneut erfasst und über eine manuelle Zahlung ausgeglichen.
- Eine Rechnung oder Rechnungskopie wird nochmals bei einem Stammdatenduplikat des Lieferanten erfasst.
- Ein Lieferant schickt die gleiche Rechnung an unterschiedliche Buchungskreise, also Gesellschaften.

4.1.3 Identifizierung der relevanten Tabellen sowie Felder in SAP ERP

Als Grundlage der Automatisierung einer Kontrolle müssen für die im Labor für Interne Kontrollsysteme und Datenanalyse vorhandene ERP-Umgebung verschiedene SAP-Tabellen ermittelt werden, die den betroffenen Transaktionen zugrunde liegen.

(1) Tabelle BSAK

Neben anderen ausgezifferten kreditorischen Vorgängen sind in der Tabelle „BSAK“ vor allem die für die Analyse notwendigen Eingangsrechnungen als FI-Beleg und auch die Zahlungstransaktionen, mit denen die Rechnungen manuell oder über den Zahllauf ausgeglichen wurden, zu finden. Folgende Felder sind für die Automatisierung der Kontrolle relevant, s. Tabelle 10.

Tab. 10
Felder aus Tabelle BSAK Nebenbuch Kreditoren – ausgeglichene Posten

Name	Feldbezeichnung	Kommentar
MANDT	Mandant	
BUKRS	Buchungskreis	Bildet mit Belegnummer und Geschäftsjahr den eindeutigen Belegschlüssel.
LIFNR	Kreditor	Die eindeutige Nummer des Kreditors innerhalb des Systems.
AUGDT	Ausgleichsdatum	Das Buchungsdatum des unten stehenden Ausgleichsbeleges.
AUGBL	Ausgleichsbeleg	Die Nummer des Belegs, der zum Ausgleich geführt hat.
GJAHR	Geschäftsjahr	Bildet mit Belegnummer und Buchungskreis den eindeutigen Belegschlüssel.
BELNR	Belegnummer	Bildet mit Geschäftsjahr und Buchungskreis den eindeutigen Belegschlüssel.
BUDAT	Buchungsdatum	
WAERS	Währung(sschlüssel)	Währung des Belegs, die sich auf das Feld WRBTR bezieht. Relevant für die Doppelzahlungsanalyse.
XBLNR	Referenz	Beinhaltet die Referenznummer, also häufig die Rechnungsnummer, die auf der Lieferantenrechnung aufgedruckt ist. Relevant für die Doppelzahlungsanalyse.
BSCHL	Buchungsschlüssel	Der Buchungsschlüssel wird benötigt, um die Verbindung zur Tabelle TBSL herzustellen, in der die Attribute der Buchungsschlüssel gespeichert sind. Die wesentlichen, für die Analyse interessanten Eigenschaften, sind die Kennzeichen „Umsatzwirksam“ und „Zahlungsvorgang“.
SHKZG	Soll/Haben-Kennzeichen	Ausgehende Zahlungen sind – in Kombination mit dem Kennzeichen „Zahlungsvorgang“ = „X“ – mit Soll/Haben-Kennzeichen „S“ versehen. Eingebuchte Rechnungen mit Soll/Haben-Kennzeichen „H“ in Verbindung mit dem Kennzeichen „Umsatzwirksam“ aus der Tabelle TBSL der Buchungsschlüssel.
DMBTR	Betrag Hauswährung	Der Betrag in der Währung des Buchungskreises. Gerade bei Belegen in Fremdwährung kann dieser Betrag unterschiedlich sein, obwohl möglicherweise eine Doppelzahlung vorliegt.
WRBTR	Betrag	Der Betrag in Fremdwährung. Falls es sich um einen Beleg handelt, der in der gleichen Währung gebucht ist wie die Hauswährung, ist dieser Wert gleich dem Wert aus Feld DMBTR.
XZAHL	Zahlungsvorgang	Handelt es sich um einen Zahlungsvorgang, ist dieses Feld mit dem Kennzeichen „X“ gefüllt.

Name	Feldbezeichnung	Kommentar
SHTXT	Text	Kann zusätzliche Textinformationen beinhalten, die für die Doppelzahlungsanalyse interessant sein können.

(2) Tabelle BSIK

Die Tabelle „BSIK“ der offenen Posten teilt sich die Datenstruktur mit der Tabelle „BSAK“. In BSIK sind lediglich die Felder „AUGBL“ (Ausgleichsbeleg) und „BUDAT“ (Buchungsdatum) nicht gefüllt.

(3) Tabelle LFB1

In der Tabelle „LFB1“ befinden sich die buchungskreisabhängigen Lieferantenstammdaten, wie etwa Zahlungsverkehrsdaten (Zahlungsweg etc.) oder Einstellungen zur Prüfung auf doppelte Rechnung, s. Tabelle 11.

Name	Feldbezeichnung	Kommentar
LIFNR	Kreditor	
BUKRS	Buchungskreis	Bildet mit Lieferantennummer den eindeutigen Schlüssel für eine Verknüpfung in die Tabellen der Buchhaltung, z. B. BSAK
REPRF	Prüfung auf doppelte Rechnungen	Kennzeichen, ob Prüfung auf doppelte Rechnungen für diesen Lieferanten in diesem Buchungskreis durchgeführt wird.

Tab. 11 Felder aus Tabelle LFB1 Stammdaten Lieferanten (Buchungskreis)

(4) Tabelle TBSL

Die Tabelle „TBSL“ mit den Buchungsschlüsseln ist notwendig, da das für die Analyse wichtige Kennzeichen „Umsatzwirksam“ nicht in den Kreditorennebenbüchern geführt wird. Es ist dort nur implizit über den Buchungsschlüssel realisiert und muss zur expliziten Analyse über die Tabelle „TBSL“ – beispielsweise durch eine Verknüpfung – hinzugefügt werden. Folgende Felder sind für die Automatisierung der Kontrolle relevant, s. Tabelle 12.

Name	Feldbezeichnung	Kommentar
BSCHL	Buchungsschlüssel	
SHKZG	Soll/Haben-Kennzeichen	
KOART	Kontoart	

Tab. 12 Felder aus Tabelle TBSL Buchungsschlüssel

Name	Feldbezeichnung	Kommentar
XUMSW	Umsatzwirksam	Kennzeichnet mit einem „X“ die Einbuchung von Verbindlichkeiten oder Forderungen. Inhaltliche Aussagekraft wird nur durch Kombination mit dem Soll/Haben-Kennzeichen erreicht.
FAUS1	Feldauswahl	
XZAHL	Zahlungsvorgang	Kennzeichnet mit einem „X“ Zahlungstransaktionen. Inhaltliche Aussagekraft über die Art der Zahlungstransaktion (ein- oder ausgehend) wird nur durch Kombination mit dem Soll/Haben-Kennzeichen erreicht.

4.1.4 Inhalt der Kontrolle

Im Rahmen der Kontrolle auf Doppelzahlung werden im Einkauf die Buchungen auf eventuelle Doppelzahlungen kontrolliert. Das Soll besteht darin, dass keine doppelte Zahlung vorliegt. Das Ist besteht in den vollzogenen Zahlungen bzw. den entsprechenden Buchungsdaten. Der Soll/Ist-Vergleich ergibt die Doppelzahlung(en).

4.1.5 Ergebnis der Kontrolle

Der Administrator (oder Prüfer) erhält „per Knopfdruck“ Informationen (z. B. in Form einer Datenliste) über die Doppelzahlungen im Einkauf.

4.2 Prototypische Umsetzung einer automatisierten Kontrolle auf Doppelzahlungen

Für die Realisierung der automatisierten Kontrolle auf Doppelzahlungen werden die Datenanalysesoftware „IDEA“, das Datenexport-Tool „SmartExporter“ und das CCM-System „CaseWare Monitor“ der Fa. Audicon GmbH verwendet. Die prototypische Umsetzung der Kontrolle erfolgt in Form der Bereitstellung eines sogenannten IDEA-Skripts und beinhaltet

- den Datenimport aus dem SAP-System „IDES“ mit Hilfe von SmartExporter,
- die Verarbeitung der Daten in IDEA und
- die Implementation der automatisierten Kontrolle in CaseWare Monitor als prozessintegrierte Kontrolle, die das IKS am Beispiel der IDES AG durch Continuous Monitoring unterstützt.

4.2.1 Export der Daten aus SAP via SmartExporter

Die identifizierten SAP-Tabellen lassen sich mit Hilfe des SmartExporters exportieren. Im ersten Schritt wird dazu der Import-Assistent in IDEA aufgerufen. Dieser Schritt ist notwendig, um die aus SAP exportierten Daten anschließend in IDEA zu importieren. Der Import-Assistent bietet diverse Formate für den Import an. Der direkte Export aus SAP wird von IDEA berücksichtigt und es wird dementsprechend der Eintrag „SAP SmartExporter“ unter den Formaten angeboten. Durch die Auswahl öffnet sich die Startseite des SmartExporters, siehe Abbildung 1.

Abb. 1 Screenshot SmartExporter: Datenanforderung zur Kontrolle auf Doppelzahlungen

Bei der Erstnutzung des SmartExporters ist es notwendig, die Verbindung mit dem SAP-System zu konfigurieren. Unter dem Punkt "Verbindungen verwalten" gelangt man zu der Konfiguration der Verbindungen. In den Registerreitern „Systemdaten“ und „Anmeldedaten“ sind dementsprechend die SAP-Anmeldedaten einzutragen. Der Registerreiter „Diagnose“ bietet die Möglichkeit, die Verbindung zu testen. Nach der erfolgreichen Einrichtung der Verbindung ist es jetzt möglich, ausgehend von der Startseite eine Datenanforderung zu erstellen. Die Erstellung der Datenanforderung besteht aus acht Schritten, beginnend mit der Einführung, die aus dem Namen und einer optionalen Notiz besteht, siehe Abbildung 2.

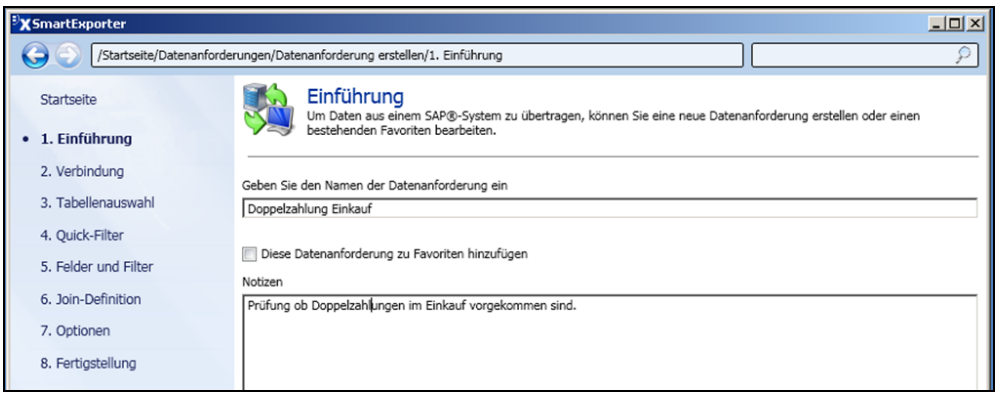

Abb. 2 Screenshot SmartExporter: Datenanforderung zur Einführung zur Kontrolle auf Doppelzahlungen

Wenn die Datenanforderung zukünftig mehrfach genutzt wird, besteht die Möglichkeit, diese den Favoriten hinzuzufügen.

Der nächste Schritt ist die Auswahl der zuvor erstellten SAP-Verbindung, gefolgt vom 3. Schritt, der Tabellenauswahl, siehe Abbildung 3.

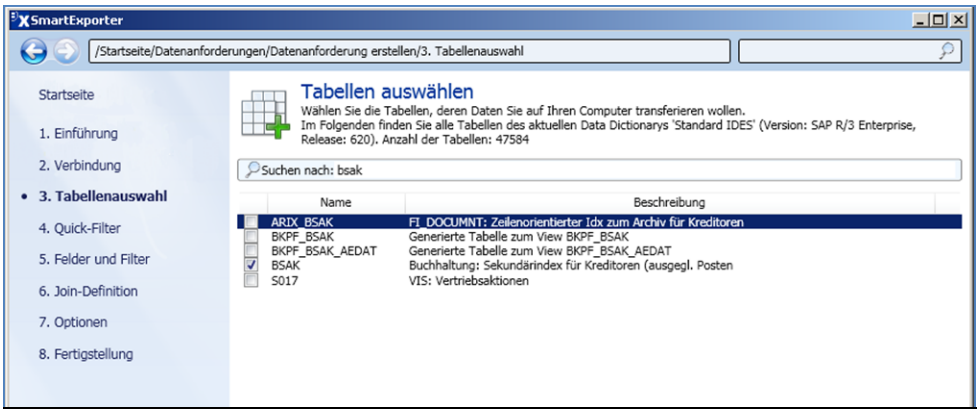

Abb. 3
Screenshot SmartExporter: Tabellenauswahl BSAK zur Kontrolle auf Doppelzahlungen

Im nächsten Schritt kann optional eine Filterung der Daten anhand von Kriterien vorgenommen werden, siehe Abbildung 4.

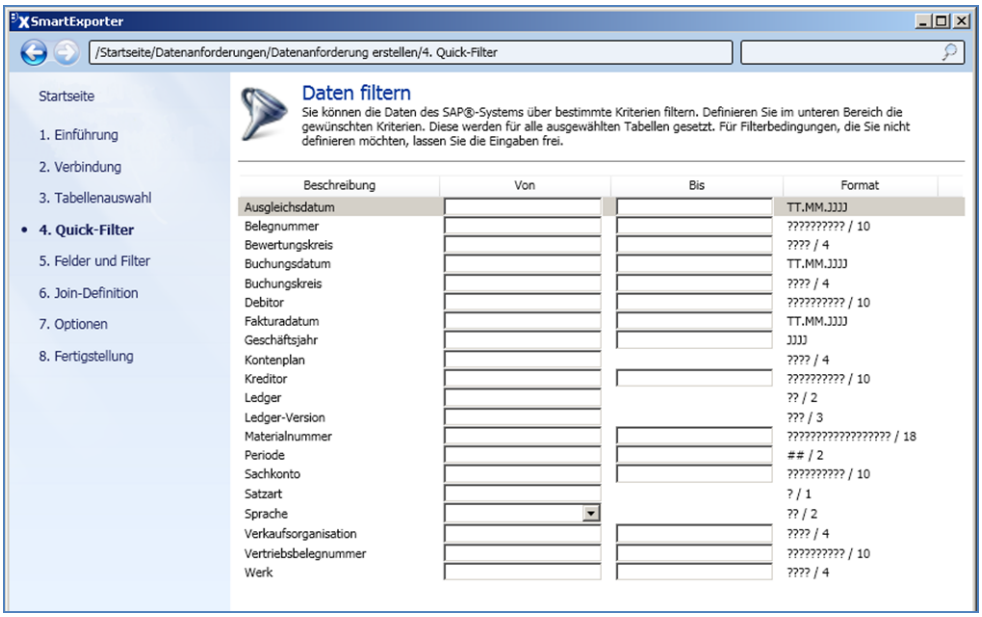

Abb. 4
Screenshot SmartExporter: Daten filtern zur Kontrolle auf Doppelzahlungen

Im Rahmen dieser Kontrolle wird eine Filterung im späteren Verlauf durch IDEA vorgenommen. Im 5. Schritt werden die zuvor identifizierten Felder der Tabelle „BSAK“ ausgewählt, siehe Abbildung 5.

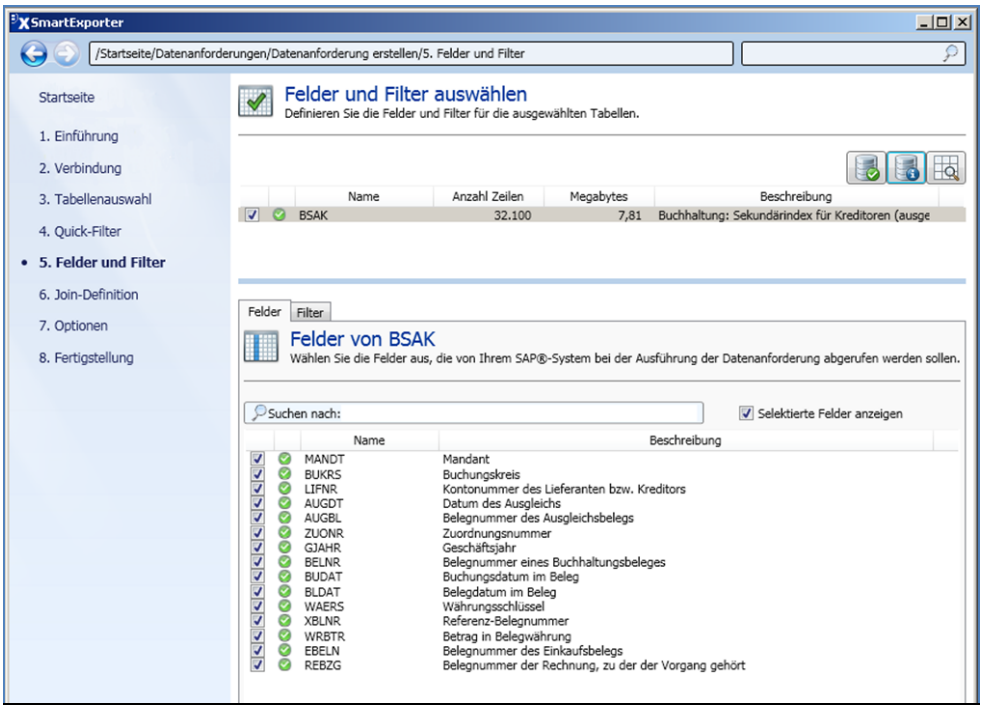

Abb. 5
Screenshot SmartExporter: Felder und Filter auswählen zur Kontrolle auf Doppelzahlungen

Aus der Tabelle „VBAK“ werden die in obiger Abbildung dargestellten Felder ausgewählt. Wie in der Abbildung zu sehen ist, bietet SmartExporter die Möglichkeit, innerhalb der Tabelle nach Spaltennamen (Feldnamen) zu suchen und nur die selektierten Felder anzeigen zu lassen. Weiterhin besteht die Möglichkeit, vor dem Export der Daten die Anzahl der Zeilen und die Größe in Megabytes der Anfrage anzeigen zulassen. Dazu wird in dem Feldauswahlbildschirm das mittlere der drei Symbole am rechten oberen Rand ausgewählt.

Im nächsten Schritt können bereits im Export die Tabellen mittels "Join" verbunden werden, siehe Abbildung 6.

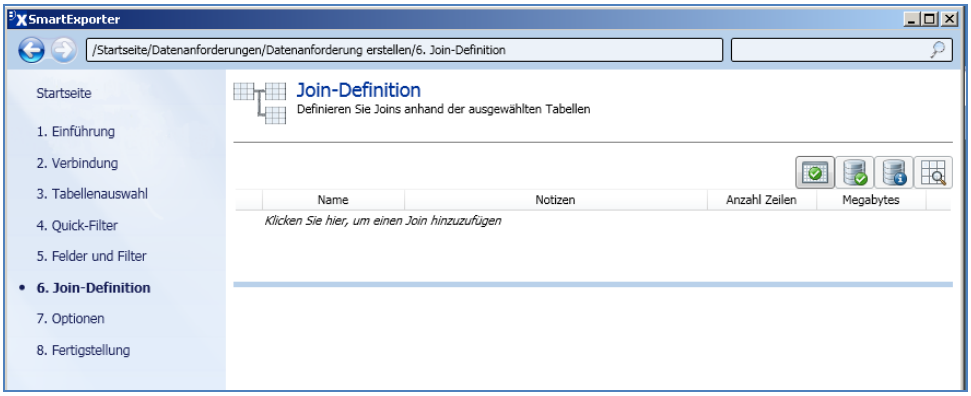

Abb. 6
Screenshot SmartExporter: Join-Definition zur Kontrolle auf Doppelzahlungen

Die Verbindung der beiden Tabellen kann jedoch auch im IDEA-Makro durchgeführt werden. In dieser beispielhaften Kontrolle erfolgt die Verbindung, im Rahmen des IDEA-Makros.

Im 7. Schritt werden die Optionen für die Datenanforderung definiert, siehe Abbildung 7.

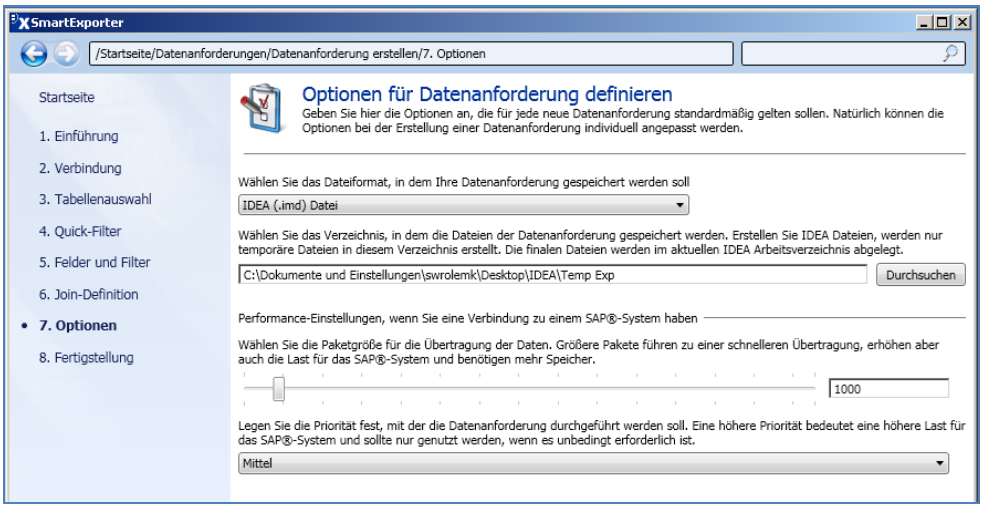

Abb. 7
Screenshot SmartExporter: Optionen für Datenanforderung definieren zur Kontrolle auf Doppelzahlungen

Hierbei muss das Datenformat „IDEA (.imd) Datei“ ausgewählt werden. Damit ist gewährleistet, dass die vom SAP-System exportierten Daten anschließend in IDEA importiert werden (können). Auch muss das Verzeichnis, in dem die Dateien der Datenanforderung gespeichert werden, angegeben werden. Im Rahmen dieser und der noch folgenden Kontrollen muss das aktuelle IDEA-Arbeitsverzeichnis gewählt werden. Zu den weiteren Optionen gehört die Änderung der Paketgröße, die bei einer Erhöhung zu einer schnelleren Datenübertragung führt, und die Priorität, die nur erhöht werden sollte, wenn es unbedingt erforderlich ist. Größere Pakete und eine Erhöhung der Priorität haben eine höhere Last des SAP-Systems zur Folge.

Der letzte Schritt, die Fertigstellung, bietet mehrere Möglichkeiten, siehe Abbildung 8.

Vor dem Start der Datenanforderung ist es ratsam, sich die Details über die Datenanforderung anzeigen zu lassen. Zusätzlich kann die Datenanforderung gespeichert oder zu einem gewünschten Zeitpunkt gestartet werden. Wenn diese Datenanforderung auf einer anderen SmartExporter-Instanz geöffnet werden soll, muss diese offline als XML-Datei gespeichert werden. Zum Abschluss wird die Datenanforderung gestartet, dadurch werden die

Daten aus dem SAP-System exportiert und anschließend in IDEA importiert.

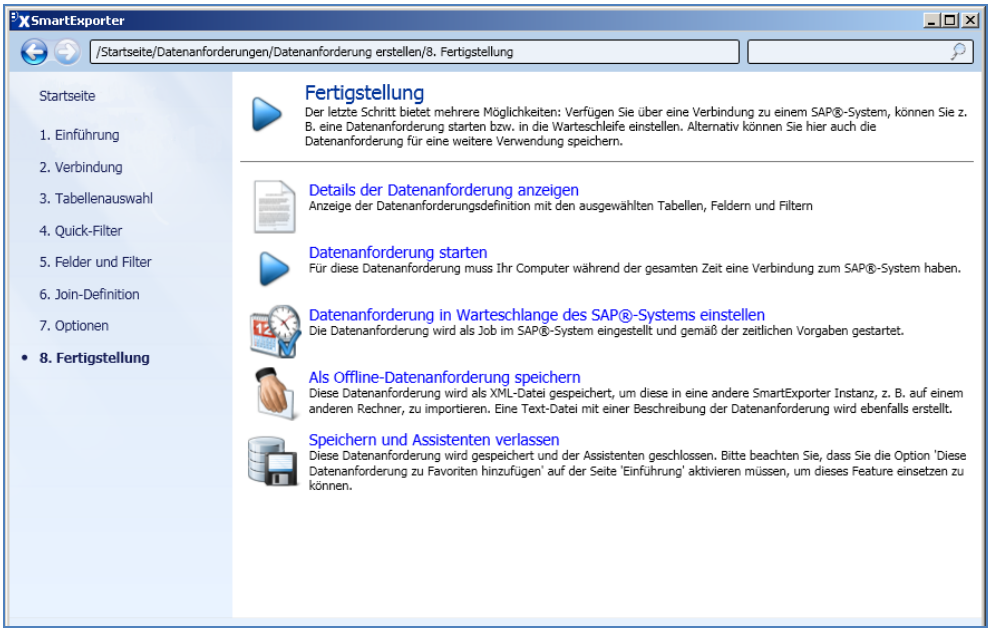

Abb. 8
Screenshot SmartExporter: Fertigstellung zur Kontrolle auf Doppelzahlungen

4.2.2 Umsetzung der Kontrolle in IDEA-Script

Nach dem Import der Tabelle mittels SmartExporter kann die Kontrolle über "Mehrfachbelegung-Ermittlung" umgesetzt werden, siehe Abbildung 9.

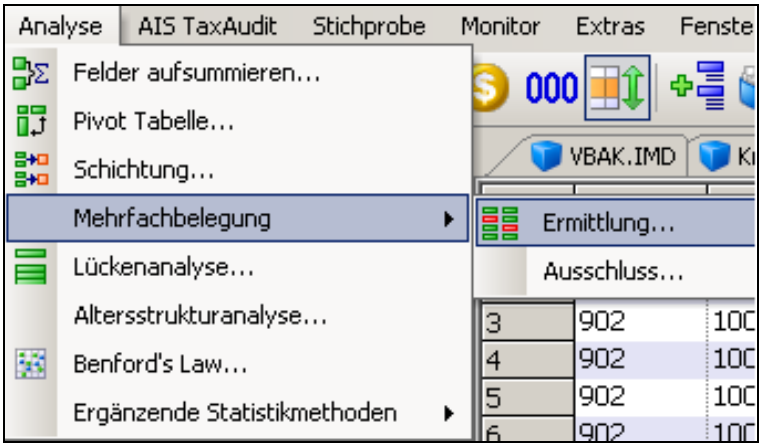

Abb. 9
Screenshot SmartExporter: Mehrfachbelegung Ermittlung

Die Felder für den Vergleich auf Übereinstimmung werden unter Schlüssel definiert, siehe Abbildung 10.

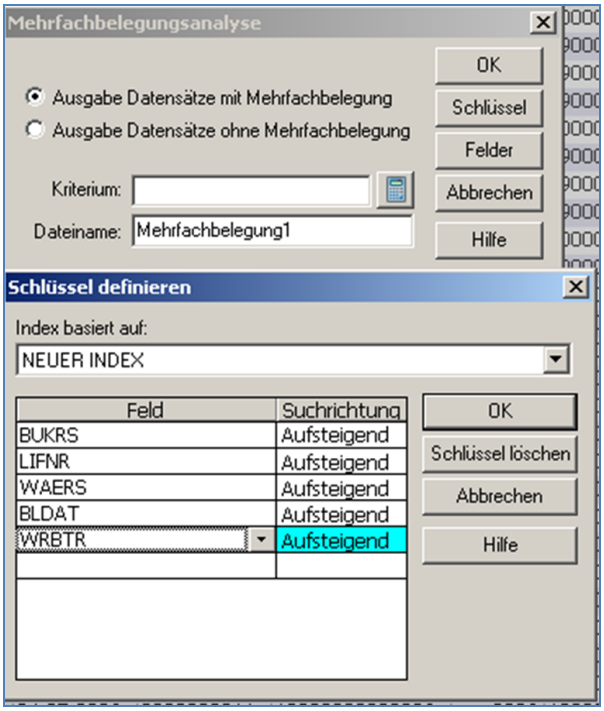

Abb. 10
Screenshot SmartExporter: Mehrfachbelegung Schlüssel definieren

Nach der Bestätigung, listet IDEA alle Datensätze mit identischen Schlüsselwerten auf, siehe Abbildung 11.

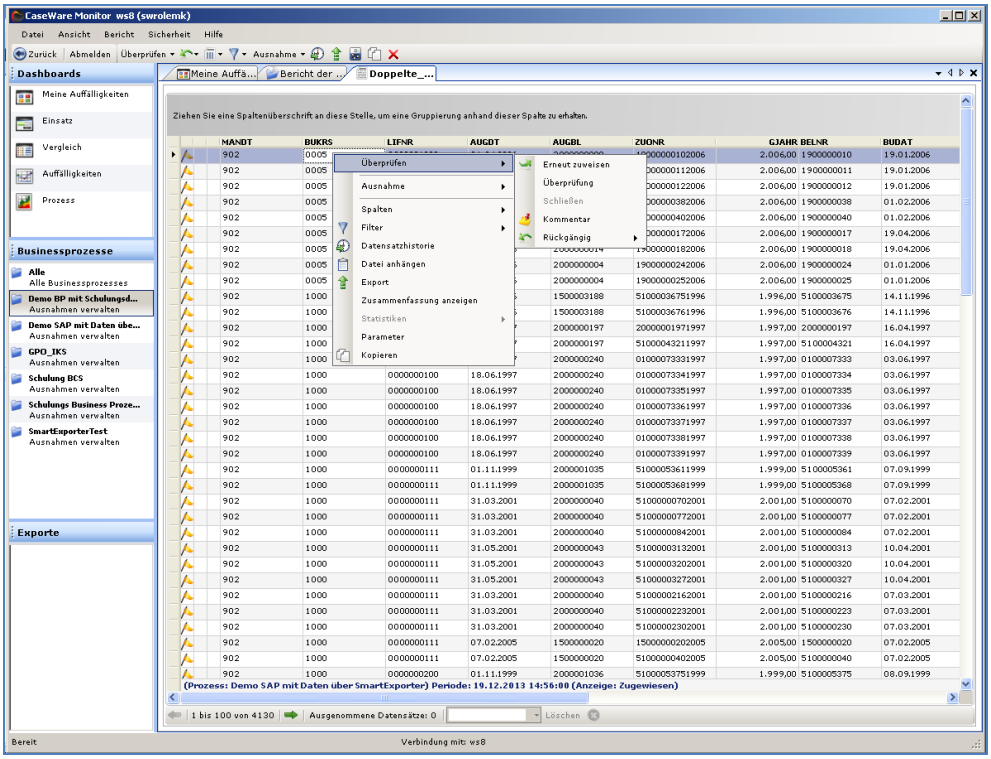

Abb. 11
Screenshot SmartExporter: Liste der gefundenen Doppelzahlungen

Als Vorbereitung für die Implementierung der Kontrolle in CaseWare Monitor werden die für die Kontrolle benötigten Dateien in einem Paket zusammengefasst. Dazu befindet sich ein Eintrag „Datei -> Paket für CaseWare Monitor“ ausgehend vom Dialogfenster des IDEA-Skripts. Die Dateien bestehen aus dem IDEA-Skript und der mittels SmartExporter exportierten Tabelle. Nach dem Bestätigen werden die Dateien als Paket in einem Upload Ordner des Case Ware-Monitor-Servers gespeichert. Für die Erstellung des Pakets werden die benötigten Dateien hinzugefügt, siehe Abbildung 12.

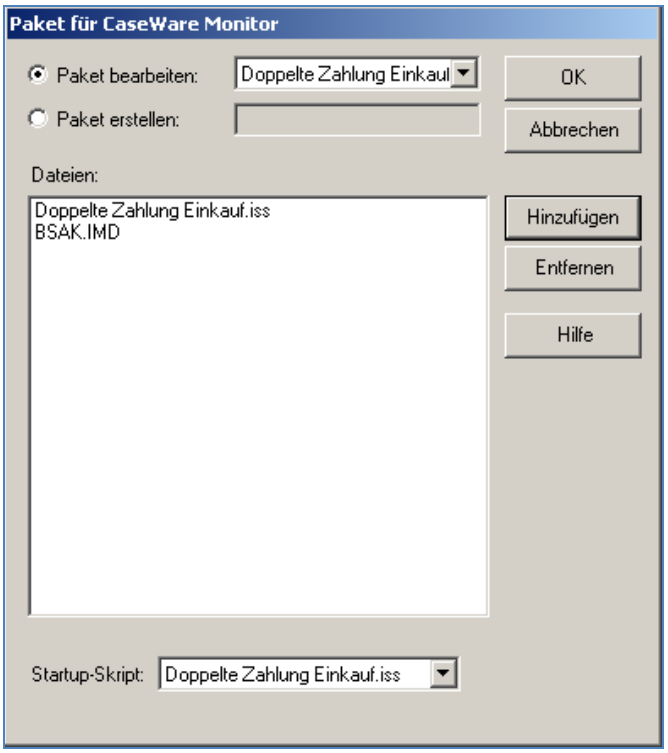

Abb. 12 Screenshot SmartExporter: Paket für Case WareMonitor

4.2.3 Implementierung der Kontrolle in CaseWare-Monitor

Nachdem die Vorbereitung getroffen und das Paket gespeichert wurde, muss dieses auf dem Server hochgeladen werden, damit die Kontrolle automatisiert auf dem Server ausgeführt werden kann. Ausgehend von IDEA befindet sich der "Monitor Navigator" unter „Monitor -> Navigator“. Nach Auswahl des zugehörigen Businessprozesses und des entsprechenden Paketes, werden erstmalig hochgeladene Pakete im "Monitor Navigator" rot markiert und können über das Symbol „  “ hochgeladen werden, siehe Abbildung 13.

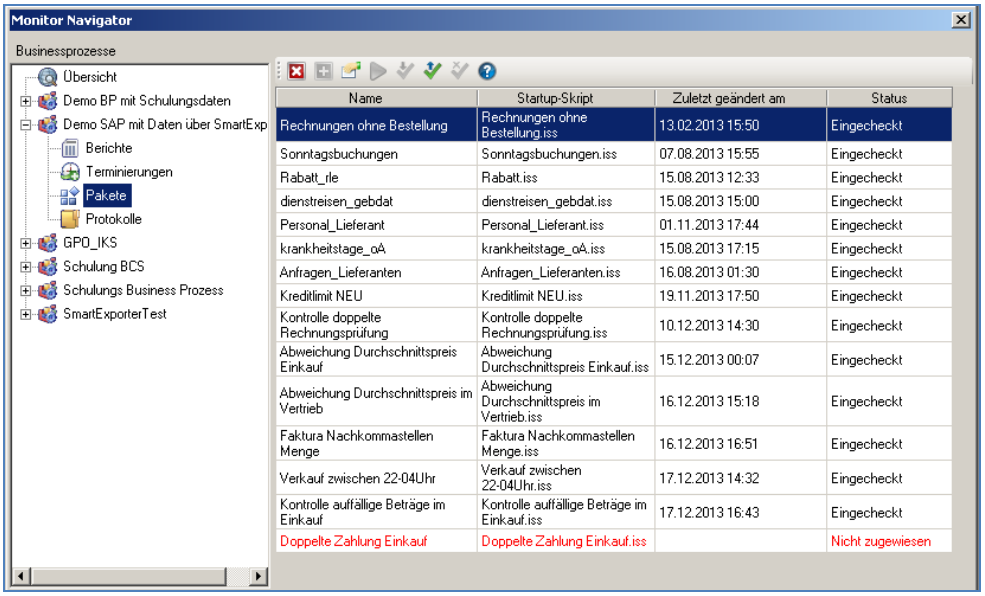

Abb. 13
Screenshot CaseWare Monitor, Pakete

Der nächste Schritt ist die Terminierung, welche eine automatisierte Ausführung der Kontrolle gewährleistet. Dazu wird der Assistent zur Konfiguration einer Terminierung genutzt, siehe Abbildung 14.

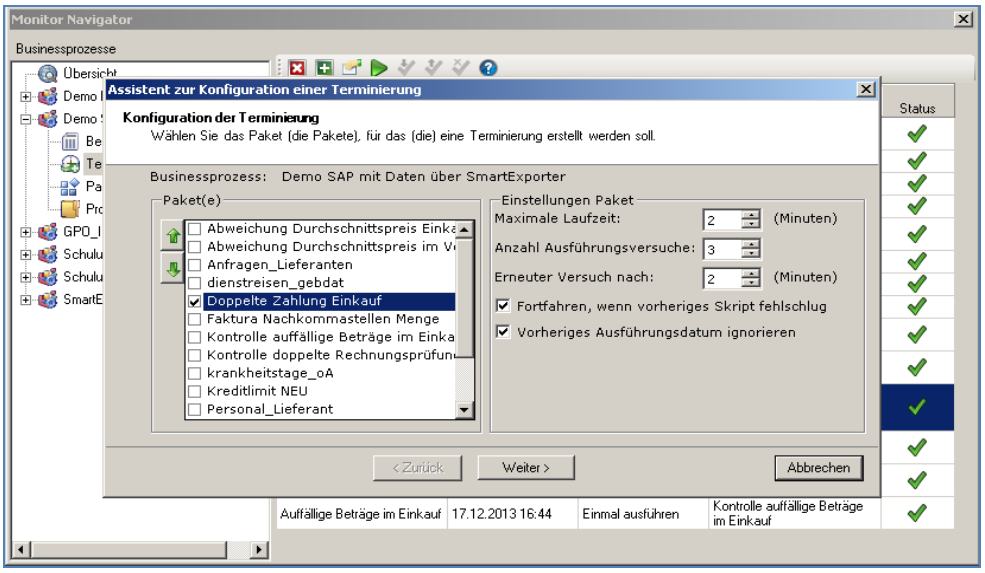

Abb. 14
Screenshot CaseWare Monitor, Terminierung erstellen

Nach der Auswahl des entsprechenden Paketes werden die „maximale Laufzeit“ und die Ausführung erneuter Versuche auf zwei Minuten beschränkt. Für die “Anzahl der Ausführungsversuche“ wird die Einstellung „2“ vorgenommen. Zusätzlich sollten die Checkboxen „Fortfahren, wenn vorheriges Skript fehlschlug“ und "Vorheriges Ausführungsdatum ignorieren“ aktiviert werden.

In dem nächsten Dialogfenster des Assistenten wird ein aussagekräftiger Name für den Vorgang angegeben, siehe Abbildung 15.

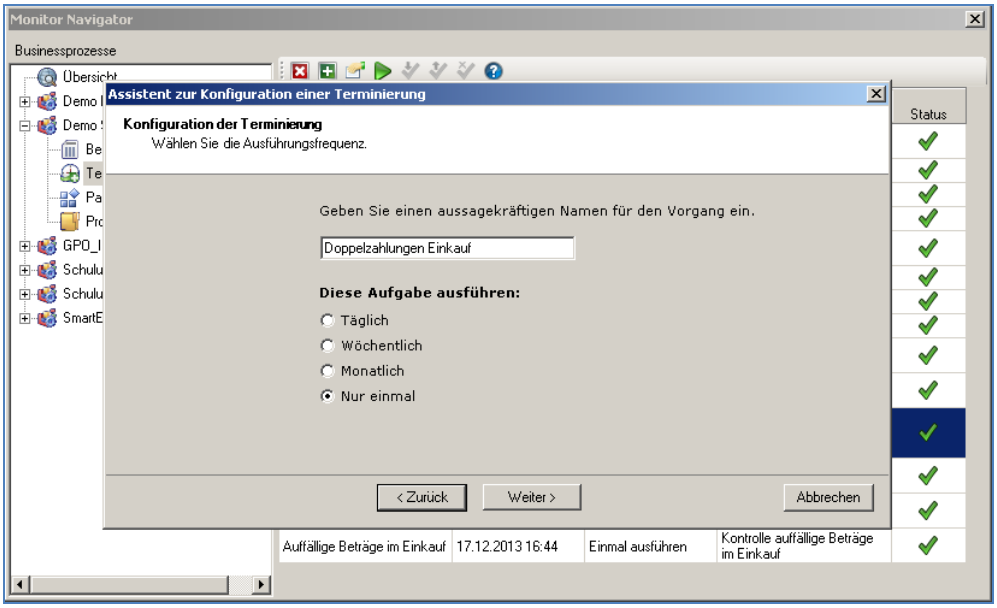

Abb. 15 Screenshot CaseWare Monitor, Ausführungsfrequenz

Weiterhin wird hier die Entscheidung zwecks Regelmäßigkeit der Ausführung getroffen. Für den Test der Kontrollen wurde die einmalige Ausführung gewählt.

Als nächster Schritt müssen die Startzeit und das Startdatum angegeben werden, siehe Abbildung 16.

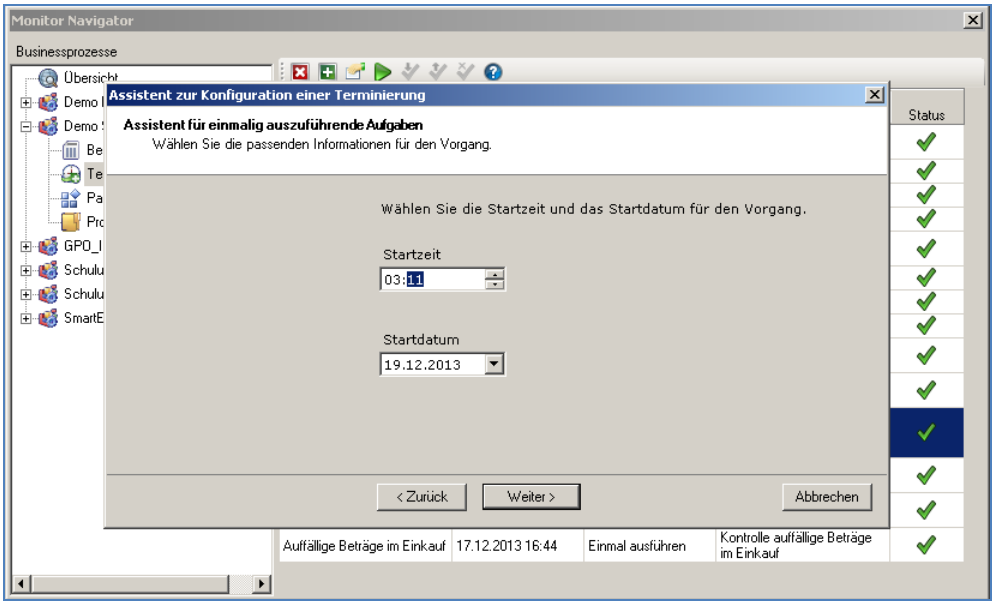

Abb. 16 Screenshot CaseWare Monitor, Startzeit, -datum

Das Enddatum und die Einstellungen für eine erneute Ausführung der Kontrolle werden in dem folgendem Dialogfenster festgelegt, siehe Abbildung 17.

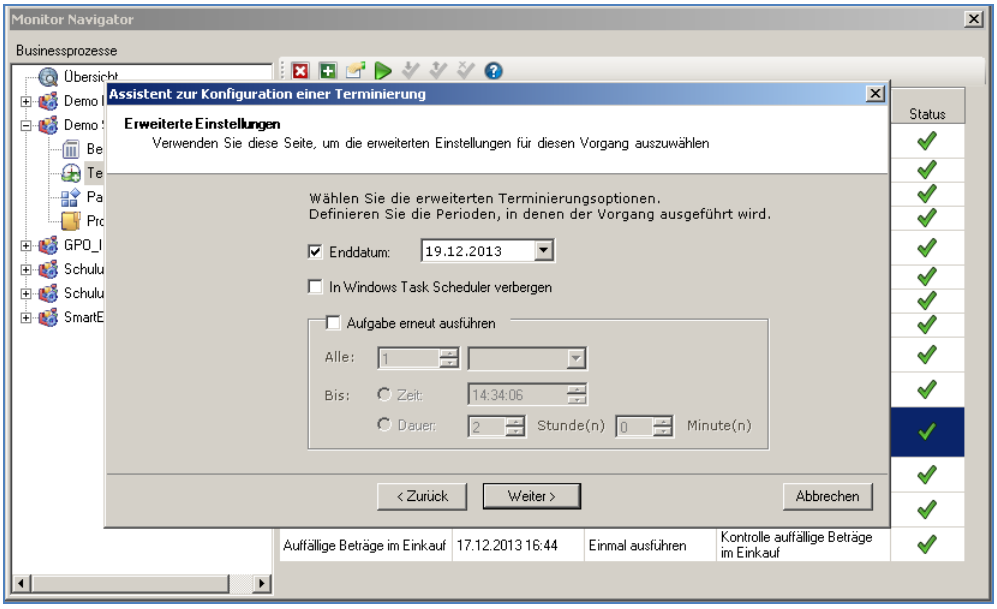

Abb. 17 Screenshot CaseWare Monitor, Enddatum

Der letzte Schritt des Assistenten zur Konfiguration einer Terminierung beinhaltet die Angabe der Nutzerdaten, siehe Abbildung 18.

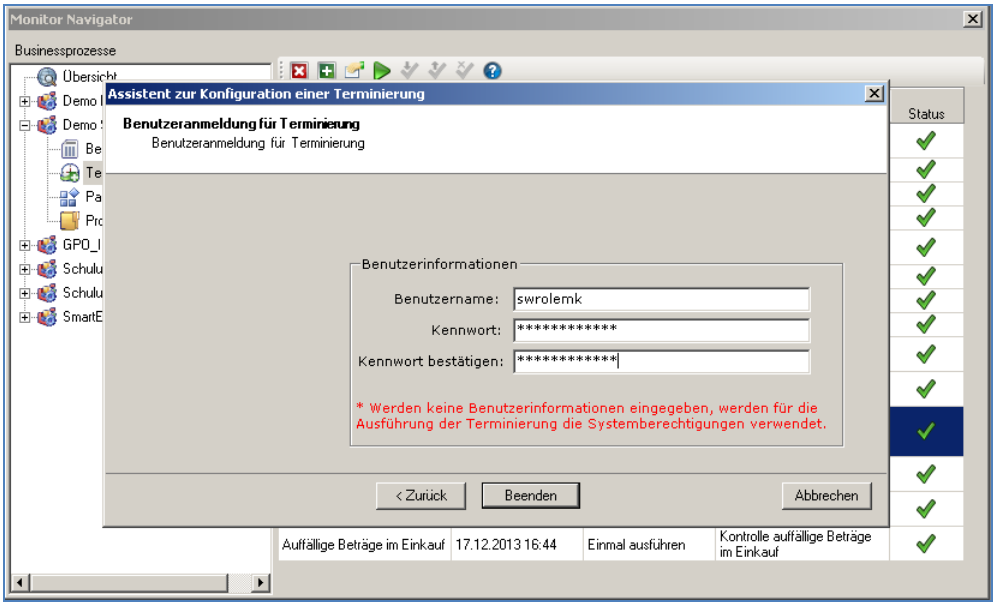

Abb. 18 Screenshot CaseWare Monitor, Benutzeranmeldung

Anschließend kann der Assistent beendet werden. Nach der Konfiguration der Terminierung wird diese mit dem entsprechenden Symbol „  “ ausge-

führt. In Folge der Ausführung wird ein Bericht erstellt, der auf Fehler überprüft werden sollte, siehe Abbildung 19.

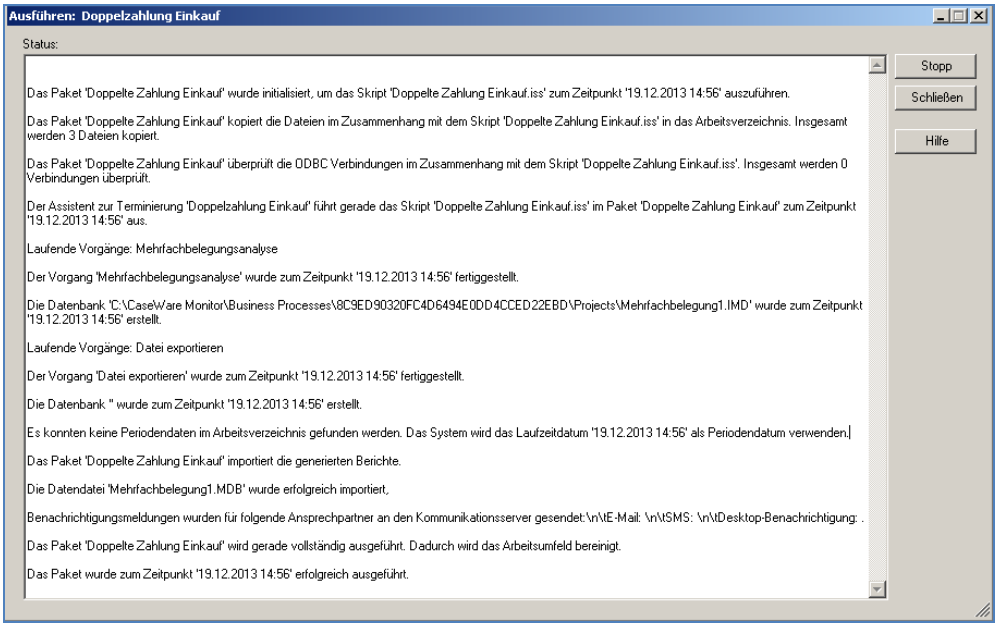

Abb. 19 Screenshot CaseWare Monitor, Ausführung der Terminierung

Sofern keine Fehler vorhanden sind, kann das Dialogfenster geschlossen werden. Die nächsten Schritte beziehen sich auf die Zuweisung der Verantwortlichkeiten. Letztendlich wird festgelegt, welche Personen für die Überprüfung der Kontrollergebnisse zuständig sind, welches Risiko besteht und in welcher Form die zuständigen Personen zusätzlich benachrichtigt werden sollen. Abbildung 20 zeigt die Auflistung der erstellten Berichte.

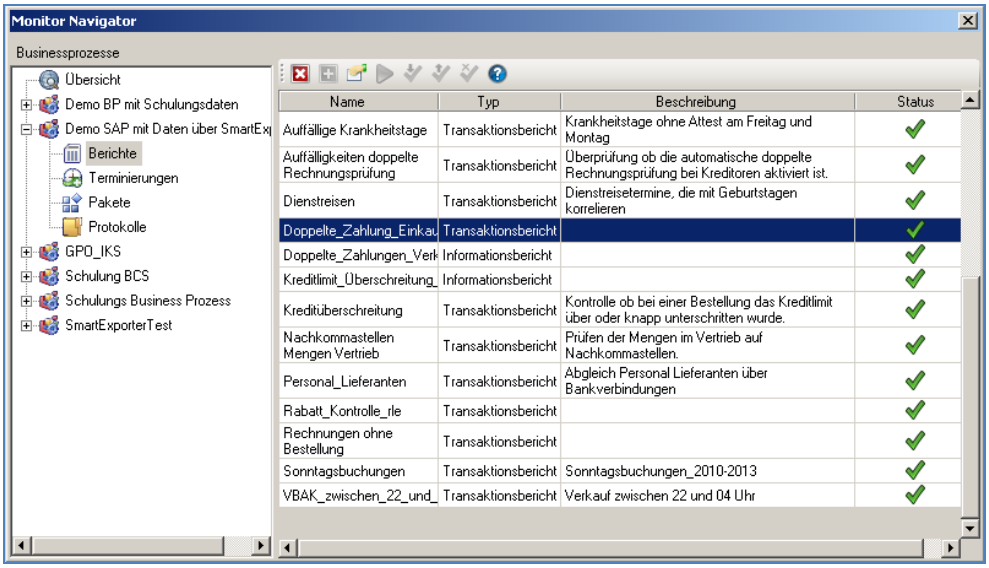

Abb. 20 Screenshot CaseWare Monitor, Bericht

Es wird der zuvor erstellte Bericht ausgewählt und durch die Betätigung des Buttons gelangt man zu den Details, siehe Abbildung 21.

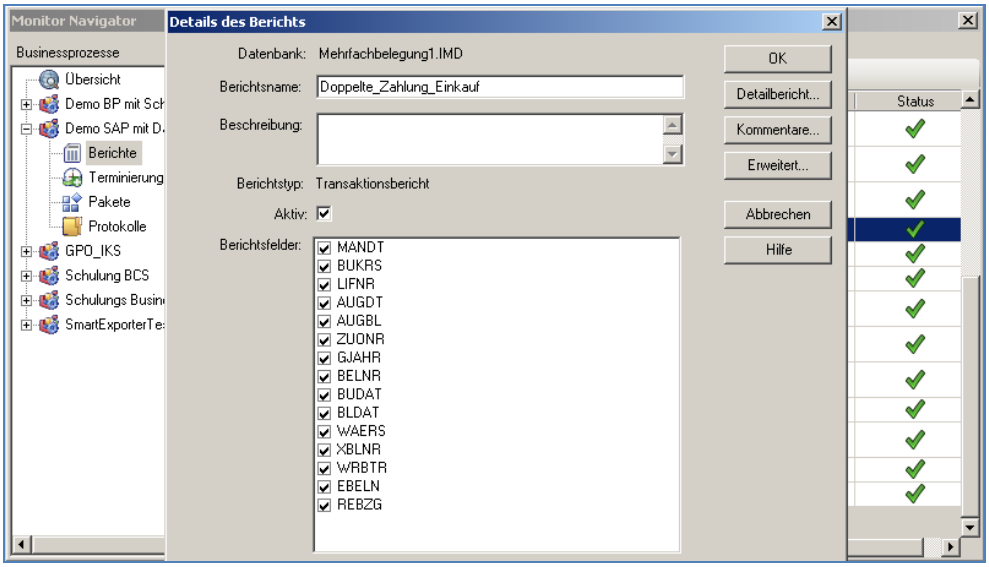

Abb. 21 Screenshot CaseWare Monitor, Berichtdetails

Die Details des Berichtes beinhalten u. a. die Felder, die der zuständigen Person angezeigt werden sollen. Optional können aus Gründen der Übersicht Felder abgewählt werden, die für die Überprüfung nicht mehr notwendig sind. Mit Hilfe des Buttons „Erweitert…“ gelangt man zum nächsten Dialogfenster, siehe Abbildung 22.

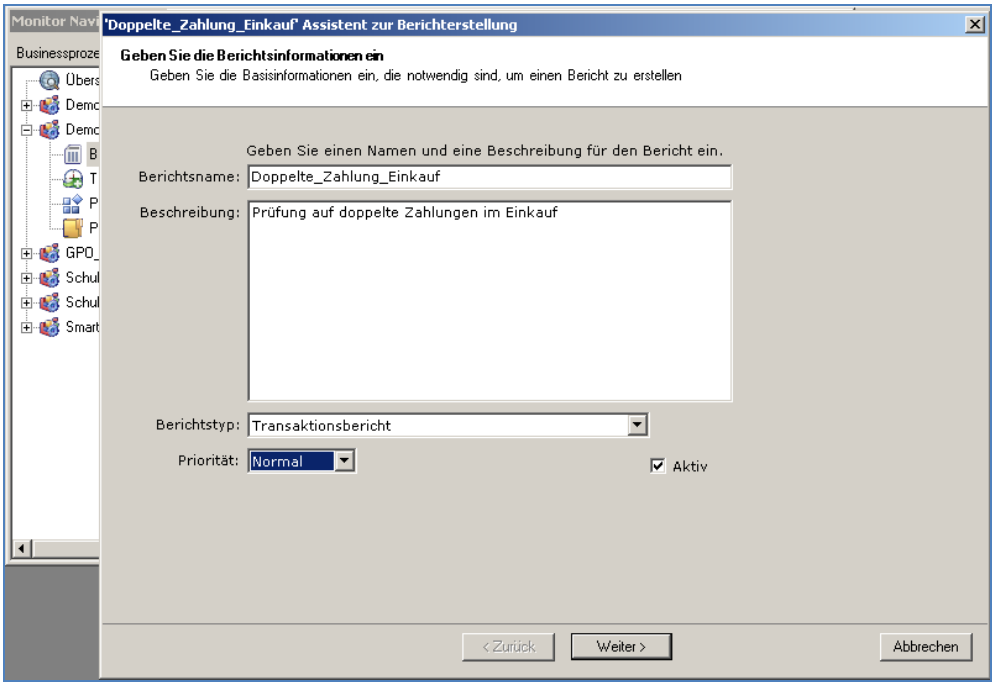

Abb. 22 Screenshot CaseWare Monitor, erweiterte Berichtdetails

Wenn der Berichtstyp nicht Transaktionstyp ist, sollte dieser geändert werden. Außerdem besteht die Möglichkeit die Priorität der einzelnen Berichte festzulegen. Die Angabe eines Risikowerts ist optional, siehe Abbildung 23.

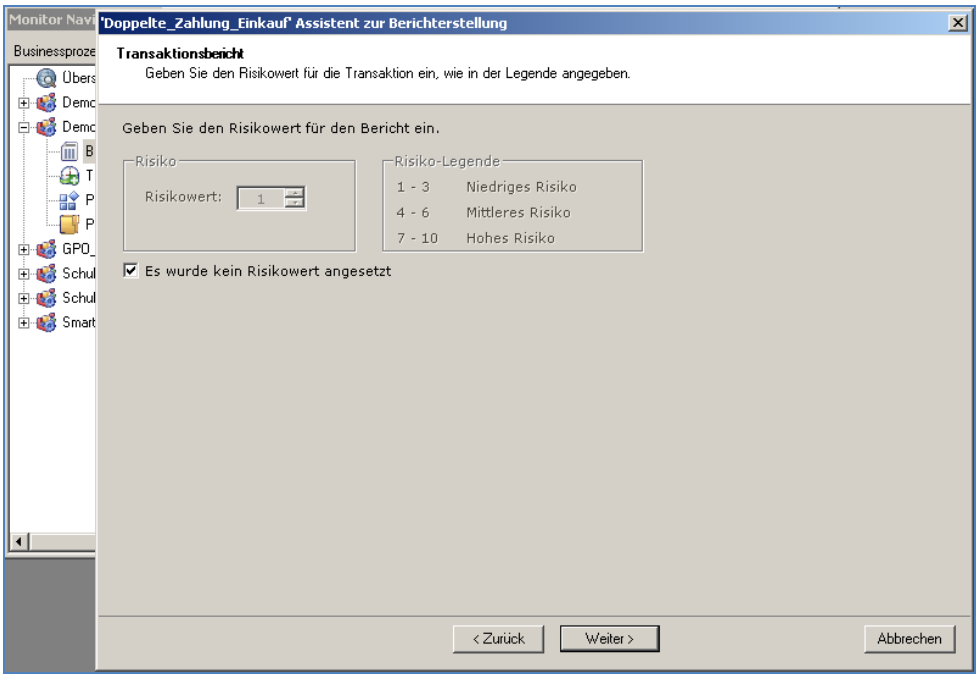

Abb. 23 Screenshot CaseWare Monitor, Risikowert

In dem nächsten Dialogfenster werden die Zuweisungen konfiguriert, siehe Abbildung 24.

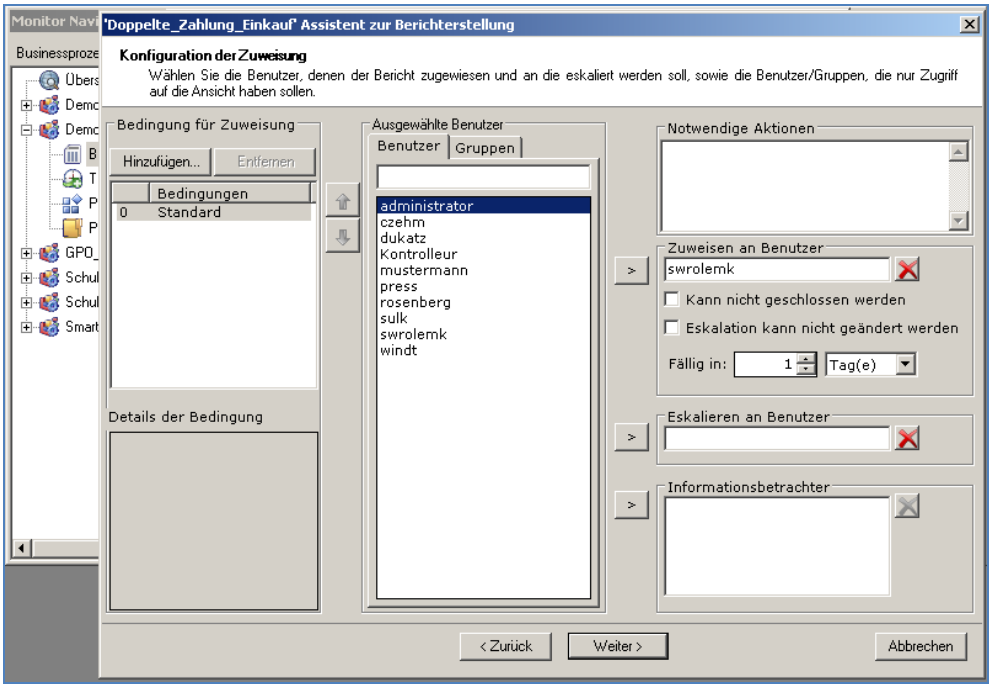

Abb. 24 Screenshot CaseWare Monitor, Benutzer-zuweisung

Dabei wird die Kontrolle einem Benutzer zugewiesen. Außerdem wird in diesem Fall ein Informationsbetrachter gewählt. Zusätzlich kann diese Kontrolle nach Ablauf einer bestimmten Frist (z. B. im Rahmen einer Eskalation) einem anderen Benutzer zugewiesen werden.

Anschließend können, wie in den Abbildungen 25 und 26 gezeigt, zusätzliche Benachrichtigungen konfiguriert werden. Es handelt sich dabei um E-Mail- bzw. SMS-Benachrichtigungen an den zugewiesenen Benutzer.

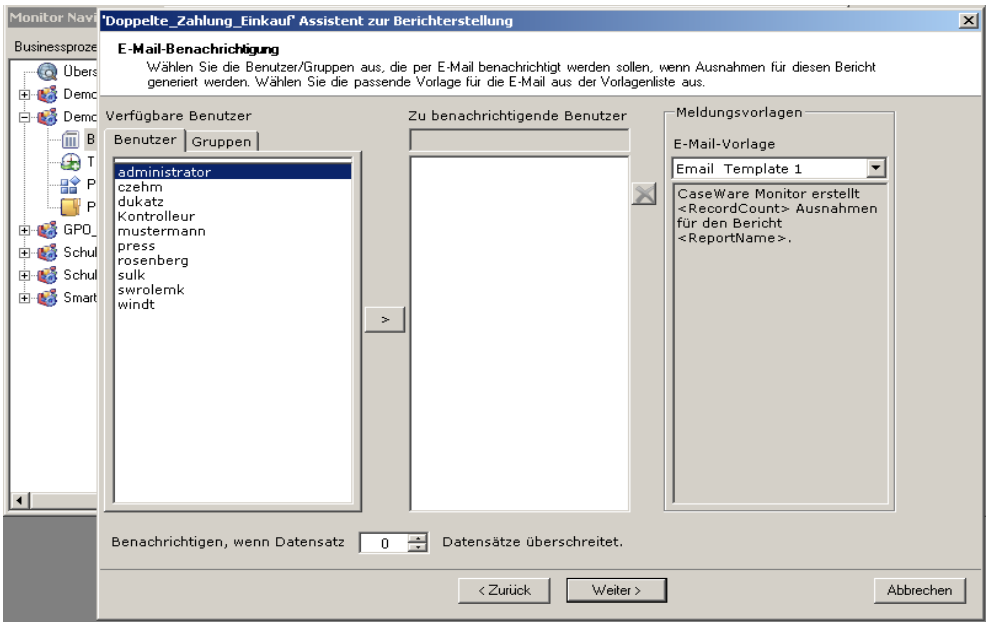

Abb. 25
Screenshot CaseWare Monitor, E-Mail Benachrichtgung

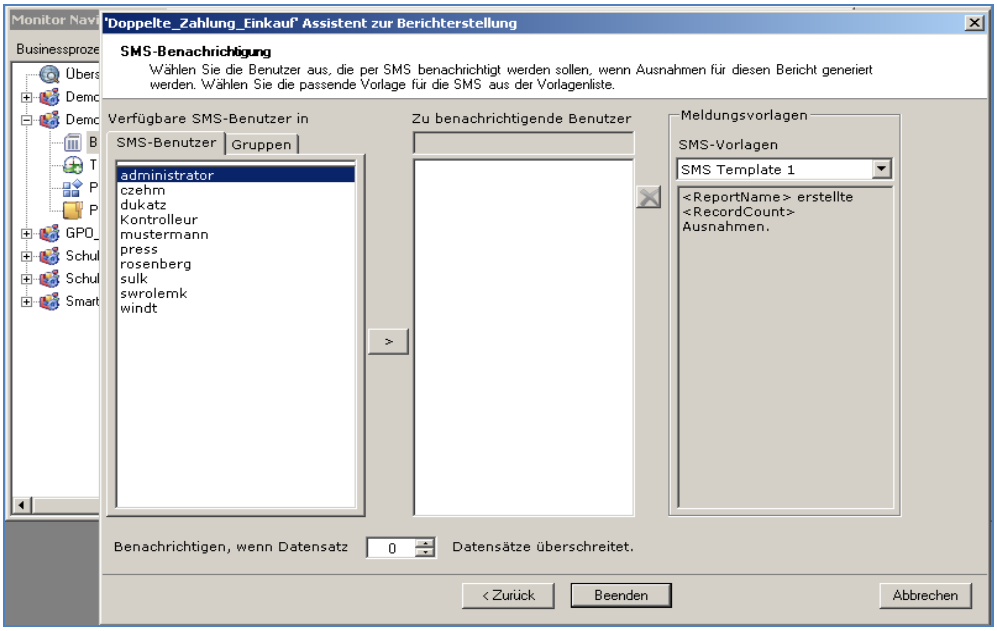

Abb. 26
Screenshot CaseWare Monitor, SMS-Benachrichtgung

Nach diesen obigen Schritten ist die Kontrolle implementiert.

Nach der Implementierung wird CaseWare-Monitor vom zugewiesenen Benutzer gestartet. Daraufhin öffnet sich das Dashboard mit den Auffälligkeiten der zugewiesenen Kontrollen. In unserem Fall werden durch diese Kontrolle 4130 Auffälligkeiten ermittelt, siehe Abbildung 27.

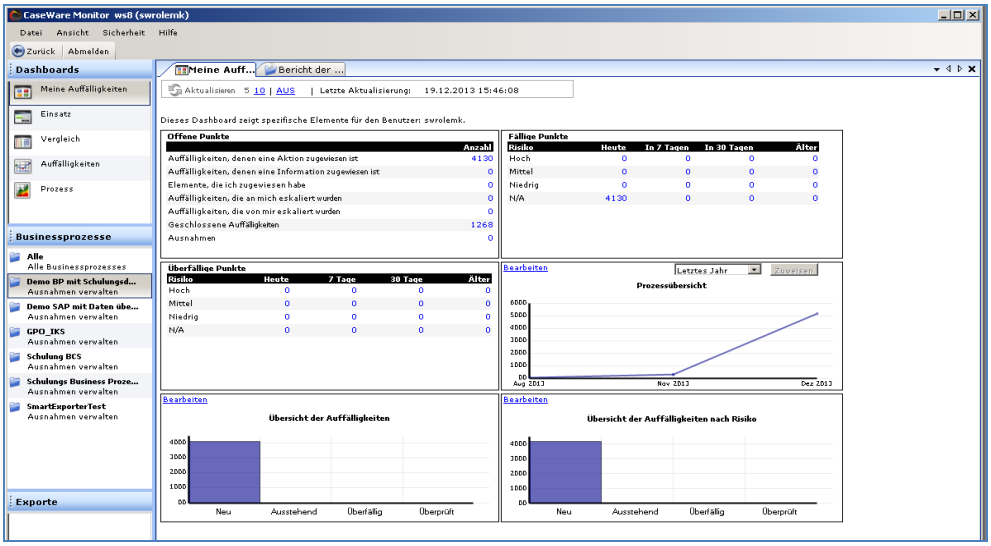

Abb. 27 Screenshot CaseWare Monitor, Dashboard

Die Detailansicht der Auffälligkeiten zeigt die Tabelle mit den einzelnen Auffälligkeiten für diese Kontrolle, siehe Abbildung 28.

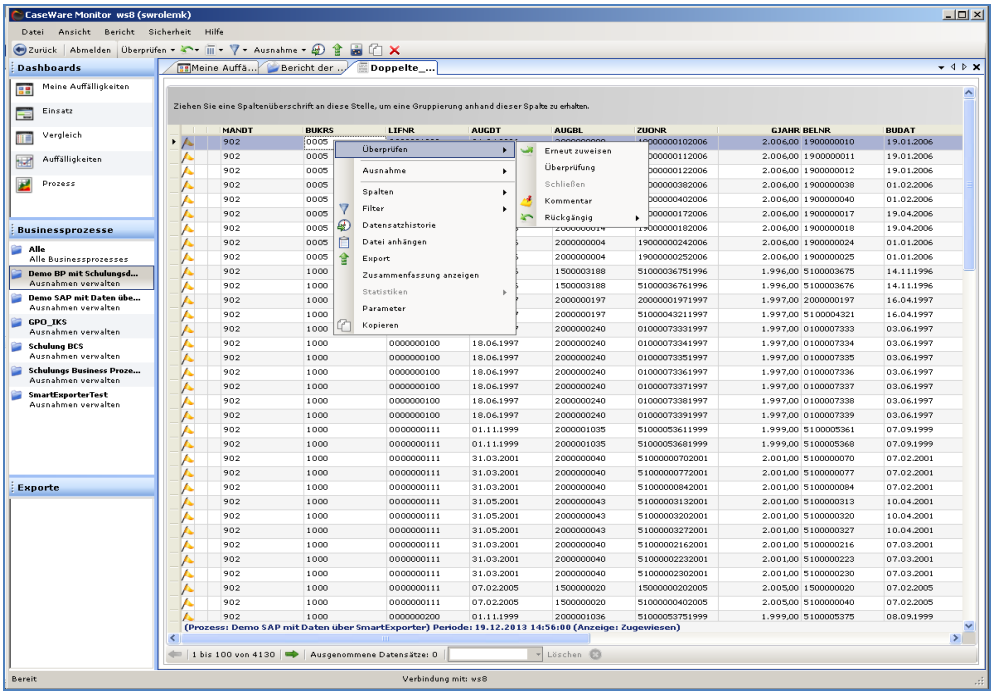

Abb. 28 Screenshot CaseWare Monitor, Übersicht der Auffälligkeiten

In dieser Ansicht kann der zugewiesene Benutzer die Auffälligkeiten überprüfen.

Der Nutzer hat weiterhin die Möglichkeit „Überprüfung“ auszuwählen, siehe Abbildung 29.

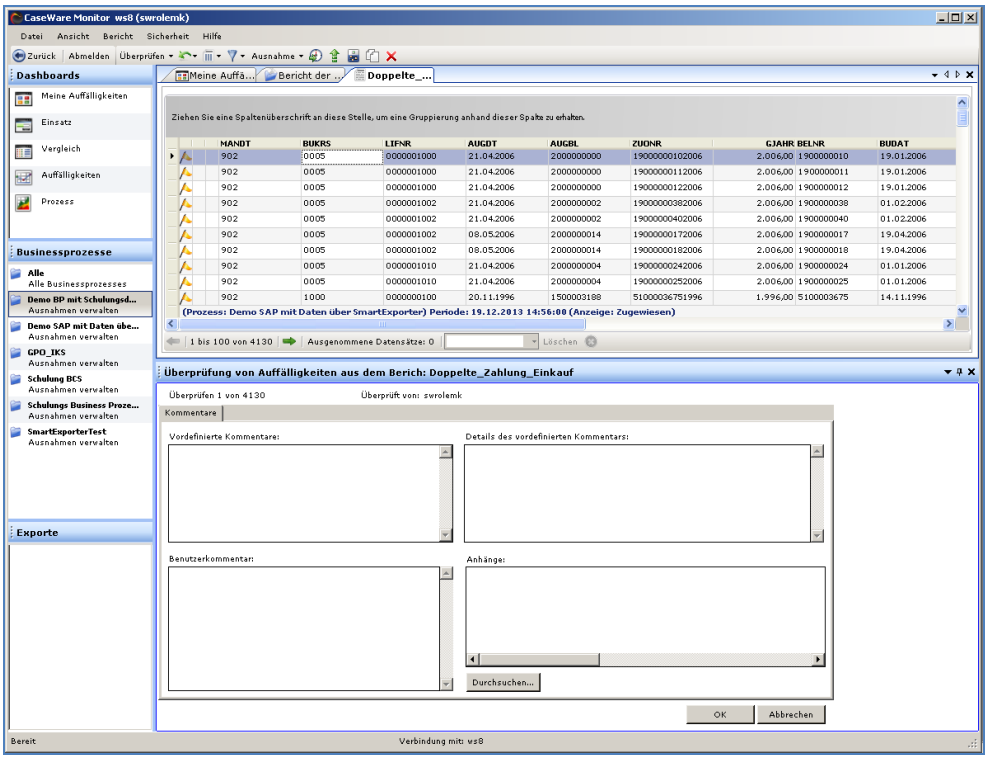

Abb. 29
Screenshot CaseWare Monitor, Überprüfung der Auffälligkeiten

In diesem Fall wird die Auffälligkeit geschlossen und archiviert. Eine weitere Möglichkeit ist die erneute Zuweisung der Auffälligkeit an andere Nutzer zu weiteren Klärung. Weiterhin ist das Hinzufügen eines Kommentars oder einer Datei möglich.

5. IDEA-Skript

```
Sub Main
Call DuplicateKeyDetection() 'BSAK.IMD
Call SendToMonitor() 'Mehrfachbelegung1.IMD
End Sub

' Analyse: Mehrfachbelegung Ermittlung
Function DuplicateKeyDetection
Set db = Client.OpenDatabase("BSAK.IMD")
Set task = db.DupKeyDetection
task.IncludeAllFields
task.AddKey "BUKRS", "A"
task.AddKey "LIFNR", "A"
task.AddKey "WAERS", "A"
task.AddKey "BLDAT", "A"
task.AddKey "WRBTR", "A"
task.OutputDuplicates = TRUE
dbName = "Mehrfachbelegung1.IMD"
task.PerformTask dbName, ""
Set task = Nothing
Set db = Nothing
Client.OpenDatabase (dbName)
End Function

' Bericht an Businessprozess senden: Demo SAP mit Daten über SmartExporter
Function SendToMonitor
Set db = Client.OpenDatabase("Mehrfachbelegung1.IMD")
Set task = db.MonitorReport
task.UseReport "Demo SAP mit Daten über SmartExporter", "Doppelte_Zahlung_Einkauf"
task.PerformTask
set db = Nothing
set task = Nothing
End Function
```

Verzeichnis der SIMAT-Arbeitspapiere

AP	Datum	Autor	Titel
01-09-001	01.2009	M. Klotz	Datenschutz in KMU – Lehren für die IT-Compliance
01-09-002	02.2009	M. Klotz	Von der Informationsgesellschaft zum Informationsarbeiter
01-09-003	09.2009	L. Ramin M. Klotz	Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT
01-09-004	10.2009	S. Kubisch	Corporate Governance gemäß BilMoG und SOX
02-10-005	06.2010	M. Klotz	PMBOK-Compliance der Projektmanagement-Software Projektron BCS
02-10-006	07.2010	A. Woltering	Kontinuierliche Verbesserung von Desktop-Services mittels Benchmarking
02-10-007	09.2010	M. Klotz	Grundlagen der Projekt-Compliance
02-10-008	11.2010	I. Karminski	Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung
02-10-009	12.2010	D. Engel/ N. Zdrowomyslaw	Benchmarking-Studie Stralsund 2010
03-11-010	02.2011	E. Tiemeyer	Kennzahlengestütztes IT-Projektcontrolling – Projekt-Scorecards einführen und erfolgreich nutzen
03-11-011	05.2011	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke
03-11-012	06.2011	M. Klotz	Konzeption des persönlichen Informations-managements
03-11-013	08.2011	H. Auerbach/ N. Zdrowomyslaw	9. STeP-Kongress „Region gestalten! Gesund-heitswirtschaft und Zukunftsmanagement“
03-11-014	08.2011	M. Klotz	Rollen der Information im Unternehmen
03-11-015	08.2011	Ahlfeldt	eGuides in kulturellen Einrichtungen – deutsch-sprachiger Museums-Apps
03-11-016	11.2011	S. J. Saatmann / I. Sulk / M. Klotz	Studie zu gewerblichen Strompreisen in Meck-lenburg-Vorpommern – Strom als Wettbewerbs-faktor und Gegenstand der Standortvermarktung
04-12-017	02.2012	M. Klotz / I. Sulk / E. Wieck	GDPdU-Konformität von Projektmanagement-software – Exemplarische Konzeption und Umsetzung
04-12-018	07.2012	M. Horn-Vahlefeld	Projektdesign als organisatorischer Rahmen des Projektmanagements
04-12-019	08.2012	M. Klotz / J. Kriegel	ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in die IT-Prozesse nach ITIL
04-12-020	09.2012	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke, 2.

			Aufl.
04-12-021	10.2012	I. Sulk / M. Klotz	Einsatz von eGuides auf der Marienburg in Malbork (Polen) – Erhebung und Analyse einer Best Practice
04-12-022	12.2012	Witty, M. / C. Kliebisch	Die Versicherungsbranche unter FATCA
05-13-023	01.2013	S. J. Saatmann	The price-link in the natural gas market – The development of the oil price-link and alternative price mechanisms
05-13-024	02.2013	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen
06-14-025	01.2014	M. Klotz	IT-Compliance nach COBIT® – Gegenüberstellung von COBIT® 4.0 und COBIT® 5
06-14-026	04.2014	L. von Blumröder	Projektpriorisierung im Rahmen eines ganzheitlichen Projektportfoliomanagements
06-14-027	06.2014	S. Press	Automatisierte Kontrollen in der Beschaffung – Exemplarische Konzeption und Umsetzung
06-14-028	07.2014	M. Klotz	IT-Compliance – Begrifflichkeit und Grundlagen
07-15-029	09.2015	M. Klotz	Projektmanagement-Normen und -Standards
08-16-030	08.2016	M. Klotz	ISO/IEC 3850x – Die Normenreihe zur IT-Governance
09-17-031	09.2017	S. Marx	Project Management Practice in Interreg Projects – Reflective Analysis and Recommendations
09-17-032	11.2017	S. Marx	Knowledge Management in Interreg Cross-Border Cooperation – a Project Perspective
10-18-033	11.2018	M. Klotz / S. Marx	Projektmanagement-Normen und -Standards, 2. Auflage
11-19-034	08.2019	M. Klotz	IT-Compliance nach COBIT® 2019
11-19-035	09.2019	I. Sulk / P. Hagen / M. Klotz	Kontrollanforderungen an ein ERP/Cloud-System und Umsetzung in automatisierte Kontrollen