TECHNISCHE UNIVERSITÄT MÜNCHEN
Fakultät für Informatik
Lehrstuhl für Wirtschaftsinformatik (I 17)
Univ.-Prof. Dr. Helmut Krcmar

Aufdeckung von Fraud im Einkaufsprozess durch die Kombination des Red Flag Ansatzes mit Process Mining

Galina Baader

Vollständiger Abdruck der von der Fakultät für Informatik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

genehmigten Dissertation.

Vorsitzender: Prof. Dr. Martin Bichler

Prüfer der Dissertation:

1. Prof. Dr. Helmut Krcmar
2. Prof. Dr. Michael Schermann

Die Dissertation wurde am 13.12.2018 bei der Technischen Universität München eingereicht und durch die Fakultät für Informatik am 24.05.2019 angenommen.

Zusammenfassung

Motivation: Wirtschaftskriminelles Verhalten, im engl. Fraud genannt, wird häufig identifiziert, indem Daten aus Enterprise Ressource Planning (ERP) und benachbarten Systemen nach Hinweisen auf wirtschaftskriminelles Verhalten durchsucht werden. Oft werden diese Daten mit induktiven Detektionsmethoden, wie beispielsweise Data Mining Algorithmen, geprüft. Induktive Detektionsalgorithmen führen zu einer Flut von Hinweisen mit einer hohen falsch-positiv Rate. Auch werden keine Analysen der sequentiellen Abläufe durchgeführt. Da aber Unternehmen größtenteils von Prozessen getrieben und Prozesse sequentieller Natur sind, werden durch das Ignorieren dieser Informationen wichtige Zusammenhänge vernachlässigt.

Ziel: Ziel dieser Arbeit ist die Flut von Hinweisen auf wirtschaftskriminelles Verhalten mit der hohen falsch-positiv Rate zu senken. Daher wird der weit verbreitete deduktive Ansatz, der Red Flag Ansatz, mit Process Mining kombiniert. Red Flags sind Hinweise auf wirtschaftskriminelles oder ungewöhnliches Verhalten. Process Mining setzt auf sequentielle Informationen von Prozessinstanzen auf. Es visualisiert den Ist-Prozess mit allen möglichen Abweichungen vom Standardprozess, indem es Prozessabfolgen aus den Daten des Informationssystems rekonstruiert. Um die falsch-positiv Rate weiter zu reduzieren, werden zusammenhängende Red Flags zu Fraud Patterns zusammengefasst und nach diesen Fraud Patterns im Datensatz gesucht.

Forschungsdesign und Methodik: Um dieses Ziel zu erreichen, wird Design Science als Basis gewählt. Anhand einer Literaturanalyse wird der aktuelle Stand der Wissenschaft zur Fraud Detektion im Allgemeinen und im Speziellen zu möglichen Fraud Szenarien mitsamt den dazugehörigen Red Flags im Einkaufsprozess erstellt. Daraufhin wird ein Prototyp entwickelt, der beide Methoden verbindet (Prototyping). Dabei wird zunächst ein low-fidelity Prototyp entwickelt, der mit der Thinking-Aloud Methode evaluiert wird. Daraus entstehen Anforderungen, die im high-fidelity Prototyp implementiert werden. Abschließend wird der Prototyp mithilfe von synthetischen Datensätzen und zwei realen Datensätzen evaluiert.

Ergebnisse: Das Ergebnis dieser Dissertation ist ein Prototyp, der Red Flags und Fraud Patterns entlang einer möglicherweise betrügerischen Prozessinstanz visualisiert. Dieser wird auf synthetische und echte Datensätze angewand. Bei den synthetischen Datensätzen wird eine Wahrheitsmatrix erstellt, um die Ergebnisse des Prototyps mit anderen Forschungsbeiträgen vergleichbar zu machen. Die falsch-positiv Werte mit einer 0,03% bzw. 0,2% sind deutlich geringer, als in vergleichbaren Studien. Angewendet auf echte Datensätze zweier Unternehmen können alle Erkenntnisse der professionellen Auditoren auch mit dem Prototyp identifiziert werden. Zusätzlich sind im ersten Datensatz doppelte Zahlungen und Unstimmigkeiten bei einer Ausschreibung aufgefallen, die sehr stark auf Fraud hindeuten. Im zweiten realen Datensatz werden die wichtigsten Erkenntnisse der Auditoren ebenfalls erkannt, jedoch auch Unstimmigkeiten bei internen Leistungsverrechnungen.

Implikationen für die Praxis: Die prototypische Implementierung ist vor allem für Auditoren, Mitarbeiter der internen und externen Revision und Fraud Forensiker hilfreich. Die komplette Sicht auf den Fall ermöglicht es dem Fraud Investigator auf einen Blick wirtschaftskriminelle Handlungen zu identifizieren, nach auffälligen Prozessinstanzen im Prozessablauf, nach Prozessinstanzen mit den meisten aufgetretenen Red Flags, der höchsten möglichen Schadenssumme oder nach bestimmten Fraud Patterns zu filtern. Darüber hinaus werden zugehörige Informationen über den Lieferanten, die gekaufte Ware und die beteiligten Mitarbeiter angezeigt. Da Fraud mit einem durchschnittlichen Verlust von 5% des Umsatzes geschätzt wird und SAP Systeme sehr verbreitet sind, ist der Prototyp in der Praxis von relevantem Nutzen. Zur Evaluation des Prototyps wird ein Datengenerator entwickelt. Die von diesem erzeugten Daten stellen ebenfalls einen Praxisbeitrag dar, da diese Daten für Benchmarking von Fraud Detektionstools verwendet werden können. Vorteil dieser Daten ist, dass Fraud als solcher gekennzeichnet ist.

Stichworte: Wirtschaftskriminalität, Fraud, Anti-Fraud Management, Process Mining, Red Flags, Fraud Detektion, SAP.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

3WM	Three Way Match
ABAP	Advanced Business Application Programming
ACFE	Association of Certified Fraud Examiners
ACL	Audit Command Language
AICPA	American Institute of Certified Public Accountants
APAC	Asia Pacific
BANF	Bestellanforderung
BAPI	Business Application Programming Interface
BDC	Batch Data Communication
BIP	Bruttoinlandsprodukt
BLS	Bureau of Labor Statistics
BPMN	Business Process Model and Notation
CAATT	Computer-Assisted Auditing Tools and Techniques
CO	Controlling
COSO	Committee of Sponsoring Organizations
CpD	Conto pro Diverse
CRM	Customer Relationship Management
CSV	Comma-Separated Values
DIIR	Deutsches Institut für Interne Revision e.V.
EDI	Electronic Data Interchange
EFT	Electronic Fund Transfer
ERM	Entity Relationship Model
ERP	Enterprise Resource Planning
ERS	Evaluated Receipt Settlement
ETL	Extract-Transform-Load
FI	Finanzbuchhaltung (SAP Modul)
GUI	Graphical User Interface
HANA	High Performance Analytical Appliance
IAASB	International Auditing and Assurance Standards Board
IDEA	Interactive Data Extraction and Analysis
IDES	International Demonstration and Education System
IDW	Institut der Wirtschaftsprüfer in Detuschland e.V.
IKS	Internes Kontrollsystem
IIA	Institute of Internal Auditors
MEA	Middle East and Africa
MICE	Money, Ideology, Coercion and Ego
MM	Materialmanagement bzw. Materialwirtschaft

OMG	Object Management Group
ODBC	Open Database Connectivity
PQL	Process Query Language (Celonis Query Language)
SD	Vertrieb
SFO	Serious Fraud Office
SoD	Segregation of Duties
SQL	Structured Query Language
TPB	Theory of Planned Behavior
WCC	White Collar Crime
WCHC	White Collar Hacking Contest
WE	Wareneingang

1 Einführung

Ziel dieser Dissertation ist die Reduktion der hohen falsch-positiv Rate im Bereich der Frauderkennung durch die Kombination von Red Flags mit Process Mining. Im ersten Schritt werden Motivation und Relevanz dargestellt, sowie das Forschungsziel mit forschungsleitenden Fragestellungen und die angewandten Methoden.

1.1 Motivation und Relevanz

Fraud wird häufig identifiziert, indem in Daten aus Enterprise Ressource Planning (ERP) und benachbarten Systemen nach Hinweisen auf wirtschaftskriminelles Verhalten gesucht wird (Bönner, Riedl, & Wenig, 2011; Coderre, 2009). Oft werden Data Mining basierte Algorithmen, wie beispielsweise Neuronale Netzwerke, Bayesian Netzwerke, Entscheidungsbäume, Regressionsmodelle und genetische Algorithmen, angewendet, um Fraud zu identifizieren (Bolton & Hand, 2002; Ngai, Hu, Wong, Chen, & Sun, 2011; Phua, Lee, Smith, & Gayler, 2010).

Die hier genannten induktiven Fraud Detektionsmethoden führen zu einer Flut von Hinweisen und Alarmen mit einer hohen Anzahl an falsch-positiven Werten. Falsch-positive Werte sind Einträge, die fälschlicherweise als Hinweise für Fraud gelten (Albrecht, Albrecht, Albrecht & Zimbelman, 2012; Alles, Brennan, Kogan & Vasarhelyi, 2006). Die Analyse von falsch-positiven Werten ist sehr zeitintensiv und führt zu Kosten ohne jeglichen Nutzen (Luell, 2010). Auch führt die Flut von Hinweisen dazu, dass diese nicht handhabbar sind und sehr häufig ignoriert werden (Henselmann & Hofmann, 2010). Das Beratungsunternehmen KPMG hat in einer Studie gezeigt, dass etwa 50% der Fraud Fälle früher hätte identifiziert werden können, wenn die entsprechenden Hinweise nicht ignoriert worden wären (KPMG, 2011). Eine weitere Studie des ACFE hat zudem gezeigt, dass in 92% aller identifizierten Fraud Fällen auch Hinweise vorhanden waren (ACFE, 2014).

Ein weiteres Problem bei den bekannten Fraud Erkennungsverfahren ist, dass diese keine sequentiellen Analysen durchführen (Phua et al., 2010). Da ERP Systeme durchweg prozessorientiert sind, limitiert das Ignorieren von sequentiellen Informationen die Genauigkeit dieser Ansätze (Aalst & Weijters, 2005; Boczko, 2007).

Daher ist das Ziel dieser Dissertation die Flut von Hinweisen mit einer hohen Anzahl von falsch-positiv Werten zu reduzieren. Hierzu wird der Red Flag basierte Ansatz mit Process Mining kombiniert. Um das Ziel zu erreichen wird zunächst ein deduktiver Ansatz der Fraudbekämpfung gewählt. Ein typischer deduktiver Ansatz ist die Identifikation von Fraud durch Red Flags, der von allen Fraud Audit Standards empfohlen wird (z.B. SAS 99) (Albrecht et al., 2012). Ein Red Flag ist ein Hinweis oder besonderer Umstand, der vom Wesen her unüblich ist und von normalen Aktivitäten abweicht. Es handelt sich um ein Signal, dass etwas aus dem Rahmen fällt und weitere Überprüfung benötigt (DiNapoli, 2008). Um die falsch-

positiv Rate noch weiter zu reduzieren, werden zusammenhängende Red Flags zu Fraud Patterns kombiniert. So wird im Datensatz nicht nach einzelnen Red Flags, sondern simultan nach zusammenhängenden Red Flags gesucht.

Process Mining setzt auf sequentielle Informationen von Prozessinstanzen auf (Aalst, Beer, & Dongen, 2005). Es visualisiert den Ist-Prozess mit allen möglichen Abweichungen des Standardprozesses, indem es Prozessabfolgen aus den Daten des Informationssystems rekonstruiert (Aalst et al., 2011). Durch die Kombination dieser beiden Ansätze ist es möglich, Red Flags entlang einer möglichen Prozessinstanz anzuzeigen.

1.2 Forschungsziel und forschungsleitende Fragestellungen

Ziel dieser Arbeit ist es im Bereich Fraud Detektion die hohe Anzahl an falsch-positiven Werten und die Flut von Hinweisen zu reduzieren, indem der deduktive Red Flag Ansatz mit Process Mining kombiniert wird. Zusätzlich werden die Red Flags zu Fraud Patterns kombiniert, um die falsch-positiv Rate weiter zu reduzieren. Es soll ein Prototyp erstellt werden, der Fraudverhalten (mit Red Flags und Process Mining) aus einem Datensatz erkennt und in einem Dashboard anzeigt.

Dabei sollen folgende Forschungsfragen beantwortet werden:

RQ1: **Welche Betrugsmöglichkeiten im Einkaufsprozess bestehen und wie können diese betrügerischen Taten mithilfe von Massendatenanalysen identifiziert werden?**

Das Ziel der ersten Forschungsfrage ist es die Wissensgrundlage für Fraud Detektion zu schaffen. Deshalb werden zunächst Literaturstudien nach den Richtlinien von Webster & Watson (2002) durchgeführt. Eine detaillierte Beschreibung der gewählten Literaturstudien ist im Kapitel 1.3 Forschungsmethodisches Design gegeben.

Als Output der ersten Forschungsfrage soll eine Übersicht über wirtschaftskriminelle Handlungen im Allgemeinen, eine Übersicht über wirtschaftskriminelle Handlungen im Einkaufsprozess, sowie eine Übersicht über technische und fachliche Detektionsmöglichkeiten gegeben werden.

RQ2: **Welche Anforderungen hinsichtlich der Gestaltung eines Prototyps für Fraud Detektion mit Hilfe von Red Flags und Process Mining ergeben sich aus der Literatur und Experteninterviews, und wie lässt sich dieser Prototyp implementieren?**

Aufbauend auf der ersten Forschungsfrage werden in der zweiten Forschungsfrage Anforderungen an den Prototypen gesammelt, sowie der Prototyp implementiert. Als Grundlage werden Red Flags zunächst aus der Literatur abgeleitet und basierend auf dem de-facto Standard für Fraud Klassifizierung – dem ACFE Tree (ACFE, 2016) – einsortiert, wodurch Fraud Patterns abgeleitet werden. In einem zweiten Schritt werden sowohl SQL Skripte zur Identifikation der Red Flags und Fraud Patterns erstellt. Auch werden entsprechende Informationen aus den SAP Tabellen extrahiert und in das für Process Mining notwendige Format gebracht. Als letztes wird ein Dashboard erstellt, welches die Red Flags, Patterns,

Prozessabweichungen und weitere Informationen visualisiert. Hierzu werden zunächst aus der Literatur Anforderungen über die Visualisierung und den gewünschten Informationen extrahiert. Anschließend wird ein low-fidelity Prototyp erstellt, der mit der Thinking Aloud Methode evaluiert wird. Daraus ergeben sich neue Anforderungen, die entsprechend im high-fidelity Prototypen umgesetzt werden.

Als Outcome dieser Forschungsfrage wird zunächst eine Liste mit Fraud Patterns inklusive der zugehörigen Red Flags erstellt. Zusätzliches Ergebnis ist ein Prototyp, der die zuvor identifizierten Anforderungen implementiert.

RQ3: **Welche Implikationen hinsichtlich der Weiterentwicklung und Nutzung des vorgestellten Prototyps zur Fraud Detektion resultieren durch die Anwendung am Beispiel des Einkaufsprozesses?**

Ziel der dritten Forschungsfrage ist die Anwendung des Prototyps auf einen synthetischen, einen semi-synthetischen und zwei echten Datensätzen aus der Praxis, um die Fraud Erkennungsrate und die falsch-positiv Rate zu bestimmen.

Zunächst wird ein Datengenerator entwickelt, der sowohl prozesskonforme Daten, wie auch wirtschaftskriminelles Verhalten (basierend auf der Literatur) generiert. Dieser generierte Datensatz wird mit Hilfe des in Forschungsfrage 2 entwickelten Prototypen analysiert und die Ergebnisse in Form einer Wahrheitsmatrix dargestellt. Weitere Red Flags zur Verbesserung der Trefferquote werden hinzugefügt. Anschließend wird der Prototyp mit Daten aus dem White Collar Hacking Contest (WCHC) validiert. Der WCHC ist ein Wettbewerb, bei dem die Teilnehmer abwechselnd Fraud im Einkaufsprozess begehen und anschließend den Fraud der gegnerischen Teilnehmer identifizieren. Die dabei entstandenen Daten werden verwendet, um mit Hilfe des Prototypen Fraud zu identifizieren. Die identifizierten Fraudfälle werden mit den von den Teilnehmern implementierten Fällen verglichen und die Ergebnisse in Relation zu weiteren Forschungsstudien gezeigt. Als letzten Schritt wird der Prototyp auf zwei Datensätze aus der Praxis angewendet und die Ergebnisse mit den Ergebnissen der professionellen Auditoren verglichen.

Output der dritten Forschungsfrage ist ein Datengenerator zur Erstellung von Fraud Daten und regelkonformen Daten. Zusätzlich werden durch die Anwendung des Prototypens auf verschiedene Datensätze und dem Vergleich der Ergebnisse mit dem professionellen Audit bzw. dem tatsächlichen Fraud in synthetischen Datensätzen, Implikationen für die Weiterentwicklung des Prototyps aufgezeigt.

1.3 Forschungsmethodisches Design

In der deutschen Wirtschaftsinformatik gibt es zwei generell akzeptierte Arten der Forschung: empirisch (qualitativ oder quantitativ) oder Design Science. Das Ziel der empirischen Forschung ist es Phänomene zu verstehen. Dazu werden diese beobachtet und mit Ursache-Wirkungsdiagrammen erklärt. Bei Design Science ist das Ziel etwas zu schaffen, das den menschlichen Zwecken dient (March & Smith, 1995). Wichtig ist, dass Wissen in Form von

produktiv einsetzbaren Applikationen generiert wird (Hevner, March, Park, & Ram, 2004). Es verfolgt keinen beobachtenden, sondern problemlösenden Ansatz.

Das Ergebnis des Design Science Vorgangs ist ein Artefakt (Hevner et al., 2004). Dieses soll auf Grundlagenwissen aufgebaut werden, welches zuvor mittels Behavioral Science festgestellt wird (Hevner et al., 2004). Design Science verbessert, erschafft und evaluiert Artefakte. Artefakte lassen sich nach March & Smith (1995) in vier Kategorien einteilen:

- Konstrukte: Konstrukte sind Begrifflichkeiten, die neu aufgetretene Phänomene beschreiben.
- Modelle: Modelle sind Repräsentationen eines Ausschnitts der realen Welt.
- Methoden: Methoden beschreiben Prozesse zum Lösen eines Problems. Hier kann es sich um mathematische Formen, Algorithmen oder textuelle Beschreibungen handeln.
- Instanziierung: Instanziierungen stellen prototypische Softwaresysteme dar, die anhand von implementierten Methoden ein zuvor gestelltes Problem lösen. Dabei werden Konstrukte und Modelle verwendet, die laut Briggs (2006) die Lösbarkeit eines Problems beschreiben.

Design Science kann als ein Suchprozess verstanden werden. Es gibt keine genauen Angaben, wie dieses Artefakt erstellt werden soll (Hevner et al., 2004). Die Gestaltung des Artefakts kann anhand von weiteren Theorien entstehen (Briggs, 2006).

In dieser Dissertation soll ein Prototyp auf Basis von bestehenden Artefakten erstellt werden. Entsprechend soll eine Instanziierung von prototypischen Softwaresystemen entstehen. Der Ablauf der Forschung ist in Abbildung 1-1 dargestellt.

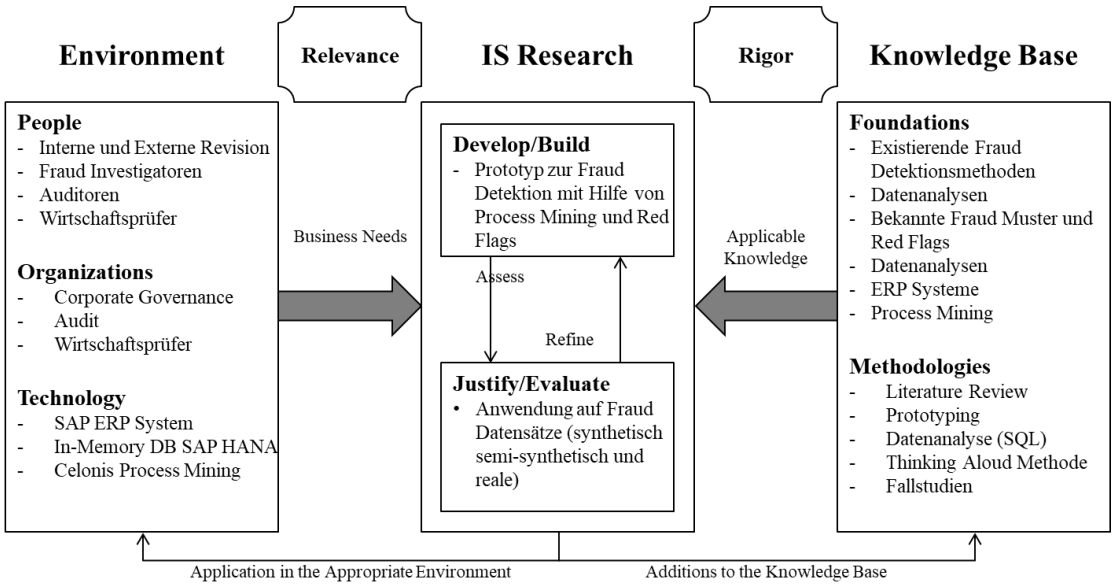


Abbildung 1-1: Design Science Forschung

Quelle: Eigene Darstellung basierend auf Hevner et al., (2004)

Eine genaue Übersicht über die Bestandteile wird im Folgenden gegeben:

- **Umwelt**

Die prototypische Implementierung kann in Unternehmen jeglicher Größe vorwiegend mit Nutzung von ERP Systemen verwendet werden. Speziell profitieren vor allem das Audit, die interne und externe Revision, Wirtschaftsprüfer und Träger des Corporate Governance. Als technologische Einheiten dient ein SAP ERP System 6.04 mit IDES bzw. GBI Datensatz, eine In-Memory Datenbank SAP HANA mit SPS 9 und das Process Mining Tool Celonis Version 4.0. Zur Simulation der Unternehmensumwelt wurde der White Collar Hacking Contest mehrfach durchgeführt, bei dem die Teilnehmer abwechselnd als Wirtschaftskriminelle und Wirtschaftsprüfer agieren. Ein Datengenerator wurde entwickelt und Datensätze aus zwei realen Unternehmen analysiert.

- **Wissensbasis**

Für die Implementierung des Prototyps werden etablierte Ansätze von Process Mining, Red Flag Detektion, ERP Systeme und Datenanalyse zurückgegriffen. Für die Schaffung der Wissensgrundlage werden drei Literaturstudien durchgeführt. Anschließend wird ein Prototyp erstellt, der auf Grundlage der zuvor identifizierten Red Flags und den Process Mining Algorithmen, wirtschaftskriminelles Verhalten identifiziert. Für die Identifikation von Fraud wird das Framework von Albrecht et al. (2012) und Bozkaya, Gabriels, & Werf (2009) verwendet.

- **Relevanz**

Der Bedarf einer Lösung existiert durch den hohen Verlust durch Fraud. Laut einer aktuellen Studie der ACFE liegt der durchschnittliche, weltweite Verlust durch Fraud bei 5% des jährlichen Umsatzes eines Unternehmens (ACFE, 2018). Bei den gängigen Fraud Detektionsverfahren ist oft eine Flut an Hinweisen mit einer hohen Anzahl an falsch-positiven Werten zu erkennen (Luell, 2010). Um dieses Problem zu lösen, soll der etablierte Red Flag Ansatz mit Process Mining ergänzt werden, sowie Red Flags zu Fraud Patterns kombiniert werden.

- **Rigor**

Die theoretischen Grundlagen werden aus der Wissensbasis genommen und bilden das Fundament des Prototyps. Konkret werden existierende Fraud Fälle und Red Flags aus der Literatur extrahiert. Zusätzlich wird auf bereits existierendes Wissen zur Datenanalyse, ERP Systeme und Fraud Detektionsmethoden aufgebaut. Zur Wissensbasis werden die Fraud Detektionsmuster, die prototypische Implementierung von Process Mining und Red Flags, sowie die Erkenntnisse aus der Evaluierung des Prototyps hinzugefügt.

- **IS Research**

Es wird ein Prototyp erstellt, der eine existierende und etablierte Fraud Erkennungsmethode durch eine relativ neue ergänzt. Der Forschungsprozess basiert auf der zyklischen Abwechslung zwischen der prototypischen Implementierung (Develop/Build) und der Evaluation (Justify/

Evaluate). Dabei wird zunächst ein low-fidelity Prototyp erstellt, der mit Hilfe der Thinking Aloud Methode evaluiert wird. Daraus werden Anforderungen für einen high-fidelity Prototyp abgeleitet. Für die funktionale Evaluierung des Prototyps wird dieser zunächst auf künstlich generierten Daten und zwei realen Datensätzen aus der Praxis angewendet.

Zum Durchführen der Design Science Forschung werden folgende Richtlinien beachtet (Hevner et al., 2004):

1. Design von Artefakten: Forschung gemäß Design Science muss als Resultat ein anwendbares Artefakt hervorbringen. In dieser Arbeit soll eine prototypische Implementierung erstellt werden.
2. Problemrelevanz: Mittels Technologie-Einsatz soll ein in der realen Welt relevantes Problem gelöst werden. In dieser Arbeit soll das Problem der hohen falsch-positiv Rate bei existierenden Fraud Detektionsverfahren gelöst werden.
3. Evaluation des Designs: Nutzen, Qualität und Effizienz des Artefakts müssen nachgewiesen werden. Die prototypische Entwicklung wird zunächst durch die Thinking Aloud Methode evaluiert, um weitere Anforderungen zur Verbesserung der Gestaltung des Prototyps zu erhalten. Zusätzlich wird die Funktionalität mit verschiedenen synthetischen, semi-synthetischen und realen Datensätzen evaluiert.
4. Forschungsbeitrag: es muss ein klar ersichtlicher Beitrag zum Wissensbestand geleistet werden. Die vorliegende Arbeit leistet einen Beitrag zur Forschung, indem zunächst Red Flags aus der Literatur abgeleitet und diese zu Fraud Patterns zusammengefasst werden. Zusätzlich wird der klassische Red Flag Ansatz zur Fraud Detektion mit Process Mining kombiniert. Dadurch soll im Vergleich zu herkömmlichen Verfahren die falsch-positiv Rate gesenkt werden.
5. Forschungsgenauigkeit: Sowohl im Entwurf des Artefakts, wie auch in der Evaluierung müssen präzise Forschungsmethoden eingesetzt werden. Zur Implementierung wird Prototyping verwendet, für das Testen werden funktionale Tests, Fallstudien und die Thinking Aloud Methode angewendet. Für die Erstellung der Fraud Patterns und den dazugehörigen Red Flags werden Literature Reviews verwendet.
6. Design als Suchprozess: Erstellung eines Artefakts verläuft als Suche in einem Problemraum. In dieser Arbeit wurden drei Literatur Reviews durchgeführt, um die Wissensbasis für bestehende Fraud Detektionsalgorithmen, Red Flags und im speziellen Process Mining zu identifizieren.
7. Kommunikation der Forschung: Die Ergebnisse der Forschung sind umfassend zu präsentieren. Die Implementierung wird dokumentiert und der Quellcode bereitgestellt. Zusätzlich werden die Ergebnisse entsprechend publiziert.

Erster Literature Review: Fraud im Einkaufsprozess

Die erste Literaturstudie hat zum Ziel Fraud Fälle und Red Flags aus der Literatur abzuleiten. Zur Erstellung des Literature Reviews wurden die Grundlagen von Webster & Watson (2002)

verfolgt. Dieses Review ist nicht auf wissenschaftliche Publikationen reduziert, sondern umfasst auch Publikationen aus Praxismagazinen.

Literaturauswahl

Um eine möglichst hohe Anzahl an Journale, Magazine und Konferenzen zu erhalten, wurde auf die Datenbank ProQuest[1] zugegriffen. Diese kann auf mehrere Datenbanken simultan zugreifen. Die Mehrheit aller Publikationen wurde in der ABI/INFORM Datenbank identifiziert. Die Suche hat explizit Zeitungsartikel, Internetdokumente, Interviews und Kommentare ausgeschlossen, da diese nicht wissenschaftlich sind. Zusätzlich wurden die Datenbanken Science Direct, IEEE Xplore Digital Library, Springer Link und Ebscohost durchsucht.

Kombinierte Stichwort		
"fraud" "white collar crime" "misappropriation" "corruption" "conflict of interest" "bribery" "kickback" OR "kick back" "shell company"	×	"purchase to pay" "procure to pay" "accounts payable" "procurement"

Individuelle Stichwörter		
"payment fraud"	"purchasing fraud"	"gratuities"
"billing schemes"	"extortion"	

Tabelle 1: Suchbegriffe für das Literaturreview
Quelle: Eigene Darstellung

Die verwendeten Stichwörter und ihre Kombinationen werden in Tabelle 1 dargestellt. Zunächst wird nach jeder Kombination aus den beiden Spalten des Bereichs ‚Kombinierte Stichwörter' gesucht, also beispielsweise nach „bribery" und „procurement". Dabei zeigt die erste Spalte häufig verwendete Begriffe für Fraud, während die zweite Spalte Synonyme für den Einkaufsprozess darstellt. Anschließend wird nach den Begriffen aus dem Bereich ‚Individuelle Stichwörter' gesucht. Diese Liste enthält Fraud Arten die primär im Einkaufsprozess stattfinden. Zusätzlich wird eine Rückwärtssuche nach Webster & Watson (2002) durchgeführt, indem das Literaturverzeichnis nach weiteren Quellen untersucht wird.

Anschließend werden alle Artikel exkludiert, die sich nicht auf den Einkaufsprozess beziehen. Insgesamt werden 72 Artikel als relevant identifiziert. Wissenschaftliche Artikel werden vor allem in Journalen, wie das Journal of Financial Crime oder Journal of Business Ethics

[1] Der Zugriff wurde über den Studenten Julian Lebherz und seinem Universitätsaccount der Illinois University gewährt

veröffentlicht. Praxisorientierte Artikel in Journalen wie das CPA Journal oder Magazinen wie das Journal of Accountancy.

Zweiter Literature Review: Fraud Detektionsverfahren

Die Literaturanalyse von Fraud im Einkaufsprozess hat gezeigt, dass sich wenige Artikel speziell mit dem Einkaufsprozess beschäftigen. Dadurch können Fraud Detektionstechniken nicht ausreichend verglichen werden (Allan & Zhan, 2010). Fraud in benachbarten Gebieten, wie Betrug an Kreditkarten, Telekommunikation oder Versicherungen, wird häufiger von Wissenschaftlern adressiert. Deshalb wird in einem zweiten Literatur Review nach verschiedenen Algorithmen zur Erkennung von Fraud in benachbarten Gebieten gesucht. Dabei wird ein zweistufigen Review Prozess nach den Richtlinien von Bandara, Miskon & Fielt (2011) durchgeführt. Die erste Stufe (A) identifiziert häufig verwendete Fraud Erkennungstechniken, ohne sich auf einen bestimmten Fraudfall oder Prozess zu konzentrieren. Laut Allan Zhan (2010) können die Erkennungsmethoden auf verschiedene Domänen angewandt werden. Die am häufigsten genannten Techniken kommen als Input in die zweite Stufe (B). Dort werden diese miteinander hinsichtlich ihrer Möglichkeit Fraud im Einkaufsprozess zu erkennen verglichen.

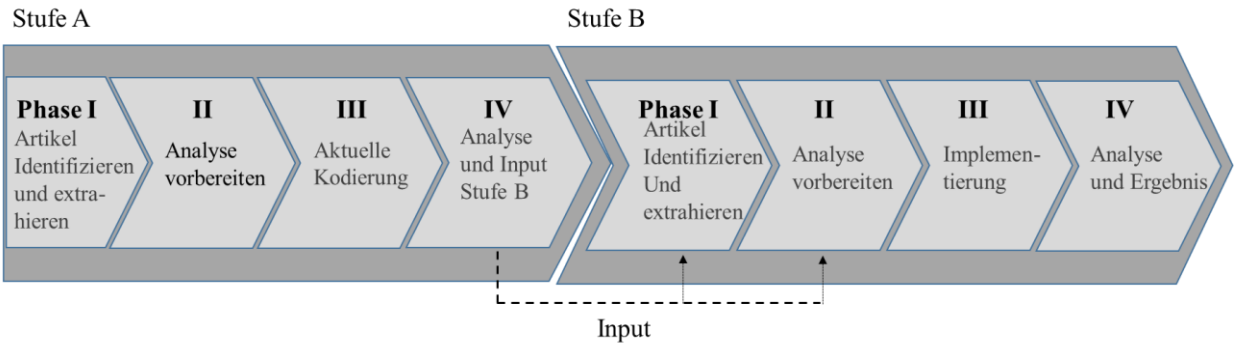


Abbildung 1-2: Vorgehen der Literaturstudie
Quelle: Basierend auf Bandara et al. (2011).

Die Methode ist in Abbildung 1-2 dargestellt und kann in verschiedenen Phasen durchgeführt werden. In der ersten Phase werden alle relevanten Artikel identifiziert und gesammelt. Die Nutzung von verschiedenen Datenbanken und Stichpunkten erlaubt einen transparenten und reproduzierbaren Suchverlauf. Die zweite Phase bereitet das Kodierschema vor, während die eigentlich Kodierung in der dritten Phase durchgeführt wird. Die letzte Phase ist die Analyse und Darstellung der Ergebnisse. Die Ergebnisse aus der ersten Stufe (A) dienen als Input für die Stufe B.

Literaturauswahl [Stufe A – Phase 1]

Es sollen Detektionstechniken für wirtschaftskriminelles Verhalten identifiziert und diese auf den Einkaufsprozess angewendet werden. Laut Bandara et al. (2011) sollen nur die am häufigsten genannten Methoden in die zweite Stufe aufgenommen werden. Deshalb wird nach

publizierten Literaturübersichten gesucht und darauf basierend eine Rückwärts- und Vorwärtssuche durchgeführt.

Zunächst werden die zugänglichen Datenbanken (IEEE Xplore, ABI/Norm (ProQuest), ScienceDirect, JSTOR, EBSCOhost und Google Scholar) durchsucht. Als Suchbegriffe gelten „fraud detection“ und „survey“ oder „review“. Dies führt zu elf Literaturübersichten, die in Tabelle 2 dargestellt sind. Als nächstes werden alle relevanten und in den Studien referenzierten Artikel eingeschlossen. Dabei werden nur Fraud bezogene Quellen analysiert. Viele der gefundenen Artikel werden mehrfach benannt. Dennoch hat die Suche 177 verschiedene Artikel identifiziert.

Identifizierte Reviews von Fraud Detektionsmöglichkeiten		
Referenz	Titel	#Quellen
(Allan & Zhan, 2010)	Towards Fraud Detection Methodologies	33
(Richard J Bolton & Hand, 2002)	Statistical Fraud Detection: A Review	30
(Ngai et al., 2011)	The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature	49
(Pejic-Bach, 2010)	Profiling Intelligent Systems Applications in Fraud Detection and Prevention	31
(Phua et al., 2010)	A Comprehensive Survey of Data Mining-based Fraud Detection Research	57
(Sabau, 2012)	Survey of Clustering based Financial Fraud Detection Research	25
(Sharma & Panigrahi, 2012)	A Review of Financial Accounting Fraud Detection based on Data Mining Techniques	20
(Sudjianto et al., 2010)	Statistical Methods for Fighting Financial Crimes	41
(Wang, 2010)	A Comprehensive Survey of Data Mining-Based Accounting-Fraud Detection Research	19
(Yue, Wu, Wang, Li, & Chu, 2007)	A Review of Data Mining-Based Financial Fraud Detection Research	18
(Kou, Lu, Sirwongwattana, & Huang, 2004)	Survey of Fraud Detection Techniques	11
	Insgesamt (ohne doppelte Einträge)	177

Tabelle 2:Verwendete Surveys in der Literaturstudie

Quelle: Eigene Darstellung

Kodierungsschemata [Stufe A – Phase 2]

Nachdem die Literaturübersichten aus Tabelle 2 analysiert werden, ist eine High-Level Struktur ersichtlich. Abbildung 1-3 zeigt die High-Level Struktur, die zwischen Klassifikation, Clustering, Statistik und Andere unterscheidet.

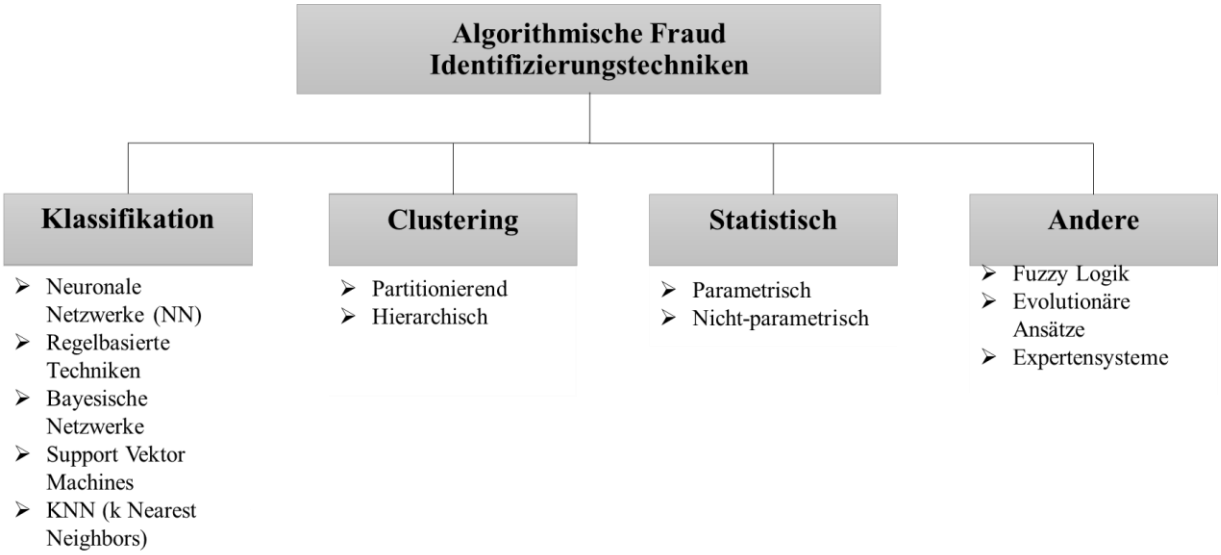


Abbildung 1-3: Klassifikation von Data Mining Techniken für Fraud Erkennung
Quelle: Basierend auf Chandola et al. (2009), Bolton & Hand (2002) und Sabau (2012).

Zur Kategorie ‚Klassifikation' werden Algorithmen eingeordnet, die Trainingsdaten benötigen. Clusteringalgorithmen benötigen keine, da diese aus den Parametern ähnliche Cluster bilden. Statistische Verfahren beinhalten als parametrisierte Verfahren Regression und für nicht-parametrisierte Verfahren beispielsweise die Kernel Methode[2].

Die vorgeschlagenen Kategorien werden als Kodierungsschema verwendet, um die häufigsten Fraud Detektionstechniken zu identifizieren. Da die Artikel verschiedene Fraud-Bereiche abdecken, werden die am häufigsten genannten betrachtet:

- Kreditkartenfraud
- Geldwäsche
- Interner Fraud/Mitarbeiterfraud
- Jahresabschluss Fraud
- Versicherungsfraud
- E-commerce Fraud
- Telekommunikationsfraud
- Insiderhandel
- Finanzbetrug

[2] Details bezüglich der einzelnen Techniken können hier nachgelesen werden: Chandola, Banerjee, and Kumar (2009), Sabau (2012), Sheskin (2003) und Sharma and Panigrahi (2012).

- Fraud im Allgemeinen

Kodierung [Stufe A – Phase 3]

In dieser Phase werden die identifizierten Quellen analysiert und nach dem Kodierungsschema klassifiziert. Drei Artikel behandeln mehrere Bereiche von Fraud, während sich neun Artikel mit Fraud im Allgemeinen beschäftigen. Diese werden zur Kategorie ‚Genereller Fraud' eingeordnet. Um die Anzahl der Kategorien zu beschränken, wird bspw. Versicherungsbetrug in der Gesundheits- und in der Automobilbranche zu der allgemeinen Kategorie ‚Versicherungsbetrug' zusammengefasst. Eine genaue Ausführung aller Kategorien zeigt Tabelle 3.

Fraud	Beschreibung	Zusammengefasst mit
KF	Kreditkartenfraud	-
ECOM	E-Commerce Fraud	Fraud in Online Auktionen
FinBet	Finanzbetrug	Steuerfraud, Außenhandelsfraud
Vers.	Versicherungsfraud	Gesundheitsversicherung- und Automobilversicherungsfraud
Geldw.	Geldwäsche	-
Mitarb.	Mitarbeiterfraud	Lagerzyklus Fraud, Lagerungsfraud, Beschaffungsfraud
TELCO	Telekommunikationsfraud	-
TRAD	Insiderfraud	-
GEN	Genereller Fraud	[generelle Behandlung von Fraud]

Tabelle 3: Fraudkategorien für die Kodierung
Quelle: Eigene Darstellung.

Zusätzlich werden alle Artikel zu den zuvor identifizierten Fraud Detektionstechniken zugeordnet. Einige Publikationen vergleichen mehrere Ansätze und werden entsprechend zu mehreren Kategorien zugeordnet[3].

Analyse [Stufe A – Phase 4]

Alle 177 Quellen werden zu dem Kodierschema zugeordnet. Die Ergebnisse werden in der Literaturanalyse in Kapitel "4.2 Fraud im Einkaufsprozess" vorgestellt.

[3] Diese sind Viaene, Derrig, Baesens, and Dedene (2002), Kotsiantis, Koumanakos, Tzelepis, and Tampakas (2006) und Yeh & Lien (2009).

Dritte Literaturstudie: Fraud Detektion mit Process Mining

Ziel der zweiten Literaturstudie ist die am häufigsten verwendeten Detektionsalgorithmen für Fraud zu identifizieren. Da Process Mining ein relativ neues Verfahren ist und somit aus den vorherigen Suchkriterien fällt, soll gezielt nach Literatur zu Process Mining gesucht werden. Dabei wird nach Process Mining im Allgemeinen und nach bestehenden Ansätzen zur Identifikation von Fraud durch Process Mining gesucht.

Hierzu werden die Richtlinien von Webster & Watson (2002) verwendet. Zunächst werden alle der TU München verfügbaren Datenbanken (Science Direct, IEEE Xplore Digital Library, Springer Link und Ebscohost) durchsucht. Zusätzlich werden auch Researchgate und Google Scholar verwendet. Als Suchwörter werden folgende Begriffe und Begriffskombinationen verwendet:

Kombinierte Keywords		
"process mining" "workflow mining" "process model"	×	Fraud detection Conformance checking Fraud

Abbildung 1-4: Kombinierte Stichwörter
Quelle: Eigene Darstellung

Zusätzlich wird nach *Process Mining*, *Workflow Mining* und *Process Model* gesucht. Dies führt zu etwa 19000 Treffern in den entsprechenden Datenbanken. Nach Durchsicht des Titels und Abstracts, werden die meisten Artikel wieder verworfen. Übrig bleiben 60 Artikel, bei denen eine Rückwärts- und Vorwärtssuche durchgeführt wird. Insgesamt wird so auf eine Literaturbasis von 68 Artikeln zu Process Mining im Allgemeinen und Process Mining für Fraud Erkennung im Speziellen zugegriffen.

2 Begriffsbestimmung und aktueller Forschungsstand

Nachdem die grundlegenden Forschungsmethoden dargestellt werden, soll als nächstes ein Verständnis über die im Bereich Fraud verwendeten Begriffe geschaffen werden.

2.1 Fraud Terminologie

Über die gesamte Fraud Forschung hinweg, werden unterschiedliche Begrifflichkeiten für Fraud und wirtschaftskriminelles Verhalten geprägt. Zunächst soll an dieser Stelle eine Übersicht über Fraud Bezeichnungen gegeben werden.

White Collar Crime (WCC)

Im Jahre 1916 hat erstmalig ein niederländischer Kriminologe eine Theorie über ‚Kriminalität in den Suiten (crime in the suites)' aufgestellt. Üblich war es bis dato nur über ‚Kriminalität in den Straßen (crime in the streets)' zu forschen (Bonger, 1916). Erste Forschungsvorhaben werden im Jahre 1939 durch den Soziologen Edwin Sutherland bei einer Rede in der American Sociological Sociaty vorgestellt. Dort wird erstmalig der Begriff White Collar Crime (WCC) geprägt (Sutherland, 1940). Später definiert er WCC als *"a crime committed by a person of respectability and high social status in the course of his occupation"* [4] (Sutherland, 1983).

Edelhertz (1970) baut auf die Arbeiten auf und analysiert die Eigenschaften von solchen Straftaten. Er verfeinert die Definition von WCC zu *"an illegal act or series of illegal acts committed by non-physical means and by concealment or guile, to obtain money or property, to avoid the payment or loss of money or property, or to obtain business or personal advantage".*[5] (Edelhertz, 1970).

Oft werden gleichbedeutend auch die Begriffe ‚Elite Devianz' (Simon & Eitzen, 1982) oder ‚Geschäftskriminalität' (Conklin, 1977) verwendet. Diese drücken essentiell dieselbe Art von Verbrechen aus. Einen Konsens über die gemeinsame Terminologie gibt es in der Literatur nicht. Um dieses Problem zu lösen, haben sich im Jahre 1995 führende Wissenschaftler im Bereich WCC zu einem Workshop getroffen, um eine verständliche und präzise Definition von WCC zu erzielen. Ihre Definition von WCC ist: *"illegal or unethical acts that violate fiduciary responsibility or public trust, committed by an individual or organization, usually during the course of legitimate occupational activity, by persons of high or respectable social status for personal or organizational gain"*[6] (Helmkamp, Ball, & Townsend, 1996). WCC beschreibt dabei eine Vielzahl von Straftaten, einschließlich Unternehmenskriminalität, Kriminalität gegen das Unternehmen, Untreue, Bestechung oder Korruption.

Fraud

Im Gegensatz zu WCC wird der Begriff ‚Fraud' häufig in der Unternehmenswelt verwendet.[7] Wissenschaftler (wie bspw. Albanese (1996)) sehen Fraud als eine Unterordnung von WCC, wohingegen eher praktisch orientierte Publikationen (wie Clinard & Quinney (1967) und Silverstone & Sheetz (2007)) WCC als eine Unterordnung von Fraud sehen. *"In its broadest terms, fraud means obtaining something of value or avoiding an obligation by means of*

[4] Frei übersetzt: „ein Verbrechen, dass von einer respektablen Person mit hohem sozialen Status im Laufe seiner Tätigkeit [im Unternehmen] begangen wird."

[5] Frei übersetzt: „eine illegale Handlung oder eine Serie von illegalen Handlungen, die durch nicht-physische Mittel und durch Verschweigung oder List begangen wird, um Geld oder Eigentum zu erlangen, um die Zahlung oder den Verlust von Geld oder Eigentum zu vermeiden, oder um geschäftliche oder persönliche Vorteile zu erlangen"

[6] Frei übersetzt: „illegale oder unethische Taten, die treuhändische Verantwortung oder öffentliches Vertrauen verletzen, durchgeführt durch eine einzelne Person oder Organisation, normalerweise während legitimen beruflichen Tätigkeiten, durch eine Person eines hohen oder respektvollen sozialen Status als persönliche oder organisatorische Bereicherung"

[7] KPMG (2013a); ACFE (2012); AICPA (2002); IAASB (2009); Wells (2013); Vona (2011); Coenen (2008).

deception"[8] (Duffield & Grabosky, 2001). Der Begriff "Fraud" wird hauptsächlich in der Konzernrevision oder Forensik verwendet. Entsprechende Organisationen (AICPA, 2002; IAASB, 2009; IIA, 2012) haben ein hohes Interesse präzise Richtlinien, Industrie Standards und Definitionen der entsprechenden Terminologie zu entwickeln. Das Institut of Internal Auditors (IIA) definiert Fraud als: *"any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage"*[9] (IIA, 2012).

Jede Straftat besteht aus drei Elementen: die Handlung, die Vertuschung und die Umsetzung (Albrecht et al., 2012). Während die Handlung die eigentliche Durchführung der Straftat beinhaltet, verwischt die Verschleierung die Spuren und bei der Umsetzung wird die Beute kassiert (Dorminey, Fleming, Kranacher, & Riley, 2012). Diese essentiellen Fraud Elemente werden oft als Fraud Elementdreieck zusammengefasst (Albrecht et al., 2012), welches auch als Dreieck der Fraud Handlung bezeichnet wird (Dorminey et al., 2012). Dies sollte allerdings nicht mit dem Fraud Dreieck verwechselt werden, welches in Kapitel 2.4.1 beschrieben wird.

Occupational Fraud (Mitarbeiterfraud, interner Fraud, dolose Handlungen)

Wie der Name bereits sagt handelt es sich bei dieser Art von Fraud um eine Straftat, die durch Mitarbeiter durchgeführt wird (Clinard & Quinney, 1967). Dabei beschreiben verschiedene Begriffe diese Art von Fraud, wie beispielsweise Mitarbeiterfraud, Mitarbeiterdiebstahl, interner Fraud oder Unterschlagung (Coenen, 2008). Diese Begriffe beziehen sich auf dieselbe Art von Fraud, die folgendermaßen definiert werden kann: *"The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets"*[10] (ACFE, 2012).

Diese Definition exkludiert einige Formen von WCC, wie bspw. Meineid, Erpressung, Behinderung der Justiz oder Ordnungswidrigkeiten. Sie konzentriert sich hauptsächlich auf die persönlichen Vorteile des Täters und beinhaltet keine Vorteile der Organisation, wie in der Definition von WCC oder Fraud. Jedoch beinhaltet sie alle Formen von Veruntreuung, Korruption und Jahresabschlussfraud, solange die Fälschung monetäre oder berufliche Vorteile für den Täter hat. Da sich diese Dissertation mit Mitarbeiterfraud befasst, wird diese Definition als zugrundeliegende Definition verwendet.

Im deutschsprachigen Raum wird häufig in diesem Zusammenhang von dolosen Handlungen gesprochen. Dolose Handlungen sind Handlungen, bei denen „[d]er Mitarbeiter, der eine dolose

[8] Frei übersetzt: Im weitesten Sinne bedeutet Fraud etwas von Wert zu erhalten oder eine Verpflichtung durch Täuschung zu vermeiden

[9] Frei übersetzt: jegliche illegale Handlung gekennzeichnet durch Täuschung, Verschleierung oder Vertrauensbruch. Diese Handlungen sind nicht abhängig von Androhung von Gewalt oder körperlicher Gewalt. Frauds werden von Parteien oder Organisationen begangen um Geld, Eigentum oder Dienstleistungen zu erhalten, die Zahlung oder den Verlust von Leistungen zu vermeiden, oder persönliche oder geschäftliche Vorteile zu sichern

[10] Frei übersetzt: Die Nutzung seiner Beschäftigung für die persönliche Bereicherung durch den vorsätzlichen Missbrauch oder falsche Anwendung von Ressourcen oder Vermögen der arbeitgebenden Unternehmen

Handlung begeht, […] sich zum Zeitpunkt des Delikts darüber im Klaren [ist], dass er gegen Gesetze und/oder interne Regelungen verstößt. […] Hierbei ist der verursachte Schaden für das Unternehmen vorsätzlich oder grob fahrlässig in Kauf genommen worden. […] Eine dolose Handlung ist durch die Erlangung eines persönlichen Vorteils für den Täter gekennzeichnet" (Deling, 2005).

Corporate Fraud (Unternehmensfraud)

Im Gegensatz zu Occupational Fraud ist Corporate Fraud charakterisiert durch Angriffe, die im Namen des Unternehmens stattfinden. Dabei sind die eigenen Vorteile der Mitarbeiter indirekter Natur (Gerber & Jensen, 2007). Ähnliche Begriffe sind Corporate Deviances (Unternehmensabweichungen) (Ermann & Lundman, 1982) und Corporate Crime (Unternehmensverbrechen) (Clinard, Yeager, & Clinard, 1980). Diese werden seltener benutzt, können aber als Synonyme verwendet werden. Unternehmensfraud wird von Clinard & Quinney (1967) definiert als: *"illegal activities of large corporations [...] and the executives acting on their behalf. It involves violations of laws, statutes and regulatory standards affecting corporations for corporate profit and not for the sake of personal gain by an individual [...] working for the corporation"*[11] (Clinard & Quinney, 1967).

Diese Handlungsweisen werden selten in den elektronischen Daten der Unternehmen gespeichert und entgehen dementsprechend der automatischen Frauderkennung. Auch ist es nicht Gegenstand dieser Dissertation sein.

Internes Kontrollsystem und Compliance

Ein internes Kontrollsystem (IKS) eines Unternehmens ist definiert als ein System aus Kontrollen, das Unternehmensziele sicherstellt und Risiken minimiert (Chuprunov, 2011). Es umfasst alle Prüfungen über die Einhaltung von Compliance Vorgaben und Gesetzeskonformitäten. Auch zählt zu den Zielen eines IKS die Prüfung von Effizienz und Wirtschaftlichkeit eines Unternehmens. In dieser Dissertation wird davon ausgegangen, dass Täter möglichst unbemerkt Kontrollen umgehen, um Fraud zu begehen.

Compliance hingegen bezeichnet das Einhalten von Regeln und die Konformität gegenüber gesetzlichen Regelungen, Regelungen der Finanzberichterstattung oder der rein unternehmensinternen und branchenspezifischen Regelungen (Chuprunov, 2011).

Audit

Unter Audit wird das regelmäßige Prüfen der Finanzdaten eines Unternehmens mit dem Ziel Unregelmäßigkeiten im Jahresabschluss und den Unternehmensdaten zu identifizieren (Wells, 2011). Dabei wird zwischen gewöhnlichen, grundlosen Audit und Fraud Examination

[11] Frei übersetzt: illegale Aktivitäten großer Unternehmen [...] in dessen Namen die Führungskräfte handeln. Es beinhaltet den Verstoß gegen Gesetze, Satzungen und regulatorische Standards die Unternehmen und Unternehmensgewinne beeinflussen und nicht zum Zwecke der persönlichen Bereicherungen der einzelnen im Unternehmen dienen

unterschieden. Bei Fraud Examination wird bei Verdacht überprüft, ob sich dieser erhärtet (Wells, 2011).

2.2 Fraud Verbreitung

Die Verbreitung von Fraud hat einen signifikanten Einfluss auf alle Unternehmen weltweit. Obwohl es verschiedene Ansätze und Maßnahmen zur Reduktion von Fraud gibt, ist der durch Fraud entstandene Schaden kaum zurückgegangen. Zweijährlich bringt die weltweit größte Fraud Organisation, die Association of Certified Fraud Examiners (ACFE), einen ‚Bericht an die Nation' über die aktuelle Fraud-Entwicklung heraus. Abbildung 2-1 zeigt den durchschnittlichen Verlust durch Fraud in den letzten 20 Jahren basierend auf den genannten Fraudberichten. Dabei setzt die Grafik die geschätzten Verluste durch Fraud in Relation zu dem amerikanischen Bruttoinlandsprodukt.

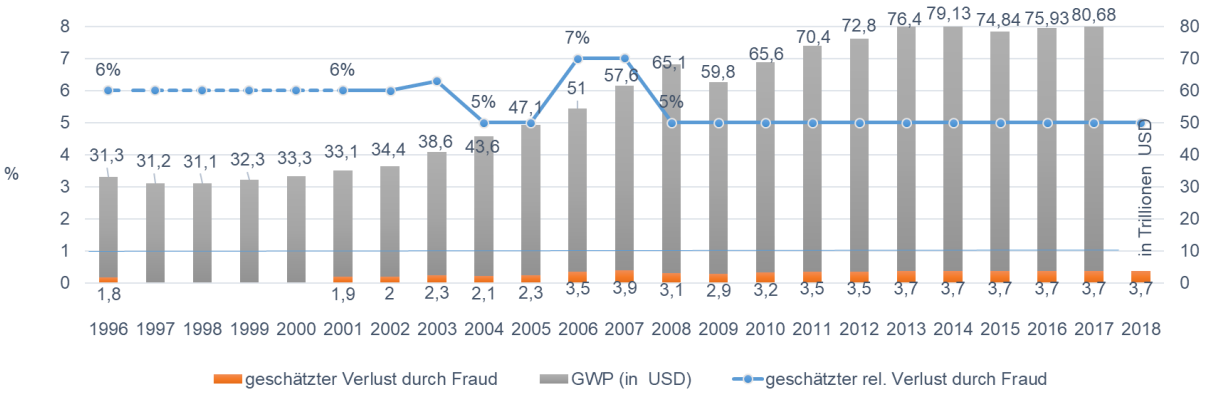


Abbildung 2-1: Zusammenhang zwischen den Umsätze eines Unternehmens und den Verlust durch Fraud
Quelle: Basierend auf den weltweiten Bruttoinlandsproduktdaten von Bank (2018) und den geschätzten Fraud Verlusten (ACFE, 1996, 2002, 2004, 2006, 2008, 2010, 2012, 2014, 2016, 2018)

Die Fraud-Prognosen sind relativ stabil und schwanken zwischen 5% und 7%, wobei es in den letzten Jahren konstant bei 5% geblieben ist. Beachtet man, dass erfolgreiche Unternehmen, wie beispielsweise Airlines, mit Profitmargen von ca. 3%[12] operieren, so kann man die Wichtigkeit der Bekämpfung von Fraud weltweit erahnen. Experteneinschätzungen zu Folge lässt sich trotz vieler anti-Fraud und anti-Korruptionsmaßnahmen kein signifikanter Rückgang in den Fraudfällen erkennen (ACFE, 2016). Wenn man dies mit dem Bruttoinlandsprodukt vergleicht, so zeigt sich ein noch düsteres Bild. Während das nominale Bruttoinlandsprodukt zwischen 1996 und 2018 fast kontinuierlich gestiegen ist, so hat sich der relative Verlust durch Fraud nicht reduziert. Im Umkehrschluss bedeutet dies, dass der absolute Verlust durch Fraud stetig wächst.

Alle hier zugrunde gelegten Kennzahlen sind Schätzwerte. Es liegt in der Natur des Problems, dass keine exakte Messung von Fraud möglich ist. Die ACFE reflektiert aggregierte Meinungen

[12] Profitmargen entnommen aus: http://www.gevestor.de/details/software-und-it-hohe-ebit-margen-im-branchenvergleich-753237.html.

von Fraud Experten (ACFE, 2018). Andere Studien adressieren leitende Angestellte und sammeln Daten über die aktuellen Vorfälle. Kroll (2017) zum Beispiel erstellt eine jährliche Umfrage, an der hunderte Manager teilnehmen. Diese zeigt, dass der Verlust durch Fraud lediglich bei 1,4% des durchschnittlichen Umsatzes eines Unternehmens liegt. Diese Schätzung ist signifikant tiefer als von der ACFE und hängt mit der Umfragestrategie zusammen. Kroll befragt leitende Angestellte nach den tatsächlich in ihrem Unternehmen vorkommenden Fraudfällen und den dazugehörigen Verlusten. Viele Angriffe bleiben unentdeckt und tauchen somit nicht in Krolls Report auf. Laut Coenen (2008) bleiben drei Viertel der Fraud Schemata unter dem Radar der Ermittler. Auch sind viele aufgedeckte Angriffe strikt vertraulich und werden nur intern behandelt, um das Vertrauen der Stakeholder nicht zu gefährden und um nicht in den Medien zu erscheinen (ACFE, 2016; Pedneault, 2009; PWC, 2016). Abhängig von den Umständen dieser Szenarien, werden diese auch in anonymen Antworten nicht erwähnt. Krolls Umfrage führt sicherlich zur Untertreibung der aktuellen Fraud Zahlen, während die ACFE Studie den finanziellen Einfluss von internen Fraud durch persönliche Motive der befragten Experten vermutlich überschätzt. Die tatsächliche Prozentzahl der Verluste durch Fraud liegt vermutlich zwischen den beiden Studien. Trotzdem hat Fraud einen hohen Einfluss auf die Profitmargen der Unternehmen und ihrer Reputation.

Nach der globalen Analyse des internen Frauds, wird im Folgenden die Verbreitung von Fraud in verschiedenen Regionen, Ländern und Industrien betrachtet. Nach Kroll (2013) ist die öffentliche Wahrnehmung von Fraud auf geographischen Gegenden beschränkt. So wird angenommen, dass Fraud vor allem in Entwicklungsregionen und -ländern (bspw. Mexiko, Indien) vorkommt, während es in westlichen Ländern (bspw. USA, Westeuropa) als weniger verbreitet gilt. Abbildung 2-2 fasst die Verbreitung von Fraud basierend auf den Umfragen von Kroll zusammen. Betrachtet man die konkreten Zahlen, kann die öffentliche Wahrnehmung nicht bestätigt werden. Vergleicht man die durchschnittlichen Fraud Zahlen von 2015 in den fortgeschrittenen Nationen (69,3%) mit dem Durchschnitt in den Entwicklungsländern (70,4%), ist die Differenz sehr gering (ca. 1%)[13]. Die Zahlen müssen allerdings vorsichtig betrachtet werden, da es Unterschiede in den Erhebungsinstrumenten der Studien gibt.

Geographische Entität	**Fraud Verbreitung**					**Trend**
	2011	**2012**	**2013**	**2015**	**2017**	**2011 → 2018**
Umfragenperiode	09/2010 08/2011	09/2011 08/2012	09/2012 08/2013	01/2015 03/2015	07/2017 08/2017	
# Befragte	1,265	839	901	768		
Afrika	85%	77%	77%	84%	77%	→
Brasilien	---	(54%)	74%	77%	84%	→
Kanada	70%	(47%)	69%	65%	92%	↗
China	84%	65%	67%	73%	86%	↗
Kolumbien	---	(49%)	63%	83%	61%	→
Europa	71%	(63%)	73%	74%	-	→
Golfstaaten	68%	(49%)	72%	63%	66%	→
Indien	84%	68%	69%	80%	89%	↗

[13] Die Kategorisierung nach Entwicklungs- und Fortschrittsland wird aus den Daten des IMF, (2016) entnommen.)

Mexiko	69%	59%	63%	80%	85%	↗
Russland	---	(61%)	76%	73%	89%	↗
USA	66%	60%	66%	75%	91%	↗

Abbildung 2-2: Verbreitung Fraud nach geografischer Aufteilung
Quelle: Basierend auf (Kroll, 2011, 2012, 2013, 2015, 2017)

Betrachtet man Abbildung 2-2 genauer, so erscheinen einige der Daten im 4-jahres Kontext fehlerhaft zu sein. Beispielsweise ist die Fraudverbreitung in Kanada von 70% auf 47% gesunken und anschließend wieder auf 69% gestiegen. Aus diesem Grund werden die unwahrscheinlichen Zahlen in Klammern gesetzt. Die unerwarteten Werte für das Jahr 2012 können durch die geringe Anzahl an Befragungen erklärt werden, wobei die Verteilung der Befragten pro Region unverändert geblieben ist (Nord Amerika, Europa und APAC ca. jeweils 25%, Lateinamerika und MEA ca. jeweils 12,25%).

Die letzte Spalte in Abbildung 2-2 zeigt den Trend von 2011 zu 2018 an. Leider veröffentlicht Kroll Advisory Solutions weder detaillierte Informationen über die Befragten pro Land, noch kann das Design des Fragebogens eingesehen werden. Im Gegensatz zur öffentlichen Wahrnehmung zeigen die Daten, dass es keine substantiellen Unterschiede zwischen westlichen und Entwicklungsländern gibt.

Es konnte keine Korrelation zwischen dem Wirtschaftsfortschritt und Fraud festgestellt werden. Es stellt sich die Frage, ob es eine Korrelation zwischen der Fraud Verbreitung und Industrie gibt. Banken erscheinen beispielsweise durch die hohen Geldtransaktionen besonders anfällig für Fraud zu sein. Auch könnte man annehmen, dass es einen Zusammenhang zwischen Fraud und dem Level der Regulierung in der Industrie gibt. Eine offensichtliche Relation wäre: je regulierter eine Industrie, desto weniger anfällig für Fraud ist diese. Die größte Vereinigung von Fraudexperten, die ACFE, haben in ihrem Bericht verschiedene Industrien und die entsprechende Verbreitung von Fraud untersucht. Abbildung 2-3 fasst die Ergebnisse basierend auf Verlust und Verbreitung von Fraud zusammen. Laut dem ACFE Report (2018) ist (interner) Fraud besonders im Bereich *Bankenwesen und Finanzdienstleistungen* (16,8%), *Regierung und Verwaltung* (10,5%) und *Fertigung* (8,1%) verbreitet (ACFE, 2018). Die finanziell größten Schäden wurden im Bereich der *Bergbauindustrie* (mittlerer Verlust von 500 Tsd. USD), *Großhandel* (450 Tsd. USD) und *Dienstleistungen* (310 Tsd. USD) erfasst.

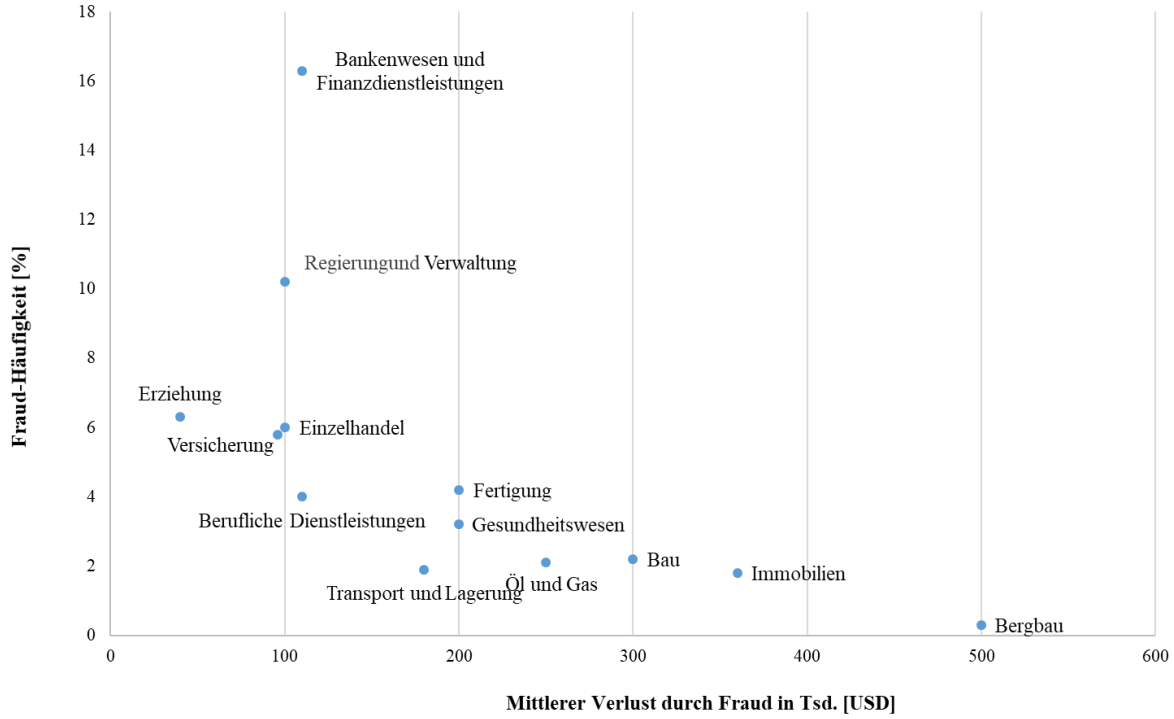


Abbildung 2-3: Fraud Verbreitung und durchschnittlicher Verlust nach Industrie
Quelle: Basierend auf (ACFE, 2016)

Bei einzelnen Unternehmen zeigt eine Studie von Wilson (2004), dass eine überwältigende Mehrheit der Risk Management Experten die Mitarbeiterunehrlichkeit im Allgemeinen als ein großes Problem ansieht. Wenn man dieselben Experten jedoch über das Risiko in ihrem eigenen Unternehmen befragt, so sehen weniger als ein Viertel ein Risiko in ihrem Unternehmen. Diese substantiellen Unterschiede in der Wahrnehmung können durch die Theorie des Optimistic Bias erklärt werden (Kahneman & Lovallo, 1993; Klein & Helweg-Larsen, 2002). Basierend auf dem starken Unterschied zwischen Selbstwahrnehmung und Risiko, unterschätzen Fraud Experten und Vorstände die Unehrlichkeit der Mitarbeiter und das Risiko für Fraud im eigenen Unternehmen. Jedoch sind selbige Personen für die Aufdeckung von Fraud und die Sicherstellung von regelkonformen Aktivitäten zuständig. Ernsthafte Fehleinschätzung durch den Optimistic Bias kann die Effektivität und Effizienz einer etablierten anti-fraud Landschaft zerstören und sogar neue, angebrachte Maßnahmen verhindern. Deshalb ist es sinnvoll auch externe Berater oder Dienstleister zu Rate zu ziehen, um den Optimistic Bias zu reduzieren.

Wenn man nun die vorgestellten Ergebnisse rekapituliert, so zeigen die Daten keine geographischen Ungleichheiten in der Verbreitung von Fraud. Jedoch ist es lohnenswert die Unterschiede in den Industrien zu betrachten, da es einen Zusammenhang zwischen Industrie und dem Verlust und Verbreitung von Fraud gibt. Dieses Wissen kann dabei helfen richtige Maßnahmen für die Aufdeckung von Fraud zu etablieren. Zusätzlich ist es wichtig den Optimistic Bias zu verstehen. Menschen unterschätzen Risiken in ihrem eigenen Unternehmen, so dass der Einbezug von externen Experten zur Reduktion des Optimistic Bias beiträgt.

2.3 Charakteristik eines typischen Wirtschaftskriminellen

Um Fraud effektiv und effizient aufzudecken, müssen Fraud Aufdeckungsmechanismen strikt eingehalten und sorgfältig ausgerichtet werden. Es wird versucht eine Überwachung von Mitarbeitern und deren Geschäftspartner zu etablieren (Coenen, 2008). Ein großes Problem bei der Überwachung von Mitarbeitern ist, dass nicht in ihre Privatsphäre eingegriffen werden darf (ACFE, 2018). Es scheint ein Balanceakt zwischen einer gesunden Transparenz und einer unmoralischen und sogar illegalen Kontrolle von Mitarbeitern zu sein. Eine Studie der KPMG hat gezeigt, dass in 44% aller im Nachhinein identifizierten Fraud Cases eine erhöhte Gefahr von einzelnen Mitarbeitern ausging (KPMG, 2011). Deshalb werden im Folgenden typische Eigenschaften von bekannten Tätern aufgelistet.

Geschlecht

Fraud ist ein geschlechtsabhängiges Phänomen. Das Verhältnis der Anzahl von Taten bei Männern und Frauen ist mit 45% zu 65% relativ ausbalanciert (ACFE, 2018). Jedoch gibt es große Unterschiede im finanziellen Verlust. Der finanzielle Schaden durch Frauen ist von 60 Tsd. USD auf über 90 Tsd. USD (+50%) gestiegen (ACFE 2016; ACFE, 2018). Bei Männern liegt der Verlust bei durchschnittlich 250 Tsd. USD. Diese Summe ist um 25% seit 2001 gestiegen (ACFE, 2012; ACFE 2018). Angenommen die Wahrscheinlichkeit erwischt zu werden sei bei Frauen und Männer gleich, so begehen Männer mehr Taten und unterschlagen höhere Summen.

Zusammenarbeit

Fraud wird nicht nur durch interne Mitarbeiter begangen, sondern auch von Partnern, wie Kunden, Lieferanten oder Agenten (PWC, 2016). Diese sind für mehr als 40% aller Delikte verantwortlich, allen voran Kunden mit einem Drittel dieser Delikte. Demgegenüber hat die KPMG (2011) herausgefunden, dass ca. 90% aller Fraudtäter interne Mitarbeiter des Unternehmens sind. Da der Zugang zu externen Partnern erschwert ist, konzentrieren sich Auditoren und Anti-Fraud Experten oft auf interne Mitarbeiter. Die Mehrheit aller Fraudfälle wird durch eine Kooperation mehrerer Täter durchgeführt. So berichtet die ACFE (2016) von einer Kooperation in 42% aller Fälle, während die KPMG (2013) bei mehr als 70% von Kooperationen ausgeht. Da der durchschnittliche finanzielle Schaden von Gruppen über 2.5x höher ist als bei Einzeltäter (ACFE, 2014), sollten Fraud Investigationen Gruppen berücksichtigen.

Alter

Das Alter des Täters ist ein einfach zu messender Einflussfaktor. Es scheint plausibel, dass junge Angestellte verhältnismäßig selten bei wirtschaftskriminellen Taten erwischt werden, da diese zunächst mit den Prozessen und Kontrollen des Unternehmens vertraut werden müssen und weniger Berechtigungen in den entsprechenden Systemen haben. Mit dieser Argumentation einhergehend berichtet die KPMG (2013), dass nur 3% aller Täter unter 26 Jahre alt sind und nur 17% der Täter 35 Jahre oder junger sind. Die Studie der ACFE (2018) berichtet einen höheren Prozentsatz. Demnach sind 6% aller Täter unter 26 Jahre und 32% unter 35 Jahre alt. Vergleicht man diese Angaben mit der durchschnittlichen Altersverteilung in Unternehmen in den USA (BLS, 2015), verstärkt dies die zuvor aufgestellte Hypothese. Die höchste Anzahl von Taten werden im Alter zwischen 36-45 Jahren begangen. Älteres Personal ist weniger geneigt sich strafbar zu machen. Diese bilden 21% der Arbeitnehmer, sind jedoch nur für ca. 10% der identifizierten Betrüge verantwortlich. Allerdings sind vor allem ältere Täter für große finanzielle Schäden verantwortlich. Außerdem kann die Erfahrung und Betriebszugehörigkeit älterer Arbeitnehmer dazu führen, dass diese weniger in Verdacht stehen und somit seltener erwischt werden. Während betrügerische Handlungen von Berufseinsteiger (unter 26 Jahren) durchschnittlich nur 50 Tsd. USD Verlust verursachen, so steigt der finanzielle Schaden durch Fraud mit dem Alter des Täters. Der Peak von 360 Tsd. USD ist in dem Alter der 46-55-jährigen Mitarbeiter zu sehen (ACFE, 2018). Abbildung 2.4 fasst die Anzahl der Frauddelikte pro Alter zusammen.

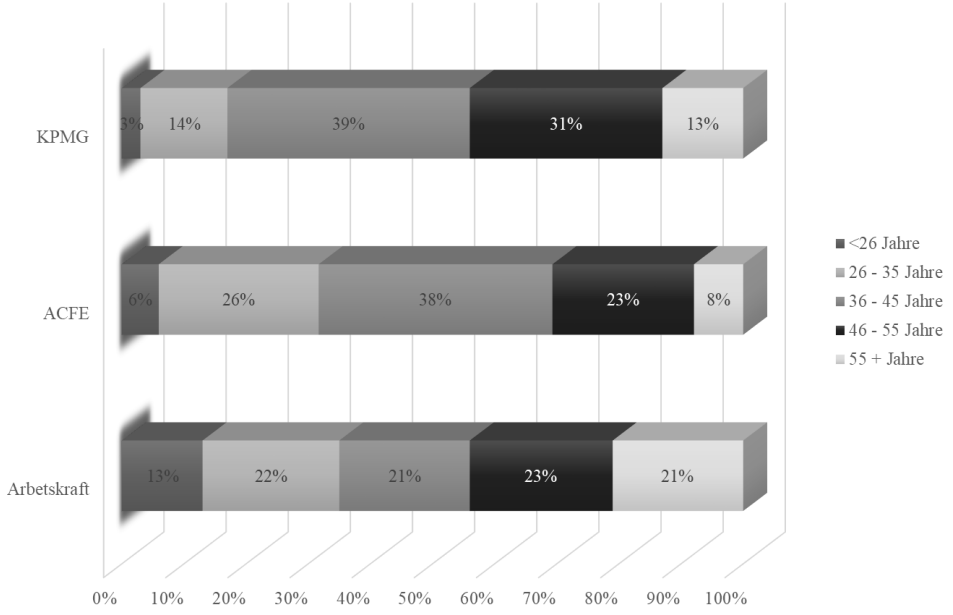


Abbildung 2-4: Fraud nach Alter und US Arbeitskraft

Quelle: Basierend auf KPMG (2011); ACFE (2018); BLS (2013)

Betriebszugehörigkeit

Das Alter des Täters ist indirekt mit der Amtszeit in einem Unternehmen verbunden, allerdings nicht ausschließlich. Arbeitnehmer können eine Umorientierung oder einen Arbeitgeberwechsel vollzogen haben. Diese müssen sich im neuen Unternehmen zunächst ein Netzwerk aufbauen, um bei Ungereimtheiten nicht verdächtigt zu werden und gegebenenfalls

Komplizen zu finden. Abbildung 2-5 zeigt die Abhängigkeit von Betriebszugehörigkeit zu Anzahl der Fraudfälle und zum finanziellen Schaden.

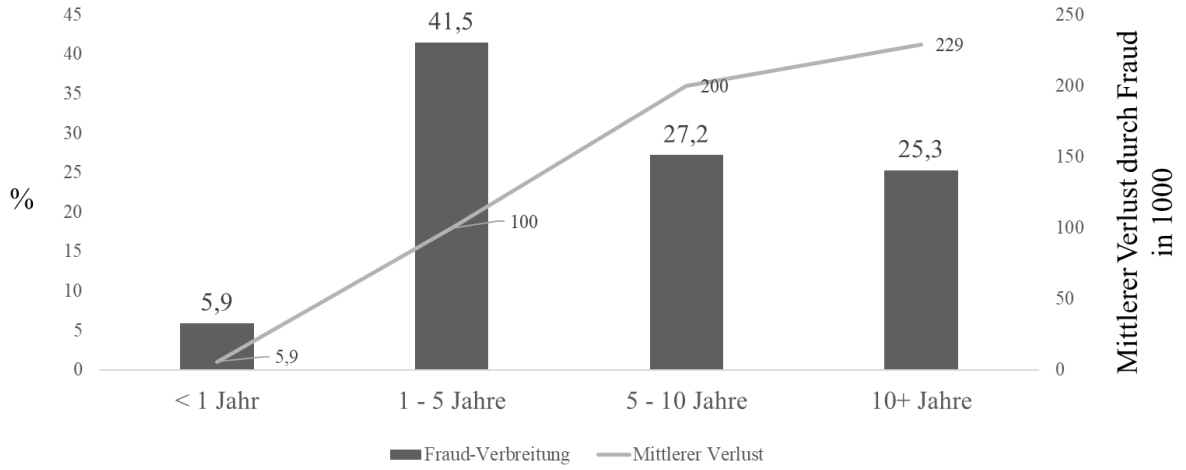


Abbildung 2-5: Fraud Verbreitung und Verlust (Median) sortiert nach Arbeitszugehörigkeit
Quelle: Basierend auf ACFE (2018).

Weniger als 6% aller Fraudfälle werden von Mitarbeitern getätigt, die weniger als ein Jahr in einem Unternehmen sind. Am häufigsten (mit 41,5%) begehen Mitarbeiter mit einer Betriebszugehörigkeit von 1-5 Jahren Fraud. Der durchschnittliche finanzielle Verlust steigt mit der Betriebszugehörigkeit von 25 Tsd. für Neueinsteiger (unter einem Jahr Betriebszugehörigkeit) zu 229 Tsd. USD.

Rang

Auch der Rang in der Unternehmenshierarchie hat statistisch gesehen eine Auswirkung auf Fraud. Wenn untergeordnete Mitarbeiter Ungereimtheiten bei ihrem Vorgesetzten entdecken, entscheiden sich diese oft aus Furch vor persönlichen Konsequenzen gegen jegliche Handlungen. ACFE (2016) und PWC (2016) unterscheiden in ihren Berichten zwischen Mitarbeitern, Managern und leitenden Angestellten und Besitzern, während KPMG (2011) noch zusätzlich das Senior Management betrachtet. Allerdings unterscheiden sich ihre Ergebnisse nicht signifikant von der Management Kategorie der anderen Berichte, so dass die Studien vergleichbar sind. Zusammenfassend zeigen die Studien, dass ca. 43% der Mitarbeiter, ca. 43% der Manager und ca. 16% der leitenden Angestellten und Eigentümer Fraud begehen. Da in Unternehmen üblicherweise wesentlich weniger Manager im Vergleich zu Angestellten beschäftigt sind, ist die gleiche prozentuale Verteilung erstaunlich. Die ACFE hat zusätzlich auch den Durchschnittsverlust durch Fraud am Rang des Mitarbeiters gemessen. So steigt der durchschnittliche unterschlagene Wert von 60 Tsd. USD für einfache Mittarbeiter auf 182 Tsd. USD für Manager und 573 Tsd. USD für Eigentümer und leitende Angestellte (ACFE, 2016). Fraud Detektionsverfahren sollten also ein besonderes Augenmerk auf leitende Angestellte, Manager und Eigentümer haben.

Abteilung

Ein Einflussfaktor für die Wahrscheinlichkeit wirtschaftskriminelle Handlungen zu begehen, ist die Funktion des Mitarbeiters und damit einhergehend seine Abteilung. Mitarbeiter mit Kunden- oder Lieferantenkontakt oder der Bearbeitung hoher Zahlungsströme, stehen in Verdacht häufiger Fraud zu begehen. Ähnliches gilt auch für Buchhalter, da diese zwar nicht direkt im Transfer von Geldern involviert sind, aber wirtschaftskriminelle Taten in der Buchhaltung verstecken können. Auch sind leitende Angestellte und hohes Management häufiger in solchen Taten verwickelt, da ihre Entscheidungen durch ihre hohe Macht-, Kontroll- und Autoritätsstellung im Unternehmen selten hinterfragt werden. Abbildung 2-6 zeigt sechs Abteilungen in denen am häufigsten Fraud begangen wird. Mitarbeiter der Buchhaltung sind mit 22% aller Fälle und einem durchschnittlichen Verlust von 183 Tsd. USD am häufigsten für Fraud verantwortlich, gefolgt vom Betrieb (17,4% aller Taten) mit einem Durchschnittsverlust von 100 Tsd. USD (ACFE, 2018). Die hohe Anzahl von Delikten im Betrieb kann durch die Beteiligung der Mitarbeiter in allen wertbeitragenden Prozeduren erklärt werden. Außerdem erstellen diese meist Anforderungen für Rohmaterial, IT Dienstleistungen oder Maschinen, die in Bestellanforderungen, Bestellungen oder auch direkt in einen Vertrag mit Dienstleister oder Lieferanten übergehen. Dies führt zu einem erhöhten Risiko für Bestechungen, Überbezahlungen oder für Scheinfirmen. Die Vertriebsabteilung ist für 12,8% aller Fälle mit durchschnittlich 90 Tsd. USD Verlust verantwortlich, gefolgt von leitenden Angestellten und oberes Management. Diese sind für 11,9% aller Fälle verantwortlich und unterschlagen durchschnittlich 500 Tsd. USD (ACFE, 2018). Diese hohen Verluste sind vor allem ihrem großen Vertrauensnetzwerk zuzuschreiben.

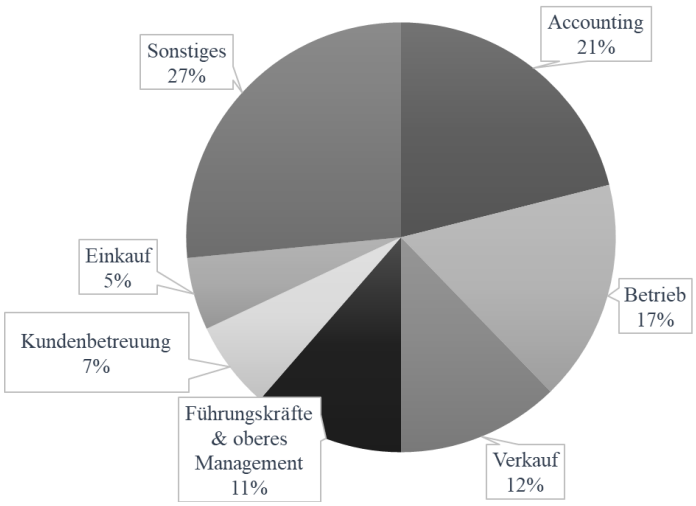


Abbildung 2-6: Täter sortiert nach Abteilung
Quelle: basierend auf ACFE (2018)

Kundenservice und die Einkaufsabteilung sind für 6,9% (30 Tsd. USD) und 5,7% (200 Tsd. USD) aller Betrüge verantwortlich (ACFE, 2018). Im Personalwesen, Rechtsabteilung oder F&E sind wirtschaftskriminelle Handlungen seltener vorhanden. Multipliziert man die veruntreute Summe mit dem prozentuellen Anteil, so sind die meistgefährdeten Abteilungen in

absteigender Reihenfolge: Leitende Angestellte und höheres Management, Accounting, Betrieb, Verkauf und Einkauf.

Kriminelle Vergangenheit

Die Mehrzahl aller Täter hat keine kriminelle Vergangenheit und ist auch nicht aufgrund von Fraud gekündigt worden. Über 87% der Täter sind nie erwischt und über 84% nie bestraft worden (ACFE, 2018). Hintergrundrecherchen der Mitarbeiter sind daher nur selten hilfreich.

Nach den hier gezeigten Dimensionen lässt sich ein typischer Fraudster beschreiben als:
- männlich
- zwischen 36 und 55 Jahre alt
- ohne Vorstrafen
- hat typischerweise eine Managementrolle im Unternehmen (bevorzugt im Accounting) inne
- Kooperiert mit anderen Tätern

Solche Profile erlauben Risikoeinschätzungen für Mitarbeiter im Unternehmen durchzuführen und dadurch die Effizienz der Anti-Fraud Aktivitäten zu steigern.

2.4 Fraud Theorie

Neben der Verbreitung von Fraud sollen an dieser Stelle die gängigen wissenschaftlichen Theorien zu Fraud vorgestellt werden.

2.4.1 Fraud Dreieck

Kriminalität im Allgemeinen hat mehrere Elemente: motivierte Täter, verfügbare und geeignete Ziele, sowie die Abwesenheit von fähigen Wächtern (Cohen & Felson, 1979). Diese Elemente gelten auch für wirtschaftskriminelle Taten. Basierend auf der Arbeit von Sutherland (1949) entwickelt der Kriminologe Cressey (1953) eine Theorie, in der er die drei Hauptfaktoren für Fraud beschreibt: Fraud ist die Kombination von empfundenen Druck, empfundener Möglichkeit und Rationalisierung. Ein potentieller Täter lässt sich nur dazu hinreißen, wenn alle Elemente vorhanden sind (vergl. Abbildung 2-7).

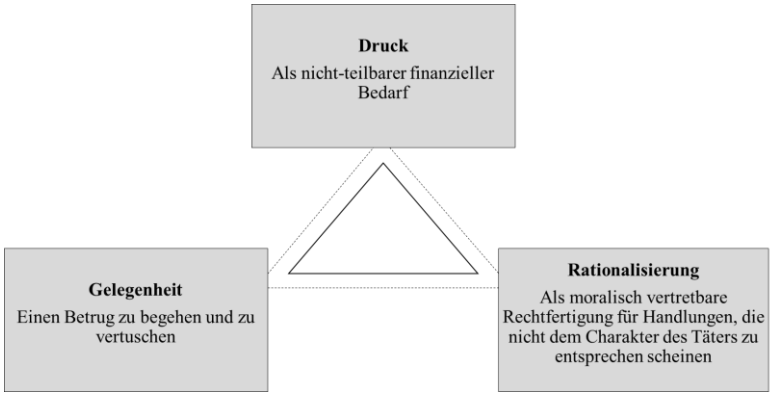


Abbildung 2-7: Fraud Dreieck
Quelle: Basierend auf Cressey (1953)

Das von Cressey entwickelte Modell, das sogenannte Fraud Dreieck, hat Einzug in alle wesentlichen Regulationsstandards gefunden, wie bspw. die Statements of Auditing Standards (SAS) no. 99 (AICPA, 2002) oder die International Standard on Auditing 240 (IAASB, 2009). Verschiedene akademische Publikationen haben einen Nachweis für die positive Wirkung des Fraud Dreiecks auf Fraud Risikoeinschätzung geliefert (Bell & Carcello, 2000; Hogan, Rezaee, Riley, & Velury, 2008; LaSalle, 2007).

Jedoch gibt es auch Kritik an der Unvollständigkeit des Originalmodells (Dorminey, Fleming, Kranacher, & Riley, 2010; Dorminey et al., 2012). Um ein kohärentes Bild über dieses fundamentale Konzept zu erlangen, werden zunächst die drei Kernelemente beschrieben. Auch die in der Literatur vorgeschlagenen Erweiterungen, wie der Fraud Diamant (Wolfe & Hermanson, 2004) und die Theorie des geplanten Verhaltens (Cohen, Ding, Lesage, & Stolowy, 2010), werden vorgestellt.

Druck

Ausgehend von einem persönlichen und situativen Problem kann der wahrgenommene Druck verschiedene Motivationen aufweisen. Mit der ursprünglichen Definition von Druck als eine *nicht-teilbare finanzielle Sorge*, ist der finanzielle Druck die größte Motivation (Albrecht et al., 2012; Biegelman, 2013). Oft haben die Täter das Gefühl, dass die Last unteilbar sei. Dabei spielen weitere Faktoren zusammen, wie ein erhöhtes Ego, Stolz oder Stigmatisierung in der Gesellschaft (Dorminey et al., 2012). Fraudexperten unterscheiden vier verschiedene Arten von Druck: Finanzieller Druck, Laster (Sucht), arbeitsbedingter Druck und weiterer Druck (Albrecht et al., 2012).

Finanzieller Druck kann als Ursprung echte oder gefühlte finanzielle Sorgen haben. Typische Beispiele für echte finanzielle Sorgen sind nicht bezahlte medizinische Rechnungen, Rechnungen zur Unterstützung von Kindern oder finanzielle Verluste durch Fehlinvestitionen oder Entlassungen (Albrecht et al., 2012; Coenen, 2008). Gefühlte finanzielle Nöte können durch das große Verlangen von exklusiven und teuren Produkten, einem exzessiven Lebensstil, einer schlechten Bonität oder einer gierigen Persönlichkeit im Allgemeinen entstehen (Albrecht et al., 2012; Biegelman, 2013; Coenen, 2008).

Laster (Sucht) wie Drogen, Alkohol, Spielsucht oder außerehelich Verhältnisse sind dem finanziellen Druck sehr ähnlich (Albrecht et al., 2012; Biegelman, 2013; Coenen, 2008). Alle diese Laster benötigen kontinuierlich höhere Geldbeträge, um Verschleierungsmaßnahmen zu bezahlen, bzw. um die sich steigernde Dosis im Bereich der Sucht zu finanzieren. Viele Spielsüchtige zum Beispiel leben mit der Illusion ihre Verluste zurückzuerhalten, wenn sie die Einsätze im Spiel erhöhen und somit im Spiel bleiben. Das Vertuschen von außerehelichen Affären kann ebenfalls zu wirtschaftskriminellem Verhalten führen, obwohl es oft vom normalen Gehalt abgedeckt werden könnte. So soll das Familienkonto nicht angerührt werden, um den Partner nicht misstrauisch werden zu lassen. Ein potentieller Täter benötigt eine zusätzliche Einnahmequelle, die nicht durch den Lebenspartner kontrolliert werden kann.

Arbeitsbedingter Druck kann durch hohe Leistungsanforderungen mit unerreichbaren Zielen oder der Verlustangst entstehen (Albrecht et al., 2012; Biegelman, 2013; Coenen, 2008). Weiterer Druck beschreibt die Rache am Unternehmen, emotionale Instabilität oder einfach die Lust am Besiegen des Systems (Albrecht et al., 2012; Biegelman, 2013).

Die Unterteilung von Druck in vier Kategorien weist einige Mängel auf. Zunächst können viele Fraud Szenarien zu verschiedenen Kategorien zugeordnet werden. Beispielsweise führen Laster oft zu realem finanziellen Druck und können somit nicht eindeutig zugeordnet werden. Die generische Kategorie ‚weiterer Druck' enthält konträre Motivationen, wie Rache oder emotionale Instabilität. Daher schlagen Kranacher, Riley & Wells (2011) ein Klassifikationsschema namens MICE[14] vor: money, ideology, coercion und ego (Geld, Ideologie, Zwang und Ego). Diese Einteilung verhindert nicht, dass sich einige Szenarien in mehrere Kategorien einordnen lassen. Es löst die generische Kategorie ‚weiterer Druck' durch den Fokus auf das Motiv des Täters. Wirtschaftskriminelle Taten aufgrund von bestimmten Ideologien kommen selten vor, sind aber möglich. Ein Beispiel wäre Steuerhinterziehung durch Zwang (Dorminey et al., 2012).

Gelegenheit

Neben dem gefühlten Druck braucht Fraud ebenfalls eine Entstehungsmöglichkeit. Dieses zweite Element des Fraud Dreiecks ist ursprünglich als eine Möglichkeit Fraud zu begehen und zu verschleiern (engl. Opportunity to commit and conceal the fraud act) definiert (Cressey, 1953). Im Allgemeinen kann die Möglichkeit durch vier Faktoren beschrieben werden (Coleman, 1987; Dorminey et al., 2012; Hollinger & Clark 1983):

- wie viel Gewinn erwartet der Täter
- wie riskant scheint die wirtschaftskriminelle Handlung
- wie kompatibel ist die Tat mit dem Gewissen des Täters
- wie verlockend ist die Tat im Vergleich zu anderen dem Täter bekannten Taten

Die wahrgenommene Gelegenheit kann durch verschiedene Prozeduren, Richtlinien und Regularien beeinflusst werden, die üblicherweise in einem internen Kontrollsystem zusammengefasst werden. Das Committee of Sponsoring Organization of the Treadway Commission hat ein solches Rahmenwerk etabliert, welches durch eine Mehrheit der Unternehmen weltweit genutzt wird (Albrecht et al., 2012; Moeller, 2011). Das sogenannte COSO integrierte Framework identifiziert fünf Hauptelemente der internen Kontrollen (Albrecht et al., 2012; Moeller, 2011):

- Kontrollumgebung
- Information und Kommunikation
- Risikobewertung
- Monitoring und
- Kontrollaktivitäten

Diese Elemente des umfassenden internen Kontrollsystems sind auf die Überwachung der Geschäftsprozessdurchführung ausgelegt, um jegliche Möglichkeit von Fraud auszuschließen.

[14] Für Details über MICE vergleiche Kranacher et al. (2011) und Dorminey et al. (2012)

Die Kontrollumgebung beinhaltet Führungskräftekommunikation und Auswahl der Mitarbeiter bei der Einstellung (Albrecht et al., 2012). Information und Kommunikation beinhaltet die Kommunikationsflüsse in einem Unternehmen (Albrecht et al., 2012). Risikobewertung beinhaltet alle Aktivitäten, die zur Identifikation, Strukturierung und Analyse aller relevanten, internen und externen Risiken dient. Dabei sollen mögliche Fraud Szenarien in Relation zu möglichen Schaden gesetzt werden (Moeller, 2011). Monitoring hingegen versichert, dass das Kontrollsystem regelmäßig nach Qualität und Performance überprüft wird (Albrecht et al., 2012). Die Kontrollaktivitäten beinhalten alle Prozeduren und Artefakte, die die Befolgung von Anweisungen sicherstellen, wie beispielsweise die Aufgabentrennung, Autorisierungsverfahren und unabhängige Daten- und Dokumentenkontrollen (Albrecht et al., 2012).

Die meisten anti-fraud Experten gehen davon aus, dass raffinierte interne Kontrollen die Möglichkeiten Fraud zu begehen eliminieren können. Dadurch konzentrieren sich viele anti-fraud Initiativen auf neue Kontrollen oder die genaue Einhaltung der implementierten Kontrollen (Albrecht et al., 2012). Ziel ist es den Faktor Gelegenheit aus dem Fraud-Dreieck zu eliminieren.

Rationalisierung

Cressey (1953) definiert das dritte Element des Fraud-Dreiecks als moralisch vertretbare Rechtfertigung für ungewöhnliche und nicht zum Charakter des Täters passende Handlungen. Die meisten Täter halten sich selbst für ehrliche Menschen und rechtfertigen ihre Taten (Biegelman, 2013). Abhängig von den moralischen Ansprüchen des Täters kann die Rationalisierung entweder einfach oder sehr verzwickt sein (Coenen, 2008).

Typische Beispiele der Rechtfertigung für das Vergehen werden im Folgenden dargestellt[15]. Mitarbeiterfraud:

- „Etwas muss geopfert werden - meine Integrität oder meine Reputation“
- „Ich habe das Geld nur geliehen und werde es eventuell zurückzahlen“
- „Das Unternehmen kann sich den Verlust sehr leicht leisten“
- „Das Unternehmen ist es mir schuldig“
- „Das Unternehmen verdient es nicht besser“
- „Ich verdiene mehr, als ich bekomme“
- „Jeder macht es“
- „Es ist für einen guten Zweck“

Aus Managersicht:

- „Es ist für das Unternehmen“
- „Der Aktienkurs muss so hochgehalten werden“
- „Alle anderen Unternehmen nutzen ebenfalls aggressives Accounting“
- „Das Problem ist nur von temporärer Natur und die Bücher werden sich bald normalisieren“

[15] Vergleiche Albrecht et al. (2004); Albrecht et al. (2012); Biegelman (2013); Coenen (2008)

Da Rationalisierung persönlicher Natur und damit nicht direkt beobachtbar ist, ist es das am schwierigsten zu evaluierende Element des Fraud Dreiecks (Cohen et al., 2010). Einige Wissenschaftler und Fraud Experten messen persönliche Integrität als Proxy für die potentielle Rationalisierung (Dorminey et al., 2010).

Um ein besseres Verständnis über die Rechtfertigung von Taten zu erlangen, können weitere Theorien aus der Psychologie-Literatur zur Rate gezogen werden. Beck & Ajzen (1991) wandten die Theorie des geplanten Verhaltens (theory of planned behavior TPB[16]) an, um Straftaten vorherzusagen. Insgesamt betrachten diese vier Dimensionen: *Einstellung gegenüber Fraud, subjektive Normen, wahrgenommene Verhaltenskontrollen* und *moralische Verpflichtungen*. Nach Carpenter & Reimers (2005) hilft die Theorie des geplanten Verhaltens die Rationalisierung des Täters zu verstehen. Damit einhergehend zeigt eine Studie von Cohen et al. (2010), dass diese Theorie als Erweiterung des Fraud Dreiecks verwendet werden kann, um Rationalisierung zu erklären. Trotzdem bleibt Rationalisierung der unsicherste Faktor im Fraud Dreieck (Coenen, 2008).

2.4.2 Fraud Diamant

Ergänzt man das bekannte Fraud Dreieck um eine weitere Dimension, so ergibt dies einen Fraud Diamanten. Die zusätzliche Dimension berücksichtigt, ob ein potentieller Täter in der Lage ist die Straftat zu begehen. Jede wirtschaftskriminelle Tat benötigt Fähigkeiten, Zugriffsrechte und eine gewisse Intelligenz. Diese fehlende Dimension wird durch Wolfe & Hermanson (2004) adressiert, die das Element *Fähigkeit* hinzufügen. Die Autoren argumentieren, dass die vierte Dimension einfach zu beobachten ist und damit signifikant zur Frauderkennung und -prävention beitragen kann. Abbildung 2-8 zeigt die Faktoren, die die Fähigkeiten des Täters beeinflussen (Wolfe & Hermanson, 2004). Zusätzlich wird die Grafik um die bereits genannten Erweiterungen (MICE, COSO und TPB) ergänzt.

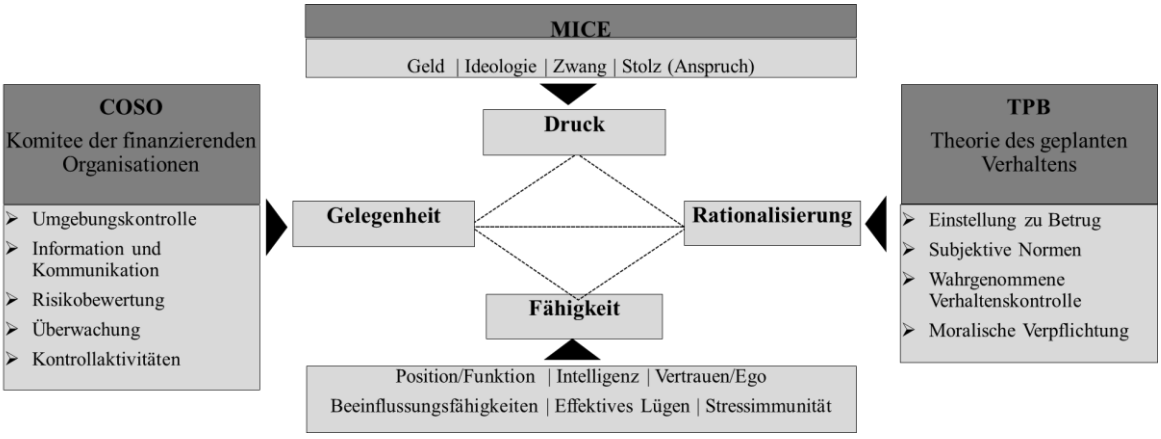


Abbildung 2-8: Erweiterter Fraud Diamant

Quelle: Basierend auf Cressey (1953); Kranacher et al. (2011); Cohen et al. (2010); Moeller (2011); Wolfe & Hermanson (2004)

[16] Details zur Theorie des geplanten Verhaltens (theory of planned behavior TPB) sind nicht bestandteil dieser Dissertation. Ausführliche Informationen sind hier enthalten: Beck and Ajzen (1991)

2.4.3 Principal Agent Theory und Verwaltungstheorie

Das Fraud Dreieck (bzw. der Fraud Diamant) ist die am weitesten verbreitete Theorie zur Erklärung von Fraud Verhalten. Es können aber auch etablierte Managementtheorien auf den Kontext von Fraud angewendet werden. Die Agententheorie[17] (Agency Theory) beispielsweise kann angewendet werden, um die oftmals gegensätzlichen Interessen von Mitarbeitern und Managern zu erklären.

Die Prinzipal Agenten Theorie wurde von Jensen & Meckling (1976) eingeführt und beinhaltet im Kern, dass alle rationalen Akteure ihre persönlichen Vorteile maximieren (Albrecht et al., 2004; Choo & Tan, 2007). Ein Verhältnis zwischen Prinzipal und Agent wird daher über einen Vertrag definiert, bei dem eine oder mehrere Personen (Prinzipale) andere Personen (Agenten) beauftragen eine Dienstleistung auszuführen. Dies beinhaltet auch die Übertragung der Entscheidungsauthorität zum Agenten (Jensen & Meckling, 1976). Als Problem wird gesehen, dass beide Parteien ihre eigenen Interessen vertreten. Dabei hat ein Geschäftspartner Informationsvorsprünge gegenüber dem anderen (sogenannten Informationsasymmetrie), was zu zwei Hauptproblemen führt: (1) Beim Vertragsabschluss verfügt der Agent über Informationen (wie Leistungsfähigkeit, Qualität usw.) die der Prinzipal nicht hat. Daher kann es zu versteckten Eigenschaften (sogenannte *Hidden Characteristics*) kommen. (2) Der Agent hat Informationen über den Umweltzustand von dem seine Aktionen abhängen, die sogenannten versteckten Informationen *(Hidden Information).*

Die Informationsasymmetrien sind zum Zeitpunkt des Vertragsabschlusses noch unbekannt. Deshalb spricht man über das Modell des moralischen Wagnisses (Moral Hazard). Um die entstandenen Probleme zu beheben, werden Maßnahmen zur Überwachung des Agenten und zur Bindung des Prinzipals eingeleitet, wodurch Kosten für das Anreizsystem und Strafen entstehen. Die Prinzipal Agenten Theorie von Jensen & Meckling (1976) wird vor allem für die Beschreibung des Verhältnisses von Geschäftsführung und Manager verwendet. Durch ihre allgemeine Gültigkeit, findet diese in verschiedenen Anwendungsgebieten Anklang. Im Bereich von Fraud wird angenommen, dass die Interessen der Aktionäre oft im Konflikt mit den Interessen der Mitarbeiter stehen, indem beide ihren Profit maximieren wollen (Albrecht et al., 2004; Choo & Tan, 2007).

Im Gegensatz zur Agententheorie basiert die Verwaltungstheorie (stewardship theory) auf psychologische und soziologische Grundlagen (Albrecht et al., 2004). Diese nimmt an, dass Mitarbeiter und vor allem Manager eines Unternehmens bestmöglich für ihr Unternehmen handeln (Albrecht et al., 2004; Davis et al., 1997; Donaldson & Davis, 1991).

Albrecht et al. (2004) entwickeln auf Basis der Agententheorie die Theorie des ‚gestörten Vertrauensverhältnisses '. Choo & Tan (2007) erweiterten diese Theorie zur *American Dream*[18] Theorie, um die Nachteile zu adressieren. Jedes dieser Konzepte hat ihre Daseinsberechtigung

[17] Für Details der Agententheorie siehe: Jensen & Meckling (1976) und Davis, Schoorman, & Donaldson (1997)
[18] Die American Dream Theorie basiert auf der Anomie Theorie von Merton (1938) und wurde von Messner and Rosenfeld (1994) vorgestellt.

und weist Vor- und Nachteile auf. Bei jeder Risikobewertung ist es hilfreich mehrere Theorien anzuwenden. Diese Theorien sind allerdings nicht Teil dieser Dissertation.

3 Einkaufsprozess

Das Ziel dieses Kapitels ist einen detaillierten Einblick in den Einkaufsprozess zu gewähren. Der Einkaufsprozess als Referenzprozess für die Identifikation von wirtschaftskriminellem Verhalten ist besonders geeignet, da über viele Industrien und Unternehmen hinweg die fundamentalen Aktivitäten ähnlich sind. Deshalb wird dieser Prozess aus Prozess- und Implementierungssicht beschrieben.

Obwohl sich die exakte Ausführung in Unternehmen unterscheiden kann, unterliegen alle Prozesse einer generischen Abfolge von Transaktionszyklen (Boczko, 2007). Die drei Hauptzyklen sind Ausgabezyklus, Konversionszyklus und Einnahmezyklus (Hall, 2011; Porter, 1998). Einige Autoren, wie Boczko (2007) und Romney & Steinbart (2012), zählen auch Management- und Administrationszyklen hinzu. Im Hinblick auf Frauderkennung sind die durch die Zyklen generierten Daten sehr wichtig. In allen Unternehmen werden zwingend Daten im Hauptbuch gespeichert. Werden die Unternehmen durch Enterprise Ressource Planning (ERP) Systemen unterstützt, so sammeln diese ebenfalls Daten und können entsprechend analysiert werden.

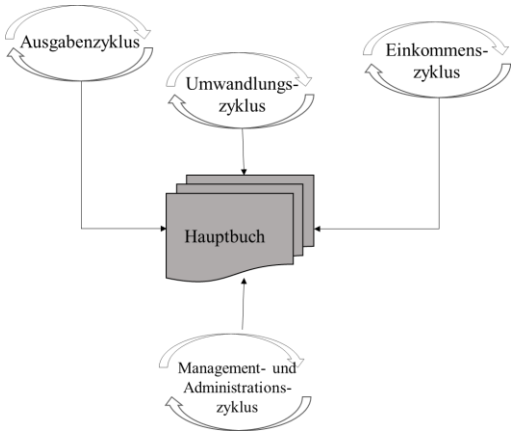


Abbildung 3-1: Unternehmens Transaktionszyklen
Quelle: Basierend auf Romney & Steinbart (2012), Boczko (2007) und Hall (2011)

Der Einkaufsprozess ist Teil des Ausgabezyklus und umfasst alle Aktivitäten vom Bedarf eines Produkts, einer Ware oder Dienstleistung, bis hin zur Bestellung und Bezahlung des entsprechenden Gutes oder der Leistung. Die Art des Unternehmens spielt für den Ausgabezyklus keine Rolle (Okrent & Vokurka, 2004).

3.1 Einkaufsprozess im Allgemeinen

In jedem Unternehmen gibt es mindestens zwei Varianten des Einkaufsprozesses: der Einkauf von physischen Gütern[19] oder von Dienstleistungen. Die augenscheinliche Unterscheidung ist, dass bei Dienstleistungen keine physischen Güter ausgetauscht werden. Somit wird auch keine formale Dokumentation der Dienstleistungen im Prozess dargestellt. Selbst wenn die Firmenrichtlinien die Bestätigung des Erhalts von Dienstleistungen vorgeben, so ist dies vor allem im Bereich des Wareneingangs schwierig. Oft wird in Arbeitsstunden gemessen, wobei die Qualität und Anzahl schwierig zu beurteilen ist. Im Gegensatz dazu kann bei physischen Gütern die Quantität und Qualität der gelieferten Waren einfach gemessen werden. Dennoch sind beide Prozesse außerhalb des Wareneingangs sehr ähnlich. Bei Dienstleistungen gibt es keinen Wareneingang, jedoch eine Bedarfserkennung, Bestellung, Rechnungseingang und eine Bezahlung. Hier wird zunächst nur auf die Bestellung von physischen Gütern eingegangen. Verschiedene Variationen, wie beispielsweise Vertragsabsprachen, Katalogbestellungen oder Bestellungen von mehreren Unternehmen, werden hier nicht betrachtet. Eine Übersicht über den Einkaufsprozess ist in Abbildung 3-2 abgebildet. Als Modellierung wird die BPMN 2.0 Notation nach Silver (2011) und OMG (2013) verwendet. Anschließend werden die einzelnen Aktivitäten inklusive Artefakte und Datenquellen beschrieben.

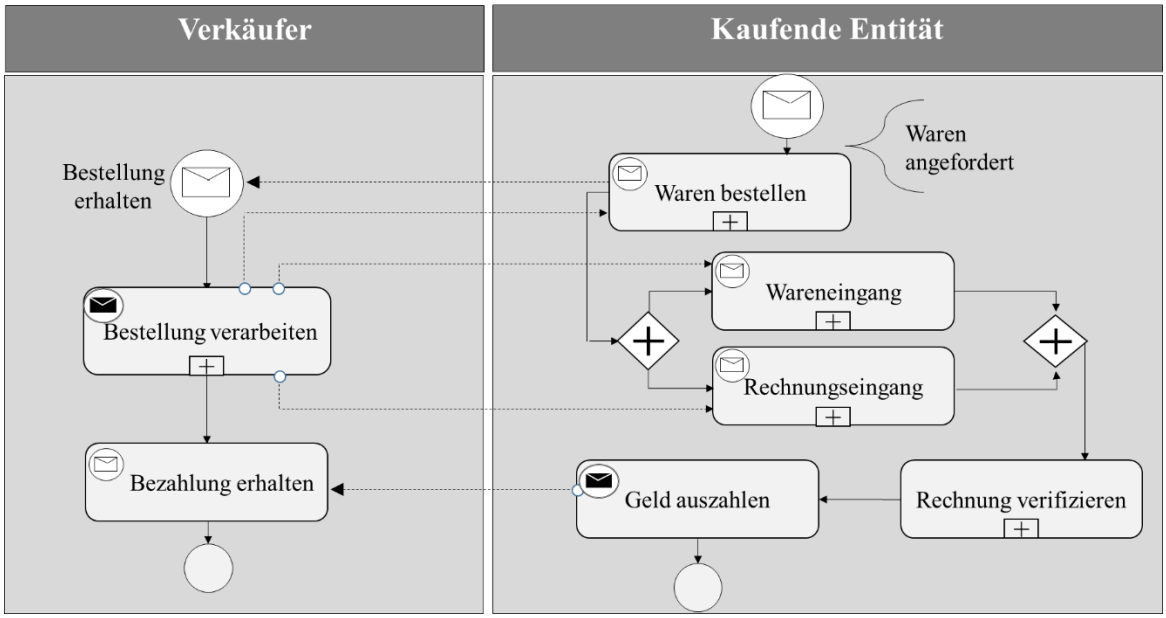


Abbildung 3-2: Einkaufsprozess (High Level)

Quelle: Eigene Darstellung nach der BPMN 2.0 Notation (OMG, 2013)

Jede Prozessinstanz des Einkaufsprozesses beginnt mit einer Nachfrage, die entweder manuell oder automatisch durch ein Kontrollsystem identifiziert wird (Bagranoff, Simkin, Strand, & Strand, 2010). Die Nachfrage wird in Form einer Bestellanforderung an die Einkaufsabteilung übergeben. Diese erstellen daraus eine Bestellung und übermitteln sie an einen Lieferanten, der

[19] Physische Güter können Rohmaterialien, Zubehör, Halbfabrikate oder Waren sein, nachstehend werden diese nur noch als Güter oder Ware bezeichnet

üblicherweise eine Bestätigung zurücksendet. Der Lieferant verschickt anschließend die bestellte Ware mit der dazugehörigen Rechnung, jedoch nicht zwangsläufig an dieselbe Adresse. Bei Erhalt von Waren oder Rechnungen werden die Daten im ERP System erfasst, um einen vollständigen Dokumentenfluss zu gewährleisten. Üblicherweise wird die Rechnung durch den Abgleich von Daten aus Bestellung, Wareneingang und Rechnung geprüft. Falls die Ware korrekt geliefert und berechnet wurde, wird der Zahlungsvorgang initiiert. Eine direkte Überweisung oder Barzahlung wird selten sofort getriggert, da Käufern meistens eine Zahlungsfrist gewährt wird. Diese wird im Voraus mit dem Verkäufer verhandelt.

Bestellung

Wie in Abbildung 3-3 abgebildet, beinhaltet der Bestellprozess alle Aktivitäten von der Vorbereitung der Bestellanforderung bis zur Bestellung und der entsprechenden Bestätigung vom Verkäufer. Die Bestellanforderung wird mit Hilfe von Stammdaten des Verkäufers und des entsprechenden Materials erstellt, die meist bereits im ERP System hinterlegt sind. Inventursysteme können automatisiert Bestellanforderungen erstellen. Bestellanforderungen und/ oder Bestellungen müssen standardmäßig autorisiert werden. Mitarbeiter mit Autorisierungsberechtigungen sind meist keine Angestellten der Einkaufsabteilung, sondern der bedarfsmeldenden Fachabteilung. Nach Genehmigung der Bestellanforderung wird die Abwicklung der Bestellung meist von der Einkaufsabteilung durchgeführt.

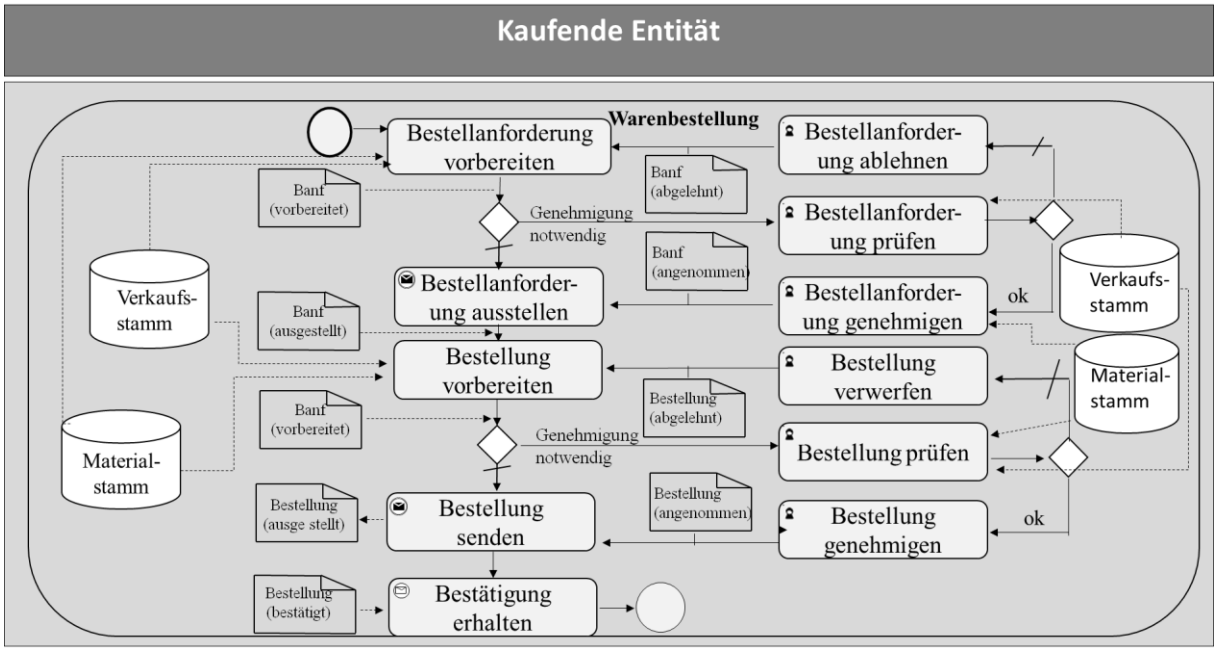


Abbildung 3-3: Einkaufsprozessaktivitäten – Warenbestellung
Quelle: Eigene Darstellung basierend auf BPMN 2.0 (OMG, 2013).

Der Genehmigungsprozess für Bestellungen ist ähnlich zu dem der Bestellanforderung, jedoch sind keine Fachabteilungen oder automatisierte Inventursysteme beteiligt. Eine weitere Unterscheidung ist der eigentliche Genehmigungsprozess, da er mehrere Genehmigungsstufen enthalten kann. Meist basieren diese auf den Kosten für die entsprechenden Waren oder

Dienstleistungen. Beispielsweise könnte ein normaler Angestellter Bestellungen bis 400 USD aufgeben. Alle Bestellungen oberhalb müssen durch den Teamleiter genehmigt werden, der wiederum nur Summen bis 40.000 USD genehmigen darf. Alles darüber hinaus muss durch den Chef der Einkaufsabteilung genehmigt werden. Die jeweiligen Genehmigungsstufen sind von Unternehmen zu Unternehmen unterschiedlich hoch angesetzt. Ziel dieser Genehmigungsstufen ist die Reduktion von Fraud. Sobald eine Bestellung von allen erforderlichen Parteien genehmigt wird, kann diese entweder elektronisch (meist durch das Electronic Date Interchange (EDI) Format) oder per Post an den Lieferanten übertragen werden. Wenn der Lieferant die Bestellung akzeptiert, sendet er eine Empfangsbestätigung. Steht der Lieferant noch nicht fest, muss zunächst ein geeigneter Lieferant durch eine Ausschreibung identifiziert werden. Dabei müssen mehrere Angebote eingeholt werden, wobei das beste Angebot hinsichtlich Preis/Leistung ausgewählt wird.

Wareneingang

Nach dem Bestellprozess erfolgt meist der Wareneingang. Dabei stößt die Lieferung den Wareneingangsprozess an (vergleich Abbildung 3-4). Die Ware wird meist mit einem Frachtbrief und Lieferschein versendet (Bagranoff et al., 2010; Boczko, 2007). Der Frachtbrief ist ein Liefervertrag und wird vom Frachtführer erstellt (Cavinato, 2000). Er enthält alle Informationen über die Fracht, den Absender, den Empfänger und den eigentlichen Transport. Die Lieferung ist komplett, sobald der Frachtbrief übergeben wird[20]. Es kann auch ein papierloser Frachtbrief verwendet werden (Cavinato, 2000). Dieser wird elektronisch übermittelt und enthält dieselben Informationen. Ein Lieferschein wird meist der Ware beigelegt. Dieser ist auch als Packschein oder Versandliste bekannt und enthält Informationen über die verpackten Produkte (ohne Preisinformationen) (Cavinato, 2000).

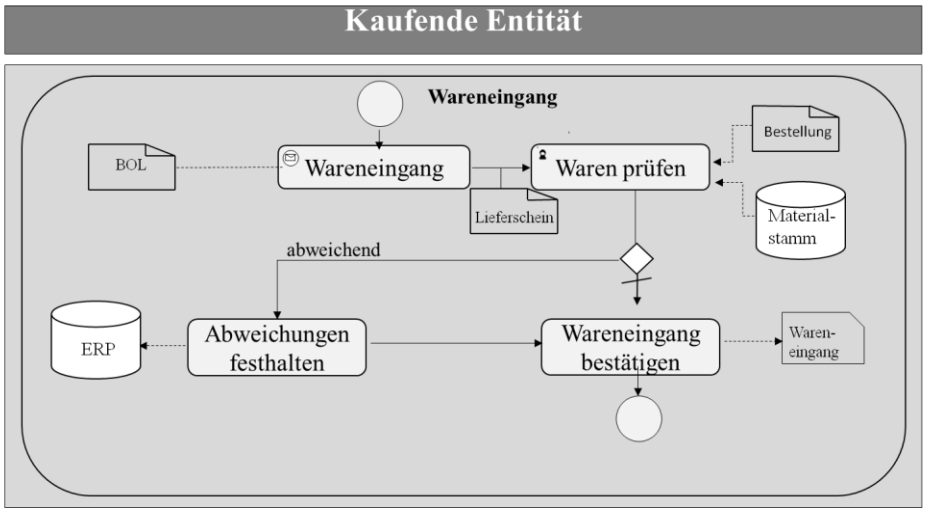


Abbildung 3-4:Einkaufsprozess - Wareneingang

Quelle: Eigene Darstellung basierend auf der BPMN 2.0 Notation (OMG, 2013).

[20] Normalerweise spezifizieren Incoterms gefährliche Überfahrten. Bei dieser Arbeit wird eine Lieferung zum Bestimmungsort Incoterm vorgenommen (der Verkäufer ist sowohl für die Fracht, wie auch Lieferung verantwortlich). Detallierte Informationen können hier eingesehen werden: "International Chamber of Commerce 2011 – ICC Guide to Incoterms 2010" 2011)

Der Lieferschein wird meist verwendet, um die versendeten Waren zu überprüfen. Hierzu wird auf die Bestellung und Stammdaten aus dem ERP System zurückgegriffen. Stimmen diese überein, kann der Wareneingang ohne Abweichungen im System erfasst werden. Eine mögliche Abweichung könnte eine Differenz zwischen gelieferter und bestellter Menge sein, die ebenfalls im ERP System erfasst werden sollte, um die Inventarisierung und die Rechnungsprüfung zu ermöglichen. Wenn es keine Inkonsistenzen gibt, bzw. wenn alle Abweichungen aufgenommen sind, wird ein Wareneingangsbeleg erstellt. Bei Teillieferungen wird für jede Teillieferung ein Wareneingang gebucht.

Rechnungseingang

Wie in Abbildung 3-5 dargestellt, sendet der Verkäufer die Rechnung für die bestellten und versandten Waren.

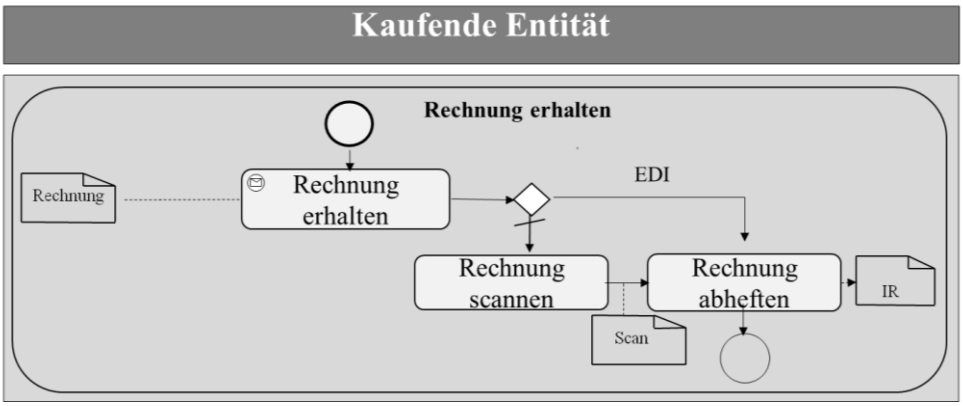


Abbildung 3-5: Einkaufsprozess Aktivitäten - Rechnungseingang
Quelle: Eigene Darstellung basierend auf dem BPMN 2.0 Standard (OMG, 2013).

Die Rechnung liegt meist der Ware bei, kann jedoch auch separat oder an einen anderen Empfänger gesendet werden. Viele große Unternehmen nutzten ein zentrales Dienstleistungscenter für die Verarbeitung der Rechnung, wodurch Waren und Rechnungen in verschiedenen Abteilungen bearbeitet werden. Wenn die IT Systeme des Lieferanten mit dem Käufer verbunden sind, werden alle Rechnungen automatisch als Rechnungseingang verbucht. Andererseits müssen diese zunächst eingescannt und im ERP System verfügbar gemacht werden. Rechnungen müssen standardmäßig vor der Bezahlung verifiziert werden.

Verifizierung der Rechnung

Nach dem Erhalt der Waren und Rechnung wird die Rechnung üblicherweise durch die Buchhaltung geprüft (Romney & Steinbart, 2012) (vergl. Abbildung 3-6). Dabei wird der sogenannten Three Way Match (3WM) durchgeführt (Hall, 2011), bei dem die Mengen und Preise aus Bestellung, Lieferung und Rechnung verglichen werden (Boczko, 2007; Hall, 2011). Bei Abweichungen von Preis oder Menge über einen bestimmten Toleranzbereich muss das Problem vor der Zahlung der Rechnung geklärt werden. Wenn die Dokumente keine Abweichung aufzeigen wird die Bezahlung genehmigt und in eine Art Warteschleife gelegt.

Die Fälligkeit wird durch den Verkäufer bestimmt. Teilweise werden pro Material bestimmte Zahlungsziele vereinbart. Bei Fälligkeit der Rechnung wird diese bezahlt.

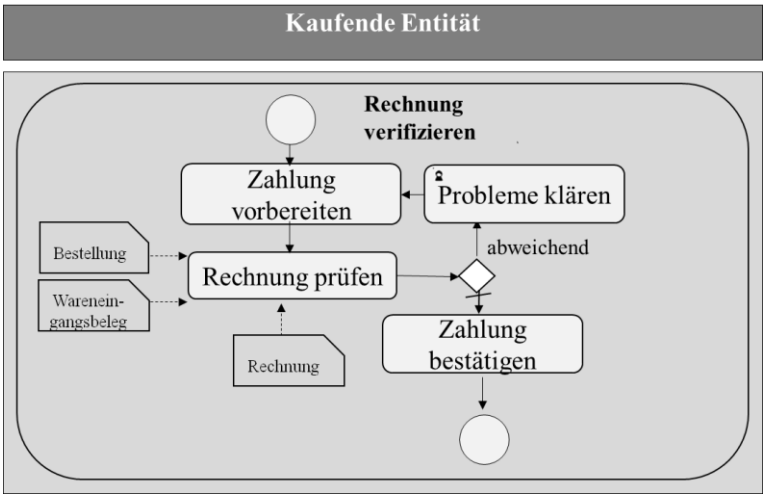


Abbildung 3-6. Einkaufsprozess – Rechnung verifizieren

Quelle: Eigene Darstellung basierend auf der BPMN 2.0 (OMG, 2013).

Einige Systeme nutzen Zahlungsbelege um Rechnungen für einen Verkäufer zu gruppieren und nur einmal zu bezahlen. Dies vereinfacht besonders bei Lieferanten mit vielen Rechnungen den Zahlungsprozess. Bei häufig bestellter Ware kann der Three Way Match auch durch einen Two Way Match substituiert werden, wobei die Rechnung nicht geprüft wird. Dieses Verfahren wird automatisches Wareneingangsabrechnungsverfahren (Evaluated Receipt Settlement (ERS)) genannt und wird genutzt, wenn bei der Bestellung der Preis bereits bekannt ist. Dabei wird das Wareneingangsdokument lediglich mit der Bestellung verglichen. Wenn es eine Übereinstimmung gibt, wird die Bezahlung genehmigt. Typischerweise wird der Matching Prozess automatisiert im ERP System vorgenommen. Ein manueller Handgriff ist nur notwendig, wenn die Dokumente nicht übereinstimmen (Romney & Steinbart, 2012).

Zahlungsprozess

Nach der Prüfung der Rechnung wird der Zahlungsprozess angestoßen um die Waren oder Dienstleistungen zu bezahlen. Die dazugehörigen Prozeduren sind oft Bestandteil des Accounting Information Systems oder Teil des ERP Systems und werden mindestens einmal wöchentlich ausgeführt. Die sogenannten Zahlungsläufe bearbeiten alle genehmigten und bereits fälligen Rechnungen und überweisen das entsprechende Geld an den Lieferanten (Hall, 2011). Die eigentliche Bezahlung wird meist durch den elektronischen Zahlungsverkehr (Electronic Funds Transfer EFT) durchgeführt, da die Ausstellung von Checks oder die Barzahlung zu arbeitsaufwendig sind (Boczko, 2007).

Meist ist der Einkaufsprozess durch den Zahlungsprozess abgeschlossen. Alle gezeigten Schritte des Einkaufsprozesses sind wichtig, um die darunterliegende Implementierung des Prozesses zu verstehen. Deshalb wird im nächsten Abschnitt die technische Implementierung innerhalb eines SAP ERP Systems beschrieben.

3.2 Einkaufsprozess im SAP ERP System

Um bestimmte Fraud Detektionsverfahren zu verstehen, reicht das reine Prozesswissen nicht aus. Alle automatisierten Fraud Detektionsverfahren verwenden Daten, die im Einkaufsprozess gespeichert werden. Da in dieser Dissertation der Fokus auf SAP ERP liegt, wird auf die Implementierung im SAP ERP System eingegangen. SAP zählt mit über Tausend Unternehmen in über 150 Ländern zu den Marktführern im ERP Bereich (SAP, 2013a) und das SAP ERP System ist das weltweit Meistverbreitete (Pang, Dharmasthira, Eschinger, Motoyoshi, & Brant, 2013).

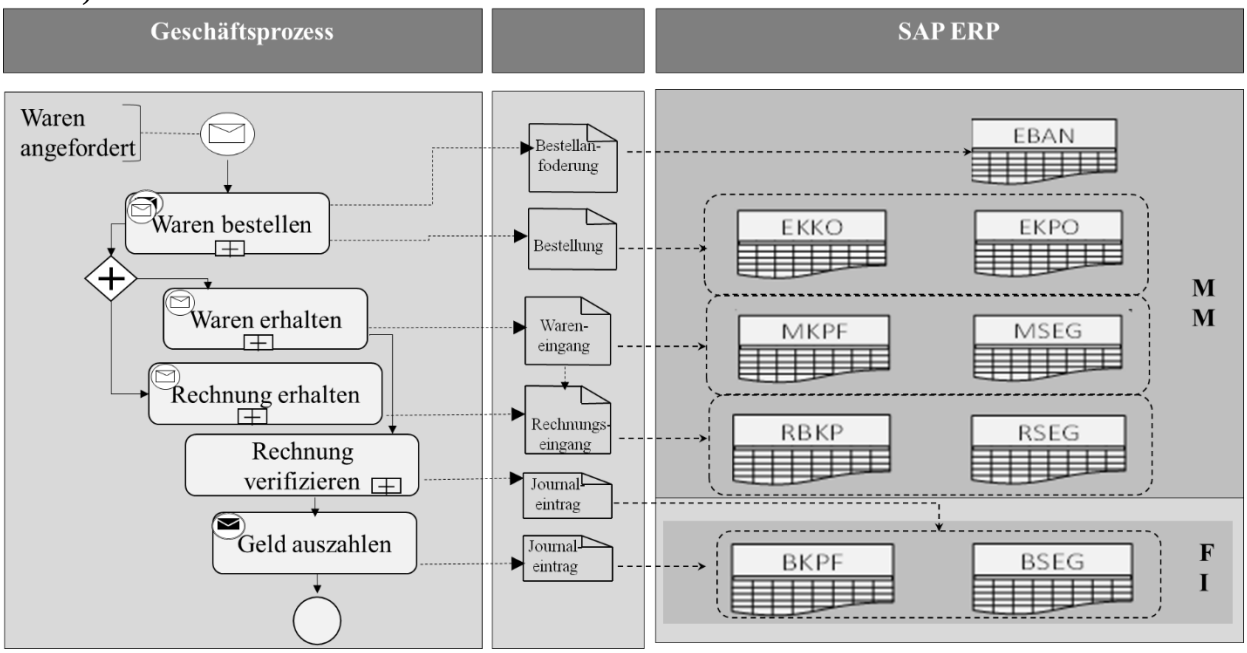


Abbildung 3-7: Artefakte des Einkaufsprozesses entsprechender SAP Tabellen

Quelle: Eigene Darstellung, Prozessdiagramm entspricht den BPMN 2.0 Notation, SAP Tabellennamen aus SAP (2013a) entnommen.

Abbildung 3-7 zeigt den Einkaufsprozess in sehr kompakter Form mit dem Fokus auf die im Prozess generierten Dokumente. Der Bestellprozess generiert eine Bestellanforderung und eine Bestellung. Der Wareneingangsprozess erstellt einen Wareneingangsbeleg und der Rechnungseingang eine Rechnung. Diese wird an die Buchhaltung weitergegeben, um dort eine Verbuchung zu erstellen. Sobald eine Rechnung bestätigt wird, wird diese verbucht und die Bezahlung initiiert. Im SAP System findet der Geschäftsprozess in den Modulen Materialmanagement (MM) und Finanzbuchhaltung (FI) statt. Die Symbole in den dunkelgrauen Tabellen symbolisieren Datenbanktabellen. Alle Daten mit Ausnahme der Daten in der EBAN Tabelle, werden auf mehrere Tabellen aufgeteilt. So bestehen SAP Tabellen meist aus einer Kopftabelle und einer Tabelle für die einzelnen Posten. Da eine Bestellung mehrere (unterschiedliche) Waren beinhalten kann, wird die allgemeine Information (z.B. Adresse des Verkäufers) in der Kopftabelle und damit nur einmalig gespeichert. Jede einzelne Position wird in der zweiten Tabelle ausgelagert. Im Folgenden werden alle Subprozesse des Einkaufsprozesses, sowie deren Implementierung im SAP ERP System beschrieben.

Bestellanforderung

Zunächst wird im SAP Einkaufsprozess eine Bestellanforderung erstellt. Dieses Dokument wird in einer einzelnen Tabelle (EBAN) gespeichert. Dabei ist irrelevant wie viele einzelne Positionen die Bestellanforderung beinhaltet. Jeder Eintrag in der EBAN Tabelle entspricht einer Bestellposition. Da bei einer Bestellanforderung wenige das gesamte Dokument umfassende Informationen vorliegen, wird keine separate Kopftabelle benötigt. Individuelle Bestellanforderungen können durch den Primärschlüssel (PS) unterschieden werden, der sich aus einer Kombination des Mandanten (MANDT) und der Bestellanforderungsnummer (BANFN) zusammensetzt. Jede Bestellposition kann identifiziert werden, indem zusätzlich die Positionsnummer der Bestellanforderung (BNFPO) betrachtet wird. Tabelle 4 zeigt einen Auszug aus der EBAN Tabellenstruktur. Alle Informationen die Events erstellen oder ändern sind besonders für die Detektion von Fraud nützlich. Auch sind Felder mit Referenzen auf Stammdaten von Bedeutung, da diese auf die Täter schließen lassen. Da die Genehmigungsprozesse oft mit Schwellwerten verbunden sind, sind Preis und Anzahl auch interessante Felder.

EBAN - Bestellanforderungen **(Auszug)**

Feld	PS	Feldname	Kommentar
MANDT	X	Mandant	-
BANFN	X	Bestellanforderungsnummer	Identifiziert die Bestellanforderung
BNFPO	X	Positionsnummer der Bestellanforderung	Identifiziert die Bestellpositionen einer Bestellanforderung
ERNAM		Name des Sachbearbeiters, der das Objekt hinzugefügt hat	-
ERDAT		Datum der letzten Änderung	Datum als die Bestellanforderung geändert wurde
AFNAM		Name des Anforderers	-
MATNR		Materialnummer	Identifiziert das benötigte Material
MENGE		Bestellanforderungsmenge	Spezifiziert die benötigte Menge
BADAT		Anforderungsdatum	Datum, an dem die Bestellanforderung erstellt wurde
FRGDT		Freigabedatum der Bestellanforderung	-
PREIS		Preis in der Bestellanforderung	Preis jeder einzelnen Bestellposition
LIFNR		Wunschlieferant	-
FLIEF		Fester Lieferant	-
WAERS		Währungsschlüssel	Identifiziert die Währung
PRIO_URG		Bedarfsdringlichkeit	-
⋮		⋮	⋮

Tabelle 4: EBAN Tabellenstruktur (Bestellanforderung)

Quelle: Felder Primärschlüssel und Feldnamen entnommen aus SAP (2013a).

An dieser Stelle werden die wesentlichen Attribute der EBAN Tabelle vorgestellt. Bei der Erstellung der initialen Bestellanforderung wird der verantwortliche Mitarbeiter (ERNAM), das Erstellungsdatum (BADAT), eine Referenznummer auf die benötigten Materialien (MATNR), die benötigte Quantität (MENGE) und der erwartete Preis (PREIS) gespeichert. Bei anschließenden Änderungen wird das Änderungsdatum gespeichert (ERDAT). Zusätzlich kann jede Bestellanforderung eine Referenz auf den gewünschten Lieferanten (LIFNR) oder auf

einen festen Lieferanten (FLIEF) enthalten. Damit wird der Auswahlprozess der möglichen Lieferanten beeinflusst. Es ist auch möglich die Dringlichkeit der Ware zu spezifizieren (PRIO_URG), um möglicherweise die Geschwindigkeit des nächsten Prozessschrittes zu erhöhen. Falls die Bestellanforderung keinen Freigabeprozess erfordert, wird diese direkt freigegeben. Andernfalls wird der Freigabeprozess initiiert. Bei Erteilung der Freigabe wird das Datum der Freigabe gespeichert (FRGDT).

Bestellung

Die Daten der Bestellung werden in Informationen über die gesamte Bestellung (sogenannte Kopfdaten) und spezifische Informationen einzelner Bestellpositionen aufgeteilt. Das Entity Relationship Model (ERM) in Abbildung 3-8 zeigt das Verhältnis zwischen der Kopftabelle (EKKO) und der Bestellpositionen in der EKPO Tabelle.

Abbildung 3-8: Bestellung (ERM)

Quelle: Eigene Darstellung, basierend auf Chen (1976) Notation für ERMs

Jeder Bestellkopf wird zu einer beliebigen Anzahl von Bestellpositionen zugeordnet. Jede Bestellposition kann allerdings nur einem Bestellkopf zugeordnet werden. Um eine Bestellanforderung zu rekonstruieren, müssen beide Tabellen betrachtet werden. Tabelle 5 zeigt einen Ausschnitt aus der EKKO Tabelle.

EKKO - Einkaufsbelegkopf **(Auszug)**			
Feld	**PS**	**Feldname**	**Kommentar**
MANDT	X	Mandant	-
EBELN	X	Belegnummer des Einkaufsbelegs	Identifiziert die Bestellung
BSTYP		Typ des Einkaufsbelegs	BSTYP = ‘F’ zeigt eine Bestellung an
AEDAT		Datum, an dem der Satz hinzugefügt wurde	Datum, an dem die Bestellung erstellt wurde
ERNAM		Name des Sachbearbeiters, der das Objekt hinzugefügt hat	-
LIFNR		Identifikationsnummer des Lieferanten	-
ZTERM		Zahlungsbedingungsschlüssel	Spezifiziert die Zahlungsbedingungen
WAERS		Währungsschlüssel	-
BEDAT		Datum des Einkaufsbelegs	Datum (auf der Bestellung)
VERKF		Zuständige VerkäuferIn beim Lieferanten	-
LIFRE		Abweichender Rechnungssteller	Identifiziert den Verkäufer, der die Rechnung stellt (falls dieser Abweicht)
⋮		⋮	⋮

Tabelle 5: EKKO Tabellenstruktur

Quelle: Felder, Primärschlüssel und Feldnamen extrahiert aus SAP (2013a)

Jede Bestellung kann durch die Belegnummer des Einkaufsbelegs (EBELN) und den Mandanten (MANDT) eindeutig identifiziert werden. Da Angebotsanforderungen (Request for

Quotation RFQ) und Rahmenverträge ebenso in diesen beiden Tabellen gespeichert werden, enthält der Einkaufsbelegtyp (BSTYP) die entsprechenden Werte. Da dieses Feld auf Bestellungen gefiltert werden kann, ist es für die Identifikation von Fraud von Relevanz.

Sobald ein Mitarbeiter eine Bestellung erstellt, wird sein Benutzername (ERNAM) gespeichert. Zusätzlich werden das Erstelldatum (AEDAT), die Identifikationsnummer des Lieferanten (LIFNR) und der Rechnungsersteller (LIFRE) (falls dieser vom Lieferanten abweicht) erstellt. Jeder Eintrag enthält Informationen über Zahlungsbedingungen (ZTERM), die verantwortliche Kontaktperson des Lieferanten (VERKF) und das Referenzdatum der Bestellung (BEDAT).

Für jeden Eintrag in der Kopftabelle (EKKO) gibt es mindestens einen Verweis auf die Positionstabelle (EKPO). Die Daten in Tabelle 6 zeigen einen Auszug aus der Positionstabelle. Beide Tabellen werden eindeutig über den Schlüssel der EKKO Tabelle mit der Positionsnummer des Einkaufsbelegs (EBELP) identifiziert.

Jede Bestellposition enthält Informationen über das bestellte Material (MATNR), die bestellte Menge (MENGE) und den Preis (NETPR). Zusätzlich referenziert es das Werk, welches die Ware bestellt hat (PLANT). Bei Änderungen in den Positionsdaten wird das Änderungsdatum protokolliert (AEDAT).

EKPO - Einkaufsbelegposition **(Auszug)**

Feld	PS	Feldname	Kommentar
MANDT	X	Mandant	-
EBELN	X	Belegnummer des Einkaufsbelegs	Identifiziert die Bestellung
EBELP	X	Positionsnummer des Einkaufsbelegs	Identifiziert die Bestellpositionen der Bestellung
AEDAT		Änderungsdatum der Einkaufsbelegposition	Datum, an dem eine Bestellposition geändert wurde
MATNR		Materialnummer	Identifiziert das Material
WERKS		Werk	-
MENGE		Bestellmenge	-
NETPR		Nettopreis im Einkaufsbeleg in Belegwährung	-
UEBTO		Toleranzgrenze für Überlieferung	In Prozent
UEBTK		Kennzeichen: unbegrenzte Überlieferung erlaubt	-
BANFN		Bestellanforderungsnummer	Identifiziert die dazugehörige Bestellanforderung
BNFPO		Positionsnummer der Bestellanforderung	-
LOEKZ		Löschkennzeichen im Einkaufsbeleg	Markiert sobald ein Einkaufsbeleg versucht wurde zu löschen
⋮		⋮	⋮

Tabelle 6: EKPO Tabellenstruktur

Quelle: Felder, Primärschlüssel und Feldnamen extrahiert aus (SAP, 2013a).

Wareneingang

Nach dem Erhalt der Ware wird für jede Lieferung ein Wareneingangsdokument erstellt, welches zur Rechnungsprüfung verwendet wird. Wareneingangsdaten werden wie bei Bestellungen in Kopf- und Positionstabellen aufgeteilt. Während die Kopftabelle (MKPF) übergreifende Daten enthält, werden die einzelnen Positionen in der MSEG Tabelle gespeichert.

Abbildung 3-9: Wareneingang ERM

Quelle: Eigene Darstellung basierend auf Chen (1976) Notation für ERMs.

Abbildung 3-9 zeigt die Beziehung dieser beiden Tabellen in einem ERM Diagramm. Jede Position ist einem Kopftabelleneintrag zugeordnet, während Kopftabelleneinträge mehrere Positionen enthalten können. Beide Tabellen sind notwendig, um den Wareneingang zu rekonstruieren. Der Belegkopf Material (MKPF) (Tabelle 7) ist eindeutig über Mandant (MANDT), Materialnummer (MBLNR) und Dokumentenjahr (MJAHR) referenzierbar.

MKPF – Belegkopf Material **(Auszug)**			
Feld	**PS**	**Feldname**	**Kommentar**
MANDT	X	Mandant	-
MBLNR	X	Nummer des Materialbelegs	Identifiziert den Wareneingang
MJAHR	X	Materialbelegjahr	Spezifiziert das Jahr des Wareneingangs
BLDAT		Belegdatum im Beleg	Datum, wie es im Wareneingangsdokument spezifiziert wird
CPUDT		Tag der Erfassung des Buchhaltungsbelegs	Erstellungsdatum des Dokuments
CPUTM		Uhrzeit der Erfassung	-
AEDAT		Datum der letzten Änderung	-
USNAM		Name des Benutzers	Identifiziert den Benutzer, der den Wareneingang erstellt hat
⋮		⋮	⋮

Tabelle 7: MKPF Tabellenstruktur

Quelle: Felder, Primärschlüssel und Feldnamen extrahiert aus SAP (2013a).

Bei Verbuchung des Wareneingangs wird der Benutzername des Mitarbeiters (USNAM), das Datum (CPUDT) und die Uhrzeit (CPUTM) gespeichert. Das Datum der Anzeige im User Interface kann manuell gesetzt werden und wird im Attribut BLDAT gespeichert. Sobald das Wareneingangsdokument geändert wird, wird das letzte Änderungsdatum im Feld (AEDAT) gespeichert. Für jeden Eintrag in der MKPF Tabelle gibt es mindestens einen Eintrag in der MSEG Tabelle. Die einzelnen Positionen sind in der Tabelle Belegsegment Material (MSEG) gespeichert.

MSEG – Belegsegment Material **(Auszug)**			
Feld	**PS**	**Feldname**	**Kommentar**
MANDT	X	Mandant	-
MBLNR	X	Nummer des Materialbelegs	Identifiziert den Wareneingang
MJAHR	X	Materialbelegjahr	Spezifiziert das Jahr des Wareneingangs
ZEILE	X	Position im Materialbeleg	Identifiziert die Positionen des Wareneingangs
MATNR		Materialnummer	Identifiziert das Material
WERKS		Werk	Identifiziert das Zielwerk
LIFNR		Kontonummer des Lieferanten	Identifiziert den Lieferanten
EBELN		Bestellnummer	Link zwischen Position des Wareneingang und einer Bestellung
EBELP		Positionsnummer des Einkaufsbelegs	Link zwischen einer Position im Wareneingang und in der Bestellung
BSTMG		Wareneingangsmenge in Bestellmengeneinheit	-
XBEAU		Bestellung wurde beim WE angelegt	Spezifiziert ob der Wareneingang retrospektiv erstellt wurde
⋮		⋮	⋮

Tabelle 8: MSEG Tabellenstruktur

Quelle: Felder, Primärschlüssel und Feldnamen extrahiert aus SAP (2013a).

Der Primärschlüssel der MSEG Tabelle besteht aus MANDT, MBLNR, MJAHR und der Positionsnummer ZEILE. Jeder Eintrag enthält Informationen über das Material (MATNR), den Lieferanten (LIFNR), der Menge (BSTMNG) und das Werk, welches die Ware bestellt hat (WERKS). Zusätzlich referenziert jeder Eintrag die dazugehörige Bestellposition (EBELN, EBELP). Auch wird protokolliert, ob ein Eintrag retrospektiv erstellt wird (XBEAU) und somit nicht den Richtlinien entspricht.

Rechnung

Die Rechnung hat Einfluss auf das Materialmanagement (MM) und Finanzwesen (FI). Im Materialmanagement werden die Tabellen im Belegkopf Eingangsrechung (RBKP) und Belegposition Eingangsrechnung (RSEG) gespeichert, während diese im Finanzwesen in den Tabellen Belegkopf für Buchhaltung (BKPF) und Belegsegment Buchhaltung (BSEG) gespeichert werden.

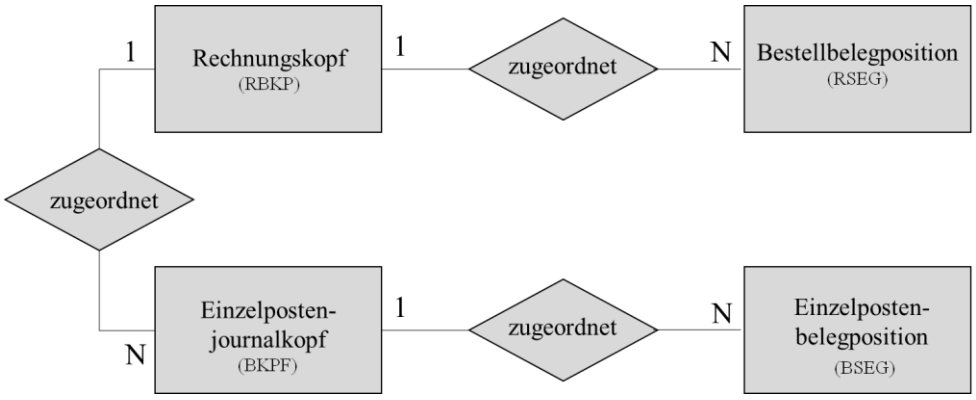


Abbildung 3-10: Rechnungseingang und Journaleintrag (ERM)

Quelle: Eigene Darstellung, basierend auf der Chen (1976) Notation für ERMs

Während RBKP und RSEG den Rechnungskopf und Positionen beinhalten, enthalten die Tabellen BKPF und BSEG jede einzelne Buchungstransaktion, wie beispielsweise Verbindlichkeiten. Abbildung 3-10 zeigt die Beziehung zwischen den Tabellen in einem ERM Diagramm.

Die Positionsdaten jeder Rechnung werden in der RSEG Tabelle gespeichert. Jeder Eintrag ist genau einem Eintrag in der Kopftabelle zugeordnet (RBKP), während jeder Rechnungskopf mehrere Rechnungspositionen enthalten kann. Die Verbindung zwischen BKPF und BSEG ist analog. Jedem Kopf (BKPF) wird eine beliebige Anzahl an Positionen (BSEG) zugeordnet, während jeder Position genau ein Kopf (BKPF) zugeordnet ist. Da es Umbuchungen ohne Rechnung gibt, werden nicht alle Umbuchungen in der RBKP Tabelle eingetragen. Andererseits existieren beispielsweise bei Stornierungen mehrere Buchungen die entsprechend mehrfach eingetragen werden.

Tabelle 9 zeigt einen Auszug aus der RBKP Tabelle. Jede Rechnung hat als Primärschlüssel den Mandanten (MANDT), die Nummer der Rechnung (BELNR) und das entsprechende Geschäftsjahr (GJAHR). Sobald eine Rechnung eingeht, wird der dazugehörige Benutzer (ERFNAM), das Erstellungsdatum (CPUDT), die Uhrzeit (CPUTM) und das Rechnungseingangsdatum (REINDAT) gespeichert. Warenspezifische Daten, wie Informationen über den Lieferanten (LIFNR), die Liefermenge (RMWWR), die Bezahlmethode (ZLSCH), das Zahlungsziel (ZTERM) und das Fälligkeitsdatum der Rechnung (ZFBDT), werden ebenfalls gespeichert. Bei Modifikationen der Rechnung wird der Benutzername ebenfalls gespeichert (USNAM). Das Datumsfeld BLDAT zeigt das Erstelldatum der Rechnung beim Lieferanten an, während das Datumsfeld BUDAT das Bearbeitungsdatum beim Kunden anzeigt.

Sind durch den Three Way Match (3WM) Abweichungen (MAKZN) identifiziert, können Mitarbeiter diese manuell bestätigen. Diese Option könnte für wirtschaftskriminelle Handlungen missbraucht werden, ist aber für Abstimmungen sinnvoll. Ein weiteres interessantes Feld ist der Indikator Conto pro Diverse (CpD) in der Spalte (XCPDK). Dieses Konto wird für einmalige Lieferanten verwendet, die keine Stammdaten haben. Bei jeder Buchung müssen die Adressdaten des Lieferanten manuell eingegeben werden. Dies erhöht das Risiko für einen Missbrauch.

RBKP – Belegkopf Eingangsrechnung **(Auszug)**

Feld	PS	Feldname	Kommentar
MANDT	X	Mandant	-
BELNR	X	Belegnummer eines Rechnungsbeleges	Identifiziert die Rechnung
GJAHR	X	Geschäftsjahr	Spezifiziert das Geschäftsjahr, zudem diese Rechnung gehört
BLDAT		Belegdatum im Beleg	Datum, welches in der Rechnung angezeigt wird
BUDAT		Buchungsdatum im Beleg	Datum, an dem die Rechnung gebucht wurde
USNAM		Name des Benutzers	Identifiziert den Benutzer, der die Rechnung geändert hat
CPUDT		Tag der Erfassung des Buchhaltungsbelegs	Datum, als die Rechnung in das System erfasst wurde

CPUTM	Uhrzeit der Erfassung	Uhrzeit, bei der die Rechnung im System erfasst wurde
LIFNR	Abweichender Rechnungssteller	Zeigt an, ob ein abweichender Rechnungssteller die Rechnung erstellt hat
RMWWR	Rechnungsbruttobetrag in Belegwährung	-
ZTERM	Zahlungsbedingungsschlüssel	Identifiziert die Zahlungsbedingungen
MAKZN	Manuell akzeptierter Differenzbetrag Netto	Monetäre Differenz, die manuell akzeptiert wurde
ZLSCH	Zahlweg	-
ZFBDT	Basisdatum für Fälligkeitsberechnung	-
XCPDK	Kennzeichen: Ist das Konto ein CPD-Konto?	Handelt es sich hierbei um ein einmaliges Konto
REINDAT	Rechnungseingangdatum	-
ERFNAM	Name des Sachbearbeiters, der das Objekt erfasst hat	Identifiziert den Benutzer, der die Rechnung im System eingegeben hat
⋮	⋮	⋮

Tabelle 9: RBKP Tabellenstruktur

Quelle: Felder, Primärschlüssel und Feldnamen extrahiert aus SAP (2013a).

Mindestens eine Position in der RSEG Tabelle existiert für jeden Eintrag in der Kopftabelle. Ein Auszug aus der RSEG Tabelle ist in Tabelle 10 dargestellt. Der Primärschlüssel dieser Tabelle setzt sich aus den Feldern MANDT, BELNR, GJAHR und einer Positionsnummer (BUZEI) zusammen. Die wichtigen Spalten zur Verifikation von Rechnungen sind die berechnete Menge (RBMNG) und die Summe der Positionen (RBWWR). Die Referenz zur Bestellposition wird durch die Felder EBELN und EBELP erreicht. Auch enthält die RSEG Tabelle Informationen über das Material (MATNR), das Zielwerk (WERKS) und dem Verkäufer (LIFNR).

RSEG – Belegposition Eingangsrechnung **(Auszug)**			
Feld	**PS**	**Feldname**	**Kommentar**
MANDT	X	Mandant	-
BELNR	X	Belegnummer eines Buchhaltungsbeleges	Identifiziert die Rechnung
GJAHR	X	Geschäftsjahr	Spezifiziert zu welchem Geschäftsjahr die Rechnung gehört
BUZEI	X	Belegposition im Rechnungsbeleg	Identifiziert die einzelnen Positionen
EBELN		Belegnummer des Einkaufsbelegs	Link zwischen Rechnungsposition und Bestellung
EBELP		Positionsnummer des Einkaufsbelegs	Link zwischen Rechnungsposition und Bestellposition
MATNR		Materialnummer	Identifiziert das Material
WERKS		Werk	Identifiziert das Zielwerk
RBMNG		Rechnungsmenge laut Lieferantenrechnung in Bestellmengeneinheit	Spezifiziert die zu berechnende Menge
RBWWR		Rechnungsbetrag in Belegwährung laut Lieferantenrechnung	Spezifiziert den in Rechnung gestellten Betrag
LIFNR		Kontonummer des Lieferanten bzw. Kreditors	Identifiziert den Rechnungsstellenden Verkäufer
⋮		⋮	⋮

Tabelle 10: RSEG Tabellenstruktur

Quelle: Felder, Primärschlüssel und Feldnamen extrahiert aus SAP (2013a).

Alle bisher beschriebenen Tabellen gehören zum SAP MM Modul. Diese Transaktionen haben keinen Einfluss auf die Buchhaltung des Unternehmens. Laut Hall (2011) ist es üblich die Zahlungen bis zum Erhalt der Rechnung zu verzögern. Deshalb gibt es beim Wareneingang keinen Eintrag in die Haupt- bzw. Nebenbücher. Nach dem Erhalt der Rechnung und der erfolgreichen Three Way Match (3WM) Prüfung, wird eine Buchung durchgeführt. Typischerweise wird dann eine Zahlungsverpflichtung im Nebenbuch des Verkäufers erstellt. Im SAP ERP System werden alle Buchungen unabhängig von ihrer Art (Abschreibungen, Erträge oder Rechnung) in den Tabellen BKPF und BSEG gespeichert. BKPF enthält Buchungsübergreifende Informationen, während die BSEG Positionensdaten enthält. Ein Auszug aus der BKPF Tabelle ist in Tabelle 11 gezeigt:

BKPF – Belegkopf für Buchhaltung **(Auszug)**

Feld	**PS**	**Feldname**	**Kommentar**
MANDT	X	Mandant	-
BUKRS	X	Buchungskreis	-
BELNR	X	Belegnummer eines Buchhaltungsbelegs	Identifiziert die Buchung
GJAHR	X	Geschäftsjahr	Spezifiziert zu welchem Geschäftsjahr die Buchung gehört
BUDAT		Buchungsdatum im Beleg	Datum, an dem die Buchung erfolgt
CPUDT		Tag der Erfassung des Buchhaltungsbelegs	Datum, an dem die Buchung angelegt wurde
CPUTM		Uhrzeit der Erfassung	Uhrzeit, in der die Buchung angelegt wurde
AEDAT		Datum der letzten Änderung per Transaktion	Datum, wann die Buchung zuletzt geändert wurde
USNAM		Name des Benutzers	Identifiziert, wer die Rechnung erstellt hat
AWTYP		Referenzvorgang	AWTYP = 'RMRP' zeigt einen Rechnungseingang
AWKEY		Referenzschlüssel	Identifiziert ein Dokument aus dem Feld AWTYP (Beispielsweise Rechnungsnummer, falls Rechnung)
⋮		⋮	⋮

Tabelle 11: BKPF Tabellenstruktur

Quelle: Felder, Primärschlüssel, Feldnamen extrahiert aus SAP (2013a).

Jede Buchung wird durch die Kombination des Mandanten (MANDT), dem Buchungskreis (BUKRS), der Belegnummer des Buchhaltungsbelegs (BELNR) und dem entsprechenden Geschäftsjahr (GJAHR) identifiziert. Sobald eine Buchung angelegt wird, wird die Person (USNAM), der dazugehörige Zeitstempel (CPUDT, CPUTM), das Datum der letzten Änderung (AEDAT) und das Buchungsdatum (BUDAT) gespeichert. Das Feld AWTYP speichert die Herkunft der Buchung. Beispielsweise wird eine Rechnung aufgrund einer Buchung durch den Eintrag RMRP im Feld AWTYP gekennzeichnet. Die entsprechende Rechnung wird dann in dem Feld AWKEY referenziert. Für jede Buchung gibt es mehrere Einträge in der BSEG Tabelle.

Einträge in der BSEG Tabelle werden eindeutig über die ID des Eintrags (BUZEI) identifiziert. Jede Zeile enthält den entsprechenden Buchungswert (WRBTR), den Kontotyp (KOART) und den Buchungsschlüssel (BSCHL) zur Spezifikation der Buchungsart. Der Buchungsschlüssel ‚31' steht beispielsweise für eine Rechnung, während der Buchungsschlüssel ‚40' für die Übertragung ins Hauptbuch steht. Für Buchungen aufgrund einer Rechnung wird das zu

verbuchende Material (MATNR) gespeichert. Nach Bezahlung der Rechnung wird eine weitere Buchung durchgeführt. Dabei wird die Rechnungszeile mit dem Ausgleichsdatum (AUGDT), einem Link zum Ausgleichsdokument (AUGBL), der entsprechenden Buchungszeile (AGZEI) und dem Geschäftsjahr (AUGGJ) aktualisiert.

Das Ausgleichsdokument wird ebenfalls in den Tabellen BKPF und BSEG gespeichert, um die Belastung des entsprechenden Kontos und die Zahlung nachvollziehbar zu machen. Zahlungsinformationen werden ebenfalls in den Tabellen REGUH und REGUP gespeichert, enthalten aber die selben Informationen wie BKPF und BSEG. Deshalb weden diese hier nicht im Detail erläutert.

BSEG – Belegsegment Buchhaltung **(Auszug)**

Feld	**PS**	**Feldname**	**Kommentar**
MANDT	X	Mandant	-
BUKRS	X	Buchungskreis	-
BELNR	X	Belegnummer eines Buchhaltungsbelegs	Identifiziert die Buchung
GJAHR	X	Geschäftsjahr	Spezifiziert zu welchem Geschäftsjahr die Buchung gehört
BUZEI	X	Nummer der Buchungszeile innerhalb des Buchhaltungsbelegs	Identifiziert die Buchung
AUGDT		Datum des Ausgleichs	-
AUGBL		Belegnummer des Ausgleichsbelegs	Identifiziert den Ausgleichbeleg
BSCHL		Buchungsschlüssel	‘31’ = Rechnung des Verkäufers / ‘40’ = Hauptbuchschult
KOART		Kontoart	‘K’ = Konto des Verkäufers / ‘A’ = Aktivkonto
WRBTR		Betrag in Belegwährung	-
MATNR		Materialnummer	Identifiziert das Material
AGZEI		Ausgleichsposition	Identifiziert die Buchung im Ausgleichsdokument
AUGGJ		Geschäftsjahr des Ausgleichsbelegs	Spezifiziert das Geschäftsjahr, indem es beglichen wurde
⋮		⋮	⋮

Tabelle 12: BSEG Tabellenstruktur

Quelle: Felder, Primärschlüssel und Feldnamen extrahiert aus SAP (2013a).

Abbildung 3-11 zeigt den Zusammenhang aller hier vorgestellten Tabellen. Diese Beziehungen sind für die Rekonstruktion des Einkaufprozesses wichtig. Zusätzlich können diese Tabellen mit den Stammdaten des Verkäufers (Tabellen: LFA1, LFB1, LFM1, LFM2) und dem Material (MARA, MARC) kombiniert werden. Die Tabellen CDHDR und CDPOS enthalten alle Änderungen im SAP System und sind für die Erkennung von Fraud ebenfalls sehr wichtig.

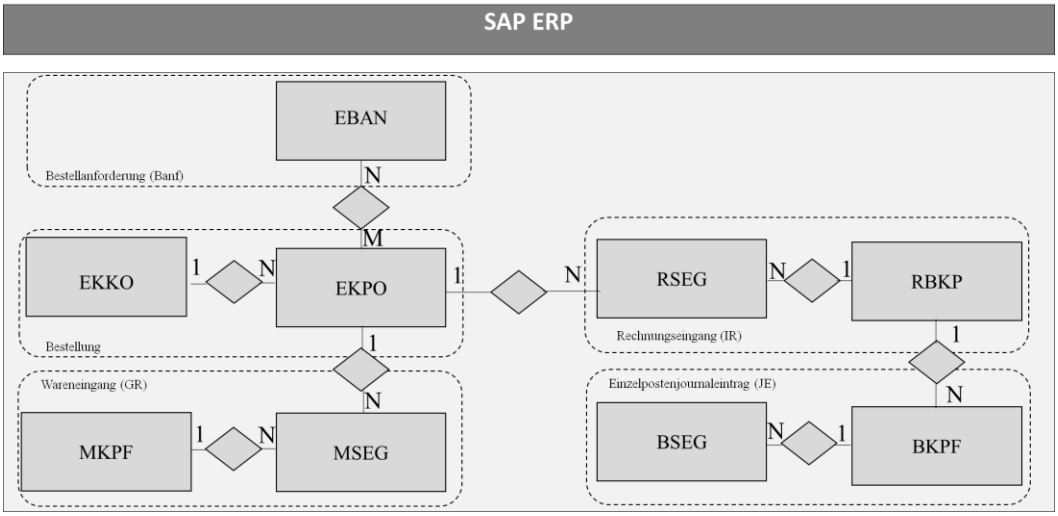


Abbildung 3-11: ERM des Einkaufsprozesses

Quelle: Eigene Darstellung basierend auf der Chen (1976) Notation für ERMs.

3.3 Sicherheitskonzept im SAP ERP System

Zunächst soll kurz auf das bereits Implementierte Sicherheitskonzept im SAP ERP System für Fraud Detektion eingegangen werden. Diese Maßnahmen schützen das ERP System vor Fraud und sind von Chuprunov (2011) entnommen:

- Architekturkonzept: Die Daten im SAP System werden intern in Tabellen gespeichert. Bei einer unerlaubten Manipulation in den Tabellen kann es zu Inkonsistenzen führen.
- Berechtigungskonzept: Durch Rollen und Profile lassen sich logische Zugriffskontrollen erstellen. Da sich ein Benutzer am System anmelden muss, um damit arbeiten zu können, ist das System vor unangemeldeten und nicht berechtigten Usern geschützt.
- Identitätsprinzip: Ein Benutzer muss sich mit Benutzername und Passwort anmelden, damit seine Identität eindeutig bestimmt werden kann. Bei der Ausführung jeder Transaktion wird eine Berechtigungsprüfung durchgeführt. Es ist zu jeder Zeit möglich nachzuvollziehen, welcher Benutzer welche Objekte angelegt, geändert oder gelöscht hat. Identitäten werden im SAP Identity Management (zentrale Nutzerverwaltung) gepflegt.
- Grundprinzip der Datenunveränderlichkeit: Bei jeder Ausführung von Transaktionen werden Systembelege angelegt, die nachträglich (bis auf einige wenige Datenfelder) nicht geändert werden können. Es gibt hierbei allerdings einen Workaround, den Administratoren gegebenenfalls nutzen können. Belegeinträge lassen sich im Debugging Modus ändern. Allerdings werden diese Änderungen im Systemlog gespeichert.

- Schutz vor Stammdatenänderungen: Stammdaten, wie beispielsweise die Kontoverbindung eines Lieferanten, lassen sich mit der entsprechenden Berechtigung ändern. Allerdings werden solche Änderungen protokolliert und lassen sich nachverfolgen.
- Vier-Augen-Prinzip: Unter dem Vier-Augen-Prinzip versteht man oft eine Freigabestrategie, die auch im SAP ERP System implementiert ist. Ein berechtigter Benutzer (beispielsweise ein Vorgesetzter) muss entsprechende Dokumente (Rechnungen, Bestellungen, Bestellanforderung) freigeben, bevor eine Maßnahme durchgeführt werden darf.
- Three-Way-Match: Der Three-Way-Match überprüft bei einem Rechnungseingang die Menge und den Preis der Bestellung und des Wareneingangs. Sollte eine Differenz über einer bestimmten Toleranzschwelle liegen, wird die Rechnung automatisch gesperrt und muss manuell wieder freigegeben werden.
- Datenübernahme: Die einzelnen Prozessschritte im SAP System bauen aufeinander auf. So werden in jedem Prozessschritt automatisiert Daten aus dem vorhergehenden übernommen.
- Automatische Prüfung von doppelten Rechnungen: Bei jeder Rechnung wird geprüft, ob diese bereits erfasst wurde. Das Erfassen der selben Rechnung in unterschiedlichen Währungen erkennt die Prüfung nicht.
- Prüfung vor automatischen Zahlungslauf: Vor dem automatischen Zahlungslauf wird überprüft, ob eine Sperre vorliegt und ob der Nutzer berechtigt ist den Zahlungslauf zu starten.

Trotz dieses Sicherheitskonzepts kann es zu Fraud kommen. Viele der hier vorgestellten Eigenschaften können mit den Customizing Einstellungen geändert werden.

4 Interner Fraud

Nach dem forschungsmethodischen Konzept, der grundlegenden Begriffsdefinitionen und einer Einführung in den Einkaufsprozess, soll an dieser Stelle interner Fraud beschrieben werden. Dabei werden bestehende Ansätze aus der Literatur zur Fraud Klassifikation, konkrete Fraud Szenarien und Verfahren zur Fraud Identifikation dargestellt. Dieses Kapitel stellt Ergebnisse der in Kapitel 1.3 vorgestellten Literaturstudie vor.

4.1 Klassifikation von wirtschaftskriminellen Angriffen

Wirtschaftskriminelle entwickeln immer raffiniertere Betrugsideen, während Anti-Fraud Experten ihre Aufdeckungsmethoden und -prozeduren verbessern. Durch die Zunahme der Digitalisierung stehen immer mehr Daten in elektronischer Form zur Verfügung, die zur Identifikation von Fraud ausgewertet werden können. Hier werden Ansätze zur Klassifikationen von Fraud (speziell Mitarbeiterfraud) dargestellt, sowie konkrete Szenarien beschrieben. Anschließend werden Detektionsverfahren zusammengefasst.

Klassifikation von Fraud

Eine internationale und allgemeingültige Klassifikation von Fraud gibt es nicht. Kroll (2013) unterscheidet in seinen ausführlichen Umfragen zwischen verschiedenen Fraudkategorien:

- Diebstahl von physischen Gütern
- Informationsdiebstahl
- Interessenkonflikt des Managements
- Verkäufer-, Lieferant- oder Einkaufsfraud
- Interner finanzieller Betrug
- Verstoß gegen Regeln oder Compliance Vorschriften
- Korruption und Bestechung
- Identitätsklau
- Marktabsprachen
- Unterschlagung von Unternehmensgeldern
- Geldwäsche

Kritik an dieser Kategorisierung ist das Fehlen wesentlicher Betrugsversuche im Finanz- und Wohltätigkeitssektor und auf dem Finanzmarkt. Pedneault (2009) ergänzt weitere Kategorien, wie Steuerhinterziehung, Bankenfraud, Wohltätigkeitsfraud und Versicherungsfraud. Zusätzlich hat er eine Hierarchie eingeführt, mit der er Mitarbeiterfraud (z.B. Unterschlagung) von Management Fraud (z.B. bei der Offenlegung der Finanzen) unterscheidet. Jedoch sind einige Arten von Fraud auch in Pedneaults Liste nicht abgedeckt. Dazu gehören Insiderhandel, Falschgeld oder korrupte Spiele.

In der akademischen Literatur haben sich zwei Ansätze der Kategorisierung durchgesetzt. Entweder wird nach dem Geschädigten oder dem Tatverlauf klassifiziert. Levi (2008) adoptiert die opferzentrierte Klassifikation von Levi & Burrows (2007) um kriminelle Netzwerke zu analysieren. Er unterscheidet zwischen dem Sektor des Opfers (Privat oder Öffentlich) und die sogenannten Subsektoren. Zu dem privaten Sektor gehören die Subsektoren Finanzdienstleistungen, keine Finanzdienstleistungen und Individuelles. Der öffentliche Sektor wird in die Subsektoren kommunale und internationale Einrichtungen unterteilt. Kritik dieser Einordnung ist, dass eine Tat in mehrere Subkategorien unterteilt werden kann. Beispielsweise kann Fraud im Einkaufsprozess sowohl in kommunalen Einrichtungen, wie auch im Finanzdienstleistungssektor stattfinden. Die Klassifikation nach dem Tatverlauf fokussiert auf die charakteristischen Eigenschaften und die verwendeten Tools, um die Tat zu begehen und zu verschleiern. Laleh & Azgomi (2009) entwickelten so einen sehr IT-zentrierten Ansatz, der alle Arten von internem Fraud zur Kategorie Intern zusammenfasst. Andere Kategorien sind Kreditkarten, Internet und Computerfraud. Dieses Framework verbessert die Schwächen von Levi (2008) und Pedneault (2009) nicht und wird daher nicht weiter dargestellt.

Vergleicht man die bestehenden Rahmenwerke bezüglich Vollständigkeit und Ganzheitlichkeit, so ist das Framework vom Serious Fraud Office (SFO) am detailliertesten (SFO, 2014). Das SFO ist eine unabhängige Regierungsabteilung der Strafjustiz in Großbritannien. Ihre *Taxonomy of Fraud* zeigt nicht nur eine konsistente und mehrstufige Hierarchie, sondern adressiert auch die fehlenden Fraud Arten der vorher genannten Rahmenwerke. Die ersten zwei Level der Hierarchie sind in Abbildung 4-1 gezeigt. Die SFO hat sieben Hauptgruppen für wirtschaftskriminelle Handlungen identifiziert, die im Folgenden kurz dargestellt werden sollen.

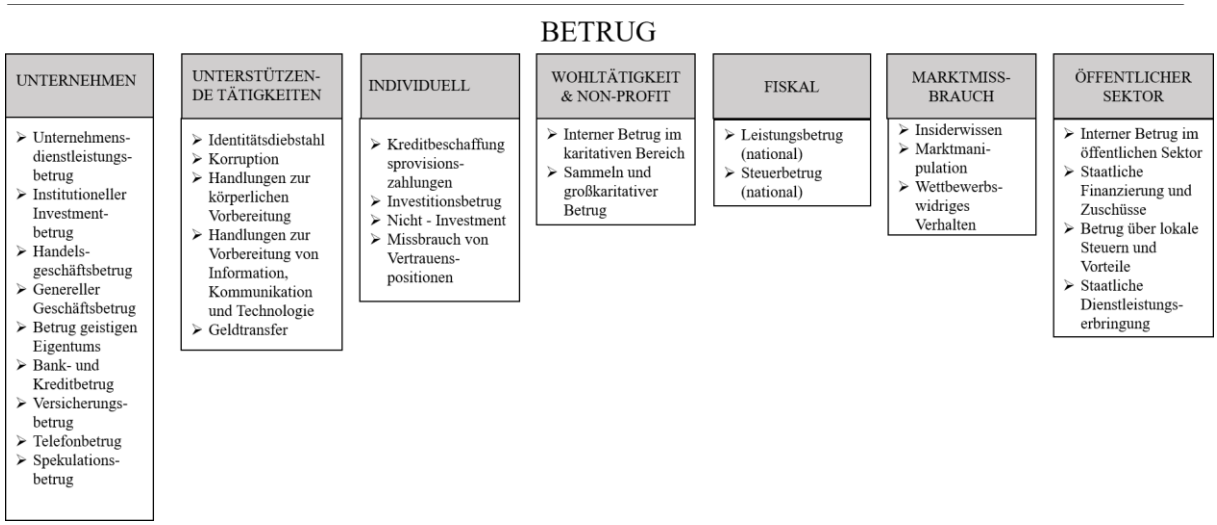


Abbildung 4-1: High Level Fraud Taxonomie

Quelle: Basierend auf SFO (2014)

Laut SFO (2014) beinhaltet die Kategorie *Unternehmen* alle Betrugsfälle, die sich gegen ein Unternehmen richten. Die Tat ist unabhängig vom Täter und kann sowohl von einer dritten Person oder einem Mitarbeiter durchgeführt werden. Da diese Dissertation die Aufdeckung von Fraud im Einkaufsprozess zum Ziel hat, sind die Kategorien *Genereller Geschäftsbetrug* und *Unternehmensdienstleistungsbetrug* von besonderer Bedeutung. Genereller Geschäftsbetrug beinhaltet alle Angriffe, die den internen Geschäftsprozess missbrauchen, während Unternehmensdienstleistungsbetrug gefälschte Rechnungen beinhaltet. Die anderen Subkategorien, wie fälschliche Investitionen, illegales Handeln, industriespezifische Typen (Darlehensfraud, manipulierte Wetten oder Scheckfraud) und Persönlichkeitsverletzungen sind nicht Bestandteil dieser Dissertation.

Klassifikation von Mitarbeiterfraud und Missbrauch

Die umfangreichste Klassifikation von Mitarbeiterfraud hat Wells (2011) und die Association of Certified Fraud Examiners ACFE (2014) erstellt. Die im ‚Report to the Nation' publizierte Klassifizierung gilt als de-facto Standard. Ein Auszug aus dem Klassifikationsbaum ist in Abbildung 4-2 dargestellt.

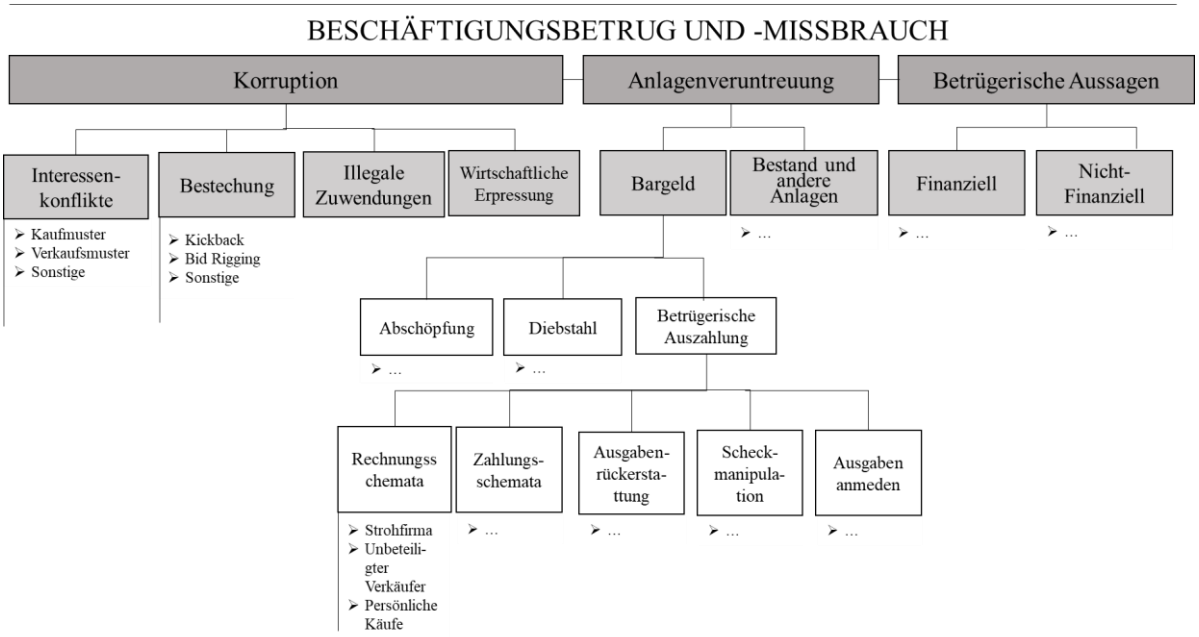


Abbildung 4-2: Klassifikation von Beschäftigungsfraud und Missbrauch
Quelle: Basierend auf Wells, (2011); (verkürzt: für die gesamte Klassifikation Anhang A: Fraud Klassifikationsbaum)

Auf höchster Ebene des Klassifikationsbaumes lassen sich die drei Hauptkategorien Korruption (Corruption), Anlagenveruntreuung (Asset Misappropriation) und betrügerische Angaben (Fraudulent Statements) einordnen (Wells, 2011). Korruption und Anlagenveruntreuung beinhalten Diebstahl oder absichtlichen Missbrauch von Vermögen oder der Machtposition. Betrügerische Angaben enthalten absichtliche Falschangaben. Die einzelnen Kategorien werden im Detail erklärt.

Korruption (Corruption)

Korruption kann in vier Unterkategorien eingeteilt werden: *Interessenkonflikt, Bestechung, illegale Zuwendungen* und *wirtschaftliche Erpressung*. Ein *Interessenkonflikt* existiert, wenn ein leitender Angestellter oder Mitarbeiter persönliches, meist finanzielles Interesse nicht bekannt gibt und damit gegen seine Firma handelt (Wells, 2011). Oft kommen diese Interessenkonflikte im Einkaufsprozess vor, da beteiligte Mitarbeiter Beziehungen zu Lieferanten aufbauen und pflegen. Beispielsweise könnte ein Angestellter der Einkaufsabteilung stets Geschäftsreisen für alle Mitarbeiter in einem bestimmten Reisebüro buchen, das ihm im Gegenzug Vergünstigungen auf seine privaten Urlaube gewährt (Wells, 2011).

Bestechung hingegen beinhaltet die Akzeptanz, Gabe oder das Angebot eines Guts oder einer Dienstleistung, um eine Transaktion zu beeinflussen (ACFE, 2011). Allein das Angebot einer Bestechung ist bereits eine Straftat, unabhängig von der Höhe des Angebots (Wells, 2011). Zwei Arten von Bestechung sind *Invoice Kickback* und Angebotsmanipulation (ACFE, 2011). An *Kickback* Schemata sind oft Mitarbeiter mit Genehmigungsbefugnissen beteiligt (Wells, 2011). Während der Lieferant überhöhte Rechnungen stellt, sorgt der Mitarbeiter für die interne Genehmigung der Rechnung. Die Differenz zwischen dem erhöhten und dem eigentlichen Preis wird meist geteilt (Wells, 2011). *Angebotsmanipulation* entsteht, wenn Lieferanten ein Ausschreibeverfahren durch Zuwendungen beeinflussen (Wells, 2011). Dabei kann beispielsweise die Spezifikation der Ausschreibung beeinflusst oder die Spezifikation vorzeitig ausgegeben werden (ACFE, 2011)[21].

Bei *illegalen Zuwendungen* werden nach einer Entscheidung Vorteile gewährt. Diese scheinen auf dem ersten Blick nicht unethisch, da sie die Entscheidung nicht beeinflussen (ACFE, 2011). Allerdings kann durch die Erwartungshaltung bei der Vergabe eines (Folge-) Auftrags die Entscheidung beeinflusst werden.

Erpressung bezeichnet die aktive Forderung eines Guts oder einer Dienstleistung, um eine Entscheidung zu beeinflussen (Wells, 2011). Meist entstehen *Interessenkonflikte* durch den Mismatch von finanziellen oder persönlichen Interessen des Arbeitnehmers und des Arbeitgebers (ACFE, 2011; Wells, 2011).

Veruntreuung von Vermögenswerten (Asset Misappropriation)

Innerhalb dieser Kategorie wird typischerweise zwischen *Veruntreuung von Geld* oder von *Inventar und weitere Sachwerte* unterschieden (Wells, 2011). *Inventar und weitere Sachwerte* beinhalten Diebstahl von Bürobedarf, Verbrauchsgütern, Maschinen oder den Missbrauch von Firmengütern zum eigenen Bedarf, wie beispielsweise der Ausdruck von privaten Dokumenten oder die Nutzung des Firmenfahrzeugs für private Strecken (ACFE, 2011). Diese Taten sind allerdings für den Einkaufsprozess nicht von Belang und werden deshalb nicht weiter aufgeführt. *Unterschlagung von Geld* hingegen beinhaltet *Abschöpfung* (Skimming), *Ausgaben* (Fraudulent Disbursements) und *Diebstahl* (von Geld) (Wells, 2011). *Abschöpfung* und *Diebstahl* sind sehr ähnlich, da beide den Diebstahl von Geld beschreiben. *Abschöpfung* beinhaltet Diebstahl vor dem Erfassen des Geldes in der Buchhaltung, während Diebstahl danach geschieht und damit auch in den Daten erkennbar ist (ACFE, 2011). Der Diebstahl von Geld ist allerdings nicht Teil des Einkaufsprozesses, da selten mit Bargeld bezahlt wird.

Ausgaben (Fraudulent Disbursment) beinhaltet *Abrechnungsschemata* (Billing Schemes), *Gehaltsschemata* (Payroll Schemes), *Vergütungsschemata* (Expense Reimbursement Schemes), *Scheckfälschung* (Check Tempering) und *Kassenauszahlungsschemata* (Register Disbursement Schemes) (Wells, 2011). Diese Arten von Fraud nutzen alle legitime Geschäftsprozesse, um Geld abzuschöpfen. Bei *Vergütungsschemata* (Expense Reimbursement Schemes) lassen sich Mitarbeiter fiktive Ausgaben erstatten (beispielsweise auf

[21] Weitere Beispiele vergl.: Wells (2011)

Geschäftsreisen). Bei *Gehaltsschemata* (Payroll Schemes) geben Mitarbeiter falsche Angaben über Gehalt oder geleistete Arbeitsstunden an. Es können sogar Geisterarbeiter, oft Pensionäre oder ehemalige Arbeitnehmer, vorkommen. (ACFE, 2011). S*checkfälschung* (Check Tempering) enthält die Fälschung von ausgehenden Checks (ACFE, 2011). *Kassenauszahlungen* (Register Disbursement) bewerten Erstattungen über und nehmen den Überschuss auf, oder aber führen Verkäufe als ungültig und nehmen das komplette Geld ein (ACFE, 2011). Auch diese Fraudarten sind nicht für den Einkaufsprozess relevant und werden nicht näher betrachtet.

Im Bereich von *Abrechnungsschemata* (Billing Schemes) sind einige für den Einkaufsprozess relevante Schemata beschrieben. Drei verschiedene Arten von Abrechnungsschemata sind hierbei von Bedeutung: *Scheinfirmen* (Shell Companies), *unbeteiligter Lieferant* (Non-accomplice Vendor) und *persönliche Käufe* (Personal Purchases).

Scheinfirmen arbeiten nicht im herkömmlichen, ökonomischen Sinne, sondern werden nur für wirtschaftskriminelle Handlungen gegründet (Wells, 2011). Diese Unternehmen versenden überteuerte Rechnungen, liefern minderwertige Waren oder berechnen fiktive Buchungen (ACFE, 2011). Sobald ein Unternehmen eine Rechnung der Scheinfirma erhält, sorgt ein Mitarbeiter für eine ordnungsgemäße Abwicklung des Einkaufsprozesses, um keinen Verdacht zu erwecken (Wells, 2011). Zusätzlich gibt es auch die Möglichkeit unschuldige Verkäufer zu beteiligen (Wells, 2011). Beim *unbeteiligten Lieferanten* wird eine zu hohe Summe, eine Rechnung doppelt oder „fälschlich“ Geld an den Lieferanten überwiesen. Anschließend verhandelt der wirtschaftskriminelle Täter mit dem unbeteiligten Lieferanten, wie das „falsch“ überwiesene Geld zurückerstattet werden kann. Beispielsweise fordert er den unbeteiligten Lieferanten auf das Geld auf (s)ein Konto zu überweisen und behält die Rückerstattung (Wells, 2011). *Persönliche Käufe* beinhalten Einkäufe für den persönlichen Gebrauch, die den normalen Geschäftsprozess durchlaufen (Wells, 2011). Oft werden Firmenkreditkarten verwendet, um persönliche Käufe zu tätigen. Auch werden vom Unternehmen benötigte Waren eingekauft und anschließend privat veräußert (ACFE, 2011).

Obwohl betrügerische Angaben (Fraudulent Statements) nicht im Einkaufsprozess stattfinden, werden diese der Vollständigkeit halber vorgestellt.

Betrügerische Angaben (Fraudulent Statements)

Bei *betrügerischen Angaben* werden oft Vermögenswerte oder Einnahmen zu hoch angesetzt, indem Belastungen oder Ausgaben verschwiegen werden. Ziel ist es Firmenziele zu erreichen oder den Investoren wohlwollend zu sein, um hohe Boni zu erhalten (ACFE, 2011). Beispielsweise kann der Täter geplante Einnahmen einrechnen, um ein besseres Bild des Unternehmens an Investoren zu präsentieren. Dadurch steigt seine Wahrscheinlichkeit weitere Finanzierung zu erhalten. Diese Art von Fraud ist weit verbreitet, jedoch nicht Bestandteil des Einkaufsprozesses[22].

[22] Für weitere Informationen, vergl. Wells, 2011

Nach der Beschreibung der verschiedenen Klassifizierungsmöglichkeiten von Fraud, wird als nächstes speziell auf den Einkaufsprozess eingegangen. Aus dem hier dargestellten Fraud Tree sind Schemata im Bereich von Conflict of Interest, Bribery, Illegal Gratuities, Economic Extortion und die drei Arten von Billing Schemes von besonderer Bedeutung. Die Ergebnisse einer umfangreichen Literaturstudie werden als nächstes vorgestellt.

4.2 Fraud im Einkaufsprozess

Da diese Dissertation primär den Einkaufsprozess betrachtet, werden vor allem typische Fraud Szenarien im selbigen dargestellt. Dieses Wissen hilft ein Verständnis über Möglichkeiten von Fraud zu erlangen und sollen mit dem zu entwickelnden Fraud Prototypen erkannt werden. Die Literaturstudie hat folgende zugrundeliegende Fragestellung:

Welche Arten von wirtschaftskriminellen Handlungen treten im Einkaufsprozess auf?

Die Literatursuche, samt der Schlüsselwörter wird im Methodenteil genau beschrieben. Die Resultate werden hier dargestellt. Alle Artikel werden in die eben vorgestellte Klassifizierung eingeordnet (ACFE Tree).

Publikation	Rechnungsschemata (gesamt)	Rechnungsschemata	unbeteiligter Lieferant	Persönliche Einkäufe	Scheinfirmen	Korruption (gesamt)	Korruption	Interessenkonflikt (Einkaufsschemata)	Bestechung (Kickbacks, Angebotsmanipulation)	Illegale Zuwendungen	Erpressung
(Barron, 2011)	X				X	X	X	X	X		
(Wilder, 2005)	X				X	X			X		
(Brandman, 2000)	X				X						
(Jaeger, 2011)	X				X						
(Jaeger, 2009)						X		X	X		
(Tabuena, 2010)	X				X	X		X	X		
(Tabuena, 2008)						X		X			
(Henderson, 2011)						X	X		X		X
(Dye, 2007)						X	X		X		
(Wiersema, 2002)	X			X		X			X		
(Verick, 2013)						X	X	X	X	X	
(Avellanet, 2010)	X			X	X	X		X	X		

(Muehlmann, Burnaby, & Howe, 2010)						X	X	X	X	X	
(Strand, Nowlin, & Wier, 2003)	X				X						
(Taylor, 2004)	X	X		X	X	X	X		X		
(Holsbeck, Canter, Johnson, & Taylor, 2008),						X			X		
(Byington & McGee, 2012)	X			X	X						
(Christensen & Byington, 2002),						X	X		X		
(Christensen & Byington, 2003b)	X	X		X	X						
(Christensen & Byington, 2003a)						X	X		X		
(Johnson & Rudolph, 2009)	X	X			X	X	X		X		
(Tackett, 2010)	X				X	X	X	X	X	X	X
(Lehman, 2008)	X				X						
(McNeal, 2012)						X		X	X		
(Nilsen, 2010)	X	X			X	X		X			
(Joseph T. Wells, 2004)	X			X	X	X	X	X	X		
(Anand, Ashforth, & Joshi, 2004)						X	X				
(Baughn, Bodie, Buchanan, & Bixby, 2010)						X	X		X		
(Joseph T. Wells, 2003b)	X	X			X	X	X		X		
(Joseph T. Wells, 2003c)	X	X			X						
(Büchner, Freytag, González, & Güth, 2008)						X	X		X		
(Graycar & Sidebottom, 2012)						X	X	X	X		
(Joseph T. Wells, 2002a)	X	X	X	X	X						
(Joseph T. Wells, 2002b)	X	X		X	X						
(Joseph T. Wells, 2002c)	X				X	X	X		X		
(Joseph T. Wells, 2003a)						X	X	X	X	X	
(Joseph T. Wells & Gill, 2007)	X				X	X		X			
(Jonas, Pattak, & Litchko, 2001)	X				X	X	X		X		
(Brulenski & Zayas, 2004)	X				X	X			X		
(Handfield & Baumer, 2006)						X		X	X		
(Meiners, 2005)	X			X	X						
(Imoniana, Antunes, & Formigoni, 2013)						X	X		X		X
(Viton, 2003)	X	X	X	X	X	X			X	X	X
(May, 2005)	X				X	X	X				
(Buckhoff & Parham, 2009)						X			X		
(Kayrak, 2008)	X			X	X	X	X	X	X		X
(Strand, Judd, & Lancaster, 2002)	X			X	X						
(Strand, Welch, Holmes, & Strawser, 2000)	X				X						
(Taylor, 2006)	X				X						
(Allen, 2007)						X	X		X		
(Cowan, 2005)						X	X	X	X		
(Desrosiers, 2010)						X		X			
(Lambert-Mogiliansky & Sonin, 2006)						X	X		X		
(Ellinor, 2005)	X				X	X	X				

(Ellinor, 2009)	X				X	X	X		X		
(Levi, 2010)						X	X		X		
(Lord, 2010)	X	X				X	X	X	X	X	X
(Morehead, 2007)						X	X		X		
(Nguyen, 2005)						X	X	X	X		
(Roberts, 2010)						X	X	X	X		
(Seetharaman, Senthilvelmurugan, & Periyanayagam, 2004)	X				X	X	X				
(Sikka, 2008)	X	X				X	X	X	X		
(Sammons, 2005)						X	X		X		
(Buckhoff, 2003)	X				X						
(Song, 2008)						X	X		X		
(Buckhoff, 2002)	X				X						
(Thai, 2001)						X	X	X	X		
(Fishman, 2001)	X				X						
(Kranacher, 2008)						X			X		
(Lander, Kimball, & Martyn, 2008)						X	X	X	X		
(Tran, 2009)						X	X		X		
(Lehman & Weidenmier, 2005)	X	X		X	X						
(Ulinski, Girasa, & Fanelli, 2013)						X			X		
(Leinicke, Ostrosky, Rexroad, Baker, & Beckman, 2005)	X				X	X			X		
(Zikmund, 2008)	X				X						
(Vitell, Dickerson, & Festervand, 2000)						X		X	X	X	
(Grieshober, 2001)						X			X		X
(Langley, 2003)	X				X						
(Pacini & Brody, 2005)	X	X				X		X	X		X
(Thompson, 2000)	X				X						
(Ramamoorti & Curtis, 2003)	X	X				X	X		X		
(Al-ajwad & Carr, 2016)						X			X		
(Bhattacharya & Suri, 2017)						X					
(Boag, 2015)							X		X		
(Dhurandhar et al., 2015)	X				X						
(Erven, Holanda & Carvalho, 2017)									X		
(Fazekas et al., 2016)							X		X		
(Ferwerda et al., 2016)							X		X		
(Fuseini et al., 2017)									X		
(Gong & Zhou, 2015)							X		X		
Hudon & Garzon, 2016)							X		X		
(Kohler et al., 2015)									X		
(McNamee, 2016)					X				X		
(Nag, 2015)									X		
(Nanang & Misman, 2016)									X		

	Abrechnungsschemata (gesamt)[23]	Abrechnungsschemata	unbeteiligter Lieferant	Persönliche Einkäufe	Scheinfirmen	Korruption (gesamt)[24]	Korruption	Interessenkonflikt (Einkaufsschemata)	Bestechung (Kickback, Angebotsmanipulation)	Illegale Zuwendungen	Erpressung
(Rahmani & Koohshahi, 2015)									X		
(Rendon & Rendon, 2016)					X						
(Brannon, 2018)							X				
(Vona, 2017)									X		
(Yang et al., 2017)	X										
(Zasada & Fellmann, 2016)							X		X		
(Horme. Lochner, & Ventner, 2018)									X		
Gesamt	48	5	2	13	44	63	45	27	70	7	8

Tabelle 13: Literaturergebnisse zu internem Fraud
Quelle: Eigene Darstellung

Literaturstudie – Ergebnisse

Die Literatur wird eingehend nach den genannten Fraud Schemata untersucht. Auffällig an den Ergebnissen in Tabelle 13 ist, dass vor allem Kickback und Angebotsmanipulation, gefolgt von Korruption im Allgemeinen und Scheinfirmen behandelt werden. Diese Fraud Schemata scheinen die größte Aufmerksamkeit von Wissenschaft und Praxis auf sich zu ziehen. Dies kann darauf zurückzuführen sein, dass diese Fraud Schemata besonders häufig auftreten oder besonders gut beforscht sind. Die Schemata unbeteiligter Lieferant und Abrechnungsschema werden nur von zwei bzw. sieben Publikation behandelt. Zu illegalen Zuwendungen und Erpressung lassen sich nur sieben bzw. acht Publikationen zuordnen. Überraschend ist die große Differenz in der Behandlung der einzelnen Schemata (z.B. 70 versus 2).

Digitale Massendatenanalyse für Fraud Detektion

Um Fraud im Unternehmen aufzudecken werden in der Litaretur Maßnahmen genannt, die hier kurz vorgestellt werden. Detailliert wird auf Algorithmen und Techniken der Datenanalyse für Frauderkennung eingegangen. Diesen Ergebnisen geht eine Literaturstudie voraus, deren Durchführung aus dem Methodenteil hervorgeht.

[23] Bei der Berechnung der Gesamtsummen werden doppelte Einträge nicht addiert
[24] Bei der Berechnung der Gesamtsummen werden doppelte Einträge nicht addiert

4.2.1 Fachliche Ansätze zur Identifikation von Fraud

Fraud Bewusstsein Training

Eine Fraud Bewusstseinstrainingsmaßnahme scheint einfach in einem Unternehmen umsetzbar zu sein. Laut der letzten ACFE (2018) Umfrage haben weniger als die Hälfte aller Unternehmen ein Anti-Fraud Training etabliert. In einem solchen Training lernen die Mitarbeiter auf welche Hinweise für Fraud sie achten sollen und wie diese bei Beobachtung dieser Hinweise reagieren sollen (Albrecht et al., 2012). Die Mitarbeiter werden nicht direkt geschult, wie man Fraud begeht. Diese Trainings sollen Fraud durch die abschreckende Wirkung verhindern. So erwarten die Mitarbeiter von den Kollegen entlarvt zu werden und sollen Fraud als zu riskant einstufen (ACFE, 2016).

Mitarbeiteruntersuchung

Bevor ein Mitarbeiter eingestellt wird, sollen die vorhergehenden Arbeitgeber nach ethischen Werten und Ehrlichkeit befragt werden (Albrecht et al., 2012). Die Sicherstellung dieser Werte soll durch Hintergrundrecherchen, Hinterfragung der Referenzen der Bewerber und ein spezielles Testen der moralischen Vorstellungen im Jobinterview identifiziert werden (Frankenfield & Kleiner, 2000).

Enthüllungssystem (Whistle-Blowing System)

Laut der ACFE (2018) Umfrage sind Hinweise der Mitarbeiter die wirkungsvollste Detektionsmethode von Mitarbeiterfraud. Enthüllungssysteme sind oft Hotlines oder Webseiten auf denen Mitarbeiter, Kunden oder Lieferanten anonym Hinweise auf verdächtiges Verhalten geben können (Albrecht et al., 2012). Jedoch bieten diese Systeme oft wenig Anreiz, um ein Fehlverhalten zu melden. Dadurch kommt es zur geringen Nutzung der Systeme (Dyck, Morse, & Zingales, 2010). Jedoch hat allein die Existenz solcher Systeme einen signifikanten Einfluss auf das Verhalten der Täter (ACFE, 2018).

Physische Dokumentenanalyse

Obwohl immer mehr Daten elektronisch vorhanden sind, existieren auch physische Dokumente, die nicht digitalisiert werden. Diese Informationen können nicht für die automatische Frauderkennung verwendet werden. Die physische Dokumentenanalyse beinhaltet die Identifikation von gefälschten Dokumenten (zum Beispiel gefälschte Checks), von gefälschten Unterschriften und von fehlenden Dokumenten (Vona, 2011). Da solche Verfahren sehr umständlich und kostspielig sind, werden sie meist erst bei einem konkreten Verdacht durchgeführt.

Analyse von Texten

- Die Analyse von Texten nimmt eine wichtige Funktion bei der Frauderkennung ein. Nicht alle Informationen sind in numerischer Form vorhanden. Deshalb müssen mitunter auch Texte miteinander verglichen werden. Zwar lässt sich ein einfacher Textvergleich in den

meisten Programmier- und Abfragesprachen durchführen, die Ergebnisse sind jedoch meist nicht zufriedenstellend. Das für Menschen einfach lösbare Problem ist für einen Computer ungleich komplizierter. Dabei wirkt sich eine nicht standardisierte Formatierung, die in vielen Datensätzen vorherrscht, weiter negativ auf die Ergebnisse aus. So ist es für einen einfachen Vergleichsalgorithmus schwer den Unterschied, beziehungsweise die Gleichheit, von verschiedenen Formatierungen zu erkennen. Ein gutes Beispiel ist hier Adresse. Die folgenden Schreibweisen sind für einen Menschen als identisch zu erkennen, ein einfacher Algorithmus hat damit jedoch Probleme (Albrecht et al., 2012):

- Musterstr. 10, 12345 Großstadt
- Musterstrasse 10, 12345 Großstadt
- 12345 Großstadt, Musterstr. 10

Um dieses Problem zu lösen wurde eine Vielzahl von Algorithmen der Kategorie Fuzzy-Text Matching entwickelt.

Numerische Analysen/Benfords Gesetz

Eine weitere Möglichkeit Daten auf Unregelmäßigkeiten zu analysieren ist in Form von Benfords Gesetz. Benfords Gesetz ist eine Wahrscheinlichkeitsverteilung, die bisher vor allem Anwendung in der Buchhaltung gefunden hat (Lu, Boritz, & Covvey, 2006). Das Gesetz spezifiziert die Wahrscheinlichkeit mit der führende Ziffern einer mehrstelligen Zahl in einem natürlichen, d.h. einem nicht künstlich erzeugten, Datensatz erscheinen (Bhattacharya & Kumar, 2008). Das folgende Beispiel soll diesen Zusammenhang veranschaulichen (Lu et al., 2006):

$$S = (231, 432, 1, 23, 634, 23, 1, 634, 2, 23, 34, 1232)$$

Formel 1: Datensatz S
Quelle: Lu et al., 2006

Der Datensatz S enthält zwölf Einträge bei dem vier mit der Ziffernsequenz ‚23' starten. Um die Wahrscheinlich zu berechnen, dass diese beiden Ziffern an erster Stelle stehen, dürfen nur Einträge in Datensatz S betrachtet werden, die mindestens die Länge der gesuchten Ziffernfolge aufweisen. Dies würde zu einer Wahrscheinlichkeit von $\frac{4}{9} \approx 0{,}44$ führen (Lu et al., 2006). Benfords Gesetz kann Unregelmäßigkeiten in Lieferantenrechnungen entdecken, bei denen Rechnungsbeträge automatisch generiert werden (Albrecht et al., 2012).

Dieser Abschnitt gibt einen Überblick über fachliche Ansätze zur Prävention und Erkennung von internem Fraud. Im Folgenden wird ein Überblick über Methoden der Datenanalyse gegeben, sowie eine Einschätzung über deren Eignung für den Einkaufsprozess.

4.2.2 Interne Kontrollen vs. Fraud

Bevor Algorithmen zur Fraud Detektion beschrieben werden, soll zunächst auf interne Kontrollen eingegangen werden. Diese dienen der Vorbeugung von Fraud.

Interne Kontrollen

Interne Kontrollen können entweder vorbeugend oder erkennend sein. Eine beispielhafte vorbeugende Kontrolle wäre ein vorgegebener Wertebereich für die Eingabe in IT Systemen. Solche Kontrollen sind in ERP Systemen implementiert und verhindern durch die Einschränkung der erlaubten Eingaben, Transaktionen oder Zugangsrechten Fraud (Albrecht et al., 2012).

In Zeiten des hohen Produktivitätsdrucks helfen Datenanalysen den Fokus auf Bereiche mit hohem Risiko zu legen (Coderre, 2009). Beispiele für Datenanalysen sind die Anwendung von Data Mining, Process Mining, Datenprofilierung oder Kennziffernanalyse auf unterschiedliche, oft zusammengeführte Quellen. Einige Softwarepakete (Computer-Assisted Auditing Tools and Techniques (CAATTs)) wurden zu diesem Zweck entwickelt. Die am weitesten verbreiteten sind die Audit Control Language (ACL) und die Interactive Data Extraction and Analysis (IDEA) Tools (Albrecht et al., 2012; Mooney, Harrell, & Ludwig, 2000).

Einige dieser datengetriebenen Techniken können dahingehend automatisiert und integriert werden, dass man vom durchgehenden Auditing (continuous auditing) oder Monitoring spricht. Ziel ist es die Auditoren zu unterstützen und gleichzeitig auch zu entlasten (Albrecht et al., 2012). Da die meisten Unternehmen ERP Systeme zur Verwaltung ihrer Operationen nutzen, werten Auditoren und anti-fraud Experten die Daten aus diesen Systemen zur Frauderkennung aus. Da die Anzahl der Daten in großen und ggf. multinationalen Unternehmen sehr große Dimensionen erreicht, ist eine manuelle Kontrolle nicht mehr möglich (Ramamoorti & Curtis, 2003).

Statische und dynamische automatisierte Kontrollen werden verwendet, um die Auditoren bei der Untersuchung großer Datenmengen zu unterstützen. Die Vorgabe der Wertebereiche, wie rollenbasierte Autorisierungsregeln oder vordefinierte Wertebereiche, sind von Natur aus statisch. Um eine solche Kontrolle zu implementieren, müssen Regeln entwickelt werden, die alle möglichen Szenarien abdecken. Solche Techniken sind nicht flexibel und bei einer hohen Anzahl von Szenarien ineffizient. Deshalb gibt es dynamische Kontrollen, die typischerweise zwischen legitimem und wirtschaftskriminellem Verhalten unterscheiden. Diese benötigen wenige Regeln im Voraus und haben zum Ziel den manuellen Aufwand zu verringern.

4.2.3 Algorithmische Fraud Erkennung

Algorithmische Fraud Erkennungstechniken können überwacht oder nicht überwacht sein. Ein Set mit gekennzeichneten Transaktionen wird für das Training eines überwachten Algorithmus benötigt. Basierend auf der Trainingsphase klassifiziert dieser Algorithmus neue Transaktionen (Chandola et al., 2009). Unüberwachte Algorithmen teilen Transaktionen in Gruppen, die sich sehr ähneln (Kou et al., 2004; Sabau, 2012). Instanzen, die nicht zu diesen Clustern gehören, werden als fehlerhaft oder betrügerisch eingeschätzt (Chandola et al., 2009). Bei diesen Algorithmen gibt es keine absolute Genauigkeit und die Unterscheidung zwischen unüblichem Verhalten und wirtschaftskriminellen Handlungen ist nicht gegeben. Jedoch wird die Arbeit

eines Fraud Ermittlers durch die Reduktion der Transaktionen auf die relevantesten erleichtert, können dessen Arbeit aber nicht ersetzen (Allan & Zhan, 2010).

Lange Zeit wurden algorithmische Fraud Erkennungsverfahren rein reaktiv eingesetzt, indem periodisch Transaktionen des letzten Geschäftsjahrs nach Auffälligkeiten durchsucht wurden. Der Trend geht in Richtung proaktiver oder kontinuierlicher Fraud Erkennung. Auditoren sollen in der Lage sein einzugreifen, bevor die Transaktion durchgeführt wird (Allan & Zhan, 2010). Daher werden an dieser Stelle die gängigsten Fraud Erkennungsverfahren erklärt.

Das Vorgehen der Literaturrecherche kann aus dem Methodenkapitel dieser Dissertation entnommen werden. Insgesamt werden 177 Quellen ausgewählt und in Kategorien unterteilt. Abbildung 4-3 zeigt die Anzahl der wissenschaftlichen Artikel pro Fraudtyp und verwendeter Detektionsmethode. Die Kategorie ‚Andere' umfasst Fuzzy Logic und Evolutionsmechanismen (bspw. Expertensysteme).

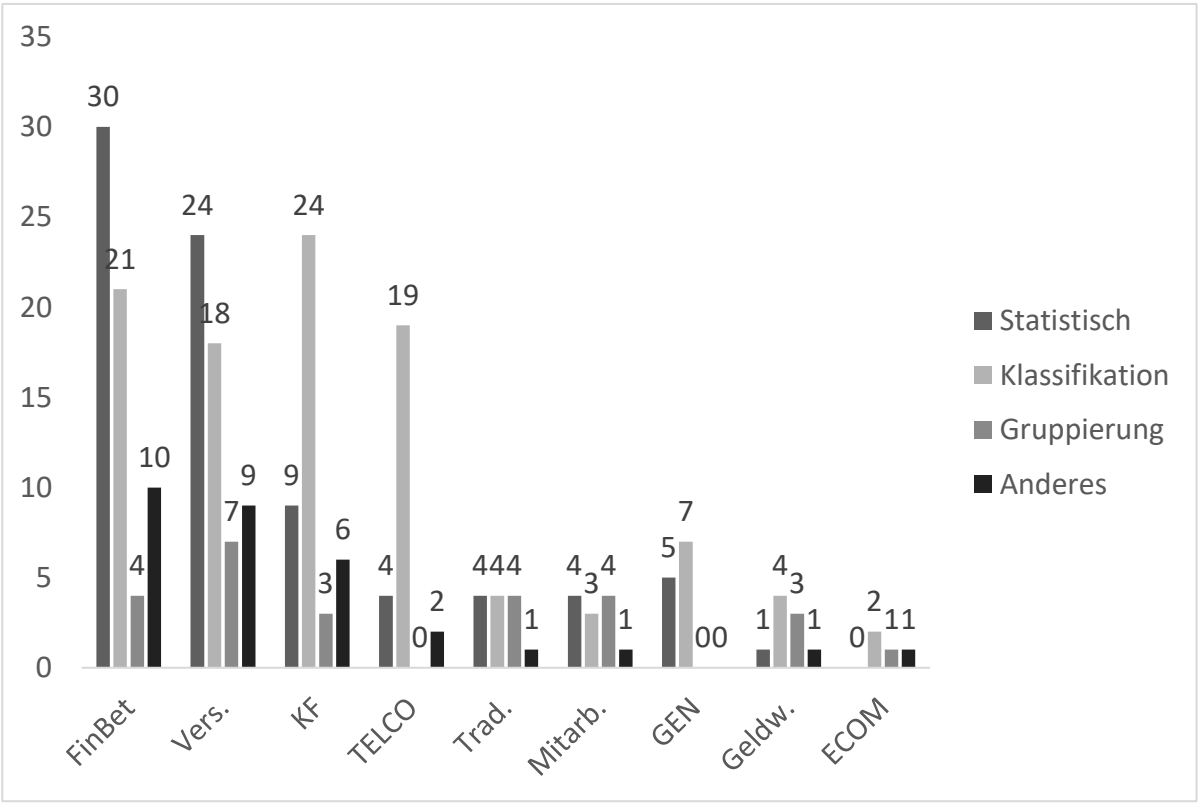


Abbildung 4-3: Literaturanalyse der Fraud Detektionstechniken basierend auf Fraudbereiche[25]
Quelle: Eigene Darstellung, für eine detaillierte Übersicht vergl. Anhang B: Algorithmen zur Fraud)

Die meisten identifizierten Artikel befassen sich mit Finanzbetrug (FinBet), Versicherungsbetrug (Vers), Kreditkartenbetrug (KF) und Betrug in der Telekommunikation (TELCO). Bei Finanzbetrug (65 Publikationen) werden statistische Detektionsverfahren (30 Artikel) am häufigsten adressiert, gefolgt von Klassifikationsalgorithmen (21 Artikel). Dieses

[25] FinBet: Finanzbetrug; Vers.:Versicherungsfraud; KF: Kreditkartenfraud; TELCO: Telekommunikationsfraud; Trad: Insiderfraud; Mitarb.: Mitarbeiterfraud; GEN: Genereller Fraud; Geldw.: Geldwäsche; ECOM: E-Commerce Fraud

Bild ist für alle Typen recht ähnlich. Clustering und weitere Methoden (z.B. Fuzzy Logik) spielen eine kleine Rolle in der algorithmischen Frauderkennung.

Die am häufigsten genutzten algorithmischen Ansätze zur Fraudidentifikation werden, wie in Abbildung 4-4 dargestellt, verglichen. Die am weitesten verbreiteten Algorithmen sind parametrisierbare Algorithmen (v.a. Regressionsalgorithmen), regelbasierte Algorithmen (v.a. Entscheidungsbäume) und Neuronale Netze. Neuronale Netze haben eine detaillierte Struktur und werden deshalb nicht weiter untergliedert.

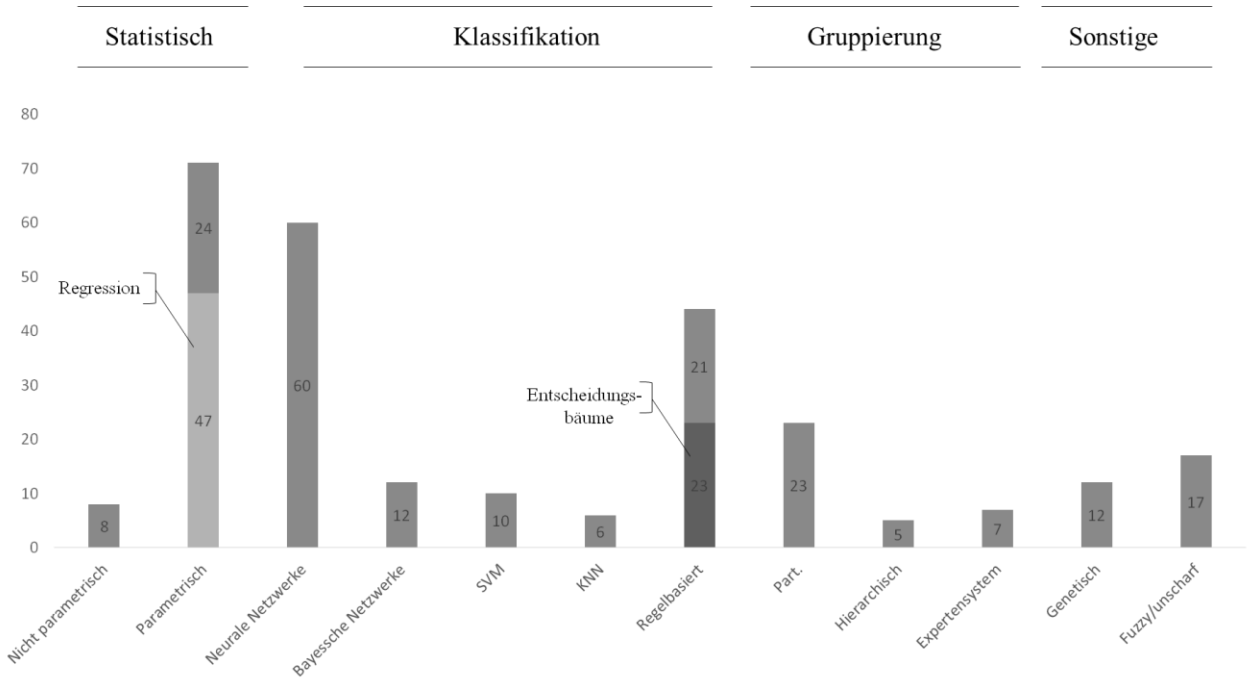


Abbildung 4-4: Literaturanalyse der Fraud Detektionstechniken

Quelle: Eigene Darstellung, Artikel können in Anhang B: Algorithmen zur Fraud angesehen werden

Im Folgenden sollen die am häufigsten verwendeten algorithmischen Fraud Detektionsverfahren mit dem relativ neuen Ansatz ‚Process Mining' und dem etablierten ‚Red Flag' Ansatz verglichen werden. Da Process Mining ein relativ neuer Ansatz ist, findet dieser noch keinen Einzug in der Statistik.

Regression

Die Regression ist ein parametrisierbarer, statistischer Ansatz, bei dem Inputvariablen in Relation zu einer Ausgabe gesetzt werden. Wenn man dies auf Frauderkennung anwendet, so ist die Ausgabe meist binär (Fraud oder kein Fraud). Deshalb finden meist die für die Ausgabe von Binärwerte optimierten Logit Modelle Anwendung (Ngai et al., 2011). Diese Verfahren zeigen ebenfalls die Wahrscheinlichkeit für Fraud von unbekannten Instanzen. Die Inputvariablen haben fast kein restriktives Format (numerisch, binär). Auch können kategorische Werte verwendet werden, die jedoch meist in ein Set von binären Inputwerten transformiert werden.

Dieses Verfahren ist besonders für Zeitanalysen geeignet. Einige Frauds zeichnen sich durch den langsamen Anstieg von Werten aus, da die Täter zunächst vorsichtig agieren und die Anzahl von Käufen und die Rechnungssumme verhältnismäßig klein sind. Mit der Zeit steigen diese aber, da Täter immer gieriger werden und ihre Hemmungen verlieren (Albrecht et al., 2012). Auch eine Statistik der ACFE (2018) zeigt, dass die erbeuteten Fraud Summen steigen, je länger Fraud unentdeckt bleibt. Dadurch hilft eine Zeitanalyse wichtige Indizien zu liefern, da das Aufzeigen von Datenpunkten über die Zeit hinweg Trends und Ausreißer erkennen lässt (Albrecht et al., 2012).

Regressionsbasierte Verfahren werden zur Aufdeckung in verschiedenen Bereichen angewendet, wie beispielsweise bei Versicherungsbetrug, Mitarbeiterbetrug oder Finanzbetrug (Sharma & Panigrahi, 2012). Die entsprechenden Algorithmen sind einfach zu implementieren und verwenden wenige Ressourcen. Jedoch können diese Algorithmen mit einer entsprechend hohen Anzahl von Eingabevariablen sehr komplex und rechenintensiv werden. Daher ist es wichtig die unabhängigen Inputvariablen mit Bedacht auszuwählen.

Neuronale Netze

Neuronale Netze sind dem menschlichen Gehirn mit verbundenen Synapsen nachempfunden. Es ist ein Netz aus Neuronen bzw. Knoten, die bestimmte Inputsignale in eine mathematische Funktion füttern und die ausgehenden Synapsen bzw. Kanten ausführen. Die Idee ist elementare Entscheidungseinheiten (Neuronen) zu einem mehrschichtigen Netz zu schachteln (Multi-Layer Perzeptron). Umso mehr Neuronen und Schichten das Netz aufweist, desto mehr Fraud Szenarien lassen sich erkennen (Burge & Shawe-Taylor, 1997). Um allerdings das Netz aufzubauen, ist eine sehr große Menge an Trainingsdaten mit einer eindeutigen Kennzeichnung (Fraud/ Kein Fraud) notwendig, da dieser Algorithmus zu den überwachten Lernalgorithmen zählt (Burge & Shawe-Taylor, 1997). Dabei berechnet sich das Ergebnis durch nichtlineare Transformationen eines gewichteten Eingabevektors x und eines Ausgabewert y. Die Formel für die Berechnung ist laut Burge & Shawe-Taylor (1997):

$$y = \sigma(\sum_{i=1} w_i x_i + w_0)$$

Formel 2: Output eines Neurons in einem Multi-Layer Perzeptron
Quelle: Burge & Shawe-Taylor (1997)

Dabei ist x_i die i-te Zeile des Eingabevektors, w_i ihre Gewichtung und σ eine geeignete nicht-lineare Transformation. Als Eingabe dienen Attribute aus dem Trainingsdatensatz (bspw. die Transaktionssumme), während die Transformation σ (bspw. Tangens hyperbolicus) einen Ergebniswert zwischen 0 und 1 (Betrug/kein Betrug) zurück gibt. Jedem Knoten wird ein Gewicht zugewiesen, wodurch das Verhalten des gesamten Netzwerks gesteuert wird. Anfänglich hat jeder Knoten ein zufälliges Gewicht zugewiesen. Durch den Trainingsdatensatz wird das Gewicht verändert, so dass das Netzwerk verstärkt das gewünschte Verhalten nachweist (Chandola et al., 2009). Oft wird für die Gewichtung der Levenberg-Marquardt-Algorithmus (Burge & Shawe-Taylor, 1997) verwendet. Diese schrittweise Anpassung der

Gewichtung und der Anzahl von Schichten und Neuronen ist sehr rechenintensiv, da der Trainingsdatensatz häufig durchgegangen werden muss. Dennoch können neuronale Netze sehr komplexe Fraud Szenarien identifizieren und werden deshalb im Bereich Betrugserkennung häufig verwendet. Eingesetzt werden diese Kreditkartenbetrug, Telekommunikationsbetrug (Allan & Zhan, 2010; Peter Burge & Shawe-Taylor, 1997; Kou et al., 2004) und zur Erkennung von Managerbetrug (Fanning & Cogger, 1998).

Regelbasierte Klassifikatoren - Entscheidungsbaum

Das am häufigsten verwendete Verfahren zur regelbasierten Klassifikation von Fraud ist der Entscheidungsbaum. Laut Witten & Frank (2005) wird eine baumartige Datenstruktur von ihrer Wurzel her durchlaufen. Verzweigungspunkte sind Vergleichsoperationen für Charakteristika (Attribute). In Abbildung 4-5 ist ein möglicher Entscheidungsbaum dargestellt.

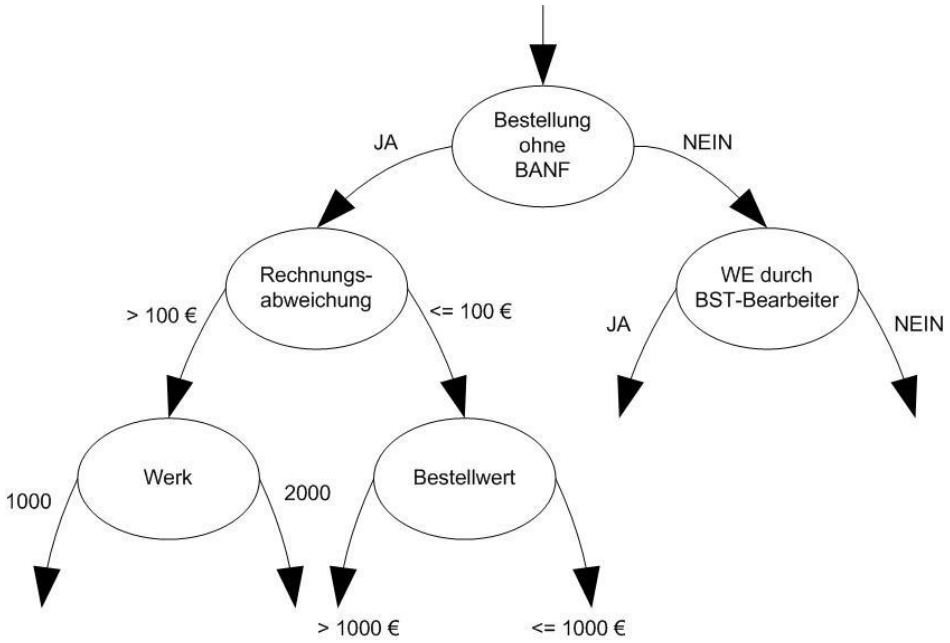


Abbildung 4-5: Beispiel eines Entscheidungsbaums (Ausschnitt)
Quelle: Eigene Darstellung

Beim Entscheidungsbaum wird zunächst eines der eingegebenen Attribute als Wurzelattribut ausgewählt und jede Wertausprägung des Attributs in einem Ast dargestellt. (Witten & Frank, 2005). Die Daten werden anhand des Baumes in Untermengen aufgeteilt und den entsprechenden Ästen zugewiesen. Für jeden Ast wird anhand der Untermenge ein neuer Entscheidungsbaum erzeugt. Diese Rekursion terminiert, sobald das Datensubsets eines Astes nur noch aus einem einzigen Element besteht und somit ein Blatt wird. Im Beispielbaum aus Abbildung 4-5 sind Betrugsversuch und kein Betrugsversuchen die Blätter. Wichtig ist bei diesem Algorithmus die Auswahl des Attributs zum Splitten des Datensets pro Ast (Witten & Frank, 2005). Ziel ist es möglichst früh einen möglichst hohen Reinheitsgrad bezüglich des Zielattributs zu erreichen. Der Informationsgehalt der einzelnen Untermengen bezüglich des Zielattributs wird als Maß für den Reinheitsgrad gemessen (Witten & Frank, 2005). Dabei wird die Differenz aus dem Informationsgehalt des Datensatzes vor einem Split und dem gewichteten

Mittel der Informationsgehalte der resultierenden Untermengen als Info-Gain einer Split Operation bezeichnet (Witten & Frank, 2005). In jedem Rekursionsschritt wird zum Aufteilen des Datensatzes das Attribut verwendet, das den höchsten Info-Gain verspricht. Der Vorteil dieses Verfahrens ist, dass man die Wahrscheinlichkeitsverteilung approximieren kann (Witten & Frank, 2005).

Process Mining

Der Begriff Process Mining bezieht sich nicht auf eine einzelne Methode oder einen Algorithmus. Es beschreibt ein Konzept zur Erstellung von Prozessmodellen durch die Daten der Transaktion und wird als Prozessentdeckung (Process Discovery) bezeichnet. Für die Implementierung sind beispielsweise die Verwendung des α- Algorithmus (Aalst, Weijters, & Maruster, 2004; Dongen, Medeiros, & Wen, 2009), des zwei-Phasen Ansatzes (Aalst et al., 2010), des künstliche Intelligenz Ansatzes (bspw. genetische Programmierung) (Aalst, Medeiros, & Weijters, 2005) oder Fuzzy Mining (Aalst & Günther, 2007; Günther & Aalst, 2007) geeignet. Nachdem das Prozessmodell erstellt wird, können Prozessinstanzen anhand dieses untersucht werden. Ein Beispiel ist in Abbildung 4-6 dargestellt.

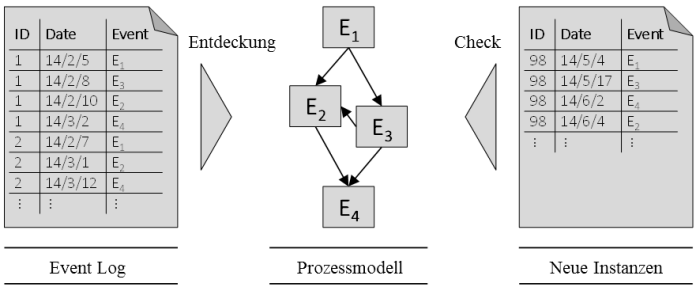


Abbildung 4-6: Process Mining Ansatz zur Fraud Detektion
Quelle: Eigene Darstellung

Alle Transaktionen eines Systems müssen ein Attribut haben, welches die eigentliche Transaktion beschreibt, sowie ein entsprechendes Datums- und ggf. Uhrzeitsattribut. Anhand dieser Daten erstellt ein Algorithmus ein Prozessmodel. Wirtschaftskriminelles Verhalten wird häufig in Abweichungen vom Standardprozess nachgewiesen. Abbildung 4-6 zeigt eine Prozessinstanz (ID 98), bei der die Events in der Reihenfolge $E_1>E_3>E_4>E_2$ vorkommen. Das Prozessmodel zeigt allerdings, dass E_2 nicht nach E_4 erfolgen darf. Im Einkaufsprozess hat eine Prozessinstanz über 100 verschiedene Events, die automatisiert überprüft werden können.

Red Flag Ansatz

Ein Red Flag (auch Fraud Risikofaktor oder Fraud Indikator) ist ein Hinweis auf eine möglicherweise betrügerische Handlung. Indikatoren sind keine Beweise und können bei isolierter Betrachtung keine oder nur eine geringe Aussagekraft haben. Erst wenn sie wiederholt, gehäuft oder in gewisser Konstellation auftreten sind sie zur Anzeige von Fraud geeignet (Diir, 2011). Die Anzahl der identifizierten Red Flags korreliert mit dem Fraud Risiko (Bungartz, 2012). Häufig werden Red Flags aufgrund einer Flut von Informationen von den entsprechenden Auditoren ignoriert (Henselmann & Hofmann, 2010). Dennoch ist der Red Flag Ansatz der am häufigsten verwendete Ansatz in der Praxis. Verschiedene Indikatoren werden

zu Checklisten zusammengefasst, die oftmals der persönlichen Erfahrung des Prüfers entsprechen. Diese Checklisten haben den Nachteil, dass sie nicht untersuchen, wie einzelne Red Flags relativ zueinander zu bewerten sind (Hofmann, 2008).

4.3 Vergleichende Analyse

Die hier vorgestellten Entscheidungsbäume und Neuronale Netze haben den Vorteil, dass sie selbständig lernen und kein explizites Expertenwissen benötigen. Der größte Nachteil ist, dass sie Trainingsdaten zur Unterscheidung von normalem und wirtschaftskriminellem Verhalten benötigen (Barse, Kvarnström, & Jonsson, 2003). Ein weiteres Problem ist die verzerrte Verteilung der Daten. Normalerweise sind Betrugsversuche selten und kommen entsprechend selten im Datensatz vor. Deshalb stuft der Detektionsalgorithmus häufig alle Daten als regelkonform ein und erzielt eine hohe Trefferquote (Chan et al., 1999). Auch die Höhe der Schadenssumme wird durch die genannten Algorithmen nicht gesondert beachtet. Verdachtsfälle mit einem hohen Schadensvolumen sollten priorisiert behandelt werden (Chan et al., 1999).

Alle vorgestellten Verfahren werden nach bestimmten Kategorien verglichen. Bei der *Genauigkeit* der Algorithmen werden Messwerte, wie die falsch-positiv und richtig-positiv Rate, bestimmt. Die zweite Dimension vergleicht die *Performanz* solcher Techniken und misst die Rechenlast in der Trainingsphase bzw. Entdeckungsphase und die Rechenlast bei der Klassifizierung neuer Instanzen. Auch die *Skalierbarkeit* in Form von Parallelisierbarkeit wird verglichen. Die nächste Dimension ist vor allem für Fraud im Einkaufsprozess von besonderer Bedeutung. Da der Prozess sequentiell ist, sollte das Verfahren im Stande sein mit sequentiellen Informationen umzugehen. Diese Dimension wird unter *Prozessfähigkeit* zusammengefasst. Prozesse können sich sehr schnell durch Umstrukturierung oder der natürlichen Entwicklung ändern. Gemessen wird der manuelle Aufwand zur Anpassung des Verfahrens an den neuen Prozess *(Flexibilität)*. Eine weitere Vergleichskategorie ist die *Benutzbarkeit*. Es gibt keine Lösung, die selbständig zwischen seltenen aber legitimen, fehlerhaften und wirtschaftskriminellen Transaktionen unterscheiden kann. Auditoren müssen die zweifelhafte Transaktion manuell bewerten. Eine benutzerfreundliche Darstellung der Ergebnisse erleichtert den Auditoren die Arbeit.

Zusammenfassend soll nach *Genauigkeit, Performanz, Skalierbarkeit, Prozessfähigkeit, Flexibilität* und *Benutzbarkeit* basierend auf der Literaturstudie unterschieden werden. Bisher ist kein solcher Vergleich in der Literatur zu finden. In der Data Mining Literatur werden Algorithmen meist nach ihrer Fehlerrate, Trainingsperformanz und Skalierbarkeit gemessen (Lim, Loh, & Shih, 2000). Gleichzeitig fordern Rozinat, Medeiros, Günther, Weijters, & Aalst (2008) ein umfassendes Process Mining Evaluationsframework. Die von den Autoren vorgestellten Vergleichskriterien sind weder prägnant definiert, noch einfach quantifizierbar (Weerdt, Backer, Vanthienen, & Baesens, 2012).

Anhand der Literaturanalyse sollen die Algorithmen nach den zuvor aufgestellten Kriterien beurteilt werden. Dies unterliegt einigen Limitationen. Zunächst ist zu nennen, dass Process

Mining ein recht neues Forschungsgebiet ist. Deshalb gibt es nur wenige Publikationen die Process Mining für Fraud anwenden, wodurch ist die Vergleichbarkeit nicht immer gegeben ist. Zusätzlich gibt es keine wissenschaftliche Literatur, die Data Mining und Process Mining miteinander vergleicht. Dies soll daher einen ersten Ansatz darstellen ist jedoch nicht der Fokus der Dissertation.

Genauigkeit

Die Genauigkeit von Logit Modellen und Neuronalen Netzen wird durch die Berechnung des Durchschnitts aller in der Literatur angegebenen Genauigkeiten bestimmt. Als Ergebnis liegt die Genauigkeit von Logit Modellen bei etwa 80% und von Neuronalen Netzen bei etwa 83%. Hierbei wird nicht zwischen unterschiedlichen Algorithmen zur Bildung von Neuronalen Netzen unterschieden. Im Bereich des Process Minings gibt nur eine Quelle die Genauigkeit an. Diese liegt bei Nutzung des Threshold Algorithmus bei etwa 85% (Bezerra & Wainer, 2008a).

Dieser Vergleich hat zum Nachteil, dass es sich bei dem ersten Wert um einen Durchschnittswert handelt, während sich die Genauigkeit bei Process Mining nur aus einer Publikation zusammensetzt. Dennoch sind die Werte recht ähnlich, so dass es basierend auf der Genauigkeit keinen eindeutigen Favoriten zur Auswahl eines Algorithmus gibt.

Performanz und Skalierbarkeit

Lim et al. (2000) benötigen zum Aufbau ihres Logit Modells vier Minuten. Selbstverständlich hängt dies mit der Datenmenge und der Anzahl an Variablen zusammen. Jedoch ist das Logit Modell nicht rechenintensiv und skaliert sehr gut, indem es parallel ausgeführt werden kann (Kedia & Philippon, 2009).

Neuronale Netze können in der Trainingsphase sehr rechenintensiv sein (Lim et al., 2000), während die Klassifizierungsphase nicht rechenintensiv ist. Diese skaliert sehr gut und kann parallel ausgeführt werden (Quah & Sriganesh, 2008).

Process Mining hat eine lineare Komplexität und skaliert sehr gut (Günther & Aalst, 2007). Das Modell muss nicht durch Trainings verbessert werden. Obwohl es rechenintensiver als die anderen Algorithmen ist, skaliert es gut und kann parallelisiert werden (Bezerra & Wainer, 2013).

Als Einschränkung dieses Vergleichs ist anzumerken, dass die meisten Quellen keine Information über Trainings- oder Testperformanz beinhalten. Dies ist dahingehend wichtig, da Fraud Detektionssysteme insgesamt rechenintensiv sind und die zu bearbeitende Datenmenge hoch ist (Allan & Zhan, 2010; Kou et al., 2004).

Prozessfähigkeit

Für Logit Modelle gibt es keine native Möglichkeit sequentielle Daten zu analysieren. Diese lässt sich durch Umwege erzielen. So kann jeder Eingabewert zu einem binären Wert mit Zeitstempel umgewandelt werden. Bei größeren Prozessen wird das Modell sehr komplex (Yeh & Lien, 2009). Diese Behelfslösung lässt sich auch für Neuronale Netze verwenden (Yeh & Lien, 2009). Process Mining kann nativ sequentielle Daten bearbeiten, was zu den zentralen Stärken des Ansatzes zählt (Aalst, 2011).

Flexibilität

Jedes Logit Modell benötigt ein endliches Set von Inputparametern. Wenn ein Prozess überarbeitet wird und somit auf ein anderes Set von Attributen basiert, muss ein neues Modell erstellt werden. Auch wenn neue Prozessinstanzen eingeführt werden, muss das Modell neu erstellt werden.

Neuronale Netze müssen neu erstellt werden, sobald sich die Inputparameter ändern. Neue Prozessinstanzen, die kein Fraud darstellen, können einfach in das Modell aufgenommen werden.

Bei Process Mining benötigt das Modell keine Modifikation, da der Threshold Algorithmus die Kosten für die Aufnahme jeder neuen Spur kalkuliert (Bezerra & Wainer, 2013). Sobald der Prozess von Grund auf geändert wird, so muss die Discovery Phase wiederholt werden, die Input Struktur bleibt jedoch erhalten.

Benutzbarkeit

Logit Modelle können verdächtige Transaktionen als solche kennzeichnen. Diese bieten dem Auditor jedoch keine weitere Hilfe. Die von den Modellen generierten Artefakte sind nicht ohne Weiteres verständlich. Dennoch sind diese replizierbar (Viaene et al., 2002).

Die innere Struktur von Neuronalen Netzen ist oft als Black Box zu sehen. Auditoren können nicht nachvollziehen, wie die Klassifizierung zu Stande gekommen ist (Feroz et al., 2000). Neben der Klassifizierung bieten Neuronale Netze keine weitere Unterstützung.

Die Ergebnisse von Process Mining sind oft grafisch aufbereitet. Auditoren können Filtern, Zoomen oder den Prozess im Detail betrachten (Jans, Depaire, & Vanhoof, 2011).

Das Ziel dieser Arbeit ist Fraud im Einkaufsprozess zu untersuchen. Da dieser Prozess naturgemäß sequentiell ist, müssen sequentielle Inputdaten verarbeitet werden. Durch die Komplexität des Prozesses können nicht alle Inputvariablen in Binärvariablen umgewandelt werden, so dass sich der Einsatz von Process Mining empfiehlt. Auch können Änderungen im Geschäftsprozess vorkommen, die am besten durch Process Mining abgebildet werden. Logit Modelle und Neuronale Netze benötigen einen Trainingsdatensatz, in dem Fraud enthalten und auch als solcher gekennzeichnet ist. Dieser ist in der Praxis oft nicht vorhanden. Zusätzlich gibt

es das Problem der Superimposition, d.h. Betrüger verhalten sich überwiegend regelkonform. Das betrügerische Verhalten ist dem regelkonformen sehr ähnlich und erschwert die Detektion deutlich (Yannikos, Franke, Winter, & Schneider, 2011). Aus diesem Grund wird in dieser Dissertation Process Mining verwendet. Dieses Verfahren wird mit dem etablierten Red Flag Ansatz kombiniert. Vorteil dieser Kombination ist die Visualisierung von Red Flags entlang auffälliger Prozessinstanzen. Auch kann nach Prozessinstanzen mit vielen Red Flags gefiltert werden.

4.4 Werkzeuge zur Identifikation von Fraud

Für die Identifikation von Fraud gibt es Werkzeuge, die grundsätzlich in vier Kategorien eingeteilt werden können: Computer Assisted Audit Tools (CAATS), generische Werkzeuge, fachbezogene Werkzeuge und eigenentwickelte Werkzeuge (Albrecht et al., 2012; Hopwood, Leiner, & Young, 2007; IIA, 2012; Wells, 2011). IIA (2012) hat mit einer Umfrage die Nutzung von Werkzeugen in der Praxis bestimmt. Sie ist zum Ergebnis gekommen, dass CAATS und generische Werkzeuge besonders häufig verwendet werden.

CAATS

Computer Assisted Audit Tools sind Programme, die den Prüfer bei der Datenanalyse unterstützen. Dazu zählt das Programm ACL Audit Analytics mit der gleichnamigen Sprache ACL – Audit Commit Language. Zur Erstellung von eigenen Prozeduren wird die Programmiersprache ACLScript verwendet. Dieses Programm wird in der Praxis am häufigsten eingesetzt und ist primär auf das Audit ausgelegt, beinhaltet aber auch ein Fraud Modul. Neben ACL ist auch das Programm IDEA (Interactive Data Extraction and Analysis) weit verbreitet. Beide unterscheiden sich vom Grundsatz wenig, wobei der Hauptunterschied in den Interfaces liegt. Die Programmiersprache von IDEA basiert auf Visual Basic und dient zur Automatisierung von Prozeduren.

Generische Werkzeuge

Zu den generischen Werkzeugen gehören Data Mining oder Business Intelligence Lösungen. Diese dienen zwar nicht primär der Suche nach Fraud, haben jedoch ihren Fokus in der Datenanalyse. Einige prominente Beispiele sind SAS Data Mining, SPSS oder SAP BusinessObjects Auditing Systems.

Fachbezogene Werkzeuge

Einige Werkzeuge werden speziell für bestimmte Fraud Arten entwickelt. Zu den bekanntesten gehören das US IRS (Internal Revenue Services) Electronic Fraud Detektion System, das die US Steuerbehörde bei Steuerbetrugsaufdeckung unterstützt. FraudPoint von LexisNexis sammelt Daten von Kunden und bewertet das Risiko einzelner Personen oder Firmen Fraud zu begehen. Für Bank- und Kreditkartentransaktionsbetrug hat die Firma FraudLabs mit dem Tool ExperianDetect eine Lösung entwickelt. Speziell für die Aufdeckung von Fraud in SAP Systemen hat dab ein gleichnamiges Tool auf den Markt gebracht.

Eigenentwicklungen

Viele Wirtschaftsprüfer haben ihre eigenen Prüfwerkzeuge und Routinen entwickelt

Probleme mit diesen Werkzeugen

Die hier beschriebenen Werkzeuge haben einige Einschränkungen für den produktiven Einsatz im Einkaufsprozess. Zunächst ist das Datenvolumen in großen Unternehmen so hoch, dass dieses nicht mehr von den genannten Tools händelbar ist. Auch mittelständische Unternehmen speichern in einem ERP System oft über 10 Mio. Daten pro Jahr. Für eine Analyse werden verschiedene Datenquellen kombiniert, wobei hohe Datenvolumina extrahiert und aggregiert werden. Da CAATT Tools oft dokumentenbasiert arbeiten, stellen diese Volumina ein Problem dar.

Zusätzlich ist der Funktionsumfang dieser Tools begrenzt. Einfache Analysen, wie beispielsweise Transaktionen zu unüblichen Zeiten oder Benfords Analysen, lassen sich mit schnell und einfach durchführen. Komplexere Analysen, die beispielsweise Daten aus mehreren SAP Modulen benötigen, sind nicht performant oder sogar nicht möglich. Innerhalb des Einkaufsprozesses ist es aber oft notwendig den Link zwischen dem Einkaufsmodul und dem Finanzmodul herzustellen.

CAATT Tools beinhalten keine vordefinierten fraud-spezifischen Analysen. Red Flags müssen in komplexen und proprietären Programmiersprachen definiert werden. Diese Sprachen werden an Universitäten selten gelehrt, so dass es wenige Spezialisten in diesem Bereich gibt. Oft werden Berater eingestellt, die diese Red Flags implementieren. Diese sind für eine kurze Dauer im Unternehmen. Anschließend werden die Implementierungen nicht weiter gepflegt oder erweitert, da die Berater nicht mehr zur Verfügung stehen (Albrecht et al., 2012; Hopwood, Leiner, & Young, 2007; IIA, 2012; Wells, 2011).

5 Process Mining und Red Flags zur Fraud Erkennung

Das Ziel dieser Dissertation ist Fraud durch die Kombination von Process Mining und Red Flags aufzudecken. Deshalb werden zunächst Grundlagen von Process Mining und Red Flags beschrieben.

5.1 Process Mining

Der Hauptautor im Bereich Process Mining ist W.M.P. van der Aalst. Die hier beschriebenen Grundlagen bauen hauptsächlich auf seine Arbeiten auf. Ein Grundlagenwerk von ihm ist sein Buch “Process mining: Discovery, Conformance and Enhancement of Business Processes” (Aalst, 2011). Process Mining hat seinen Ursprung in der Prozessmodellierung. Dazu soll zunächst ein kurzer Einblick gegeben werden.

5.1.1 Prozessmodellierung

Zunächst soll der Begriff *Prozess* erklärt werden. Meist wird er als ‚eine Sequenz von Aktionen um geschäftsrelevante Objekte zu transformieren' definiert (Green & Rosemann, 2000). Solche Objekte können im Einkaufsprozess Rechnungen oder Bestellungen sein. Die Modellierung von Prozessen dient zur Übersicht, Überwachung und Kontrolle des Prozesses. Der Erfolg und Wohlstand eines Unternehmens ist stark von der Qualität der Geschäftsprozesse abhängig (Agrawal, Gunopulos, & Leymann, 1998). Deshalb werden Workflow Management Systeme zur Überwachung und Verwaltung von Prozessen eingesetzt (Green & Rosemann, 2000; Vanderfeesten, 2004). Dabei sollen Prozesse besser verstanden, Probleme erkannt und ggf. Maßnahmen ergriffen werden (Bozkaya et al., 2009; De Medeiros & Weijters, 2005).

Weitreichendes Ziel ist die Automatisierung der Geschäftsprozesse, wofür eine akkurate Prozessbeschreibung notwendig ist (Aalst, 2011). Agrawal et al. (1998) sehen diese Beschreibung als Problem, da die Erhebung von Prozessdaten schwierig ist. Prozesswissen ist von intrinsischer Natur und den am Prozess beteiligten Mitarbeitern vorbehalten (Aalst, Weijters, & Maruster, 2004). Es können zwar Prozessdefinitionen, wie Beispielsweise Prozesskarten, existieren. Diese zeigen jedoch nur einen Soll-Zustand. Ein Vergleich zwischen Soll- und Ist-Zustand ist nicht möglich. Auch ist aus der Forschung zu Business Process Reengineering und Business Process Change bekannt, dass das Prozesswissen aller Beteiligten nicht immer korrekt oder komplett ist. Viele Fallstudien[26] zeigen, dass die Mitarbeiter theoretisches Prozesswissen haben, die alltägliche Prozessdurchführung davon abweichen kann. Aus diesem Bedarf ist die Idee des Process Mining entstanden. Weijters & Aalst (2001) haben die Prozesse anhand der Logdaten rekonstruiert und anschließend das Modell in einem Workflow Management System abgebildet. Diese umgekehrte Methode haben sie *Process Mining* genannt. Später beschrieben sie die Flexibilität um Prozesse zu designen und zu verbessern (Aalst et al., 2003).

5.1.2 Grundlagen Process Mining

Process Mining ist eine Disziplin, die sich zwischen Prozessmodellierung und Analyse, aber auch zwischen Data Mining und Machine Learning, einordnen lässt (Aalst, 2011). Process Mining beschreibt die Entdeckung, das Monitoring und die Verbesserungen von realen Prozessen (also keine vermuteten Prozesse), indem Wissen von Event Logs aus Systemen extrahiert wird (Aalst, 2011).

Häufig sind in Unternehmen Systeme wie Enterprise Ressource Planning (ERP), Customer Relationship Managemen (CRM) oder Workflow Management Systeme im Einsatz. Diese registrieren jede vom Benutzer durchgeführte Aktion. Die dabei entstandenen Daten werden mit Hilfe von Process Mining rekonstruiert und als Prozessinstanz dargestellt. In der Sequenz wird jeder Prozessschritt als Aktivität oder Event bezeichnet und ist mit der Prozessinstanz verbunden. Jedes Event hat einen Datums- und Zeitstempel, der Datum und Uhrzeit der Durchführung der Aktivität angibt. Auch wird der Erzeuger, also die Person oder Maschine,

[26] Einige Business Process Reengineering Case Studies können hier nachgelesen werden: (Paper, Rodger, & Pendharkar, 2001; Larsen & Myers, 1999; Sarker & Lee, 1999)

die den Prozessschritt durchgeführt hat, gespeichert (Aalst & Weijters, 2005). Einen Ausschnitt aus einem fiktiven Eventlog ist in Tabelle 14 gezeigt. Es beinhaltet die chronische Aufzeichnung aller Aktivitäten, weshalb es auch als „audit trail“ bezeichnet wird (Jans, Alles, & Vasarhelyi, 2010). Event Log Daten setzen sich aus Eingabedaten und Metadaten zusammen. Eingabedaten sind Daten, die der Benutzer in das System eintippt, wie beispielsweise der Betrag oder die Beschreibung. Metadaten sind vom System erstellte Daten, wie beispielsweise der Zeitstempel oder der Erzeuger der Nachricht. Diese Metadaten sind wichtig, um die Transaktionen rekonstruieren zu können (Jans et al., 2010).

Transaktions ID	Aktivitäts-ID	Erzeuger	Zeitstempel
Fall 1	Aktivität A	John	9-3-2004:15.01
Fall 2	Aktivität A	John	9-3-2004:15.12
Fall 3	Aktivität A	Sue	9-3-2004:16.03
Fall 3	Aktivität B	Carol	9-3-2004:16.07
Fall 1	Aktivität B	Mike	9-3-2004:18.25
Fall 1	Aktivität C	John	10-3-2004:9.23
Fall 2	Aktivität C	Mike	10-3-2004:10.34
Fall 4	Aktivität A	Sue	10-3-2004:10.35
Fall 2	Aktivität B	John	10-3-2004:12.34
Fall 2	Aktivität D	Pete	10-3-2004:12.50
Fall 5	Aktivität A	Sue	10-3-2004:13.05
Fall 4	Aktivität C	Carol	11-3-2004:10.12
Fall 1	Aktivität D	Pete	11-3-2004:10.14
Fall 3	Aktivität C	Sue	11-3-2004:10.44
Fall 3	Aktivität D	Pete	11-3-2004:11.03
Fall 4	Aktivität B	Sue	11-3-2004:11.18
Fall 5	Aktivität E	Clare	11-3-2004:12.22
Fall 5	Aktivität D	Clare	11-3-2004:14.34
Fall 4	Aktivität D	Pete	11-3-2004:15.56

Tabelle 14: Möglicher Auszug eines Event Logs

Quelle: Eigene Darstellung basierend auf Aalst & Weijters (2005)

In Tabelle 14 ist ein beispielhaftes Event Log abgebildet. Es ist bereits in einem von Process Mining Tools lesbaren Format. Alle Daten sind direkt aus einem Informationssystem extrahiert. Aktivitäten mit derselben Transaktions-ID gehören zur selben Prozessinstanz. Typischerweise werden Event Logs für drei Typen von Analysen verwendet: Prozess Entdeckung (Process Discovery), Übereinstimmungsprüfung (Conformance Checking) und Prozesserweiterung (Process Enhancement) (vergl. Abbildung 5-1). Diese sollen im Folgenden beschrieben werden.

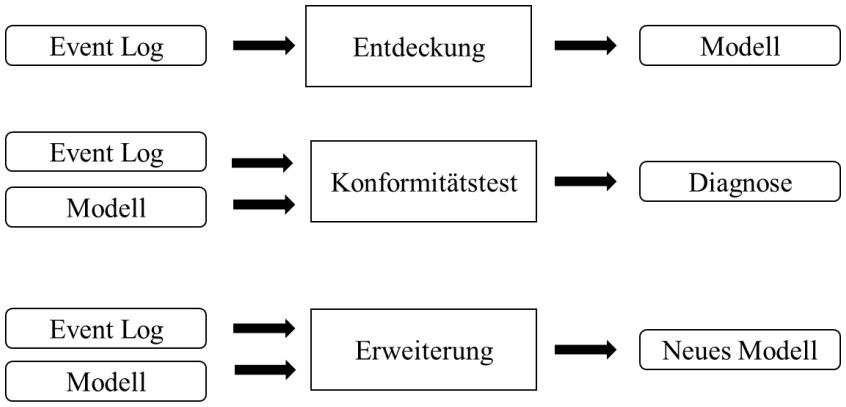


Abbildung 5-1: Analysearten von Process Mining Algorithmen, basierend auf Input und Output Werten
Quelle: Aalst (2012)

Prozess Entdeckung

Prozessentdeckung erstellt ein Prozessmodell basierend auf dem Event Log. Dazu gibt es verschiedene Algorithmen mit entsprechenden Vor- und Nachteilen (Gupta, 2014). Von den Algorithmen wird erwartet, dass diese die entsprechenden Daten selbständig finden, diese zusammenführen und bereinigen. Zusätzlich sollen diese dynamisch auf Prozessänderungen eingehen. Der Umgang mit den folgenden Besonderheiten im Datensatz sind besonders schwierig für den Algorithmus (Aalst et al., 2004; Gupta, 2014):

- Rauschen in den Daten

Es können Fehler in den Event Logs auftreten. Beispielsweise können Transaktionen eines ERP Systems abgebrochen werden oder Einträge nicht komplett oder einfach falsch sein. Der Algorithmus sollte diese Einträge herausfiltern, um die Qualität des Ergebnisses zu verbessern.

- Seltene Aktivitäten

Einige Prozessdurchläufe oder bestimmte Vorgänge sind sehr selten. Ein Algorithmus sollte die seltenen Aktivitäten nicht als inkorrekte Prozessausführungen einstufen.

- Schleifen

Unter Umständen hat ein Prozess einen Rücksprung auf eine zuvor getätigte Aktivität. Beispielsweise können Daten in einem Prozessschritt nachgetragen werden, was vom Algorithmus erkannt werden sollte.

- UND/XOR Abzweigungen oder Vereinigungen

Prozessabläufe können parallel durchlaufen oder Verzweigungen enthalten. Der Process Mining Algorithmus sollte diese Nebentätigkeiten und Verzweigungen erkennen und richtig einordnen.

- Abhängigkeiten

Es können nicht sofort ersichtliche Abhängigkeiten im Prozessverlauf existieren. So kann eine Entscheidung Einfluss auf den Prozessverlauf zu einem späteren Zeitpunkt haben. Der Algorithmus sollte diese Zusammenhänge erkennen und korrekt darstellen.

Algorithmen können teilweise mit den genannten Besonderheiten im Datensatz umgehen und ein Modell aus dem Event Log erstellen. Dabei versuchen diese eine Struktur in den Daten zu finden und aus dieser den Prozess zu rekonstruieren. Publikationen zu diesem Thema diskutieren den Einsatz von Neuronalen Netzen, den Purely Algorithmus und den Markov Ansatz (Cook & Wolf 1998a). Auch die Parallelität von Prozessmodellen findet dabei Beachtung (Cook & Wolf, 1998b). Weijters & Aalst (2001) und Aalst et al. (2004) versuchen die Häufigkeit der ausgeführten Instanzen in einem Graphen zu zeigen. Ein häufig verwendeter Algorithmus ist der α Algorithmus (Aalst, 2011). Dieser erstellt auf Basis des Event Logs ein Petrinetz und bildet daraus die Prozessinstanz ab.

Bis auf einige Sonderformen lassen sich die meisten Algorithmen in drei Kategorien einteilen (Gupta, 2014):

- Heuristische Mining Algorithmen

Heuristische Mining Algorithmen rekonstruieren aus den vorliegenden Daten das wahrscheinlichste Prozessmodell. Dazu werden Abhängigkeitsgraphen durch Einlesen von Transaktions-IDs und Zeitstempel erstellt. Dafür berechnet der Algorithmus Wahrscheinlichkeiten über die Abhängigkeit zweier Aktivitäten. Vorteil dieses Algorithmus ist sein guter Umgang mit Störungen. Er kann jedoch nicht mit Rücksprüngen im Prozess (um beispielsweise Datensätze zu ergänzen) umgehen (Saravanan & Rama Sree, 2011).

- Genetische Mining Algorithmen

Genetische Mining Algorithmen zählen zu den nicht deterministischen Algorithmen, da das Ende nicht vorhersehbar ist. Diese erzeugen das Resultat anhand einer evolutionären Weiterentwicklung (Gupta, 2014). Dazu wird eine Grundpopulation mit Hilfe von Kreuzungen und Mutationen genetisch erstellt, wobei das beste Modell stets weiterentwickelt wird (De Medeiros & Weijters, 2005). Vorteil dieser Algorithmen ist, dass sie durch den iterativen Ansatz gut mit Störungen, seltenen Aktivitäten und Sprüngen umgehen können. Sie sind jedoch sehr rechenintensiv (Gupta, 2014).

- Fuzzy Mining Algorithmen

Fuzzy Mining Algorithmen geben dem Nutzer die Möglichkeit das Ergebnis nach seinen Bedürfnissen anzupassen, indem der Nutzer beispielsweise eine vereinfachte Darstellung des Modells wählen kann (Günther & Aalst, 2007). Der Datensatz wird nicht in eine bestimmte Struktur gesetzt. Alle Instanzen werden kombiniert, wodurch das Modell sehr komplex werden kann. Deshalb aggregieren die Algorithmen nicht für das Verhalten relevante und stark korrelierende Knoten zu Clustern. Nicht signifikante und nicht korrelierende Knoten werden vom Modell ausgesondert (Günther & Aalst, 2007). Dadurch wird das Modell wieder

vereinfacht und das Rauschen im Datensatz reduziert. Besonders geeignet sind Fuzzy Mining Algorithmen, wenn genaue Vorstellungen des Endergebnisses bekannt sind und bestimmte Eigenschaften des Modells hervorgehoben werden sollen (Günther & Aalst, 2007).

Übereinstimmungsprüfung (Conformance Checking)

Die zweite Art von Process Mining ist die Delta Analyse und Übereinstimmungsprüfung. Bei der Delta Analyse ist ein Soll-Prozessmodell (bspw. ein Workflow oder Referenzmodell) bekannt und wird mit den Daten des Log Files verglichen. Für den Verglich wird unter Verwendung der Verfahren aus der Process Discovery Phase ein Ist-Prozessmodell erstellt. Das Ist- und Soll-Prozessmodell werden miteinander verglichen und gegebenenfalls Abweichungen veranschaulicht. (Aalst, 2005). Im Gegensatz dazu prüft die Übereinstimmungsprüfung (Conformance Checking) zusätzlich in wieweit die beiden Prozesse übereinstimmen (Aalst, 2005).

Hauptziel der Übereinstimmungsprüfung und Delta Analyse ist das Business und IT Alignment. Dabei wird geprüft in wieweit die Informationssysteme und Geschäftsprozesse aufeinander ausgerichtet sind (Aalst, 2011). Aalst (2005) verwendet das Token Game zur Identifikation ungewöhnlicher Prozessinstanzen. Dabei spielt er Event Log Daten in das Prozessmodell ein, um abweichende Prozessausführungen aufzudecken. Jede Prozessinstanz wird auf Regelkonformität geprüft. Rozinat & Aalst (2006) machen die Abweichung durch die Einführung der Messwerte *Fitness* und *Angemessenheit (Appropriateness)* messbar. *Fitness* ist der Grad der Abdeckung einer Prozessinstanz und wird durch die Anzahl der das Modell traversierenden Prozessinstanzen bestimmt. *Angemessenheit* hingegen zeigt die Genauigkeit in der das Prozessmodell das spezifische Verhalten darstellt. Rozinat & Aalst (2008) präzisieren die Definition von *Angemessenheit*, indem sie zwischen *Verhaltensangemessenheit* und *Strukturangemessenheit* unterscheiden. *Verhaltensangemessenheit* misst wie viele mögliche Verhalten vom Prozessmodell dargestellt werden. *Strukturangemessenheit* zeigt durch den Vergleich unterschiedlicher syntaktischer Ausdrücke zur Beschreibung einer Aktivität, wie treffend die gewählte ist. Aalst, Adriansyah, & Dongen (2012) führen drei weitere Qualitätskriterien ein: *Einfachheit*, *Generalisierbarkeit* und *Präzision*. *Präzision* beschreibt die Anzahl verschiedener Prozessinstanzen und sollte minimiert werden. *Generalisierbarkeit* verhindert die Überanpassung und sollte beispielsweise die Erstellung eines Event Logs für jede Prozessinstanz in dem Modell verhindern. *Einfachheit* verlangt, dass das einfachste Modell ausgewählt wird. Die Metrik für Einfachheit ist die Anzahl von Kanten und Knoten. Somit kann die Abweichung der Prozessinstanzen vom Prozessmodell berechnet werden.

Prozessverbesserung

Prozessverbesserung hat zum Ziel das Modell zu erweitern oder zu ändern (Aalst, 2011). Es wird die Notwendigkeit einer Verbesserung im Modell geprüft und die Stelle der notwendigen Verbesserung lokalisiert. Beispielsweise hat Aalst (2012) die Durchlaufzeiten von Prozessen und die entsprechende Zeit pro Event berechnet. Durch eine Prozessverbesserung hat er die Durchlaufzeit des Prozesses verkürzen können. Song & Aalst (2007) haben Prozesse anhand

von Ausführungsmuster erstellt. Dafür haben sie für jedes Event die Ausführzeit gemessen und Muster abstrahiert. Vom Muster abweichende Prozessinstanzen wurden markiert.

Prozessreparatur

Prozessreparatur ist der Übereinstimmungsprüfung sehr ähnlich und ist nachträglich von Fahland & Aalst (2015) ergänzt worden. Im Unterschied zur Übereinstimmungsprüfung wird bei Prozessreparatur das Prozessmodell den Logfiles angepasst. Ziel ist es sich langsam ändernde Geschäftsprozesse im Modell abbilden zu können und die die Diskrepanzen zwischen Modell und Wirklichkeit erklären zu können.

Einige Herausforderungen von Process Mining Algorithmen sind für die Implementierung des Prototyps in dieser Dissertation von besonderer Bedeutung und werden hier basierend auf Aalst (2011) dargestellt:

- Korrelation

Gewöhnlich werden Daten in Informationssystemen nicht im notwendigen Format gespeichert (vergl. Tabelle 14), sondern sind auf mehreren Tabellen verteilt. Die Korrelation zwischen den eigentlichen Events ist nicht sofort ersichtlich. Da in dieser Arbeit ein SAP ERP System verwendet wird, muss die Tabellenstruktur analysiert und die entsprechenden Daten in das notwendige Format gebracht werden.

- Zeitstempel

Zeitstempel sind vor allem bei unterschiedlichen Datenquellen ein Problem. Diese nutzen separate Uhren, wodurch es eventuell zu Abweichungen kommen kann. In dieser Arbeit ist der Fokus auf ein ERP System, so dass keine Probleme erwartet werden.

- Snapshots

Meist wird ein Snapshot der Daten erzeugt, um dieses mit Process Mining Algorithmen zu analysieren. Problematisch ist, dass der Datensatz unvollständige Prozessinstanzen enthalten kann. Dies sollte bei den Unternehmensdaten beachtet werden.

- Umfang

Informationssysteme speichern Daten in mehreren Tabellen, so dass der Analyst die Relevanten identifizieren sollte. Auch in dieser Arbeit werden relevante Informationen extrahiert.

- Granularität

Die Granularität ist dahingehend ein Problem, dass zu viele Details aus den Daten extrahiert werden können. Dadurch wird das Ergebnis unübersichtlich.

5.1.3 Tools für Process Mining

Zunächst soll in diesem Kapitel ein Überblick über vorhandene Process Mining Tools gegeben werden, die anschließend miteinander verglichen werden. Eine Übersicht vorhandener Process Mining Tools zeigt Tabelle 15.

Produktname	**Nutzung**	**Hersteller**
ARIS Process Performance Manager	Kommerziell	Software AG (www.softwareag.com)
Celonis Process Mining	Kommerziell	Celonis (www.celonis.de)
Disco	Kommerziell	Fluxicon (www.fluxicon.com)
Enterprise Visualization Suite	Kommerziell	Businessscape (www.businesscape.no)
Genet/Petrify	Akademisch	Universitat Politecnica de Catalunya (www.lsi.upc.edu)
Interstage BPME	Kommerziell	Fujitsu (www.fujitsu.com)
OKT Process Mining suite	Open Source	Exeura s.r.l. (www.exeura.com)
Perceptive Reflect	Kommerziell	Lexmark (http://www.lexmark.com)
Process Discovery Focus	Kommerziell	Iontas (Verint Systems) (www.iontas.com)
ProcessAnalyzer	Kommerziell	QPR (www.qpr.com)
ProM	Open Source	Process mining group (managed by the AIS group at TU/e) (www.processmining.org)
Rbminer/Dbminer	Akademisch	Universitat Politecnica de Catalunya (www.lsi.upc.edu)
Reflect|one	Kommerziell	Pallas Athena (www.pallas-athena.com)
Reflect	Kommerziell	Futura Process Intelligence (www.futuratech.nl)
ServiceMosaic	Akademisch	University of New South Wales (soc.cse.unsw.edu.au)
SNP Business Process Analysis	Kommerziell	SNP (www.snp-ag.com)
QPR Process Analyzer	Kommerziell	QPR (www.qpr.com)

Tabelle 15:Vorhandene Process Mining Tools
Quelle: Basierung auf Aalst (2011)

Das ProM Framework, Disco und Celonis sollen miteinander verglichen werden. ProM ist das am häufigsten verwendete Framework in der Wissenschaft. Die kommerzielle Software Disco wurde ausgehend vom Lehrstuhl von Professor van der Aalst von der hierzu gegründeten Firma Fluxicon entwickelt. Celonis Process Mining wird von SAP unterstützt und beworben. Da in dieser Arbeit mit einem ERP System der Firma SAP gearbeitet wird, wird dieses Tool ebenfalls in den Vergleich aufgenommen.

ProM

ProM ist eines der ältesten noch weiterentwickelten Frameworks für Process Mining und wurde von Dongen, Medeiros, Verbeek, Weijters, & Aalst, (2005) erstellt. Das Problem existierender Process Mining Tools war die Nutzung unterschiedlicher Formate zur Darstellung von

Informationen aus Event Logs. So konnten Wissenschaftler die gleichen Daten nicht mit unterschiedlichen Werkzeugen bearbeiten, um die Ergebnisse vergleichbar zu machen. Ziel war es das bestehende Problem von Process Mining Tools zu lösen. Die Besonderheit von ProM ist, dass es ein Framework und keine Out-of-the-Box Lösung ist. Es kann eher als Sammlung von Tools bezeichnet werden, die in der ProM Umgebung zusammenarbeiten können und durch Plug-Ins erweiterbar sind. Mittlerweile wurden schon über 286 Plug-Ins für die Version ProM 5.2 entwickelt. Zusammenfassend ist das ProM ist eine Verwaltungsmöglichkeit und grafische Schnittstelle zum Benutzer (Dongen et al., 2005). Zusätzliche Formate können durch den Plug-In Ansatz implementiert werden (Dongen et al., 2005).

Als Modellierungssprachen unterstützt ProM Petrinetze und Event-driven Process Chains (Dongen et al., 2005). Der eingebaute Conformance Checker soll Auditoren während des Process Auditing unterstützen[27]. Einer der Hauptnachteile von ProM ist, dass es nicht für „industrial size analysis“ sprich für große Datenmengen ausgelegt ist (Accorsi & Stocker, 2012). Zusätzlich ist es ebenfalls ein hoher manueller Aufwand, um das richtige Plug-In zu identifizieren bzw. zu entwickeln.

Celonis Process Mining

Celonis ist die gleichnamige Firma und das Process Mining Tool. Die Firma wurde 2011 gegründet und ist vorwiegend auf den kommerziellen Markt ausgerichtet. Das Tool ist vorwiegend auf die Analyse von Daten aus Enterprise Ressource Planning Systemenen (ERP) ausgelegt (Celonis, 2014). SAP hat Celonis 2016 in das Produktportfolio übernommen und unter dem Namen SAP Process Mining by Celonis vertrieben.[28] Das Tool basiert auf einer Java Webapplication, die in einem Tomcat Server läuft und kann daher unabhängig vom Betriebssystem betrieben werden (Stierle, 2015). Bei einer Client/Server Installation kann über den Browser auf die Applikation zugegriffen werden. Als Datenquelle dient eine frei wählbare Datenbank, die über die Open Database Connectivity (ODBC) Schnittstelle verbunden wird (Stierle, 2015). Durch eine anpassbare Konfiguration der Datenbasis und der Anzeige lässt sich Celonis im gewissen Rahmen an die Bedürfnisse anpassen, jedoch im Vergleich zu ProM deutlich weniger. Ein großer Nachteil von Celonis ist, dass der verwendete Process Mining Algorithmus weder offengelegt wird, noch verändert werden kann. Ein großer Vorteil ist die native Anbindung der In-Memory Datenbank SAP HANA für bspw. Fraud Detektion in Echtzeit.

Disco

Disco wurde von der Firma Fluxicon entwickelt und soll einen einfachen Einstieg in Process Mining bieten. Im Gegensatz zu Celonis verwendet es eine interne Datenbank. Um Daten in die Datenbank zu laden, stehen dem Benutzer entweder Excel oder eine Text Schnittstelle bereit. Somit lassen sich Formate, wie xls(x), CSV oder Text Dateien hochladen. Aus diesen

[27] Vergleich hierzu: (Accorsi & Stocker, 2012; Fabio Bezerra, Wainer, & Aalst, 2009; Fahland & Aalst, 2015; Rozinat & Aalst, 2006; Rozinat & Aalst, 2008; Rozinat, Jong, Guenther, & Aalst, 2007)

[28] Für weitere Informationen, vergl. https://www.celonis.de/news/celonis-sap-process-mining-globale-reseller-vereinbarung oder http://www.sap.com/pc/tech/business-process-management/software/process-mining/index.html

extrahiert Disco die benötigten Informationen. Jedoch müssen die Dateien in einem vorgegebenen Format abgespeichert werden. So muss eine eindeutige ID der Instanz und eine textuelle Repräsentation des aktuellen Prozessschritts eingegeben werden. Der Zeitstempel ist ebenfalls wichtig und sollte bestenfalls aus Datum und Uhrzeit bestehen (Rozinat, 2014). Auch können bereits formatierte Process Mining Daten, wie beispielsweise von ProM verwendete Daten im MXML oder XES Format eingegeben werden (Günther & Rozinat, 2012).

Disco verwendet ebenfalls einen vorkonfigurierten und nicht änderbaren Algorithmus. Hierbei handelt es sich um eine Weiterentwicklung des Fuzzy Mining Algorithmus. Dieser Algorithmus bietet ein verständliches und benutzbares Modell, indem es drei vorgefertigte Sichten auf die Daten anbietet: Map, Statistics und Cases (Günther & Rozinat, 2012). Map entspricht der Darstellung des Prozesses als Petri-Netz und kann konfiguriert werden. Statistics zeigt Analysen der Daten an und die Case-by-Case Sicht bietet die Möglichkeit Rohdaten zu inspizieren (Rozinat, 2014).

Vergleich der Lösungen

Alle hier benannten Werkzeuge haben Vor-und Nachteile. Ein Vergleich der Lösungen ist in Tabelle 16 abgebildet.

Lösung	*ProM*	*Celonis*	*Disco*
Betriebssystem	Unabhängig durch Java VM	Unabhängig durch die freie Wahl der Datenbank und Apache Tomcat Version	Angepasste Versionen für Windows und MAC
Datenhaltung	Internes Datenformat MXML/XES	Externe Datenbank über ODBC	Internes Datenformat FXL/DSC
Datenimport	Über Importer Plug-in. Daten werden in das interne Format MXML/XES umgewandelt	Daten werden entweder aus der Produktiv Datenbank oder einer zwischengeschalteten DB mit Hilfe eines SQL Skripts in die Zieldatenbank geladen	Import von Excel xsl, csv oder Textdateien. Bereits formatierte Datentypen aus anderen Process Mining Werkzeugen
Mining Algorithmus	Über Plug-ins selbst wählbar	Verbindung von verschiedenen Algorithmen	Angepasster Fuzzy Mining Algorithmus
Erweiterbarkeit/ Anpassbarkeit	Erweiterung über vorhandene oder selbst erstellte Plug-ins. Es können fast alle Aspekte von ProM verändert werden	SQL Skript kann komplett selbständig angepasst werden. Oberfläche zur Analyse kann den eigenen Bedürfnisse konfiguriert werden	Keine Informationen
Zielgruppe	Hauptsächlich Forschung	Kommerzielle Anwendung	Kommerzielle Anwendung

Tabelle 16: Vergleich Process Mining Lösungen

Quelle: (Celonis GmbH, 2014; Günther & Rozinat, 2012; Dongen et al., 2005)

Die großen Datenmengen eines ERP Systems können nicht in einer Text- oder csv Datei abgebildet werden. Dadurch entfällt die Nutzung von Disco an dieser Stelle. ProM und Celonis sind beides Werkzeuge, die sich sehr gut für die Analyse eignen. Durch die native Anbindung an SAP HANA und der Support der SAP wird in dieser Dissertation Celonis Process Mining

verwendet. Die native Anbindung an die In-Memory Datenbank der SAP ermöglicht Fraud in einem Produktivsystem zu identifizieren und ggf. Fraud in Echtzeit aufzudecken. Zusätzlich bietet Celonis den besten Trade-Off zwischen Erweiterbarkeit und einfacher Handhabung durch das frei wählbare Backend für die Implementierung von Red Flags ohne weitere Plug-Ins oder Komponenteninstallation. Auch das frei konfigurierbare Dashboard von Celonis kann genutzt werden, um dem Auditor eine Übersicht über zweifelhafte Prozessinstanzen zu bieten. So kann er direkt auf der Benutzeroberfläche die verdächtigen Fälle analysieren, ohne umständlich in das SAP System wechseln zu müssen

5.1.4 Process Mining für Fraud Detektion

Es sollen Ansätze aus der Literatur zur Aufdeckung von Fraud mit Hilfe von Process Mining zusammengefasst und diskutiert werden. Aus bestehenden Vorteilen sollen auch Anforderungen an die Eigenentwicklung des Prototyps in dieser Dissertation erhoben werden. Im Bereich Process Mining für Fraud Detektion sind die meisten bestehenden Publikationen im Bereich Finanzbetrug angesiedelt, während interner Fraud wenig akademische Beachtung findet (vergl. Jans, Van Der Werf, et al. (2011)).

Aalst et al. (2004) stellen den bereits beschriebenen α- Algorithmus vor. Auf dieser Arbeit bauen Aalst & Medeiros (2005) auf und analysieren den Beitrag von Process Mining zur Sicherheit in Systemen, indem sie Abweichungen im Prozessablauf und somit Anomalien identifizieren. Hierzu erzeugen sie den Prozess aus dem Audit Trail und testen auffällige Transaktionen gegen den normal ablaufenden Prozess (Aalst & Medeiros, 2005).

Best, Rikhardsson & Toleman (2009) stellen einen Ansatz vor, der auf das Framework zur Aufgabentrennung in einem SAP R/3 System von Little & Best (2003) aufbaut. Diese benutzen Audit Trails um den Verlauf einer Transaktion zu erfassen und diese auf Unregelmäßigkeiten, auffälliges Verhalten und kritische Kombinationen von Benutzeraktivitäten zu untersuchen (Best et al., 2009). Nachteil dieses Verfahrens ist die Möglichkeit zur Verschleierung durch einen Administrator. Auch kann Fraud von einer Gruppe von Tätern nicht erkannt werden (Best et al., 2009). Khan, Corney, Clark & Mohay (2010) bauen auf diese Arbeit auf, indem sie die Verletzung von Aufgabenteilungen ermitteln und die beteiligten Nutzer identifizieren (Khan et al., 2010). Dazu entwickeln sie einen Algorithmus der Transaktionsprofile durch die Bildung von azyklischen Graphen aus den Audit Logs ermittelt. Diese Transaktionsprofil-Graphen können zur Suche von Abweichungen verwendet werden (Khan et al., 2010). Islam et al. (2010) extrahieren Event Logs zur Prüfung eines Datensatzes auf zuvor identifizierte Muster.

Jans, et al. (2011) erweitern das Internal Fraud Risk Reduction (IFR^2) Framework von Jans, Lybaert & Vanhoof (2009) um Process Mining. Dieses Framework verwendet in der ursprünglichen Form Data Mining. Durch Process Mining werden weitere Informationen über den Prozessablauf und Prozessabweichungen hinzufügen (Jans, Werf, et al., 2011). Zur Rekonstruktion der Prozessinstanzen wenden die Forscher das Vorgehen nach Bozkaya et al. (2009) an. Neben der Prozesssicht führen diese ebenfalls eine Case-by-Case Untersuchung durch, bei der sie die Aufgabenverteilung und unternehmensspezifische Einschränkungen und Vorgaben berücksichtigen (Jans, Werf, et al., 2011).

Jans et al. (2010) nutzen Metadaten bei der Fraud Erkennung, da diese nicht von Benutzern manipulierbar sind. Nach der Rekonstruktion des Prozesses nutzen sie die Metadaten zur Erstellung eines sozialen Netzwerkes, um Anomalien zu identifizieren. Mit einer Form des Decision Minings analysieren sie das Prozessmodell, um die Wahrscheinlichkeit für die nächste Prozessaktivität zu berechnen. Alle Abweichungen inspizieren sie hinsichtlich Fraud. Diesen Ansatz wenden Jans, Alles & Vasarhelyi (2012) auf zwei Datensätze an. Beim ersten Datensatz eines Einkaufsprozesses gelingt es den Autoren Fraud Indikatoren zu finden, die nicht von Auditoren erkannt wurden. Im Datensatz einer Europäischen Bank gelingt es den Autoren Ungereimtheiten zu identifizieren, die anderen Forschern mit Standardanwendungen zur Frauderkennung nicht gelungen ist (Jans, Alles, & Vasarhelyi, 2012).

Häufig werden von der Norm abweichende Prozesse als Fraud eingestuft. Mardani & Shahriari (2013) beispielsweise ordnen Prozessdaten einzelnen Vektoren zu, um so verschiedene Arten der Prozessausführung darzustellen. Seltene Prozessausführungen stufen sie als Fraud ein (Mardani & Shahriari, 2013). Einen ähnlichen Ansatz verfolgen Bezerra et al. (2009). Sie definieren Fraud als ein seltenes Event, eine Abweichung vom normalen Verhalten, ein ungewöhnliches Ergebnis oder einen Status außerhalb der normalen Range von Variationen. Dabei verwenden sie die Werte Fitness und Angemessenheit als Metriken für normales Verhalten. Wenn eine Prozessinstanz über einen bestimmten Schwellwert ist, wird ein Alarm ausgelöst. Die Forscher verbessern 2011 ihr Framework, indem sie auch die Anzahl von Knoten betrachten. Sie gehen davon aus, dass Fraud nur bei komplexen Modellen vorkommt (Bezerra & Wainer, 2011). Mardani & Shahriari (2013) verbessern das Framework, indem sie zwischen „seltenen“ und „seltenen und auffälligen“ Instanzen unterscheiden. Bose & Aalst (2010) entwickeln ein Framework, um seltene Instanzen zu identifizieren. Dafür vergleichen sie Prozessinstanzen, um Muster zu erkennen.

Eine gut geeignete Art der Fraud Erkennung ist die Übereinstimmungsprüfung (Conformance Checking) (Accorsi & Stocker, 2012). Dadurch können Abweichungen in Zahlungen, fehlende Funktionstrennung (Segregation of Duties) und fehlendes Vier Augen Prinzip erkannt werden[29]. Durch die Analyse von Rollen und Personen können die Berechtigungen zur Ausführung von Transaktionen geprüft werden. Beispielsweise dürfte eine Person nicht die Berechtigung zur Erstellung und Genehmigung einer Bestellung haben. Die konstruktion sozialer Netzwerke aus den Daten ermöglicht die Reduzierung möglicher Mittäter bei Bekanntwerden einer Straftat (Aalst, Reijers, & Song, 2005; M. Bozkaya et al., 2009; Jans et al., 2014).

Meist wird Fraud ex-post analysiert, indem ein Abzug des Datensatzes einer bestimmten Periode analysiert wird. Process Mining kann dazu verwendet werden kontinuierlich Fraud zu untersuchen. Mit historischen Daten kann ein Prozessmodell erstellt werden, wobei im laufenden Betrieb jede Prozessinstanz auf Konformität geprüft wird. Sobald eine Abweichung auftritt, kann ein Alarm angezeigt werden (Aalst, Hee, Werf, & Verdonk, 2010).

[29] Vergl. hierzu (Aalst et al., 2005; Accorsi & Stocker, 2012; Bozkaya, Gabriels, & Werf, 2009; Jans et al., 2012a,; 2012b; Jans, Alles, & Vasarhelyi, 2014; Jans, Werf, Lybaert, & Vanhoof, 2011)

Diese Arbeit baut auf den Ergebnissen der hier beschriebenen Studien auf. Besonders die Arbeit von Best et al. (2009) ist dieser ähnlich. Dieser stellt einen Ansatz vor, der in einem mySAP System Audit Trails nach Red Flags untersucht. Dabei geht er beispielhaft vor, während in dieser Arbeit eine umfassende Anzahl an Red Flags identifiziert und implementiert wird. Auch werden die Red Flags zu Fraud Patterns zusammengefasst und entsprechend in einem Dashboard visualisiert. Eine gute Visualisierung ist in der Arbeit von Singh, Best, Bojilov & Blunt (2013) gegeben. Diese haben sich auf ein Fraud Szenario konzentriert.

Aus den bestehenden Publikationen können Anforderungen an das Process Mining Tool erstellt werden:

- Benutzeroberfläche:

Die Benutzeroberfläche sollte wie bei Singh, Best, Bojilov, et al. (2013) modular aufgebaut sein. Ein Dashboard soll eine Übersicht anzeigen, während weitere Informationen in Tabs anzeigt werden. Singh, Best, Bojilov, et al. (2013) haben in einer Umfrage evaluiert, dass diese Darstellungsform als besonders ansprechend wahrgenommen wird.

- Zusätzliche Informationen

Neben der Anzeige von Prozessgraphen sollte die Darstellung mit zusätzlichen Informationen angereichert werden. Dies sind bestenfalls Informationen aus dem SAP System, damit der Auditor nicht umständlich in das SAP System wechseln muss.

- Identifikation von Prozessabweichungen

Fraud kann durch auffällige Kombination von Nutzerverhalten erkannt werden. Es sollen die relevanten Aktivitäten im Einkaufsprozess angezeigt werden, um Prozessabweichungen analysieren zu können.

- Identifikation von Aufgabentrennungen

Auch die Identifikation von Aufgabentrennungen ist ein häufig behandeltes Mittel zur Identifikation von Fraud. Dies soll ebenfalls in der Implementierung des Prototyps aufgenommen werden.

- Methodisches Vorgehen zur Identifikation von Fraud

Im Bereich von Process Mining hat sich das Verfahren von Bozkaya et al. (2009) als hilfreich erwiesen (Jans, Werf, et al., 2011). Für die Identifikation von Red Flags empfiehlt Best et al., (2009) das Vorgehen von Albrecht et al. (2009).

Leider wird die technische Implementierung der vorgestellten Lösungen nicht näher erläutert. Auffällig ist allerdings, dass die meisten Autoren Fuzzy Mining Algorithmen verwenden[30].

5.2 Red Flags

> „Red Flags“ are like the first wisps of smoke in a forest. Detect them early can prevent a forest fire. Fail to move decisively and the whole forest will be in danger“ (Stamler 2014, S.4 f)

Ein weit verbreiteter Ansatz der (proaktiven) Fraud Erkennung ist der Red Flag Ansatz. Dieser wird von allen Audit Standards empfohlen (Albrecht et al., 2012). Red Flags sind Hinweise oder Indikatoren für wirtschaftskriminelles Verhalten. Sie zeigen ein von der Norm abweichendes Verhalten auf, welches weitere Untersuchungen erfordert. Jede Nutzeraktion hinterlässt Spuren im System. Meist wird der Datensatz nach vordefinierten Regeln untersucht und bei Eintreten dieser Regel ein Alarm ausgelöst (Coenen, 2008; DiNapoli, 2008; Nisbet, Elder, & Miner, 2009; Prenzler, 2009; Stamler, Marschdorf, & Possamai, 2014). Beispielsweise kann das Ändern von Stammdaten ein Zeichen für Fraud sein (Best et al., 2009). Red Flags sind keine Beweise, sondern Anomalien die auf wirtschaftskriminelles Verhalten hinweisen (Albrecht et al., 2012).

Red Flags werden oft in Kategorien unterteilt. Laut Grabosky sind die drei Hauptkategorien (Grabosky, Duffield, 2011, zitiert nach Stamler et al., (2014)):

- Verhalten
- Statistisch
- Organisatorisch

Albrecht et al. (2012) führen diese Kategorisierung weiter aus und unterteilt Red Flags in

- Ausschweifender Lebensstil
- Auffälliges Verhalten
- Buchhaltungsanomalien
- Analytische Anomalien
- Tipps und Beschwerden
- Schwächen der internen Kontrolle

Nicht alle Red Flags lassen sich erfassen. Während Änderungen in den Stammdaten einfach zu identifizieren sind, lassen sich beispielweise Scheidung/ familiäre Probleme nicht überwachen ohne in die Persönlichkeit des Mitarbeiters einzugreifen (ACFE, 2018). Die Detektion von Fraud ist ein dünner Draht zwischen Transparenz und Mitarbeiterkontrolle.

Für die Identifikation von Red Flags empfiehlt DiNapoli (2008) zunächst nach den am wahrscheinlichsten auftretenden wirtschaftskriminellen Handlungen zu suchen. Hierfür werden mögliche Red Flags identifiziert und ihr Auftreten untersucht. Der Autor empfiehlt den ACFE Fraud Tree (vergl. Kapitel 4.1) und das Fraud Dreieck (vergl. 2.4.1) als Basis zur Identifikation

[30] (Jans, Depaire, et al., 2011; Jans, Lybaert, Vanhoof, & Werf, 2008; Jans, Werf, et al., 2011)

von wahrscheinlichen Taten. Dieser Ansatz wird auch von Albrecht et al. (2012) spezifiziert und in dieser Arbeit verwendet (vergl. Kapitel 6).

Red Flags sind Teil aller gängigen Anti-Fraud Standards. Die wichtigsten Organisationen sind das Institute of Certified Public Accountants (AICPA), die Information Systems Audit and Control Association (ISACA) und das Institute of Intern Auditors (IIA). Alle drei Organisationen empfehlen die Verwendung von Red Flags zur Fraud Bekämpfung.

AICPA- Die AICPA's Statement on Auditing Standard (SAS) No. 99, Consideration of Fraud in a Financial Statement Audit, beinhalten eine Liste mit Red Flags. Die meisten Red Flags sind aus der Association of Certified Fraud Examiners (ACFE), bzw. aus den Publikationen deren Gründers Joe Wells, übernommen. Diese sind im Anhang der SAS No. 99 in einer Matrix dargestellt. Dabei werden diese in die Hauptkategorien des Frauddreiecks (vergl. Kapitel 2.4.1) und des ACFE Klassifizierungsbaums (vergl. Kapitel 4.1) eingeordnet.

ISACA - ISACA hat in der 2003 veröffentlichten „Irregularities and Illegal Acts" (Standard 030.020.010) für ''Procedures for Information Systems Auditing'' eine ähnliche Liste vorgestellt. In der Aufzählung von Audit Considerations sind Red Flags enthalten und auf Cumputer Assisted Auditing Tools (CAATs) abgestimmt (für CAATs vergl. Kapitel 4.4).

IIA – Die IIA Literatur stellt Beispiele für Red Flags in den ‚Standards for Professionel Practise of Internal Auditing' bereit. So muss der Auditor ausreichend Kenntnisse haben, um einen Red Flag als solchen zu erkennen, wobei es nicht dessen primäre Aufgabe ist.

Eine Übersicht aller aus der Literatur abgeleiteten Red Flags im Einkaufsprozess ist im Anhand E: Red Flags im Einkaufsprozess' gegeben. Dabei wird zwischen Red Flags beim Lieferanten, bei der Bestellung, im Waren- oder Rechnungseingang, bei der Zahlung, der Autorisierung, der Rückgabe, bei einer Ausschreibung und bei Verhalten unterschieden.

6 Vorgehen zur algorithmischer Fraud Erkennung

Ziel dieser Arbeit ist es, den Red Flag Ansatz mit Process Mining zu kombinieren. Deshalb soll im Folgenden das Vorgehen zur Identifizierung von Fraud mit Red Flags und Process Mining vorgestellt werden.

6.1 Methodisches Vorgehen

Der Red Flag Ansatz ist einer der am weitesten verbreiteten Ansätze zur Fraud Detektion und gleichzeitig einer der Ältesten. Basierend auf den Ergebnissen des Institute of Internal Auditors (2003) hat Albrecht et al. (2012) ein Vorgehen zur Identifikation von Fraud mit Hilfe von Red Flags vorgestellt. Erfolgreich eingesetzt wurde es unter anderem von Best et al. (2009). Bei dem Vorgehen handelt es sich um ein deduktives Verfahren, welches computergestützte

Analysen ausführt. Christensen & Byington (2003a) argumentieren, dass mit dem steigenden Anteil an Technologie der Computer als Auditwerkzeug an Wert gewinnt.

Das Vorgehen von Albrecht et al. (2012) beinhaltet mehrere Ebenen – die analytische-, technologische- und die Nachforschungsebene. Diese sind konkret in Abbildung 6-1 dargestellt.

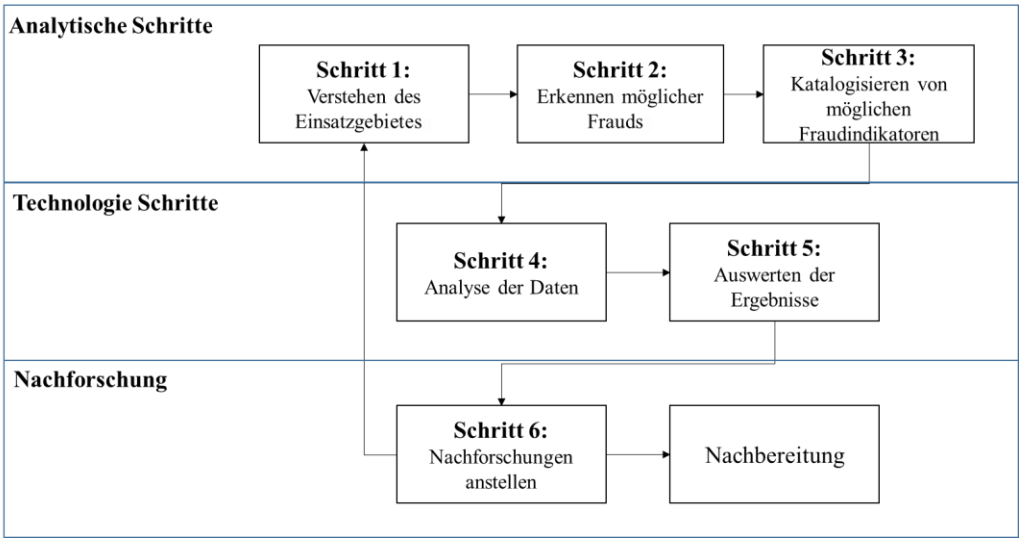


Abbildung 6-1: Vorgehensmodell zur Fraud Detektion mit Red Flags (deduktiver Ansatz)
Quelle: Basierend auf Albrecht et al. (2012)

Zur analytischen Ebene zählt die Identifikation und Katalogisierung von möglichen Indikatoren im Einsatzgebiet, wofür Experten ein spezielles Branchen- und Prozesswissen benötigen. Auf technologischer Ebene werden die Daten hinsichtlich der zuvor bestimmten Red Flags mit Hilfe der Abfragesprache SQL analysiert. Anschließend werden die Ergebnisse ausgewertet und konkreten Verdachtsfällen wird auf Ebene der Nachforschung nachgegangen. Der Vorteil dieser Methode ist die aktive Rolle des Fraud Prüfers, da dieser nicht auf Hinweise (bspw. durch ein Whistleblowing System) wartet, sondern in regelmäßigen Abständen eine Datenüberprüfung durchführt (Albrecht et al., 2012).

Bei der Analyse der Daten (Schritt 4) werden Indikatoren identifiziert. Diese sind nur Puzzleteile, bei denen das Gesamtbild noch unbekannt ist (Stamler et al., 2014). Albrecht et al. (2012) empfehlen iterativ die Anzahl der Red Flags zu reduzieren, ohne konkrete Vorschläge zum Vorgehen zu nennen. In dieser Dissertation werden zwei Ansätze zur Reduktion und Visualisierung der Daten vorgeschlagen:

(1) Zusammengehörige Red Flags werden zu Fraud Patterns kombiniert und simultan nach diesen im Datensatz gesucht. So soll die falsch-positiv Rate und die Informationsflut reduziert werden.
(2) Der Red Flag Ansatz wird mit Process Mining kombiniert. Red Flags werden entlang der Prozessinstanz visualisiert. Der Prüfer muss dadurch nicht umständlich ins Quellsystem wechseln, um den Prozess zu analysieren.

Für Process Mining im Bereich Fraud Detektion hat sich das Vorgehen von Bozkaya et al. (2009) durchgesetzt. Dies wurde erfolgreich von Jans et al. (2012a) und Jans, Werf, et al. (2011) angewendet. Das Vorgehen besteht aus sechs Schritten, die im Folgenden kurz vorgestellt werden:

(1) Log Vorbereitung – Identifikation von Aktivitäten, Fällen und Zeitstempel
(2) Log Inspektion – Sammeln von Informationen über den Prozess
(3) Kontrollflussanalyse – Analyse des Prozesses und falls vorhanden Vergleich mit dem Prozessmodell
(4) Performanzanalyse – Suche nach dem Flaschenhals im Prozess
(5) Rollenanalyse – Visualisierung der Rollen, die Aktivitäten durchführt haben
(6) Resultate Analysieren – Resultate analysieren und diskutieren

In dieser Dissertation wird das Vorgehen von Albrecht et al., (2012) mit den Prozessschritten von Bozkaya et al., (2009) erweitert, um ein Vorgehensmodell zur Aufdeckung von Fraud mit Hilfe von Process Mining und dem Red Flag Ansatz zu erstellen.

Kombination beider Ansätze

Wie bereits von Albrecht et al. (2012) vorgestellt, soll auch das bestehende Vorgehen in drei Ebenen aufgeteilt werden, die im Folgenden beschrieben werden:

6.1.1 Analytische Ebene

Die analytische Ebene beschreibt die theoretische Ebene, bei der das Geschäftsfeld verstanden und mögliche Risiken und Fraud Szenarien erkannt werden. Es werden keine Daten aus Informationssystemen gesammelt oder analysiert. Die einzelnen Schritte werden im Folgenden beschrieben.

1. Einsatzgebiet verstehen

Da jedes Unternehmen und jede Abteilung anders ist, sollen zunächst Prozesse und Eigenheiten verstanden werden. Nur so können Auditoren mögliche Fraud Szenarien identifizieren. Albrecht et al. (2012) empfehlen ein interdisziplinäres Team von Experten aus der Fachabteilungen, Auditoren und Datenbankentwickler aufzubauen. Diese sollen Prozessdokumentationen, Abschlussberichte usw. studieren und beteiligte Personen interviewen.

2. Erkennen möglicher Frauds im Einsatzgebiet

Nachdem ein Verständnis über das Einsatzgebiet aufgebaut wurde, sollen mögliche Fraud Szenarien erfasst werden. Hilfreich ist das Wissen über mögliche Risiken im Prozess. Mitarbeiterbefragung und Brainstorming der beteiligten Auditoren sind erprobte Mittel zur Identifikation. Um die Komplexität zu reduzieren, kann das Einsatzgebiet in Teilgebiete aufgeteilt werden. Beispielsweise können einzelne Abteilungen oder Prozessschritte betrachtet

werden. Das Ergebnis dieses Prozessschrittes sollte eine Liste mit möglichen Fraud Szenarien im Einsatzgebiet sein.

3. Katalogisieren von möglichen Fraud Indikatoren (Red Flags)

Red Flags sind die beste und vielleicht auch einzige Art der proaktiven Fraud Erkennung und werden von allen Fraud Audit Standards empfohlen (Albrecht et al., 2012). Ziel dieser Dissertation ist es verschiedene Red Flags zu einem Fraud Pattern zusammenzufassen. Die Analyse jedes einzelnen Red Flags führt zu einer hohen Informationsflut mit vielen falsch-positiven Werten. Ziel dieser Arbeit ist nach einer Kombination von Red Flags zu suchen, die zu einem Fraud Pattern gehören. Das Ergebnis dieses Schrittes ist eine Liste von Fraud Patterns mit dazugehörigen Red Flags (aus Schritt zwei) zu erstellen.

6.1.2 Technische Ebene

In der technischen Ebene kommt es zur Implementierung der Fraud Detektionsmethode. Da das Ziel die Kombination von Process Mining und Red Flags ist, soll hier das Framework zur Fraud Erkennung von Albrecht et al. (2012) mit dem Vorgehen von Bozkaya et al. (2009) zur Rekonstruktion des Geschäftsprozesses erweitert werden. Die dazugehörigen Prozessschritte sind:

4. Log Vorbereitung

Im Schritt der Log Vorbereitung werden die relevanten Tabellen und Felder im Geschäftsprozess identifiziert. Jede Aktivität im Geschäftsprozess entspricht einem Case in Process Mining. Für die Rekonstruktion des Geschäftsprozesses müssen Information über die Aktivität, das Datum, die Uhrzeit und den dazugehörigen Benutzer extrahiert und transformiert werden. Dabei müssen einige Entscheidungen getroffen werden, wie die Auswahl und möglichst pregnante Beschreibung der zu extrahierenden Aktivitäten. Tabellen in den Quellsystemen Systemen haben oft mehrere Zeitstempel, wie ein Erstell- und Änderungsdatum. Das genaue Verständnis über die Daten hilft den passenden Zeitstempel auszuwählen. Eine Harmonisierung der Daten zur einheitlichen Darstellung von Formaten ist notwendig. Beispielsweise sind Datumsformate mit und ohne Zeitangabe vorhanden. Das Ergebnis dieses Schrittes ist ein SQL-Skript, das aus den Quelltabellen Process Mining lesbare Tabellen erstellt (z.B. Fall- und Aktivitätstabellen).

5. Log Inspektion

Ziel dieses Schrittes ist es einen Überblick über den Prozess zu erhalten. Dabei sollen Informationen über die Anzahl von Prozessinstanzen, die Anzahl von vorkommenden Events und unvollständige Prozessinstanzen gesammelt werden. Unvollständige Instanzen die außerhalb der Stichprobe begonnen oder beendet wurden sollen entfernt werden. Dieser Prozessschritt ist nur notwendig, falls eine Teilmenge aller möglichen Daten analysiert wird. Bei Analyse des gesamten Datensatzes oder bei dem kontinuierlichen Auditing entfällt dieser Schritt.

6. Datenanalyse und Prozessanalyse (Process Mining und Red Flags)

Dieser Schritt wird in ähnlicher Weise von Albrecht et al. (2012) und von Bozkaya et al. (2009) beschrieben und hat zum Ziel den Prozess und die Hinweise auf Fraud zu analysieren. Die Prozessanalyse erfolgt durch die Darstellung des Kontrollflusses. Die notwendigen Algorithmen werden im Kapitel 5.1.3 erläutert. Bozkaya et al. (2009) empfehlen das Pareto Prinzip anzuwenden, um einen möglichen Spaghetti-Prozess zu vermeiden. Viele Algorithmen visualisieren Abweichungen oder seltene Prozessinstanzen, wodurch die Übersichtlichkeit gemindert wird. Beim Pareto Prinzip werden nur 80% der häufigsten Prozessdurchläufe dargestellt, womit die Prozessdarstellung übersichtlicher bleibt. Für die Fraud Detektion sind allerdings die verbleibenden 20% interessant, da es sich dabei oft um Prozessabweichungen und seltene Prozesse handelt. Deshalb wird an dieser Stelle nicht das Pareto Prinzip gewählt. Zur Anayse der Hinweise sollen die zuvor identifizierten Red Flags im Datensatz mit Hilfe der Structured Query Language (SQL) identifiziert werden (Albrecht et al., 2012). Ziel dieses Schrittes ist die Implementierung eines SQL Skriptes zur Identifikation der Red Flags im Datensatz und den Prozess mit Hilfe eines Process Mining Tools zu rekonstruieren und zu visualisieren.

7. Auswertung der Ergebnisse

Sobald auf Fraud hinweisende Prozessinstanzen identifiziert werden, sollen traditionelle Verfahren zur Überführung der Täter verwendet werden. Fraud Prüfer und Auditoren sollen Gründe für die identifizieren Anomalien suchen bzw. weitere Hinweise für Fraud identifizieren. Dafür analysieren diese papierbasierte Dokumente, sprechen mit Kollegen des Verdächtigen oder analysieren elektronische Nachrichten.

6.1.3 Investigative Ebene

Der letzte Prozessschritt ist der investigativen Ebene zuzuordnen und beinhaltet Nachforschungen anstellen, die im Folgenden beschrieben werden.

8. Nachforschungen anstellen

Zu dem letzten Schritt gehört es den wahrscheinlichsten Fraud Szenarien aus der Investigativen Ebene nachzugehen und nach Tätern zu suchen. Sobald ein Täter überführt wurde, können auch gerichtliche Schritte eingeleitet werden. Dieser Prozessschritt ist nicht Teil dieser Dissertation und wird hier nur der Vollständigkeit halber aufgeführt.

Insgesamt ergibt sich daraus das in Abbildung 6-2 entstandene Framework:

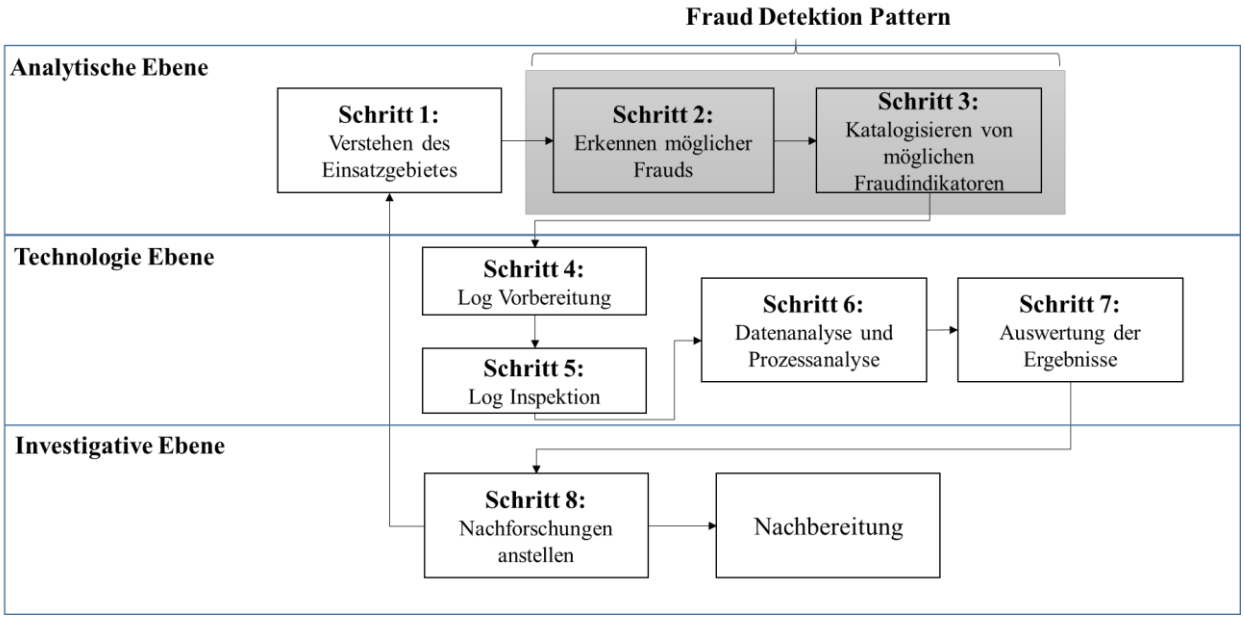


Abbildung 6-2: Vorgehen zur Fraud Detektion basierend auf Red Flags und Process Mining
Quelle: Basierend auf Albrecht et al. (2012) und Bozkaya et al. (2009)

6.2 Einordnen des Vorgehens in das Fraud Dreieck

Das zuvor beschriebene Vorgehen soll in das theoretische Konzept des Fraud Dreiecks eingeordnet werden (vergl. Kapitel 2.4 Fraud Theorie). Das Vorgehen lässt sich in den Bereich ‚Gelegenheit' einordnen. Die Dimension Druck hat überwiegend mit persönlichen und situativen Problemen zu tun, so dass das Unternehmen nur bedingt eingreifen können. Auch der Aspekt der ‚Rationalisierung', also der eigenen Rechtfertigung der Tat, lässt sich kaum beeinflussen. Die ‚Gelegenheiten' zu reduzieren ist Aufgabe des internen Kontrollsystems. Hier hilft das bereits erwähnte Rahmenwerk COSO, mit den fünf Hauptelementen des Frameworks Kontrollen (Albrecht et al., 2012; Moeller, 2011):

- Kontrollumgebung
- Information und Kommunikation
- Risikobewertung
- Monitoring und
- Kontrollaktivitäten

Der Bereich der Kontrollaktivitäten lässt sich weiter in präventive, detektive und korrektive Kontrollen untergliedern (Hopwood et al., 2007). Das hier vorgestellte Vorgehen kann bei kontinuierlicher Anwendung zur präventiven oder bei einmaliger oder regelmäßiger Anwendung zur detektiven Aufdeckung eingesetzt werden. Das interne Kontrollsystem wurde bei der Aufdeckung von Fraud bereits umgangen.

7 Aufdeckung von Fraud im Einkaufsprozess durch Process Mining und Red Flags

Im Folgenden soll nun das zuvor Identifizierte Vorgehen am Einkaufsprozess exemplifiziert werden.

7.1 Analytische Ebene – Anforderungen

Die analytische Ebene umfasst die Punkte
- Einsatzgebiet verstehen
- Erkennung möglicher Frauds im Einsatzgebiet
- Katalogisieren von möglichen Fraud Indikatoren

Als Einsatzgebiet wird der Einkaufsprozess gewählt. Dieser wird anhand der Literatur sehr ausführlich in Kapitel 3 beschrieben und an dieser Stelle nicht erneut aufgegriffen. Zur Erkennung und Katalogisierung möglicher Frauds und Red Flags werden Fraud Patterns abgeleitet, wie im Folgenden dargestellt.

7.1.1 Identifizierte Fraud Patterns

Zur Entwicklung von Fraud Patterns wird der ACFE Tree (vergl. Kapitel 4) als Kategorisierungsgrundlage verwendet. Die aus der Literatur identifizierten Red Flags werden entsprechend in das Kategorisierungsschema eingeordnet, um so Fraud Patterns abzuleiten. Eine ausführliche Darstellung aller gewählten Red Flags kann aus Anhand E: Red Flags im Einkaufsprozess entnommen werden. Die identifizierten Patterns werden im Folgenden dargestellt:

Interessenkonflikt

Name	**Interessenkonflikt**
Beschreibung	Wells (2013) beschreibt Interessenkonflikte als Situationen, in denen ein Angestellter, Manager oder Vorstand eines Unternehmens, verdeckte persönliche oder wirtschaftliche Interessen hat, die das Unternehmen nachteilig beeinflussen. Meist hat der Täter wirtschaftliche Interessen an einer Transaktion, die persönlicher Natur sein kann. Bei Interessen persönlicher Natur kann das Interesse von Familienangehörigen oder Freunden dem Interesse des Unternehmens vorangestellt werden. Wells (2013) betont, dass das zweigeteilte Interesse des Täters bei der Transaktion verdeckt bleiben muss. Sobald das Unternehmen informiert ist, kann die Situation nicht als Interessenkonflikt gewertet werden. Die meisten von Wells (2013) untersuchten Fälle von Interessenkonflikten sind Fälle von Überbezahlung beim Kauf von Waren oder Dienstleistungen, an denen ein interner Mitarbeiter verdecktes Interesse besitzt. Somit sind sich Billing- und Interessenkonflikt-Schemata in der Handlungsausführung ähnlich. Das Motiv des Täters ist das einzige Unterscheidungsmerkmal. Während bei Billing-Schemata der Täter meistens an einer Geldzahlung interessiert ist, muss er - damit es sich um einen Interessenkonflikt handelt - Interesse an einer anderen beteiligten Entität haben, deren Interessen sich mit Interessen des eigenen Unternehmens nicht decken. Genauso kann ein Angestellter der Einkaufsabteilung die Ausschreibung so manipulieren, dass sein privates Unternehmen den Zuschlag erhält.

	Interessenkonflikte können also auch Angebotsabsprachen beinhalten, der einzige Unterschied ist hier ebenfalls das Motiv des Täters. Bei Angebotsabsprachen erwartet der korrupte Mitarbeiter eine Kickback-Zahlung vom bevorzugten Lieferanten. Da das Motiv des Täters nicht im System erkannt werden kann, wird in dieser Arbeit auf die benachbarten Szenarien eingegangen.

Tabelle 17: Interessenkonflikt Fraud Pattern mit Red Flags

Quelle: Eigene Darstellung basierend auf Anhand E: Red Flags im Einkaufsprozess

Kickback Fraud

Name	**Kickback**
Beschreibung	Kickback-Schemata beschreiben verdeckt getätigte Zahlungen eines Lieferanten an einen Mitarbeiter, nachdem illegale Vereinbarungen getroffen und erfüllt wurden. Diese Vereinbarungen beinhalten typischerweise das Zustandekommen eines Vertrages und/oder die Überbezahlung von Produkten oder Dienstleistungen. Vereinfacht ausgedrückt wird durch eine Kickback-Zahlung vom Einfluss des unternehmensinternen Mitarbeiters Gebrauch gemacht.
Red Flags	Lieferant 1. Trend zu einem favorisierten Lieferanten (Übermäßiger Bezug von Waren oder Dienstleistungen von einem Lieferanten) 2. plötzlich rasant steigende Einkäufe bei einem Lieferanten 3. langsame Lieferung 4. Lieferant bietet keine üblichen Rabatte und Spezialangebote an 5. ungewöhnliche Verkäufe an einen Kunden, der gleichzeitig ein Lieferant ist 6. Nur ein kleiner Kreis an Lieferanten wird benutzt 7. Hohe Einkaufsvolumina bei einem neuen bzw. unautorisierten Lieferanten 8. Ein Lieferant stellt nur Dienstleistungen in Rechnung Bestellanforderung und Bestellung 9. Steigende Einkaufsvolumina, die nicht mit steigender Geschäftsaktivität oder steigenden Vorrat einhergehen (steigende Ausgaben für Waren und Dienstleistungen) 10. Mehrere kleine Bestellungen desselben Produkts (ein Einkauf wird in mehrere Teilkäufe unterteilt um den Genehmigungsprozess zu umgehen) 11. Unklarer Bestellgrund oder wenige Details über die erhaltene Ware 12. Einkaufswert übersteigt den letzten Wert um einen signifikanten Wert 13. Plötzliche Aktivität in nicht aktiven Konten 14. Genehmigung übersprungen Wareneingang 15. kein Wareneingangsbeleg 16. Ungewöhnlich hohe Vorräte kombiniert mit entsprechenden Einkäufen von bestimmten Lieferanten (unnötig hohe/steigende Lagerbestände) Rechnung und Bezahlung 17. Überbezahlung der bezogenen Produkte oder Dienstleistungen (Einkäufe sind über dem Marktpreis) 18. häufige Zahlungen des gleichen (runden) Betrages an einen Lieferanten 19. Geldtransaktionen zu unüblichen Zeiten / Außerhalb der Geschäftszeit 20. Doppelte Zahlungen 21. Lieferant wird regelmäßig schneller als andere Lieferanten entlohnt (Rechnungen werden sehr schnell beglichen) 22. Zahlungen die den Durchschnitt für einen Lieferanten übersteigen 23. Zahlungen die den gesamten Durchschnitt übersteigen

	24. Bestellbetrag ist höher als Rechnung 25. Lieferantenrechnung ist höher als Bestellbetrag 26. Rechnung außerhalb von normalen Arbeitszeiten erfasst

Tabelle 18: Kickback Fraud Pattern mit Red Flags

Quelle: Eigene Darstellung basierend auf Anhand E: Red Flags im Einkaufsprozess

Angebotsmanipulation (Bid Rigging)

Name	**Angebotsmanipulation (Bid Rigging)**
Beschreibung	Unter Angebotsmanipulation, Bid Rigging, Collusive Bidding oder Contract Rigging versteht man die Manipulation von Geboten oder Verträgen bei einer Ausschreibung. Diese werden zum Vorteil eines Unternehmens bspw. durch Kickback-Zahlungen an für die Ausschreibung verantwortliche Mitarbeiter beeinflusst. Illegale Zuwendungen, wie z.B. teure Geschenke, Hotelübernachtungen oder Urlaub, werden für den Vertragsabschluss geleistet (Wells, 2003a).
Red Flags	Lieferant 1. Selbe Person genehmigt einen neuen Lieferanten und die Zahlungen an ihn 2. Fiktionale Anbieter 3. Lieferanten erhalten Zuschlag übermäßig oft 4. Gleicher Lieferant bietet unter anderem Namen Ausschreibung 5. Der Vertrag geht immer an das letzte Angebot einer Ausschreibung 6. Firmen haben die Möglichkeit ihr Angebot aufzustocken 7. Starke Begrenzung der Zeitspanne zur Angebotsabgabe 8. Das Angebot ist sehr spezifisch/ sehr wenige Angebote 9. Ausschreibung wird in mehrere Ausschreibungen geteilt, um die Genehmigungsgrenzen zu umgehen 10. Ausschreibungsgebote liegen nah beieinander 11. Sehr weite Ausreißer 12. Wenn ein neuer Lieferant die Auktion beitritt, beginnen die Angebotspreise zu fallen 13. Angebote nach dem Ende der Angebotseinholungsphase akzeptiert Bestellanforderung und Bestellung 14. Waren werden ohne Ausschreibung eingekauft, obwohl diese in den Firmenrichtlinien vorgesehen ist 15. Geschätzte Kosten eines Auftrages liegen knapp unter der Genehmigungsschwelle, um eine Überprüfung und Freigabe zu vermeiden 16. Änderungen der Kostenspezifikationen nach Auftragsvergabe Rechnung und Bezahlung 17. Rechnungen für nicht gelieferte Waren 18. Preise für bezogene Waren oder Dienstleistungen über den gängigen Marktpreisen

Tabelle 19: Angebotsmanipulation Fraud Pattern mit Red Flags

Quelle: Eigene Darstellung basierend auf Anhand E: Red Flags im Einkaufsprozess

Scheinfirma

Name	Scheinfirma (Shell Company)
Beschreibung	Scheinfirma ist eine fiktive Entität ohne aktive Geschäftstätigkeit oder bedeutendes Vermögen. Dies ist nicht zwingend illegal, jedoch wird eine Scheinfirma ausschließlich zur Begehung wirtschaftskrimineller Straftaten gegründet. Um die Zahlungen an die gegründete Scheinfirma entgegenzunehmen, wird meistens ein Bankkonto im Namen der Scheinfirma eingerichtet.
Red Flags	Lieferant 1. plötzliche Geschäftsaktivitäten mit alten „schlafenden“ Lieferanten 2. Selbe Person genehmigt einen neuen Lieferanten und die Zahlungen an ihn 3. Lieferant ohne Festnetzanschluss oder nur mit Anrufbeantworter 4. Postfach als einzige Anschrift des Lieferanten oder fehlende Kontaktdaten des Lieferanten 5. Ein Lieferant stellt nur Dienstleistungen in Rechnung 6. Name der Lieferfirma besteht ausschließlich aus Initialen 7. stark steigende Einkäufe bei einem Lieferanten 8. Lieferanteninformationen stimmen mit Informationen eines Mitarbeiters überein (Anschrift, Bankdaten usw.) 9. Telefonnummern des Mitarbeiters und des Lieferanten stimmen überein 10. Lieferant nur einmalig verwendet (ohne Stammdaten) 11. Mehrere Instanzen desselben Lieferanten innerhalb der Lieferantenliste/-Datenbank (Lieferanten mit gleichem Namen, Telefonnummer oder Anschrift) Bestellanforderung und Bestellung 12. eine Genehmigung wird „vergessen/vernachlässigt“ 13. ungewöhnliche Genehmigungen (Überdurchschnittliche Anzahl an Bestellungen pro Tag genehmigt) 14. Einkäufer platzieren „dringende“ Aufträge 15. Einkäufe werden vor der Genehmigung dieser getätigt 16. Unklarer Bestellgrund oder wenige Details über die erhaltene Dienstleistung 17. Bestellsummen sind knapp unter dem Betrag, bei dem eine Autorisierung der Ausgaben erforderlich ist 18. ein Einkauf wird in mehrere Teilkäufe unterteilt, um den Genehmigungsprozess zu umgehen 19. Der Einkaufswert übersteigt den letzten Wert um einen signifikanten Wert 20. Ungewöhnliche Bestellmengen von einem Lieferanten Wareneingang 21. Rechnungen für nicht gelieferte Waren/ Dienstleistungen 22. Keine Eingangsprüfung der Waren durch einen vom Einkauf unabhängigen Mitarbeiter Rechnung und Bezahlung 23. Hohe Einkaufsvolumina bei einem neuen bzw. unautorisierten Lieferanten 24. Exzessive Rechnungen von einem Lieferanten/steigende Anzahl von Rechnungen 25. Fehlende ausgewiesene Steuer auf der Rechnung 26. Sequentielle Rechnungsnummern eines Lieferanten 27. Überdurchschnittlich häufige Rechnungsstellung (Rechnungen werden mehrmals im Monat gestellt, obwohl eine monatliche Bezahlung üblich wäre) 28. Keine oder falsche Mitarbeiter-ID in der Rechnung (Lieferant ohne Steuernummer) 29. Rechnungen eines bestimmten Lieferanten werden immer von demselben Mitarbeiter genehmigt

	30. Rechnungen mit stets gleichen (meist runden) Rechnungsbeträgen 31. Transaktionen werden zu ungewöhnlichen Zeiten durchgeführt 32. Rechnungen, werden sehr schnell beglichen 33. Überbezahlung der bezogenen Produkte oder Dienstleistungen 34. Lieferantenrechnung ist höher als Bestellbetrag 35. Bestellbetrag ist höher als Rechnung

Tabelle 20: Scheinfirma Fraud Pattern mit Red Flags

Quelle: Eigene Darstellung basierend auf Anhand E: Red Flags im Einkaufsprozess

Doppelte Bezahlung

Name	**Doppelte Bezahlung**
Beschreibung	Bei der doppelten Bezahlung wird die Rechnung mehrfach ausbezahlt. Dabei geht die zweite Zahlung meist an einen internen Täter oder an seinen Komplizen.
Red Flags	Lieferant 1. Lieferant mit Postfachanschrift 2. Lieferantenanschrift gleich Mitarbeiteranschrift Bestellanforderung und Bestellung 3. Doppelte Angaben (selbe Bestellung geht an verschiedene Lieferanten) Rechnung und Bezahlung 4. mehrere Rechnungen für dieselbe Ware 5. Es wird der exakt selbe Einkaufswert gezahlt, jedoch an zwei verschiedene Lieferanten 6. Die selbe Rechnungsnummer mit zwei verschiedenen Belegnummern 7. Same-Same-Same Test (Gleiche Person, bezahlt den gleichen Lieferanten, am gleichen Tag, denselben Betrag) 8. Same-Same-Different Test (Andere Person, bezahlt dem gleichen Lieferanten, am gleichen Tag, denselben Betrag) 9. Gleiche Rechnungsnummer, gleicher Lieferant, anderer Betrag 10. Anomalien in Rechnungssummen (frei erfundene Zahlen entsprechen nicht bestimmten mathematischen Gesetzmäßigkeiten; vgl. Benfords Law)

Tabelle 21: Doppelte Bezahlung Fraud Pattern mit Red Flags

Quelle: Eigene Darstellung basierend auf Anhand E: Red Flags im Einkaufsprozess

Pass Through

Name	**Pass Through**
Beschreibung	Beim Pass-Through Schema verkaufen Täter einem oder dem eigenen Unternehmen Waren oder Dienstleistungen zu überhöhten Preisen. Dabei kauft er das Produkt oder die Dienstleistung ein und verkauft diese zu einem erhöhten Preis weiter.
Red Flags	Lieferant 1. Hohe Einkaufsvolumina bei neuem bzw. unautorisierten Lieferanten Bestellanforderung und Bestellung 2. Steigende Einkaufsvolumina, die nicht mit steigender Geschäftsaktivität oder steigendem Vorrat einhergehen (steigende Ausgaben für Waren und Dienstleistungen)

	Wareneingang 3. Ungewöhnlich hohe Vorräte kombiniert mit entsprechenden Einkäufen von bestimmten Lieferanten (unnötig hohe/steigende Lagerbestände) Rechnung und Bezahlung 4. große Budgetabweichungen 5. Überbezahlung der bezogenen Produkte oder Dienstleistungen (Einkäufe sind über dem Marktpreis) 6. Die selbe Rechnungsnummer mit verschiedenen Belegnummern 7. Same-Same-Same Test (Gleiche Person, bezahlt den gleichen Lieferanten, am gleichen Tag, denselben Betrag) 8. Same-Same-Different Test (Andere Person, bezahlt dem gleichen Lieferanten, am gleichen Tag, denselben Betrag)

Tabelle 22:Pass Through Fraud Pattern mir Red Flags

Quelle: Eigene Darstellung basierend auf Anhand E: Red Flags im Einkaufsprozess

Unbeteiligter Lieferant

Name	**Unbeteiligter Lieferant**
Beschreibung	Bei dem Schema ‚unbeteiligter Lieferant' werden rechtmäßige und am Betrug unbeteiligte Lieferanten missbraucht, um das eigene Unternehmen zu schädigen. Dies geschieht beispielsweise, indem eine Rechnung von einem unabhängigen Lieferanten absichtlich überbezahlt wird. Danach wird der Mehrbetrag, z. B. unter dem Vorwand eines Buchungsfehlers, zurückgefordert. Die Rückzahlung wird vom Täter abgefangen, bevor sie das Unternehmen erreicht. Eine andere Methode besteht darin vorsätzlich einen falschen Lieferanten als Zahlungsempfänger zu deklarieren, von dem das Geld unter selbiger Begründung zurückgefordert und entsprechend abgefangen wird. Eine weitere Form beinhaltet den Kauf von unnötigen Waren, deren anschließende Rückgabe eine Gutschrift nach sich zieht, die entsprechend abgefangen wird. In seltenen Fällen werden sogar die Forderungen von rechtmäßigen Lieferanten direkt an die eigene Scheinfirma ausbezahlt (Wells, 2013).
Red Flags	Lieferant 1. Suspekte Anschrift des Lieferanten: gleiche Adresse wie ein anderer Lieferant 2. Hohe Einkaufsvolumina bei neuem bzw. unautorisierten Lieferanten Wareneingang 3. Rückgaben von Waren Rechnung und Bezahlung 4. Lieferantenrechnung ist höher als Bestellbetrag 5. Bestellbetrag ist höher als Rechnung 6. Überbezahlung der bezogenen Produkte oder Dienstleistungen (Einkäufe sind über dem Marktpreis) 7. Es wird der exakt selbe Einkaufswert gezahlt, jedoch an zwei verschiedene Lieferanten 8. Geldtransaktionen zu unüblichen Zeiten/ Außerhalb der Geschäftszeit 9. mehrere Rechnungen für dieselbe Ware

Tabelle 23: Unbeteiligter Lieferant Fraud Pattern mir Red Flags

Quelle: Eigene Darstellung basierend auf Anhand E: Red Flags im Einkaufsprozess

Rechnungsmanipulation

Name	Rechnungsmanipulation
Beschreibung	Bei der Rechnungsmanipulation werden legitime Transaktionen so manipuliert, dass das gezahlte Geld auf das eigene Konto überwiesen wird. Dabei muss der Mitarbeiter oder ein Komplize die Berechtigung haben die Stammdaten (v.a. die Kontonummer) des Lieferanten zu verändern. Anschließend versucht der Täter meist seine Spuren zu verwischen. Mögliche Arten der Verwischung sind bspw. die Rücksetzung der zuvor geänderten Kontonummer oder das Löschen des Lieferanten aus den Informationssystemen.
Red Flags	Lieferant 1. Änderungen in den Stammdaten (Kontonummer) 2. Ermittlung der Lieferanten bei denen die Rechnungsprüfung deaktiviert ist 3. Doppelte Angaben Rechnung und Bezahlung 4. große Budgetabweichungen 5. Lieferantenrechnung ist höher als Bestellbetrag 6. Bestellbetrag ist höher als Rechnung 7. Anpassungen der Verbindlichkeiten (in der Kreditorenbuchhaltung) 8. Lieferantenstammsatz wird für die Bezahlung geändert 9. Es wird ein Zahlungsempfänger eingetragen der einen sehr ähnlichen Namen wie der vorhergehende hat 10. Ändern der Währung zwischen Einkauf und Bezahlung, um etwaige Umrechnungsdifferenzen auszunutzen 11. Verdopplung und Umleitung einer Rechnung 12. Gleiche Rechnungsnummer, gleicher Lieferant anderen Betrag

Tabelle 24: Rechnungsmanipulation Fraud Pattern mit Red Flags

Quelle: Eigene Darstellung basierend auf Anhand E: Red Flags im Einkaufsprozess

Private Einkäufe

Name	Private Einkäufe
Beschreibung	Private Einkäufe sind Einkäufe für den privaten Zweck auf Kosten des Unternehmens. Die meisten Täter in den Studien von Wells (2013) kaufen Waren für den Eigenbedarf und verbuchen anschließend die Rechnung fälschlicherweise als Verbindlichkeit in das unternehmensinterne Abrechnungssystem. Um den tatsächlichen Zweck des Einkaufs zu verschleiern, werden gekaufte Waren als Unternehmensbedarf deklariert oder gefälschte Rechnungen eingereicht. Wie in den Scheinfirma-Schemata sind die Täter meist befugt die gestellten Verbindlichkeiten selbst zu autorisieren (Wells, 2013). Der Täter kann die dolosen Einkäufe anschließend entweder behalten oder eine Rücklieferung veranlassen, um die Erstattung einzustreichen. Oft werden private Einkäufe mit der firmeneigenen Kreditkarte durchgeführt, um vorhergehende Autorisierung der Bezahlung zu umgehen. Dieses Mittel ist allerdings nur einem bestimmten Angestelltenkreis zugänglich.
Red Flags	Bestellanforderung und Bestellung 1. Bestellsummen sind knapp unter dem Betrag, bei dem eine Autorisierung der Ausgaben erforderlich ist 2. Mehrere kleine Bestellungen desselben Produkts (ein Einkauf wird in mehrere Teilkäufe unterteilt um den Genehmigungsprozess zu umgehen) 3. Unklarer Bestellgrund oder wenige Details über die erhaltene Dienstleistung

	Rechnung und Bezahlung 4. Rechnungen, Eingangsbestätigungen und Bestelldokumente sind nicht übereinstimmend 5. Überbezahlung der bezogenen Produkte oder Dienstleistungen (Einkäufe sind über dem Marktpreis) 6. Keine oder falsche Mitarbeiter-ID in der Rechnung vorhanden 7. Rechnungseingang, obwohl die Bestellanforderung geblockt wurde 8. Rechnungseingang, obwohl die Bestellanforderung nicht genehmigt wurde 9. ungewöhnliche Genehmigungen 10. Same-Same-Same Test (Gleiche Person, bezahlt den gleichen Lieferanten, am gleichen Tag, denselben Betrag) 11. Same-Same-Different Test (Andere Person, bezahlt dem gleichen Lieferanten, am gleichen Tag, denselben Betrag

Tabelle 25: Private Einkäufe Fraud Pattern mit Red Flags
Quelle: Eigene Darstellung basierend auf Anhand E: Red Flags im Einkaufsprozess

Wie bereits erwähnt ist der Grundgedanken dieser Arbeit die parallele Suche nach zusammengehörenden Red Flags, um die Flut an Informationen mit der hohen falsch-positiv Rate zu reduzieren. Die hier aus der Literatur identifizierten Fraud Patterns werden im nächsten Schritt durch Experteninterviews validiert.

7.1.2 Validierung Fraud Patterns

Zur Evaluation der vorgestellten Fraud Patterns werden Befragungen nach den Richtlinien von Gläser & Laudel (2010) durchgeführt. Eine Befragung nutzt die Kommunikation zwischen zwei oder mehreren Personen als Grundlage zur Gewinnung von Informationen über einen Untersuchungsgegenstand (Scholl, 2009). Bei der Befragung werden durch Fragen (verbale Stimuli), Antworten (verbale Reaktionen) hervorgerufen (Atteslader, 2010). In Bezug auf die verwendete Kommunikationsart kann zwischen mündlicher (Interviews) und schriftlicher Form (Fragebögen) unterschieden werden (Bortz & Döring, 2006). Zusätzlich kann nach Scholl (2009) zwischen persönlicher, telefonischer, schriftlicher und online Befragung, unterschieden werden.

Eine weitere Unterscheidung ergibt sich durch die Strukturiertheit der Befragung. Bei wenig strukturierten Befragungen arbeiten Forscher ohne Fragebogen, was eine flexible Gesprächsführung erlaubt (Atteslader, 2010). Die Fragen ergeben sich anhand des Gesprächsverlaufs. Eine stark strukturierte Befragung hingegen beinhaltet meist einen Fragebogen, der die Anzahl und Reihenfolge der gestellten Fragen festlegt (Atteslader, 2010). Diese Art der Befragung wird häufig bei schriftlichen Befragungen mit einer hohen Anzahl von Teilnehmern durchgeführt, da hier oft Freiheitsgrade bei der Beantwortung fehlen (Scholl, 2009, Atteslader, 2010). Bei teil- (bzw. semi-) strukturierten Befragungen wird das Gespräch durch vorbereitete und vorformulierte Fragen strukturiert (Atteslader, 2010). Dabei ist die Reihenfolge der Fragen nicht festgelegt und die Forscher können jederzeit auf interessante Themen eingehen. Der Leitfaden dient als Gedächtnisstütze zur Gesprächsorientierung.

7.1.2.1 Forschungsdesign

Für die Evaluation der Fraud Patterns erscheint die persönliche Befragung als geeignet. Dabei kann der Befragte besser motiviert und durch gezielte Rückfragen unvollständige Antworten vervollständigt werden (Scholl 2009). Zudem können sowohl der Interviewer als auch der Befragte bei Unklarheiten nachfragen und so die Qualität des Interviews erhöhen (Scholl 2009). Die Befragung wird anhand eines Leitfadens in Form von semi-strukturierten Interviews (vergl. hierzu Anhang C: Fragebogen zur Validierung der Fraud Patterns) geführt. Dabei werden die Patterns und dazugehörigen Red Flags beschrieben. Die Experten sollen beurteilen, welche Red Flags sie als *besonders relevant*, *releva*nt oder *irrelevant* erachten. Zusätzlich wird nach fehlenden Red Flags und Fraud Patterns gefragt.

Der Fragebogen wird in einer Pre-Studie getestet. Dabei wird die Befragung mit zwei Experten durchgeführt, die während und nach der Befragung konkretes Feedback zum Fragebogen geben. Die Hauptkritik hierbei ist, dass der Befragte mit zu vielen Informationen konfrontiert wird (Fraud Patterns und Red Flags) und zu viele Information abgefragt werden. Es wird der Wunsch geäußert etwas kompakter antworten zu können. Als Verbesserung werden den Experten vor dem semi-strukturierten Interview die entsprechenden Fraud Patterns mit den dazugehörigen Red Flags über das Onlinefragetool Google Forms[31] bereitgestellt. Zusätzlich werden die Red Flags entlang des Einkaufsprozesses geordnet und nummeriert.

Zur Auswahl der Experten werden Personenkreise, die sich mit Fraud und dem Einkaufsprozess befassen in Betracht gezogen. Gläser und Laudel (2010) definieren Experten als Personen, die mehr als der Durchschnitt der Bevölkerung zu einem bestimmten Thema wissen. Insgesamt können zehn Experten mit folgenden Positionen im Unternehmen befragt werden: Audit Director, Audit Manager, Procurement Engineer, Internal Audit Leitung, Strategischer Einkauf, SCM Procurement Governance und Senior Data Analyst.

7.1.2.2 Ergebnisse

Die Auswertung der durchgeführten Expertenevaluation hat insgesamt zehn gültige Resultate hervorgebracht, die nachfolgend im Detail beschrieben werden. Der Expertenkreis setzt sich aus 3 weiblichen und 7 männlichen Personen zusammen, wobei 50% dieser Personen im Alter zwischen 25 und 35 Jahren, 20% zwischen 36 und 45 Jahren und 30% zwischen 46 und 55 Jahren sind.

Insgesamt kann festgestellt werden, dass die befragten Experten je nach Erfahrung unterschiedlich antworten. So wird beispielsweise das Red Flag „Ein Lieferant stellt nur Dienstleistungen in Rechnung“ von manchen als *besonders relevant* erachtet, während es für andere Experten *irrelevant* ist. Im Folgenden werden die Ergebnisse pro Fraud Pattern dargestellt. Die Detailübersicht über die Befragung befinden sich in Anhang D: Ergebnisse der Validierung.

[31] Vergl. hierzu: https://www.google.de/intl/de/forms/about/

Bei **‚Kickback Fraud'** werden mit einem Ergebnis von mindestens fünf Stimmen in der Kategorie besonders relevant die Red Flags „Hohe Einkaufsvolumina bei neuem bzw. unautorisierten Lieferanten", „Lieferant erhält Zuschlag, obwohl er nicht der niedrigste Bieter ist" und „Mehrere kleine Bestellung desselben Produkts" gekennzeichnet. Als irrelevantere Red Flags im Kickback Fraud Pattern mit mindestens 7 Stimmen zählen die Red Flags „langsame Lieferung", „Lieferant bietet keine üblichen Rabatte und Spezialangebote an", „Zahlungen, die den gesamten Durchschnitt übersteigen", „Bestellbetrag ist höher als Rechnung" und „Rechnung außerhalb von normalen Arbeitszeiten erfasst". Als fehlende Red Flags werden folgende genannt: „Lieferant hat Verbindungen mit Mitarbeitern (Einkauf oder im Projekt)", „plötzlicher Lieferantenwechsel ohne nachvollziehbaren Grund (abweichend von der Materialfeldstrategie)", „Auswertung, ob Lieferant einen "ready4business" flag hat" und „Bestellungen werden nicht in der Zentrale, sondern außerhalb aufgegeben und angenommen".

Bei **‚Bid Rigging'** Fraud Pattern werden einige Red Flags kontrovers diskutiert. So wird beispielsweise das Red Flag „Starke Begrenzung der Zeitspanne zur Angebotsabgabe" von fünf befragten Personen als *irrelevant* eingestuft, während vier Personen dieses Red Flag als *relevant* bzw. einer als *sehr relevant* empfindet. Nur das Red Flag „Ausschreibungsgebote nah beieinander" wird überwiegend als *irrelevant* kategorisiert. Als *besonders relevant* für Bid Rigging gelten nach Meinung der befragten Experten die Symptome „Fiktionale Anbieter" und „Gleicher Lieferant bietet unter anderem Namen mehrfach". Als fehlendes Symptom wird „Lieferanten haben den gleichen Inhabern oder mit gleichen Adressen, Tel. Nummern, Bankdaten usw." genannt.

Innerhalb des Fraud Patterns **‚Scheinfirma'** zählen die Experten „Lieferanteninformationen stimmen mit Informationen eines Mitarbeiters überein (Anschrift, Bankdaten, usw.)" und „Telefonnummern des Mitarbeiters und des Lieferanten stimmen überein" zu den *besonders relevanten* Red Flags. Als *irrelevante* Red Flags werden folgende Red Flags genannt: „Bestellbetrag ist höher als Rechnung", „Aktionen wurden zu ungewöhnlichen Zeiten durchgeführt", „Einkaufswert übersteigt den letzten Wert um einen signifikanten Wert", „Stark steigende Einkäufe bei einem Lieferanten" und „Ein Lieferant stellt nur Dienstleistungen in Rechnung". Ergänzt werden die Red Flags um „Lieferant hat Bankkonto oder seinen Sitz in Tax Heaven".

Die Kategorisierung hat bei dem Fraud Pattern **‚Doppelte Bezahlung'** keine *irrelevanten* Symptome aufgedeckt. Als *besonders relevant* wird das Red Flag „Lieferantenanschrift gleich Mitarbeiteranschrift" gesehen. Als zusätzliches Red Flag wird „Rechnung ohne Bestellung" hinzugefügt. Außerdem wird erwähnt, dass einige der genannten Red Flags aus diesem Bereich systemtechnisch im SAP nicht möglich seien, da kein höherer Wert als der Bestellwert ausgezahlt werden könne. Auch gleiche Rechnungsnummern seien eher ein Versehen des Lieferanten, die nur durch genehmigungspflichtige Bestellerhöhungen ausgelöst werden können. In der Literatur wird bei der doppelten Bezahlung genannt, dass die Bezahlung über das Konto „Conto pro Diverse" (CpD) und gleichzeitig über den Zahlungslauf durchgeführt werden könne (Bönner, Riedl, Wenig, 2011). Bei dem zu interviewenden Experten ist die Buchung über das CpD Konto im System deaktiviert. Der Experte kann sich allerdings in anderen Firmen vorstellen, dass es bei Aktivierung des Kontos durchaus zu doppelten Bezahlungen kommen könne.

Auch bei dem **‚Pass Through‘** Schema werden keine Red Flags als *irrelevant* eingestuft. Als *besonders relevant* werden die Red Flags „Name des liefernden Unternehmens gleicht dem eines Familienmitglieds des im Einkaufsprozess involvierten Mitarbeiters“ und „Überbezahlung der bezogenen Produkte und Dienstleistungen“. Als zusätzliches Red Flag fügt ein Experte hinzu: „Die erste Bestellung wird kurz nach der Erstellung eines neuen Lieferanten im System getätigt“. Zudem wird der Wunsch geäußert, Einkäufe unter der Genehmigungsgrenze ebenfalls diesem Pattern als potentielles Symptom hinzuzufügen. Abschließend merkte ein Teilnehmer an, dass seines Erachtens das Red Flag „Dieselbe Rechnungsnummer mit zwei verschiedenen Belegnummern“ keine klare Verbindung zu dem Fraud Pattern „Pass-Through“ aufzeigt.

Innerhalb des Fraud Patterns **‚Unbeteiligter Lieferant‘** wird keines der Red Flags als *besonders relevant* eingestuft. Das Symptom „Rückgaben von Waren“ ist kontrovers diskutiert und gleichzeitig als *besonders relevant* und *irrelevant* eingestuft worden. Als *irrelevant* werden „Bestellbetrag ist höher als Rechnung“ und „Geldtransaktionen zu unüblichen Zeiten/ außerhalb der Geschäftszeit“ gezählt. Zudem wird angemerkt, dass „kurzfristige Änderungen der Lieferantenstammdaten“ ebenfalls ein wichtiges Symptom für dieses Fraud Pattern sei und noch fehle.

Das Fraud Pattern **‚Rechnungsmanipulation‘** beinhaltet die *besonders relevanten* Red Flags „Lieferantenstammsatz wird für die Bezahlung geändert“ und „Eingetragener Zahlungsempfänger hat ähnlichen Namen zum richtigen Zahlungsempfänger“. Als *irrelevant* gelten hingegen die Symptome „Große Budgetabweichungen“ und „Bestellbetrag ist höher als Rechnung“. Weiterhin sollen folgende Red Flags hinzugefügt werden: „Mehrere Änderungen des Bestellwertes“, „Hohe Änderungen des POs“, „Temporäre Stammdatenänderungen“ und „Lieferanten ohne Bankkonto und mit Cash Bezahlung“.

Die Abstimmungsergebnisse des Fraud Patterns **‚Private Einkäufe‘** ergibt weder *besonders relevante* noch *irrelevante* Symptome.

Als allgemeine Kritik an den Fraud Patterns wird genannt, dass einige Red Flags über das Kontrollsystem unzulässig und somit irrelevant sind. Außerdem wird der Vorschlag vorgebracht, die Grundgesamtheit durch den Fokus auf bestimmte Industrien einzugrenzen, wie z. B. auf Bauwesen oder Mining in Lateinamerika. Als weitere Fraud Patterns schlagen die Experten folgende Fehlende vor: Mängel im PO und Vertragsmanagement sowie die Betrachtung von Interessenskonflikten bei der Auswahl von Zulieferer. Außerdem betonen die Experten die Wichtigkeit technischer Hilfsmittel bei der Bekämpfung von Fraud.

7.1.2.3 Anpassung der Fraud Patterns

Anhand der Ergebnisse der Evaluation werden die Fraud Patterns angepasst. Zunächst wird geprüft, ob irrelevante Red Flags aufgrund des internen Kontrollsystems als irrelevant eingestuft werden, oder ob diese wirklich irrelevant für das entsprechende Pattern sind. Es wird nicht angenommen, dass jedes Unternehmen ein Kontrollsystem eingeführt hat. Zusätzlich werden die von den Experten vorgeschlagenen Red Flags hinzugefügt. Die besonders relevanten Red Flags werden für die Initialisierung des Prototypens verwendet.

Im Fraud Pattern „Kickback Fraud“ werden die irrelevanten Red Flags „langsame Lieferung“, „Lieferant bietet keine üblichen Rabatte und Spezialangebote an“, „Zahlungen, die den gesamten Durchschnitt übersteigen“, „Bestellbetrag ist höher als Rechnung“ und „Rechnung außerhalb von normalen Arbeitszeiten erfasst“ aus dem Fraud Pattern entfernt. Als fehlendes Red Flag gilt „Lieferant hat Verbindungen mit Mitarbeitern (Einkauf oder im Projekt)“. Dieses kann im ERP System nicht dargestellt werden, da dazu eine Art des sozialen Netzwerkes nötig wäre. Es kann lediglich überprüft werden, ob Mitarbeiterkombinationen häufig vorkommen. Diese Kombinationen wären allerdings wenig aussagekräftig, da bestimmte Konstellationen auch im regulären Einkaufsprozess gehäuft vorkommen können. Bei dem „ready4business“ Flag handelt es sich um eine erweitertes Kontrollfeld des SAP Systems (individuelle Lösung des Unternehmens), die nicht standardmäßig gesetzt und deshalb nicht aufgenommen wird. Die weiteren genannten Red Flags „Plötzlicher Lieferantenwechsel“ und „Bestellungen werden nicht in der Zentrale, sondern außerhalb aufgegeben und angenommen“ werden ergänzt.

Bei Bid Rigging wird das Red Flag „Ausschreibungsgebote nah beieinander“ als irrelevant kategorisiert und entsprechend aus dem Fraud Pattern entfernt. Das vorgeschlagen Red Flag „Lieferanten mit gleichen Inhabern oder mit gleichen Adressen, Tel. Nummern, Bankdaten usw.“ ist bereits in dem Fraud Pattern enthalten und wird nicht erneut hinzugefügt.

Innerhalb des Fraud Patterns „Scheinfirma (Shell Company)“ werden die Red Flags „Bestellbetrag ist höher als Rechnung“, „Lieferant stellt nur Dienstleistungen in Rechnung“ und „Aktionen wurden zu ungewöhnlichen Zeiten durchgeführt“ aus dem Fraud Pattern entfernt. Die Red Flags „Einkaufswert übersteigt den letzten Wert um einen signifikanten Wert“ und „Stark steigende Werte bei einem Lieferanten“ werden in der Literatur häufig genannt[32]. Scheinfirmen können den Einkaufsprozess zunächst ordnungsgemäß durchlaufen und Vertrauen bei den Mitarbeitern gewinnen. Auch die Anzahl und der Wert der kriminellen Taten steigt kontinuierlich an, da diese Firmen ohne vorherige Konsequenzen mutiger werden. Durch die häufige Nennung dieser zwei Red Flags in der Literatur, werden diese beibehalten. Das Red Flag „Lieferant hat Bankkonto oder seinen Sitz in Tax Heaven“ wird in dieses Pattern aufgenommen.

Bei den Fraud Patterns „Doppelte Bezahlung“ und „Pass Through“ werden keine *irrelevanten* Symptome aufgedeckt und dementsprechend keine Red Flags entfernt. Bei „Doppelter Bezahlung“ wird „Rechnung ohne Bestellung“ vorgeschlagen, welches eine Prozessabweichung beschreibt. Da Prozessabweichungen mit Hilfe von Process Mining dargestellt werden und im Prozess Explorer analysiert werden können, bedarf es dieses Red Flag nicht. Zu dem „Pass Through“ Pattern werden die Red Flags „Eine Bestellung wurde getätigt, kurz nachdem ein neuer Lieferant im System angelegt worden ist“ und „Einkäufe knapp unter Genehmigungsgrenze“ hinzugefügt.

Bei dem Fraud Pattern „unbeteiligter Lieferant“ gelten „Bestellbetrag ist höher als Rechnung“ und „Geldtransaktionen zu unüblichen Zeiten/ Außerhalb der Geschäftszeit“ als *irrelevant* und werden entsprechend aus dem Pattern entfernt. Hinzugefügt wird das Red Flag „kurzfristige

[32] Vergleich hierzu: Wells, 2003; Wells, 2002; Christensen & Byington, 2003; Cascarino, 2013; Anand, Ashforth, & Joshi 2004

Änderungen der Lieferantenstammdaten“. Bei „Rechnungsmanipulation“ werden die Symptome „Große Budgetabweichungen“ und „Bestellbetrag ist höher als Rechnung“ als irrelevant entfernt. Hinzugefügt werden die Red Flags „Mehrere Änderungen des Bestellwertes“ und „Lieferanten ohne Bankkonto und mit Cash Bezahlung“)“. „Temporäre Stammdatenänderungen“ sind bereits als Red Flags enthalten und werden entsprechend nicht erneut hinzugefügt. Bei dem Pattern „Private Einkäufe“ werden keine Änderungen durchgeführt.

Als weitere Fraud Patterns werden „Mängel im PO und Vertragsmanagement“ und „Betrachtung von Interessenskonflikten bei der Auswahl von Zulieferern“ genannt. Bei dem Thema Interessenkonflikt wird (wie bereits erwähnt) auf benachbarte Szenarien ausgewichen, da das Motiv des Täters nicht in den Daten auslesbar ist. Mängel im PO und Vertragsmanagement lassen sich nicht im ERP System erkennen und werden deshalb nicht weiter betrachtet.

7.2 Technische Ebene – Implementierung

Auf der technischen Ebene wird ein Prototyp zur Identifikation von Fraud mit Hilfe von Process Mining und Red Flags erstellt. Die Implementierung wird im Folgenden dargestellt.

7.2.1 Methodisches Vorgehen

Für die Gestaltung des Artefaktes wird in dieser Dissertation ein Prototyp ausgewählt. Ein Prototyp ist ein repräsentatives Model oder eine Simulation des finalen Systems (Warfel, 2009). Der Erstellungsprozess von Prototypen wird als Prototyping bezeichnet, welches durch ein inkrementelles und iteratives Vorgehen geprägt ist (Warfel, 2009).

Man unterscheidet Prototypen anhand des Funktionsumfangs und der Detailierungsstufe (oft im englischen als fidelity bezeichnet). Umso höher der Umfang des Prototyps in Bezug auf die finale Gestaltung des finalen Funktionsumfangs, desto höher ist die fidelity oder wiedergabetreue des Prototyps (Dahm, 2006). In frühen Phasen des Gestaltungsprozesses werden low-fidelity Prototypen eingesetzt, um den Erstellungsaufwand zu reduzieren und schnell Evaluation und Designentscheidungen zu treffen (Dahm, 2006). In späteren Phasen wird ein high-fidelity Prototyp eingesetzt (Dahm, 2006). Diese versuchen in Bezug auf Funktionsumfang, Aussehen (Layout, Farbschema) und Anbindung an externe Systeme eine möglichst hohe Ähnlichkeit zum finalen System zu erlangen (Dahm, 2006).

Um die vorgestellten Red Flags und Fraud Patterns zu konzipieren und prototypisch zu implementieren werden zunächst Anforderungen an den Fraud Detektion Prototypen aus einem Anforderungskatalog eines Unternehmens übernommen, sowie die bereits aus der Literatur abgeleiteten Anforderungen betrachtet. Um die Umsetzbarkeit zu evaluieren, wird zunächst ein low-fidelity Prototyp erstellt. Dieser wird anschließend mit der Thinking Aloud Methode evaluiert. Da dabei auch weitere Anforderungen entstehen, werden diese in einem high-fidelity Prototyp umgesetzt.

7.2.2 Anforderungen

In diesem Bereich sollen nur funktionale Anforderungen erhoben werden, die den Prototypen betreffen. Anforderungen an das Dashboard des Prototyps und der angezeigten Informationen werden in Kapitel 7.4.1 separat identifiziert. Für eine allgemeine Definition und Erläuterung von Anforderungen wird auf Brügge & Dutoit (2004) oder Balzert (2009) verwiesen.

Die Hauptanforderung an den Prototypen ist die Identifikation aller aus der Literatur abgeleiteten und im ERP System erkennbaren Red Flags und Fraud Patterns (vergl. Kapitel 7.1.1). Ein Fraud Pattern setzt sich aus mehreren Red Flags zusammen. Der Auditor soll in einer Initialisierungsphase eine Auswahl der wichtigsten Red Flags pro Fraud Pattern treffen. Bei gleichzeitigem Auftreten dieser Red Flags soll das entsprechende Fraud Pattern anschlagen. Auch soll der Auditor firmenspezifische Grenzwerte (wie bspw. Genehmigungsgrenzen) auswählen, um so die Genauigkeit der Red Flags zu erhöhen. Der Ist-Prozess (mitsamt allen Abweichungen) soll mit Hilfe von Process Mining rekonstruiert und visualisiert werden.

Insgesamt lassen sich sehr wenige akademische Quellen identifizieren, die Anforderungen an eine Detektionslösung beschreiben. Einige Anforderungen werden in Kapitel 5.1.4 dargestellt und aus der Process Mining Literatur abgeleitet. Diese sind konkret:

- Identifikation von Prozessabweichungen. Dabei sollen auffällige Kombinationen von Nutzerverhalten erkannt und Prozessabweichungen analysiert werden.
- Benutzeroberfläche: Die Benutzeroberfläche sollte wie bei Singh, Best, Bojilov, et al. (2013) modular aufgebaut sein. Diese haben in ihrer Umfrage gezeigt, dass ein modularer Aufbau von Auditoren bevorzugt wird. Ein Dashboard soll eine Übersicht anzeigen, während weitere Informationen auf Tabs aufgeteilt werden.
- Zusätzliche Informationen: Process Mining sollte mit zusätzlichen Informationen angereichert werden. Dies sind bestenfalls Informationen aus dem SAP System.

Um dem Mangel an Anforderungen aus der Literatur entgegenzukommen, werden Anforderungen aus der Praxis entnommen. Der Autorin dieser Dissertation stehen Anforderungen in Form eines CiP Audit Approach eines Unternehmens zur Verfügung. Dieses Unternehmen hat mit der Vorstellung ihrer Auditing Lösung den ersten Platz im Audit Innovation Award gewonnen. Ziel dieses Awards ist es innovative Ideen aus der Revisions- und Prüfungswesen aus Deutschland, Österreich und der Schweiz zu generieren (ARC, 2016). Die hier genannten Anforderungen sind nicht im Sinne von Brügge and Dutoit (2004) messbar. Stattdessen werden bei den Zeiten der übernommenen Anforderungen als „möglichst schnell“ oder „angemessener Zeit“ gefordert. Da in der Literatur keine Zeitangaben für die Analyse gefunden wurden, werden diese ungenauen Zeitangaben übernommen.

- Datenanalysen sind ein wichtiger Bestandteil des Audits. Deshalb sollen im gesamten Auditprozess Daten analysiert werden.
- Datenextraktion sollte ein kleiner Bestandteil der Analyse sein und möglichst wenig Zeit in Anspruch nehmen.

- Regionale Besonderheiten, wie bspw. verschiedene Zeichensatztabellen oder unterschiedliche Währungen, sollen berücksichtigt werden.
- Auditoren sollen auf das Tool von überall in der Welt zugreifen können, ohne zusätzliche Software installieren zu müssen.
- Zugriff auf die Daten einer bestimmten Entität sollte nur autorisierten Auditoren ermöglicht werden. Autorisierte Auditoren sind Auditoren, die das Audit durchführen.
- Komplexe Analysen auf großen Datenvolumen sollen in angemessener Zeit durchgeführt werden können.
- Die Ergebnisse der Analyse sollen graphisch dargestellt werden, so dass Auditoren wirtschaftskriminelle Handlungen ohne IT Erfahrung erkennen.
- Bei großer Datenbasis sollen nur die wahrscheinlichsten Fälle dargestellt werden, um die Datenbasis für den Auditor zu reduzieren.
- Ergebnisse der Analyse sollen in einer Art dargestellt werden, die es ohne zusätzlichen Aufwand erlaubt in den Auditbericht übernommen zu werden.

Das Vorgehen zur Umsetzung dieser funktionalen Anforderungen wird im Folgenden beschrieben.

7.2.3 Log Vorbereitung

Nach dem Vorgehensmodell (vergl. Kapitel 6.1) ist auf technischer Ebene der erste Schritt die Log Vorbereitung, bei der relevante Tabellen und Felder im Geschäftsprozess identifiziert und in ein Process Mining Tool lesbares Format gebracht werden (vergl. Kapitel 6.1.2). Dieses Vorgehen wird hier beschrieben, wobei zunächst auf die verwendeten Werkzeuge und die spezifischen Eigenschaften dieser Werkzeuge eingegangen wird.

7.2.3.1 Verwendete Werkzeuge

In dieser Dissertation wird Celonis als Process Mining Tool und die In-Memory Datenbank SAP HANA verwendet. Die Begründung für die Auswahl von Celonis Process Mining erfolgt in Kapitel 5.1.3. Aufgrund der großen zu verarbeitenden Datenmengen wird eine In-Memory Datenbanken gewählt, da diese Datenbanken durch die Speicherung des gesamten Datenbestands im Hauptspeicher, vor allem eine schnelle Verarbeitung von Daten versprechen (Plattner & Zeier, 2012). Abbildung 7-1 zeigt die client- und serverseitig notwendigen Tools und ihre Interaktion für die Verwendung von SAP HANA und Celonis Process Mining. Serverseitig wird eine SAP HANA Datenbank und ein Celonis Process Mining Tool installiert, wobei Celonis auf die Daten der In-Memory Datenbank zugreift. Celonis kann über einen Web Browser (hier Firefox) gesteuert werden, während die Datenbank über das SAP HANA Studio gesteuert wird. Die Datenbank enthält die im Kapitel *3.2* beschriebenen Tabellen.

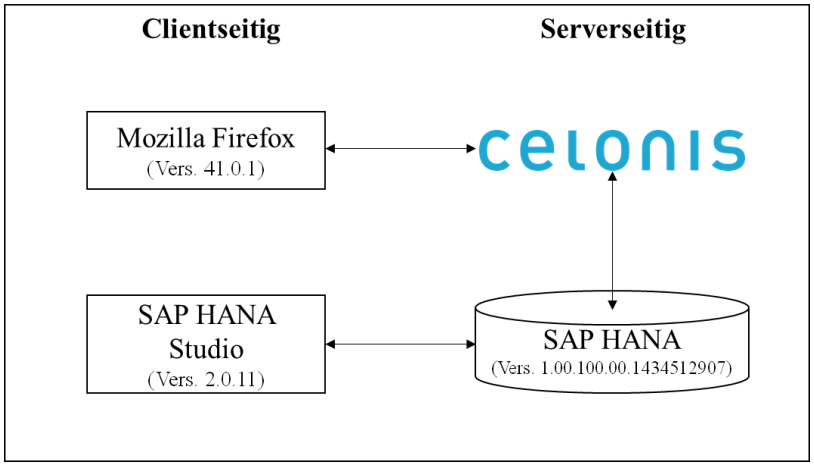


Abbildung 7-1: Zusammenspiel der eingesetzten SAP und Process Mining Tools

Quelle: Eigene Darstellung

Gemeinsam haben Process Mining Werkzeuge, dass bestimmte Tabellen zur Rekonstruktion des Prozessablaufes benötigt werden. Celonis Process Mining benötigt drei Tabellen mit vorgegebenen Spalten. Um diese zu erstellen, müssen relevante Teile aus den bestehenden SAP Tabellen extrahiert und in die entsprechende Form gebracht werden. Hierzu wird im SAP HANA Studio ein SQL Script entickelt, um die entsprechenden Fall-, Aktivitäts- und Prozess Tabellen zu erstellen. Sobald die entsprechenden Tabellen in der Datenbank vorhanden und mit Daten befüllt sind, können diese mit Celonis Process Mining analysiert werden. Dafür müssen dem Celonis Tool Rechte auf das entsprechende Datenbankschema gegeben werden. Anschließend kann über den Browser die Analyse durchgeführt werden. Die entsprechenden Fall-, Aktivitäts- und Prozess Tabellen werden im Folgenden erklärt.

7.2.3.2 Fall-, Aktivitäts-, und Prozesstabellen

Die entsprechenden Tabellen zur Rekonstruktion eines Geschäftsprozesses werden im Folgenden erläutert. Diese Erläuterung basieren auf den Schulungsunterlagen von Celonis (Stierle, 2015).

- Aktivitätstabellen

Aktivitätstabellen entsprechen jedem Event oder Prozessschritt in einem Prozess. Beispiele hierfür könnten ‚Erstellung einer Bestellung' oder ‚Änderung einer Bestellung' sein.

```
CREATE TABLE CELONIS_P2P_ACTIVITIES(
ActivityCaseID VARCHAR(18)
,Activity VARCHAR(40)
,EventTime TIMESTAMP
,Sorting INTEGER
,EventUser VARCHAR(12));
```

Abbildung 7-2 Bestandteile der Aktivitätstabelle

Quelle: Eigene Darstellung

Eine Aktivitätstabelle besteht üblicherweise aus den in Abbildung 7-2 dargestellten Spalten. Bei *ActivityCaseID* handelt es sich um den Primärschlüssel der Falltabelle, der eindeutig ist und

global im Datenmodell verwendet wird. Die *Activity* Spalte entspricht der textuellen Beschreibung der Aktivität. Eine mögliche Aktivität könnte die ‚Erstellung der Bestellanforderung' oder ‚Änderung der Bestellung' sein. *EventTime* beschreibt den Zeitstempel, bestehend aus Datum und Uhrzeit, wann die Aktivität durchgeführt wurde. *Sorting* legt die normale Ordnung im System fest. Anders ausgedrückt wird die Reihenfolge der Ausführung der Prozessschritte manuell festgelegt. So sollte eine Bestellung vor dem Wareneingang erfolgen. Dieses Sorting wird benötigt, falls zwei Events exakt denselben Zeitstempel haben. Die Reihenfolge wird dann anhand des Sortings festgelegt. Ein *EventUser* ist der SAP Systemnutzer, der die entsprechende Aktivität ausführt. Beispielsweise könnte ein EventUser eine natürliche Person oder ein maschinelles System sein.

Insgesamt werden drei zusätzliche Spalten durch ein von Celonis bereitgestelltes Skript erstellt. Die *Lifecycle* Spalte wird von den Spalten *Sorting* und *Timestamp* abgeleitet und stellt die eigentliche Position im Fall dar. *Case_Num_ID* speichert für jede *ActivityCaseID* einen Integerwert, der zur Steigerung der Performanz im System genutzt wird. Der *PrimaryKey* wird hinzugefügt, um jede Aktivität eindeutig zu referenzieren.

- Falltabellen

Die Falltabellen entsprechen dem kompletten Prozessverlauf und beinhalten alle im System vorhandenen Instanzen. Ein Fall besteht aus mehreren Aktivitäten und wird aus der Aktivitätstabelle erstellt. In dieser Dissertation ist ein Fall eine Instanz des Einkaufsprozesses und wird eindeutig durch die Pfad ID referenziert.

- Prozesstabelle

Eine Prozesstabelle verbindet Aktivitäten zu Integer-IDs um Geschwindigkeitsvorteile bei der Ausführung zu erlangen. Hierfür stellt Celonis ein Skript bereit, welches diese Prozesstabellen erstellt.

Als nächstes wird der ETL Prozess in Celonis beschrieben, wobei die Daten aus dem ERP System in das zuvor beschriebene Format gebracht werden. Die entsprechenden Informationen sind in mehreren Tabellen verteilt, so dass ein Verständnis über relevante Tabellen im SAP System notwendig ist.

7.2.3.3 ETL Prozess in Celonis

Um die Daten in das entsprechende Format zu bringen, muss der Extract Transform Load (ETL) Prozess durchgeführt werden. Die durchzuführenden Aktionen sind die Extraktion der notwendigen Daten, die Transformation in das richtige Format und das Laden in das Zielsystem (Kemper & Eickler, 2011). Da Celonis die ODBC und JDBC Schnittstelle unterstützt, hat der Benutzer die Auswahl aus verschiedenen Datenbanken (Stierle, 2015). Wie bereits erwähnt, wird an dieser Stelle eine SAP HANA Datenbank verwendet.

Die Transformation wird durch SQL Skripte erreicht, bei der die zuvor beschriebenen Tabellen (Aktivitäts-, Fall- und Prozesstabellen) mit Inhalt gefüllt werden. Das implementierte Skript

zur Befüllung der entsprechenden Tabellen ist in ‚Anhang G: Skripte zur Erstellung von Activity, Case und Process Tabelle' vorhanden. An dieser Stelle soll anhand zweier Beispiele demonstriert werden, wie ein beispielhafter Code für die ‚Erstellung einer Bestellanforderung' und für die ‚Löschung, Sperrung oder Änderung einer Position' aussehen könnte.

Abbildung 7-3 zeigt einen Ausschnitt der Skriptes zur Anlage einer Bestellanforderung. Entsprechende Informationen aus der EBAN Tabelle werden in die Aktivitätstabelle *_CEL_P2P_ACTIVITIES* geladen. *CaseID* ist der Primärschlüssel und setzt sich aus dem Mandanten, der Einkaufsbelegnummer (EBELN) und der Position auf dem Beleg (EBELP) zusammen. Das Erstelldatum (AEDAT) und die Uhrzeit (UTIME) werden über die Prozedur *GetTimeStamp()* konkateniert, um den Zeitstempel der Aktivität zu definieren. Der verantwortliche Nutzer ist in der EBAN Tabelle im Feld ERNAM gespeichert. Die Sortierung dient als Sortierungshilfe und ist frei wählbar, wobei Celonis empfiehlt in 10er Schritten vorzugehen, damit nachträgliche Aktivitäten eingefügt werden können, ohne Anpassungen am gesamten Skript durchzuführen. Aktivität ist die textuelle Beschreibung des Prozessschrittes oder Events. Diese wird manuell vergeben und sollte möglichst prägnant gewählt werden. Die zentrale Tabelle im Einkaufsprozess ist die Einkaufsbelegpositionen Tabelle (EKPO). Um eine globale ID für jede Aktivität auszuwählen, müssen alle Tabellen mit dieser verknüpft werden.

```
--New Activity: Lege Bestellanforderung an
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
       EBAN_MANDT + EBAN_EBELN + EBAN_EBELP AS CaseID,
       'Lege Bestellanforderung an' AS Activity,
       --EBAN_ERDAT AS EventTime,
       dbo.GetTimeStamp(EBAN_BADAT,EBAN_UZEIT) AS EventTime,
       10 AS Sorting,
       EBAN_ERNAM AS EventUser
FROM EBAN
JOIN EKPO
       ON EKPO_EBELN = EBAN_EBELN
       AND EKPO_EBELP = EBAN_EBELP
       AND EKPO_MANDT = EBAN_MANDT
GO
```

Abbildung 7-3: Code Beispiel Anlegen BANF

Quelle: Eigene Darstellung

Ein etwas komplizierteres Beispiel ist in Abbildung 7-4 abgebildet und zeigt die Implementierung der ‚Löschung, Sperrung oder Änderung einer Position'. Im SAP System gibt es zwei Tabellen, in denen sämtliche Änderungen gespeichert werden: CDHDR und CDPOS. Die Tabelle CDPOS kann nur über die Tabelle CDHDR an die EKKO angebunden werden (mehrere Joins). Zusätzlich besteht der Select Teil aus einem Konditional, da es unterschiedliche Löscharten gibt. So kann eine Position komplett gelöscht, gesperrt oder zuerst gesperrt und dann gelöscht werden. Das SAP System löscht Daten nicht physisch, sondern versieht dieses mit einem Löschkennzeichen und verbirgt es auf der Benutzeroberfläche, weshalb eine Löschung aufgehoben werden kann. Auch eine Sperrung kann wieder aufgehoben werden. Benutzername und Sorting sind nicht zusammengesetzt und analog zur vorhergehenden Implementierung.

```
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
       EKPO_MANDT +  EKPO_EBELN + EKPO_EBELP AS CaeID,
       CASE WHEN CDPOS_VALUE_OLD = '' AND CDPOS_VALUE_NEW = 'L' THEN 'Position gelöscht'
              WHEN CDPOS_VALUE_OLD = '' AND CDPOS_VALUE_NEW = 'S' THEN 'Position gesperrt'
              WHEN CDPOS_VALUE_OLD = 'S' AND CDPOS_VALUE_NEW = 'L' THEN 'gesperrtes
Löschen'
              WHEN CDPOS_VALUE_OLD = 'L' AND CDPOS_VALUE_NEW = '' THEN 'Löschung
aufgehoben'
              WHEN CDPOS_VALUE_OLD = 'S' AND CDPOS_VALUE_NEW = '' THEN 'Sperrung
aufgehoben'
              ELSE  'Ändere Kennezeichen'
       END AS Activity,
       --CDHDR_UDATE As EventTime,
       dbo.GetTimeStamp(CDHDR_UDATE,CDHDR_UTIME) AS EventTime,
       60 AS Sorting,
       CDHDR_USERNAME AS EventUser
FROM CDPOS
JOIN EKPO ON
       CDPOS_TABKEY = EKPO_MANDT+EKPO_EBELN+EKPO_EBELP
JOIN CDHDR ON
       CDHDR_CHANGENR = CDPOS_CHANGENR
WHERE
       CDPOS_TABNAME = 'EKPO'
       AND CDPOS_FNAME = 'LOEKZ'
GO
```

Abbildung 7-4: Code Beispiel Löschkennzeichen setzen

Quelle: Eigene Darstellung

Das gesamte Skript für den ETL Prozess befindet sich im Anhang (Anhang G: Skripte zur Erstellung von Activity, Case und Process Tabelle). Ziel ist es möglichst alle für den Einkaufsprozess relevanten Prozessschritte zu extrahieren. Tabelle 26 zeigt alle hier implementierten Prozessschritte.

#	Sortierung	Name
1	10	Lege Bestellanforderung an
2	11	Ändere Bestellanforderung
3	20	Anfrage Anlegen (Noch keine Bestellung)
4	21	Anfrage Anlegen (Bestellung bereits durchgeführt)
5	22	Absagekennzeichen geändert
6	23	Angebot eingetragen/verändern
7	30	Anlegen Bestellposition
8	31	Bestellung Freigeben
9	32	Änderung Preis oder Menge in PO
10	33	Änderung Skonto
11	34	Ändere Einkaufsorganisation
12	35	Wechselkurs manuell angepasst
13	37	Lege Retouren Position an
14	38	Allgemeine Änderung in Einkaufsbelegkopf
15	39	Allgemeine Änderungen in Einkaufsbelegposition
16	40	Warenein- und Ausgang
17	41	Verschrottung von Produkten
18	42	Verkauf von Produkten aus Warenbestand
19	43	Dienstleistung erfassen
20	44	Dienstleistung abnehmen
21	50	Rechnungsein und –ausgang

22	51	Ändere Rechnungseingang
23	60	Löschen in PO
24	80	Rechnung bezahlt

Tabelle 26: Aktivitäten für Celonis Process Mining

Quelle: Eigene Darstellung

Für das anschließende Preprocessing stellt Celonis ein Skript bereit, welches die Fall- und Prozesstabelle erstellt (Stierle, 2015).

7.2.3.4 Konfiguration in Celonis Process Mining

Nach der Erstellung und Befüllung der entsprechenden Tabellen, muss in Celonis ein ‚Data Cube' erstellt werden. In der Benutzeroberfläche wird hierzu eine neue Datenquelle eingebunden und das Datenmodell eingerichtet (Stierle, 2015). Die Datenquelle dient als Verbindung zur Datenbank und ermöglicht über die ODBC Schnittstelle den Zugriff auf die Daten. Die drei zuvor erstellten Tabellen werden über Schlüsselattribute miteinander verbunden (vergl. Abbildung 7-5). Celonis bietet die Möglichkeit die entsprechenden Tabellen graphisch zu verknüpfen und somit das Datenmodell zu erstellen.

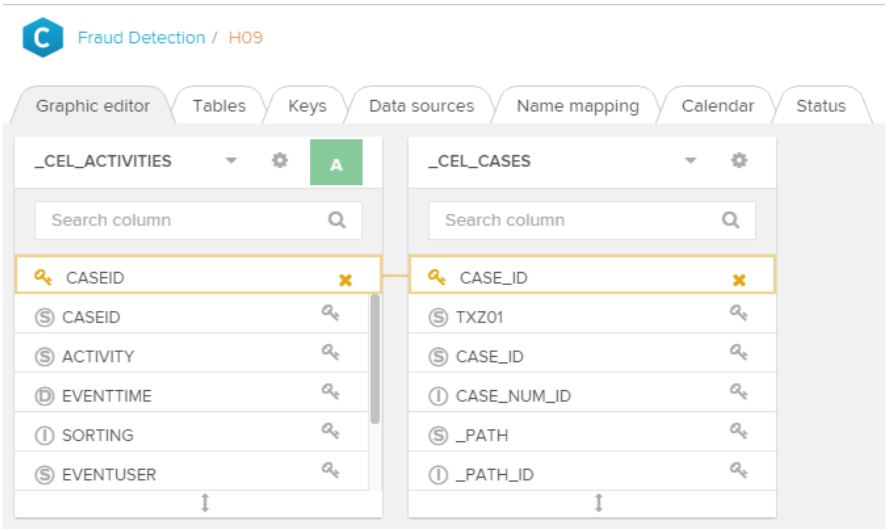


Abbildung 7-5: Konfiguration Celonis (Schlüssel definieren)

Quelle: Eigene Darstellung

Jetzt ist es bereits möglich den Prozess im Prozess Explorer zu analysieren (vergl. Abbildung 7-6).

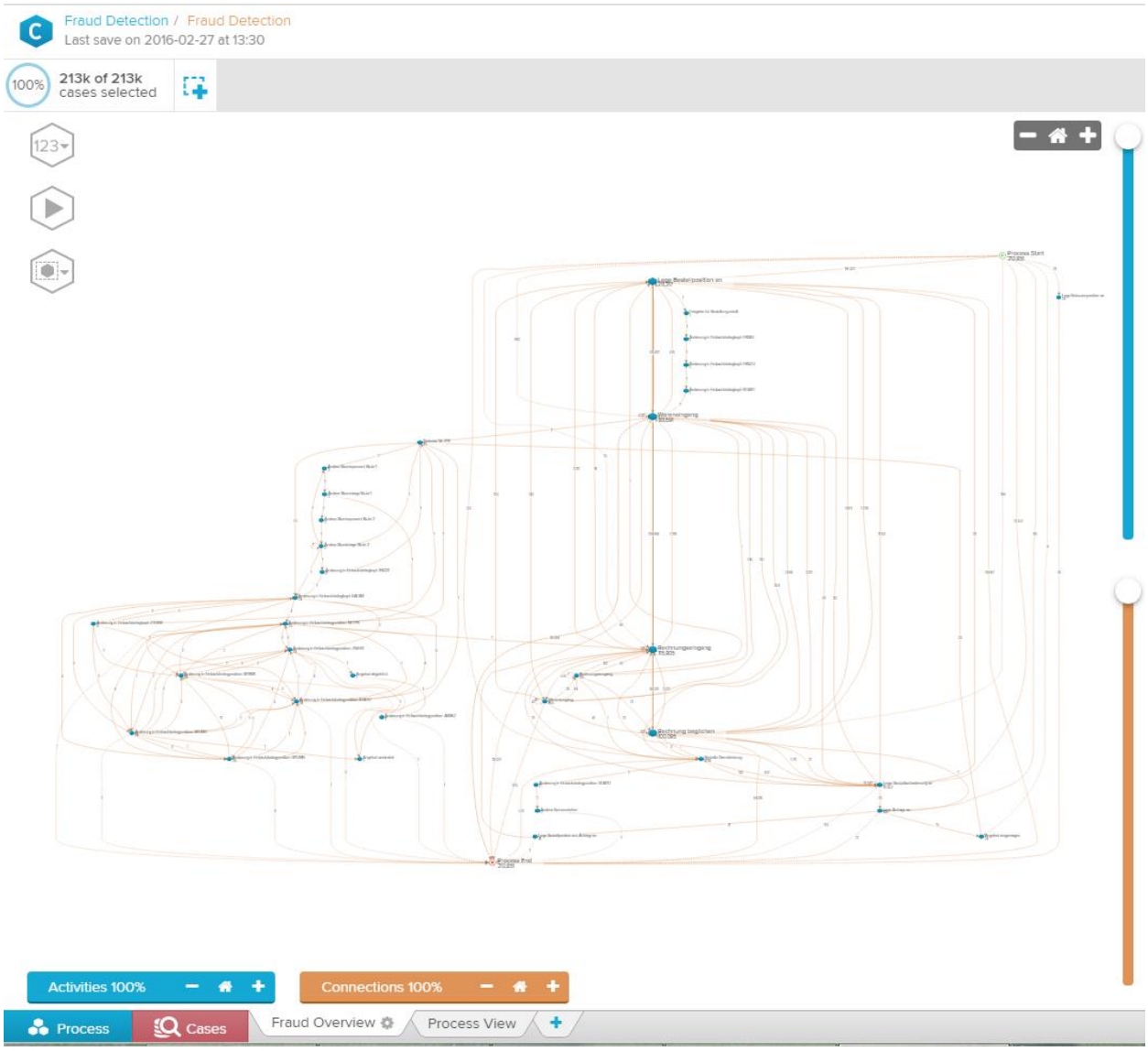


Abbildung 7-6: Identifizierte Prozessinstanzen im Datensatz

Quelle: Screenshot aus Celonis Process Mining

Abbildung 7-6 zeigt den gesamten Prozessverlauf mit allen Abweichungen. Jeder blaue Knoten stellt ein Prozessschritt dar, während jede Kante den Übergang von einem Prozessschritt zum nächsten darstellt. Man erkennt die Unübersichtlichkeit und die Schwierigkeit bei der Identifizierung von Fraud. Zur Vereinfachung wird die Prozessinstanz mit den vorgekommenen Red Flags verknüpft. Hierzu wird im Folgenden die Architektur des Prototyps und die Implementierung der Red Flags beschrieben.

7.2.4 Architektur des Prototypens

Bisher ist es möglich die Prozessinstanz darzustellen. Ziel dieser Dissertation ist verdächtige Instanzen des Einkaufsprozesses mitsamt dazugehöriger Red Flags und Fraud Patterns

darzustellen. Für die Datenanalyse bietet Celonis eine SQL ähnliche Sprache namens PQL an (Stierle, 2015). Zunächst wird versucht mit Hilfe dieser Abfragesprache Red Flags zu identifizieren. Da es allerdings nicht zu diesem Zweck entwickelt wurde, fehlen wichtige Funktionen, wie die Berechnung von Varianz oder Benford's Gesetzt. Da das Celonis PM Tool zusätzliche Datenbanktabellen einbinden und deren Inhalt darstellen kann, werden Red Flags auf Datenbankebene identifiziert und in entsprechend neue Tabellen gespeichert. Dazu wird ein SQL Skript entwickelt. Um die Red Flags entlang der Prozessinstanz anzeigen zu können, ist die eindeutige Zuordnung der identifizierten Red Flags zu einer Prozessinstanz wichtig. Durch das Filtern nach Red Flags oder Patterns wird die dazugehörige Prozessinstanz angezeigt. Umgekehrt werden bei der Filterung nach abweichenden Prozessinstanzen die zugehörigen Red Flags dargestellt.

Für die Suche der Red Flags muss das bestehende Datenmodell (Fall-, Aktivitäts- und Prozesstabelle) erweitert werden. Die hier vorgestellte Implementierung basiert auf der Arbeit von Alexander Gradischnig, der zu diesem Thema seine Masterarbeit verfasst hat (Gradischnig, 2015). Es gibt mehrere Möglichkeiten für die Erstellung der Red Flag Tabelle. So könnte die Falltabelle um eine Binärvariable (Flag/ kein Flag) ergänzt werden. Sobald ein bestimmtes Red Flag identifiziert wird, wird das Flag auf „wahr" gesetzt, alternativ auf „falsch". Der Vorteil dieser Variante ist die leichte Implementierung. Problematisch ist, dass nicht angezeigt wird, welches Red Flag angeschlagen ist. Als Lösung müsste für jedes mögliche Flag eine solche Spalte erstellt werden. Falls dieses vorkommt wird das Flag in der spezifischen Spalte auf „wahr" gesetzt, alternativ auf „falsch". Nachteil dieser Implementierung wäre das Entstehen einer sehr großen Bitmatrix, die unstabil bezüglich Änderungen im Prototyp wäre. Sobald weitere Red Flags hinzugefügt werden, muss die Tabelle geändert werden. Auch in der Anzeige ist eine solch große Tabelle unübersichtlich und hilft dem Auditor nur bedingt weiter. Außerdem ist der Link zur betroffenen Prozessinstanz so nicht möglich.

Ziel ist es zu jeder markierten Prozessinstanz die vorkommenden Red Flags anzuzeigen. Dazu wird eine externe Datenstruktur aufgebaut, die einfach im Celonis PM Tool angebunden werden kann. Die Architektur wird so gewählt, dass bei Ergänzung weiterer Red Flags oder Fraud Patterns die Tabellenstruktur nicht geändert werden muss. Abbildung 7-7 zeigt die implementierte Datenstruktur. Diese erweitert die vorgegebenen Tabellen um weitere vier Tabellen zur Erfassung und Auswertung von Red Flags und Fraud Patterns:

Flaged Cases: Haupttabelle zum Speichern von Red Flags. Wenn eine Transaktion einen Red Flag aufweist, wird dieses in dieser Tabelle vermerkt. Dazu wird die eindeutige CaseId und das erkannte Red Flag gespeichert. Diese Tabelle dient als Link zur Prozessinstanz, indem die eindeutige CaseID der Prozessinstanz gespeichert wird. Die FlagID kennzeichnet das Red Flag eindeutig und dient als Link zur Beschreibungstabelle ‚Red Flag Catalogue'.

Red Flag Catalogue: Der Red Flag Katalog enthält alle im System verfügbaren Red Flags mit einer eindeutigen Beschreibung des Red Flags. Soll der Prototyp mehrsprachig eingesetzt werden, kann hier die Beschreibung in verschiedenen Sprachen hinterlegt werden. Aktuell unterstützt es nur die deutsche Sprache.

Flag Categories: Jeder Red Flag gehört einer Überkategorie an. Dies kann dazu genutzt werden um Red Flags später zu Sortieren und gegebenenfalls zu Filtern.

Pattern Catalogue: Anstatt auf einzelne Red Flags, kann simultan nach zusammengehörigen Red Flags (s.g. Fraud Patterns) gefiltert werden. Der Patternkatalog enthält vorgefertigte Kombination von Red Flags.

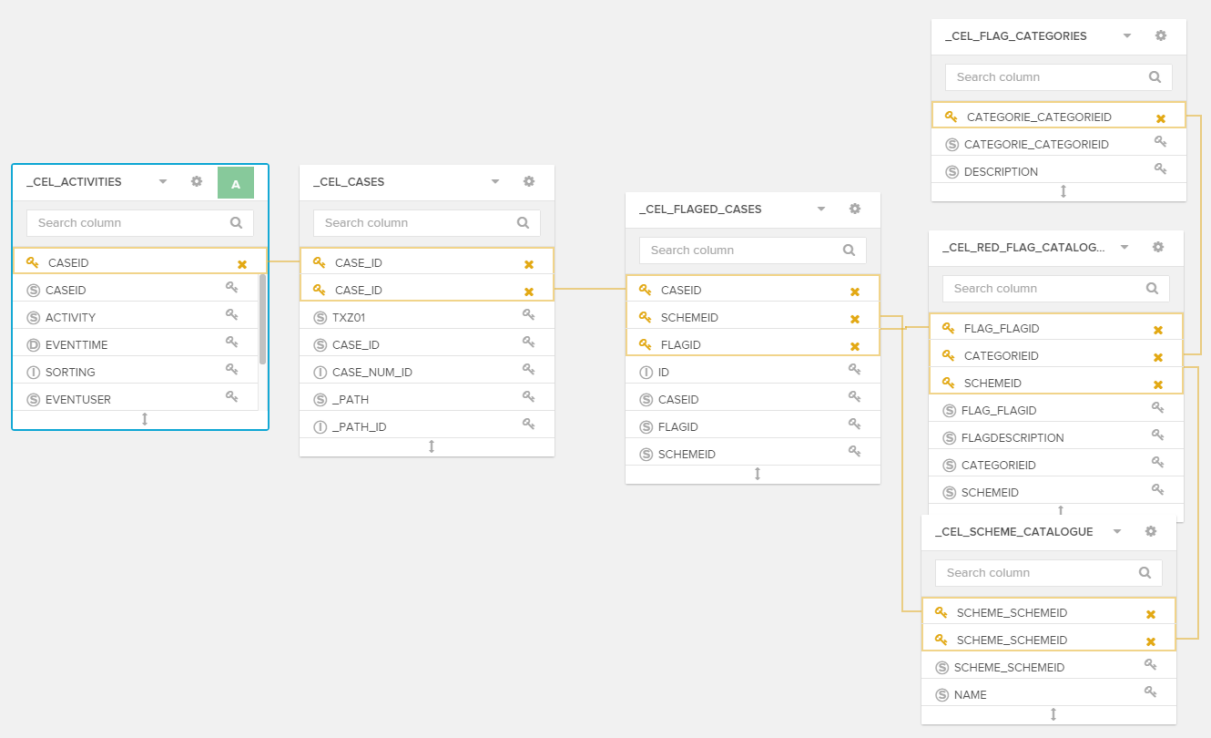


Abbildung 7-7: Implementierte Red Flag Architektur in Celonis

Quelle: Screenshot aus Celonis Process Mining

7.2.5 Datenanalyse und Prozessanalyse

Nach der Vorstellung der Prozessinstanz und Architektur wird im Folgenden die Implementierung von Red Flags und Fraud Patterns dargestellt. Albrecht et al. (2012) empfehlen hierfür die Erstellung eines SQL Skriptes. Dieses wird implementiert, um die in Kapitel 7.1.1 dargestellten Fraud Patterns und Red Flags im Datensatz zu identifizieren. Für jedes Fraud Pattern wird ein Skript erstellt, damit bei Identifikation weiterer Fraud Patterns die bestehende Implementierung nicht verändert, sondern um entsprechendes Skript ergänzt werden muss. Literatur[33] bezüglich der Implementierung von Fraud Patterns fehlt fast gänzlich. Auch gibt es wenige Hinweise in der Literatur, welche SAP Tabellen relevant für die Analyse sind. Deshalb ist in der Suchstrategie entsprechend viel Eigeninterpretation vorhanden.

An einigen Stellen sind Variablen nötig. Beispiele für Variablen sind Grenzen, ab wann eine Preiserhöhung signifikant ist. Diese Regeln sind für jedes Unternehmen anders und werden

[33] Quellen, die einige Hinweise zur Implementierung geben sind Wells (2011), Singh et al. (2011) oder Coderre (2009)

separat gepflegt. Zur Initialisierung des Prototypens werden diese Grenzwerte von den entsprechenden Auditoren gesetzt.

Der Prototyp enthält eine Initialisierungsphase, bei der der Auditor unternehmensspezifische Grenzen und Variablen einstellen kann, wie beispielsweise Genehmigungsstufen. Auch trifft der Auditor eine Auswahl von Red Flags pro Fraud Pattern, nach denen simultan im Datensatz gesucht wird. Eine Studie von Albrecht et al. (2012) hat ergeben, dass es keine aussagekräftigeren Red Flags als andere gibt. Diese hatten Auditoren nach der Wichtigkeit von Red Flags für die Identifikation von Fraud befragt. Jeder Auditor hat basierend auf seiner Erfahrung andere Red Flags bevorzugt und eine gemeinsame Schnittmenge konnte nicht gefunden werden. Die simultane Suche nach aller in der Literatur identifizierten Red Flags pro Fraud Patterns ist keine Lösung des Problems, da die Ergebnismenge verschwindend gering ist. Deshalb enthält der Prototyp eine Prozedur, bei der der Auditor basierend auf seiner Erfahrung Red Flags pro Fraud Pattern auswählen kann. Als Eingabe erwartet die Prozedur eine Liste aller Red Flags (Auswahl der Red Flags) und einen eindeutigen Namen des Patterns. Beispielsweise zeigt Abbildung 7-8, dass die Red Flags mit der ID Flag_E01, Flag_E02, Flag_E06 und Flag_E08 zum Szenario Angebotsmanipulation gehören. Bei der Suche nach dem Pattern Angebotsmanipulation, wird technisch nach allen Instanzen mit genannten Red Flags gesucht.

```
UPDATE _CEL_FLAGED_CASES SET SchemeId = 'E1-Bid Rigging'
WHERE
       CaseId IN
       (SELECT CaseId
       FROM IntersectFlagsTable('Flag_E1,Flag_E2,Flag_E6,Flag_E8'))
AND FlagId IN ('Flag_E1','Flag_E2','Flag_E6','Flag_E8');
```

Abbildung 7-8: Prozedur zur Auswahl von Red Flags in einem Fraud Pattern
Quelle: Eigene Darstellung

Im Folgenden wird beschrieben, wie die zuvor aus der Literatur identifizierten Fraud Patterns und Red Flags implementiert werden. Da Literatur zur Implementierung von Red Flags nur vereinzelt existiert, ist bei der Implementierung viel Interpretationsspielraum enthalten.

7.2.5.1 Kickback

Bei dem Pattern ‚Kickback' werden Aufträge an ein Unternehmen vergeben, das Produkte bzw. Dienste zu erhöhten Preisen anbietet. Im Gegenzug erhält ein korrupter Mitarbeiter eine Kickback Zahlung für die Genehmigung der Bestellung (Wells, 2011). Alle in Tabelle 27 dargestellten Red Flags werden implementiert, wobei die in Tabelle 28 gezeigten Grenzwerte und Variablen anzupassen sind.

FlagId	***Red Flag***	***Textuelle Suchstrategie***
Flag_D01	Trend zu einem favorisierten Lieferanten (Übermäßiger Bezug von Waren oder Dienstleistungen von einem Lieferanten)	Erstelle eine Tabelle, die das Verhältnis zwischen bestelltem Produkt zu Lieferanten abbildet. Suche anschließend Mitarbeiter aus, die mindestens FAVORITE_VENDOR_THRESHOLD (z.B. 75%) der Bestellungen bei einem Lieferanten durchführen.
Flag_D02	Überbezahlung der bezogenen Produkte oder	Erstelle eine Liste mit Durchschnittspreisen aller Materialien und suche anschließend Bestellungen, bei denen der

	Dienstleistungen (Einkäufe sind über dem Marktpreis)	Materialpreis weit vom Durchschnitt abweicht (Standardvarianz > Z_THRESHOLD).
Flag_D03	Höhere Einkaufsvolumina, die nicht mit höherer Geschäftsaktivität oder höherem Vorrat einhergehen (steigende Ausgaben für Waren und Dienstleistungen)	Erstelle eine Liste der monatlichen Bestellsummen und vergleiche diese mit den monatlichen Bestellsummen bei einem Lieferanten. Steigt der Anteil der Bestellsummen bei einem Lieferanten rasant an, so schlägt das Red Flag an.
Flag_D04	Plötzlich rasant steigende Einkäufe bei einem Lieferanten	Erstelle eine Tabelle mit den Bestellsummen pro Lieferant und vergleiche diese mit dem Vormonat/ Vorjahr/ Vorjahresmonat. Steigen diese über 15x an, so schlägt das Red Flag an.
[Flag_D05	Langsame Lieferung	Erstelle eine Tabelle mit der durchschnittlichen Lieferzeit pro Produkt und suche nach Bestellungen bei denen die Lieferzeit einen Threshold über dem Durchschnitt liegt.
Flag_D06	Mehrere kleine Bestellungen desselben Produkts (ein Einkauf wird in mehrere Teilkäufe unterteilt um den Genehmigungsprozess zu umgehen)	Erstelle eine Tabelle mit Bestellungen eines Tages und des gleichen Mitarbeiters, des gleichen Materials oder Lieferanten. Summiere diese auf und prüfe, ob diese über der Freigabegrenze liegen.
Flag_D07	Häufige Zahlungen des gleichen (runden) Betrages an einen Lieferanten	Erstelle eine Tabelle mit Lieferanten und Mitarbeitern, die runde Beträge haben und zähle wie oft ein runder Betrag bestellt wurde. Ein Betrag ist rund, wenn er beim Auf- und Abrunden gleich ist.
Flag_D08	Ungewöhnlich hohe Vorräte kombiniert mit entsprechenden Einkäufen von bestimmten Lieferanten (unnötig hohe/steigende Lagerbestände)	Erstelle eine Tabelle mit Einkaufsmengen für Waren pro Monat. Suche Bestellungen, bei denen im Vergleich zum Vormonat/Vorjahr/Vorjahresmonat eine dreifache Menge an Waren gekauft wurde.
[Flag_D09	Lieferant bietet keine üblichen Rabatte und Spezialangebote an	Suche nach Transaktionen, bei denen in den Tabellen KONH und KONP kein Rabatt vorgenommen wurde.]
Flag_D10	Geldtransaktionen zu unüblichen Zeiten/ Außerhalb der Geschäftszeit	Suche nach Transaktionen in einem bestimmten Zeitraum (z.B. 18 Uhr - 6 Uhr).
Flag_D11	Kein Wareneingangsbeleg	Suche nach bezahlten Rechnungen, für die kein Wareneingang verzeichnet wurde. Schließe dabei Dienstleistungen aus, da hier nicht zwingend ein Wareneingang verzeichnet wird.
Flag_D12	Ungewöhnliche Verkäufe an einen Kunden, der gleichzeitig ein Lieferant ist	Suche nach Lieferanten, die auch als Käufer aufgetreten sind.
Flag_D13	Lieferant, der regelmäßig schneller als die anderen Lieferanten entlohnt wird (Rechnungen die sehr schnell beglichen wurden)	Eine schnelle Begleichung einer Rechnung ist eine, die nach der Hälfte der ersten Skontozeit oder innerhalb eines Thresholds beglichen wird. Suche alle schnellen Rechnungsbegleichungen im Datensatz.
Flag_D14	Einkaufswert übersteigt den letzten Wert um einen signifikanten Wert	Erstelle eine Liste der Bestellungen, die die Gesamtsumme jeder Bestellung anzeigt. Suche nach vorhergehenden Bestellungen, deren Wert signifikant kleiner (Nettosumme sollte 3 mal so klein sein) ist und bei der es keine Bestellung dazwischen gibt.

Flag_D15	Zahlungen die den Durchschnitt für einen Lieferanten übersteigen	Erstelle eine Liste mit den durchschnittlichen Bestellmengen pro Lieferant und suche anschließend über die Z-Verteilung nach Abweichungen vom Durchschnitt.
Flag_D16	Nur ein kleiner Kreis an Lieferanten wird benutzt	Erstelle eine Liste, die die Anzahl der verschiedenen Lieferanten pro Material darstellt. Suche nach allen Mitarbeitern, die weniger als zwei Lieferanten pro Produkt enthalten.
Flag_D17	Zahlungen die den gesamten Durchschnitt übersteigen	Generiere eine Liste mit den Durchschnittssummen aller Bestellungen. Suche nach den Ausreißern über die Z-Verteilung.
Flag_D19	Manuelle Zahlungen	Suche nach Zahlungen, die nicht über den Zahlungslauf (sondern manuell) beglichen werden.
Flag_C04	Die selbe Rechnungsnummer mit zwei verschiedenen Belegnummern	Suche nach einer zweiten Rechnung mit selber Rechnungsnummer im selben Geschäftsjahr vom selben Lieferanten.
Flag_B01	Plötzliche Geschäftsaktivitäten mit alten „schlafenden“ Lieferanten	Suche Bestellungen, die an den gleichen Lieferanten gehen und bei denen die letzte Bestellung länger als ein bestimmter Zeitraum (TIME_THRESHOLD) zurückliegt. Stelle sicher, dass es bei diesem Lieferanten keine weiteren Bestellungen dazwischen gibt und der Lieferantenstammsatz vor dem gewählten TIME_THRESHOLD erstellt wurde.
Flag_B14	Hohe Einkaufsvolumina bei neuem bzw. unautorisierten Lieferanten	Suche alle Lieferanten, die eine Woche vor der Bestellung angelegt wurden und bei denen das Bestellvolumen höher als ORDER_THRESHOLD_STAGE2 ist.
[Flag_D18	Rechnung außerhalb von normalen Arbeitszeiten erfasst	Wähle alle Rechnungen, bei denen die Erstelluhrzeit nach 20 Uhr liegt.]
Flag_B11	Unklarer Bestellgrund oder wenige Details über die erhaltene Dienstleistung	Suche nach allen Bestellungen, bei denen das eingekaufte Material nicht mit einem Materialstamm verknüpft ist oder die Material bzw. Dienstleistungsbeschreibung unter einem Grenzwert (THRESHOLD_MATTXT = Anzahl der Zeichen des Materialkurztextes) liegt.
Flag_B13	[Ein Lieferant stellt nur Dienstleistungen in Rechnung	Erstelle eine Tabelle mit Lieferanten, bei denen nur Dienstleistungen bestellt wurden (Bestellmengeneinheit ist Leistungseinheit). Suche daraus alle Lieferanten, die eine Rechnung gestellt haben die entweder unter SERVICE_THRESHOLD_DOWN oder über SERVICE_THRESHOLD_UPPER liegen. Rechnungen unter der Freigabegrenze oder besonders hohe Rechnungen gelten als Auffällig.]
Flag_A02a	Lieferantenrechnung ist höher als Bestellbetrag	Vergleich den Betrag der Rechnung mit dem der Bestellung (in der gleichen Währung). Suche nach nicht übereinstimmenden Werten. Ist der Rechnungsbetrag höher, so schlägt Flag_A02a an. Umgekehrt schlägt Flag_A02b an.
Flag_A02b	Bestellbetrag ist höher als Rechnung	
Flag_B06	Einkäufe werden getätigt, bevor die Kaufanträge genehmigt sind	Suche nach Bestellungen, bei denen die Freigabe noch nicht erteilt wurde, aber schon ein Waren- oder Rechnungseingang existiert.
Flag_D20	Plötzlicher Lieferantenwechsel ohne nachvollziehbaren Grund (abweichend von der Materialfeldstrategie).	Suche nach Änderungen des Lieferanten bei Bestellanforderung, Bestellung oder Zahlung.
Flag_D21	Bestellung außerhalb der Einkaufsabteilung	Suche alle Bestellungen, bei dem der Benutzer nicht aus der Einkaufsabteilung kommt.

Tabelle 27: Implementierte Red Flags Überbezahlung

Quelle: Eigene Darstellung, tlw. basierend auf Gradischnig (2015)

Variablenname	Beschreibung	Standard	Quelle
SPENDING_THRESHOLD	Grenze ab wann eine Erhöhung signifikant ist	2 (doppelt)	(Singh et al., 2011)
ORDER_THRESHOLD_STAGE1	Grenze für erste Genehmigungsstufe	5000 (Währung)	
ORDER_THRESHOLD_STAGE2	Grenze für zweite Genehmigungsstufe	50000 (Währung)	
FAVOURITE_VENDOR_THRESHOLD	Welchen Anteil muss der Mitarbeiter bei einem Lieferanten haben, damit dieser sein Favorit ist	0.75	
MIN_ORDER_COUNT	Wie viele Bestellungen müssen bereits bei einem Lieferanten durchgeführt worden sein, um für einen übermäßigen Bezug von Waren bei einem Lieferanten relevant zu sein	10 (Anzahl)	
VENDOR_COUNT_THRESHOLD	Wie viele Lieferanten sollten für ein Produkt vorhanden sein	3 (Anzahl)	
Z_THRESHOLD	Signifikanz für Z-Wert	3	(Albrecht et al., 2012)

Tabelle 28: Variablen für Flags im Bereich Überbezahlung

Quelle: Eigene Darstellung, tlw. basierend auf Gradischnig (2015)

Bei einigen der Red Flags ist die Implementierung etwas schwieriger und wird daher im Folgenden kurz gesondert beschrieben.

Flag_D01(Trend zu einem favorisierten Lieferanten (Übermäßiger Bezug von Waren oder Dienstleistungen von einem Lieferanten)):

Alle zum Kickback Pattern gehörenden Red Flags basieren auf der Annahme, dass der bestellende Mitarbeiter eine Entlohnung, etwa in Form eines Gewinnanteils, für seine Käufe erhält. Das verleitet diesen unter Umständen dazu, häufiger bei dem auffälligen Lieferanten zu bestellen (Wells, 2004). Das in *Anhang H: Implementierung Fraud Patterns* gezeigte Skript versucht in mehreren Schritten diese Transaktionen ausfindig zu machen.

- Bilde eine temporäre Tabelle mit den totalen Bestellungen an einen Lieferanten pro Jahr
- Suche Lieferant/Mitarbeiter Kombination, welche für ein Jahr mehr als über dem Limit Einkäufe zusammen getätigt hat.
- Markiere alle Transaktionen dieses Lieferanten/Mitarbeiter-Paares dieses Jahres als auffällig

Um die Trefferquote dieses Skripts zu verändern, existieren zwei Stellschrauben: (1) Die Mindestanzahl der Bestellungen, die an einen Lieferanten getätigt werden und (2) ab welchem Prozentsatz die Bestellungen auffällig werden.

Das Skript könnte verändert werden, indem nicht die jährlichen, sondern die gesamten oder monatlichen Bestellungen überwacht werden. Zu bedenken ist jedoch, dass sich die Ergebnisse drastisch verändern können, weswegen hier der Mittelweg genutzt wurde. Bei einer Gesamtbetrachtung ist es deutlich schwieriger, den geforderten Prozentsatz zu erreichen. Im Gegensatz dazu ist der monatliche Grenzwert einfacher zu überspringen.

D16 – Nur wenige Lieferanten werden genutzt

Bei einem Kickback-Schema erhält der Mitarbeiter nur eine Gegenleistung, wenn tatsächlich neue Aufträge an den Fraud-Lieferanten übermittelt werden. Dies kann dazu führen, dass der betreffende Mitarbeiter Materialien häufig bei demselben Lieferanten einkauft (Lanza & Wells, 2003). Das Skript im *Anhang H: Implementierung Fraud Patterns* versucht diesen Sachverhalt zu erfassen. Für jedes Material wird die verwendete Anzahl an Lieferanten errechnet. Fällt diese Zahl unter einen Schwellenwert, wird dieses Material als auffällig gekennzeichnet.

7.2.5.2 Angebotsmanipulation

Nicht immer wird Ware direkt von einem Lieferanten bestellt. In einigen Fällen werden dafür Ausschreibungen gestartet, um Angebote von verschiedenen Lieferanten einzuholen. Die Gründe dafür können unterschiedlich sein. Entweder existiert noch kein bevorzugter Lieferant, da das Produkt zum ersten Mal bezogen wird oder man möchte den Markt neu sondieren. Auch gesetzliche Vorschriften (bspw. in der öffentlichen Verwaltung) können dazu führen, dass Ausschreibungen durchgeführt werden müssen. Unabhängig vom Grund für die Ausschreibung bleibt das Schema in seinen Grundzügen gleich. Die Firma holt bei mehreren Anbietern Angebote ein. Im normalen Ablauf wird nun das beste, beziehungsweise günstigste Angebot ausgewählt und bestellt. Ein korrupter Mitarbeiter kann diesen Prozess jedoch zu Gunsten eines bestimmten Anbieters steuern.

Für das Schema der Angebotsmanipulation muss der Mitarbeiter in den Biet-Prozess eingreifen. Dafür ergeben sich drei Zeitpunkte, die gesondert betrachtet werden können: (1) Die Erstellung des Angebots, (2) der Eingang der Angebote und (3) die Auswahl des besten Angebots (Wells, 2011).

In der Phase der Erarbeitung von Anforderungen für ein Angebot hat der Mitarbeiter zwei Möglichkeiten auf den Prozess Einfluss zu nehmen. Zuerst könnte der generelle Bedarf an das Produkt schlichtweg nicht vorhanden sein. Es wird also eine Angebotsrunde ausgelöst, obwohl kein Bedarf für dieses spezielle Produkt beziehungsweise Leistung besteht. Sollte der Bedarf echt sein, kann das Angebot jedoch so formuliert werden, dass nach Möglichkeit nur der bevorzugte Lieferant die Anforderungen erfüllen kann. Dazu werden beispielweise sehr spezifische Anforderungen gestellt. Auch kann der Auftrag in kleinere Einheiten unterteilt werden, da kleinere Aufträge oft unter eine Grenze fallen und ohne Ausschreibung vergeben werden können (Wells, 2011).

Nachdem die Anforderungen für den Auftrag erarbeitet und an potentielle Lieferanten verteilt werden, beginnt die Phase der Angebotserstellung durch die Zulieferer. Zu beachten ist, dass der Fokus hier auf interne Mitarbeiter und nicht auf den Bietenden liegt. Eine Möglichkeit die Gebotsabgabe zu beeinflussen ist beispielsweise durch Beschränkung des Bietzeitraums (Wells, 2011).

Für das Szenario der Angebotsmanipulation werden die in Tabelle 29 aufgeführten Red Flags implementiert. Wie bei dem vorhergehenden Pattern, können einige Variablen gesetzt werden, die in Tabelle 30 näher erklärt werden.

FlagId	*Red Flag*	*Textuelle Suchstrategie*
Flag_E01	Der Vertrag geht immer an das letzte Angebot einer Ausschreibung	Erstelle eine Liste aller abgegebenen Angebote mit ihrer Abgabezeit. Generiere das Abgabedatum aus der letzten Änderung des Produktpreises (nicht Feld IHRAN, da es nicht immer gesetzt ist). Erstelle eine temporäre Tabelle, die anzeigt, wie oft ein Lieferant den Zuschlag für eine Anfrage bekommen hat. Vergleiche die Anzahl der Zuschläge mit dem als letztes abgegebene Angebot. Übersteigt das Verhältnis einen bestimmten Wert wird der Lieferant als auffällig markiert.
Flag_E02	Dieselbe Person genehmigt den neuen Lieferanten und die Zahlungen an ihn	Vergleiche den Ersteller der Bestellung mit dem Benutzer, der den Lieferanten angelegt hat.
Flag_E03	Firmen haben die Möglichkeit ihr Angebot aufzustocken	Suche nach Anfragen, bei denen der Preis mehrfach geändert wird und der Preis anschließend niedriger ist.
Flag_E04	Die Angebotsphase ist sehr kurz	Suche nach Anfragen, bei denen die Angebotsphase kürzer als ein Threshold ist.
Flag_E05	Das Angebot ist sehr spezifisch/ sehr wenige Angebote	Suche nach Anfragen, bei denen die Anzahl der Angebote einen Threshold unterschreitet.
Flag_E06	Ausschreibungen werden stark geteilt	Erstelle eine Liste von Mitarbeitern, die mehrere Anfragen bei einem Lieferanten innerhalb eines kurzen Zeitraums haben. Suche darin als auffällig markierte Anfragen.
Frag_E07	Angebote liegen nah beieinander	Suche nach Angeboten, deren Varianz kleiner als 1 oder größer als -1 ist.
Flag_E08	Fiktionale Anbieter	Suche nach Lieferanten, deren Lieferantenstamm auffällig ist (keine Telefonnummer oder Anschrift, gleiche Anschrift wie Mitarbeiter). Suche nach Angeboten, die von diesem Lieferanten erstellt werden.
Flag_E09	Sehr weite Ausreißer	Erstelle eine Liste mit allen Durchschnittspreisen pro Anfrage. Suche über die Z-Verteilung nach Ausreißern.
Flag_E10	Waren werden eingekauft ohne konkurrenzfähige Angebote zu beachten	Suche nach Bestellungen über einen bestimmten Grenzwert (ab dem eine Anfrage gestellt werden müsste), bei der keine Anfrage für das gleiche Material bei dem gewählten Lieferanten innerhalb des letzten Monats existiert.
Flag_E11	Die geschätzten Kosten eines Auftrages sind knapp unter eine bestimmten Schwelle, damit sie nicht weiter überprüft werden	Suche nach Anfragen, bei der der geschätzte Bestellwert knapp unter der nötigen Freigabegrenze liegt.
Flag_E12	Lieferanten erhalten Zuschlag übermäßig oft	Erstelle eine Liste der gewonnenen Anfragen pro Lieferant. Suche nach überdurchschnittlich häufigen Bestellungen bei einem Lieferanten.
Flag_E13	Gleicher Lieferant bietet unter anderem Namen mehrfach	Prüfe ob eine Angebot eines Lieferanten existiert, der die gleichen Stammdaten wie ein anderer bietender Lieferant hat.
Flag_E14	Wenn ein neuer Lieferant der Auktion beitritt, beginnen die Angebotspreise zu fallen	Suche nach Anfragen, bei denen der Preis geändert wird und der Preis anschließend niedriger ist.

Flag_E15	Änderungen der Kostenspezifikationen nach Auftragsvergabe	Suche nach Anfragen, bei denen der Preis geändert wird, obwohl eine Bestellung existiert.
Flag_B08	Rechnungen für nicht gelieferte Waren/ Dienstleistungen	Suche nach Bestellungen von Waren (keine Dienstleistungen) zu denen es einen Rechnungseingang gibt, wo jedoch kein Wareneingang in der Bestellhistorie existiert.
Flag_E16	Angebote nach dem Ende der Angebotseinholungsphase akzeptiert	Suche nach existierenden Angeboten, die nach der entsprechenden Frist angenommen werden.
Flag_D02	Überbezahlung der bezogenen Produkte oder Dienstleistungen (Einkäufe sind über dem Marktpreis)	Erstelle eine Liste mit Durchschnittspreisen aller Materialien und suche anschließend Bestellungen, bei denen der Materialpreis weit vom Durchschnitt abweicht (Standardvarianz > Z_THRESHOLD).

Tabelle 29: Implementierte Red Flags für Ausschreibungsmanipulation

Quelle: Eigene Darstellung, tlw. basierend auf Gradischnig (2015)

Variablenname	Beschreibung	Standard	Quelle
BIDDING_PAPRTICIPANTS_THRESHOLD	Wie viele Teilnehmer muss eine Anfrage mindestens haben	3	
BiddingThreshold	Ab wann muss eine Anfrage ausgelöst werden	25000 (Währung)	
ORDER_THRESHOLD_STAGE1	Grenze für erste Genehmigungsstufe	5000 (Währung)	
ORDER_THRESHOLD_STAGE2	Grenze für zweite Genehmigungsstufe	50000 (Währung)	
ORDER_THRESHOLD	Grenze ab wann eine Erhöhung signifikant ist	2 (doppelt)	(Singh et al., 2011)
Z_THRESHOLD	Signifikanz für Z-Wert	3	(Albrecht et al., 2012)
BIDDING_DURATION_THRESHOLD	Wie lange sollte eine Angebotsphase mindestens dauern	5 (Wochen)	(Wells, 2011)

Tabelle 30: Variablen für Flags im Bereich Ausschreibungsmanipulation

Quelle: Eigene Darstellung

E1 – Letzter Bieter gewinnt

Meist werden Lieferanten insofern Vorteile eingeräumt, dass sie die Angebotsspezifikationen früher erhalten oder die Angebote der anderen Teilnehmer erfahren. So können sie das beste Angebot abgeben und den Zuschlag erhalten. Um alle Angebote der anderen Teilnehmer zu erfahren, müssen sie zwangsläufig als Letztes ihr Angebot einreichen (Wells, 2003a). Das Skript in *Anhang H: Implementierung Fraud Patterns* zeigt die Implementierung dieses Red Flags. Es ist in mehrere temporäre Tabellen aufgeteilt mit jeweils folgenden Funktionen:

- **SUBMISSION_TIME:** Erstellt eine Liste aller teilnehmenden Lieferanten einer Ausschreibung und wann das letzte Mal der Preis für das Angebot geändert wurde.
- **LAST_SUBMISSION**: Wählt für jede Anfrage den Lieferanten aus, der sein Angebot als Letztes abgegeben hat.
- **WON_SUBMISSIONS**: Erstellt eine Liste aller Lieferanten, die den Zuschlag für eine Anfrage erhalten haben

- **SUSPICIOUS_WIN_RATIO**: Ermittelt für jeden Lieferanten das Verhältnis der Anzahl an gewonnenen Ausschreibungen in Relation zur Anzahl der gewonnenen Ausschreibungen, in denen er als Letztes ein Angebot abgegeben hat. Übersteigt dieses Verhältnis einen gewissen Wert, werden die aus den Ausschreibungen resultierende Bestellungen für diesen Lieferanten markiert.

Ergebnisse dieser Abfrage sollten jedoch kritisch betrachtet werden, da die Ermittlung des letzten Gebots nicht einfach zu beantworten ist. Es existiert das SAP-Feld IHRAN, welches das Angebotsabgabedatum speichert. Auf das Datum allein kann jedoch keine totale Ordnung durchgeführt werden. In der hier vorliegenden Implementierung wird zusätzlich die genaue Uhrzeit der Angebotsabgabe berücksichtigt. Eine Erweiterung des Skriptes wäre, nur Angebote als wirklich letzte Angebote zu zählen, wenn sie eindeutig nach allen anderen eintreffen. Dies könnte beispielsweise bedeuten, dass am letzten Angebotstag nur ein Angebot eingehen darf, um das Red Flag auszulösen. In Zeiten von elektronischen Angebotsabgaben und direkter Vernetzung zwischen Lieferant und Einkäufer, ist es fraglich, ob die Ergebnisse dadurch eindeutiger und aussagekräftiger werden. Die Reaktionszeit ist gestiegen und ein Warten auf die postalische Zusendung des Angebotes ist nicht nötig.

E6 – Ausschreibung wird stark geteilt

Um bestimmten Lieferanten eine höhere Chance zur Gewinnung der Ausschreibung zu gewähren oder um bestimmte Grenzen nicht zu überschreiten, können Ausschreibungen geteilt werden. Dabei werden Aufträge einzeln ausgeschrieben, obwohl diese zusammen vergeben werden könnten (Wells, 2011). Es stellt sich Frage, wie aus den Daten auf eine Zugehörigkeit geschlossen werden kann, die nicht einfach verschleiert werden könnte. Eine statische Zahl, ab wann „zu viele“ Ausschreibungen abgegeben werden, ist sehr schwer festzulegen. Auch ein gleitender Durchschnitt liefert nur befriedigende Werte. Das Skript geht einen anderen Weg. Der Hintergrund der Teilung ist, möglichst viele kleine Aufträge demselben Lieferanten zuzuteilen. Das bedeutet jedoch auch, dass die Variabilität der in Frage kommenden Lieferanten für die Ausschreibung gering ist. Das Skript vergleicht nun genau diese beiden Zahlen. Gibt es einen Grund alle Anfragen an einen Lieferanten zu schicken oder für die starke Teilung einer Ausschreibung? Die Suchstrategie wurde in dem Skript *Anhang H: Implementierung Fraud Patterns* implementiert.

7.2.5.3 Scheinfirma

Scheinfirmen oder im englischen Shell Companies sind fiktive Unternehmen und werden gegründet, um einen glaubhaften Hintergrund zu schaffen. Oft haben diese Firmen keine physische Adresse und einen fiktiven Namen. Je besser die Geschichte hinter der Firma ist, desto glaubwürdiger ist es. Eine solche Scheinfirma benötigt ein Bankkonto, um Zahlungen entgegenzunehmen (Wells, 2011).

Ein mögliches Betrugsszenario mit einer Scheinfirma ist eine Rechnung ohne Gegenleistung. Dabei wird eine Bestellung für eine Ware oder Dienstleistung erstellt, die jedoch nie oder nur teilweise geliefert wird. Lediglich eine Rechnung wird versendet. Bei Dienstleistungen ist es schwer zu überprüfen, ob der volle Umfang der angebotenen Leistung erbracht wird (Wells, 2011).

Die dazugehörigen Red Flags mit einer textuellen Suchstrategie sind in Tabelle 31 dargestellt.. Die eigentliche Implementierung ist in *Anhang H: Implementierung Fraud Patterns* dargestellt.

FlagId	***Red Flag***	***Textuelle Suchstrategie***
Flag_B01	Plötzliche Geschäftsaktivitäten mit alten „schlafenden“ Lieferanten	Suche Bestellungen, die an den gleichen Lieferanten gehen und bei denen die letzte Bestellung länger als ein bestimmter Zeitraum (TIME_THRESHOLD) zurückliegt. Stelle sicher, dass es bei diesem Lieferanten keine weiteren Bestellungen dazwischen gibt und der Lieferantenstammsatz vor dem gewählten TIME_THRESHOLD erstellt wurde.
Flag_B02	Dieselbe Person erstellt einen neuen Lieferanten und eine Bestellung für diesen	Vergleiche den Ersteller der Bestellung mit dem Benutzer, der den Lieferanten angelegt hat.
Flag_B03	Eine Genehmigung wird oft vergessen/vernachlässigt	Suche nach Bestellungen, die keine Freigabestrategie haben, deren Bestellwert aber größer als ORDER_THRESHOLD_STAGE1 ist.
Flag_B04	Ungewöhnliche Genehmigungen	Erstelle eine Liste von Mitarbeitern, die an einem Tag überdurchschnittlich viele Bestellungen durchgeführt haben. Berechne hierzu die Durchschnittsbuchungen pro Tag im letzten Jahr. Das Red Flag schlägt an, wenn fünf Buchungen mehr als durchschnittlich durchgeführt werden.
Flag_B05	Einkäufer platzieren „dringende“ Aufträge	Bestellanforderung und Bestellung liegen sehr nahe bei einander. Vergleiche das Datum der Bestellanforderung mit dem Datum der Bestellung. Wenn dieser Wert höher als FAST_ORDER_THRESHOLD ist, dann setze bei dieser Bestellung ein Red Flag.
Flag_B06	Einkäufe werden getätigt, bevor die Kaufanträge genehmigt sind	Suche nach Bestellungen, bei denen die Freigabe noch nicht erteilt wurde, aber schon ein Waren- oder Rechnungseingang existiert.
Flag_B07	Exzessive Rechnungen von einem Lieferanten/steigende Anzahl Rechnungen	Erstelle eine Tabelle mit allen Rechnungen pro Lieferant pro Monat. Vergleiche innerhalb dieser Tabelle, ob im Vergleich zum Vormonat mehr Rechnungen als ein bestimmter Grenzwert (INVOICE_THRESHOLD) vorhanden sind.
Flag_B08	Rechnungen für nicht gelieferte Waren/ Dienstleistungen	Suche nach Bestellungen von Waren (keine Dienstleistungen) zu denen es einen Rechnungseingang gibt, wo jedoch kein Wareneingang in der Bestellhistorie existiert.
Flag_B09	Lieferanten ohne Festnetzanschluss oder nur mit Anrufbeantworter	Suche alle Instanzen, bei denen die Telefonnummer im Lieferantenstammsatz fehlt.
Flag_B10	Postfach als einzige Anschrift des Lieferanten oder Fehlende Kontaktdaten des Lieferanten	Suche alle Instanzen, bei denen in den Lieferantenstammdaten die Straße, Postleitzahl und Ort fehlen.
Flag_B11	Unklarer Bestellgrund oder wenige Details über die erhaltene Dienstleistung	Suche nach allen Bestellungen, bei denen das eingekaufte Material nicht mit einem Materialstamm verknüpft ist oder die Material bzw. Dienstleistungsbeschreibung unter einem Grenzwert (THRESHOLD_MATTXT = Anzahl der Zeichen des Materialkurztextes) liegt.
Flag_B12	Bestellsummen sind knapp unter dem Betrag, bei dem eine	Addiere alle Bestellpositionen, die zu einer Bestellung gehören und prüfe ob die Summe der Nettowerte zwischen 10-0.01 Währungseinheiten von

	Autorisierung der Ausgaben erforderlich ist	ORDER_THRESHOLD_STAGE1 oder ORDER_THRESHOLD_STAGE2 liegen.
Flag_B13	[Ein Lieferant stellt nur Dienstleistungen in Rechnung	Erstelle eine Tabelle mit Lieferanten, bei denen nur Dienstleistungen bestellt wurden (Bestellmengeneinheit ist Leistungseinheit). Suche daraus alle Lieferanten, die eine Rechnung gestellt haben die entweder unter SERVICE_THRESHOLD_DOWN oder über SERVICE_THRESHOLD_UPPER liegen. Rechnungen unter der Freigabegrenze oder besonders hohe Rechnungen gelten als Auffällig.]
Flag_B14	Hohe Einkaufsvolumina bei neuem bzw. unautorisierten Lieferanten	Suche alle Lieferanten, die eine Woche vor der Bestellung angelegt wurden und bei denen das Bestellvolumen höher als ORDER_THRESHOLD_STAGE2 ist.
Flag_B15	Fehlende ausgewiesene Steuer auf Rechnung	Suche nach Rechnungen, bei der der Steuerbetrag im Belegkopf null entspricht (keine Steuer ausgewiesen ist).
Flag_B16	Sequentielle Rechnungsnummern eines Lieferanten	Erstelle eine Hilfstabelle, die von allen Rechnungen die Rechnungsnummer und die logisch nächste Nummer enthält. Prüfe anschließend für jede Rechnungsnummer ob eine weitere Rechnung existiert, bei der die Rechnungsnummer der logisch nächsten entspricht.
Flag_B17	Name der Lieferfirma besteht ausschließlich aus Initialen	Lieferantenname unterschreitet eine Mindestlänge oder besteht aus vielen Punkten (A.B.C. Ldt.). Die Mindestlänge wird durch UPPER_LENGTH_THRESHOLD bestimmt.
Flag_B18	Stark steigende Einkäufe bei einem Lieferanten	Erstelle eine Hilfstabelle, die für jeden Lieferanten und Mitarbeiter die Anzahl der Bestellungen pro Monat speichert. Erstelle anschließend eine zweite Hilfstabelle, die alle Einträge enthält, bei denen im Vergleich zum Vormonat ORDER_THRESHOLD mal so oft bestellt wurde. (Beispielsweise doppelt so viele Bestellungen erstellt wurden).
Flag_B19	Rechnungen eines bestimmten Lieferanten kommen mehrmals im Monat, obwohl eine monatliche Bezahlung üblich wäre.	Suche nach Aufträgen die öfters als einmal im Monat eine Rechnung generieren. Erstelle hierzu zunächst eine Hilfstabelle, die alle Dienstleistungsbestellungen beinhaltet (Mengeneinheit = Leistungseinheit). Erstelle eine weitere Hilfstabelle, die alle Einträge beinhaltet, bei denen mehrere Rechnungseingänge für die gleiche Dienstleistung und den gleichen Lieferanten im Monat erstellt wurden.
Flag_B20	Lieferanteninformationen stimmen mit Informationen eines Mitarbeiters überein (Anschrift, Bankdaten usw.)	Vergleiche die Materialstammsätze der Mitarbeiter mit denen der Lieferanten. Prüfe dabei, ob die Straße, Postleitzahl und der Mandant identisch sind.
Flag_B21	Telefonnummern des Mitarbeiters und des Lieferanten stimmen überein	Ähnlich wie bei Flag_B20 werden die Materialstammsätze der Lieferanten und Mitarbeiter verglichen. Dabei wird überprüft, ob die Telefonnummern übereinstimmen. Es sind mehrere Spalten vorhanden, bei denen die Telefonnummer eingetragen werden kann, so dass für jede mögliche Kombination nach übereinstimmenden Telefonnummern gesucht wird.
Flag_B22	Keine oder falsche Mitarbeiter-ID in der Rechnung vorhanden (Lieferant ohne Steuernummer)	Erstelle eine Hilfstabelle, die alle Lieferanten enthält, bei denen die Umsatzsteuer-Identifikationsnummer oder Steuernummer fehlt. Suche anschließend alle Instanzen, bei denen Bestellungen bei diesem Lieferanten vorhanden sind.

Flag_B23	Rechnungen eines bestimmten Lieferanten wurden immer von demselben Mitarbeiter genehmigt	Suche alle Instanzen, bei denen die Rechnung eines Lieferanten nie von einer zweiten Person genehmigt wurde (ergo: bei denen es keine unterschiedlichen Benutzernamen der Mitarbeiter gibt).
Flag_B24	Ein Einkauf wird in mehrere Teilkäufe unterteilt um den Genehmigungsprozess zu umgehen	Erstelle eine Hilfstabelle, die alle Bestellungen enthält, die weniger als BIG_ORDER_THRESHOLD Tage auseinanderliegen. Prüfe zusätzlich ob die Summe der Bestellungen die Freigabegrenze ORDER_THRESHOLD_STAGE1 übersteigt.
Flag_B25	Rechnungen mit stets gleichen (meist runden) Rechnungsbeträgen	Erstelle eine Hilfstabelle, die alle Einkäufe beinhaltet, bei denen der auf- und abgerundete Betrag der Bestellung gleich ist. Zähle anschließend wie viele Rechnungen mit runden Beträgen pro Lieferant erstellt wurden. Suche nach Ausreißern mit Hilfe des Z-Wertes.
Flag_B26	[Aktionen wurden zu ungewöhnlichen Zeiten durchgeführt	Suche in der Änderungstabelle (CDPOS und CDHDR) nach allen Einträgen, bei denen es Inserts in einer für den Einkaufsprozess relevanten Tabelle innerhalb von UNCOMMON_TIME (z.B. 21:00-05:00 Uhr) gab.]
Flag_B27	Rechnungen, die sehr schnell beglichen werden	Suche alle Einträge, bei denen der Abstand zwischen der Erfassung und Bezahlung einer Rechnung zwischen 0 und der Hälfte der gewährten Skontozeit liegt.
Flag_B28	Einkaufswert übersteigt den letzten Wert um einen signifikanten Wert	Erstelle eine Liste der Bestellungen, die die Gesamtsumme jeder Bestellung anzeigt. Suche nach vorhergehenden Bestellungen, deren Wert signifikant kleiner (Nettosumme sollte 3 mal so klein sein) ist und bei der es keine Bestellung dazwischen gibt.
Flag_B29	Ungewöhnliche Bestellmengen von einem Lieferanten	Erstelle eine Tabelle, die die durchschnittlichen Bestellsummen pro Lieferant enthält. Suche anschließend alle Bestellungen, bei denen die Standardabweichung größer als Z_THRESHOLD ist.
Flag_B30	Einmallieferant wurde verwendet	Erstelle eine Hilfstabelle, die alle Bestellungen enthält, bei denen es keinen Lieferantenstammsatz gibt (also keine Einträge in der Lieferantenstammsatztabelle) und die über dem Wert NO_KNOWN_VENDOR liegen. Suche aus dieser Tabelle alle Prozessinstanzen.
Flag_B31	Mehrere Instanzen desselben Lieferanten innerhalb Lieferantenliste/-Datenbank (Lieferanten mit gleichem Namen, Telefonnummer oder Anschrift)	Suche alle Instanzen, bei denen eine Bestellung zu einem Lieferanten existiert, bei dem Name, Land, Postleitzahl und Ort mit einem anderen Lieferanten übereinstimmen und sich die eindeutige Lieferantennummer unterscheidet.
Flag_D02	Überbezahlung der bezogenen Produkte oder Dienstleistungen (Einkäufe sind über dem Marktpreis)	Erstelle eine Liste mit Durchschnittspreisen aller Materialien und suche anschließend Bestellungen, bei denen der Materialpreis weit vom Durchschnitt abweicht (Standardvarianz > Z_THRESHOLD).
Flag_B32	Keine Eingangsprüfung der Waren durch einen vom Einkauf unabhängigen Mitarbeiter	Suche nach Einträgen, bei denen kein Eintrag in der Wareneingangsprüfung vorhanden ist.
Flag_A02a	Lieferantenrechnung ist höher als Bestellbetrag	Vergleich den Betrag der Rechnung mit dem der Bestellung (in der gleichen Währung). Suche nach nicht übereinstimmenden Werten. Ist der Rechnungsbetrag höher, so schlägt Flag_A02a an. Umgekehrt schlägt Flag_A02b an.
Flag_A02b	Bestellbetrag ist höher als Rechnung	

Flag_B33	Bankkonto in steuerlich begünstigten Land	Als steuerlich begünstigte Länder[34] gelten Bahamas, Andorra, Monaco, Bulgarien, Panama, Mauritius, Dubai, Guernsey, Cayman Islands und Schweiz. Suche nach allen Lieferanten, die ihr Bankkonto in eines dieser Länder haben.

Tabelle 31: Implementierte Red Flags Scheinfirma

Quelle: Eigene Darstellung, tlw. basierend auf Gradischnig (2015)

Variablenname	Beschreibung	Standard	Quelle
TIME_THRESHOLD	Ab wie vielen Jahren ohne Geschäftsaktivität mit Lieferant ist eine erneute Aktivität suspekt.	1 (Jahre)	(Wells, 2002)
ORDER_THRESHOLD_STAGE1	Grenze für erste Genehmigungsstufe	5000 (Währung)	
ORDER_THRESHOLD_STAGE2	Grenze für zweite Genehmigungsstufe	50000 (Währung)	
FAST_ORDER_THRESHOLD	Ab wann gilt die Bestellung als "eilig"	1 (Tage)	
INVOICE_THRESHOLD	Grenze ab wann eine Erhöhung signifikant ist	2 (doppelt)	(Singh et al., 2011)
THRESHOLD_MATTXT	Ab wann ist der Materialtext zu kurz	6 (Anzahl Zeichen)	
SERVICE_THRESHOLD_DOWN	Kleine Dienstleistungsaufträge die normalerweise ohne zusätzliche Genehmigung durchgeführt werden können	5000 (Währung)	
SERVICE_THRESHOLD_UPPER	Sehr große Dienstleistungsaufträge	50000 (Währung)	
UPPER_LENGTH_THRESHOLD	Mindestanzahl an Buchstaben für einen Lieferant	3 (Anzahl Zeichen)	
ORDER_THRESHOLD	Grenze ab wann eine Erhöhung signifikant ist	2 (doppelt)	(Singh et al., 2011)
STANDARDABWEICHUNG	Standardabweichung für stets gleiche Beträge	10	
Z_THRESHOLD	Signifikanz für Z-Wert	3	(Albrecht et al., 2012)
UNCOMMON_TIME	Zeit, in der eine Geschäftsaktivität eher ungewöhnlich ist (bspw. Nachts)	21:00-5:00 Uhr	
BIG_ORDER_THRESHOLD	Grenze ab wann eine Erhöhung der Rechnungssumme im Vergleich zum Vormonat signifikant ist	2 (doppelt)	(Singh et al., 2011)
NO_KNOWN_VENDOR	Wie hoch darf die Bestellsumme maximal sein, damit ein Lieferant keinen Stammsatz benötigt	5000 (Währung)	

Tabelle 32: Variablen für Flags im Bereich Scheinfirma

Quelle: Eigene Darstellung

[34] Vergleich hierzu: https://www.finews.ch/news/finanzplatz/15984-steuerparadiese-steueroasen-tax-heaven-steuern-dubai-cayman-shcwiez-mauritius-bulgarien-panama-andorra

Auch hier werden etwas schwierigere zu identifizierende Red Flags gesondert beschrieben. Bei der Erstellung von kontinuierlich aufsteigenden Rechnungsnummern wird eine temporäre Hilfstabelle erstellt, die die aktuelle Rechnungsnummer und die aufsteigende Rechnungsnummer beinhaltet. Anschließend werden Rechnungspaare gesucht, bei denen zwei aufeinanderfolgende Rechnungen mit einem Eintrag in der Hilfstabelle übereinstimmen. Die hier vorgestellte Lösung unterstützt nur rein numerische Rechnungsnummern. Das Problem bei Rechnungsnummern mit Charakter und Zahlen ist die Ungewissheit, an welcher Stelle sich die aufsteigende Nummer befindet. Wird als Beispiel die Rechnung R12AB52 genommen, so kann die nächsthöhere Rechnungsnummer entweder R13AB52 oder R12AB53 sein. Um dieses Problem zu lösen, müsste eine Heuristik entwickelt werden, die für jeden Lieferanten die Aufzählungslogik berechnet.

Bei Flag_B25 sollen häufig (runde) gleiche Beträge erkannt werden, da Scheinfirmen häufig gleiche (runde) Beträge wählen (Langley, 2003). Runde Beträge sind dabei alle Bestellungen, bei denen der aufgerundete Bestellbetrag dem abgerundeten entspricht. Um kleine Ausreiser zu filtern, reicht es, wenn 10 der Bestellwerte gleich sind. Beträge die immer um den gleichen Wert schwanken werden durch die Standardabweichung identifiziert.

7.2.5.4 Doppelte Bezahlung

Bei der doppelten Bezahlung wird versucht, die Rechnung mehrfach auszubezahlen. Dabei geht die Zahlung meist doppelt an einen Komplizen des Mitarbeiters. Auch kann eine bereits bezahlte Rechnung erneut bezahlt werden. In Tabelle 33 werden die entsprechenden identifizierten Red Flags mit der entsprechenden Implementierungslogik dargestellt.

FlagId	***Red Flag***	***Textuelle Suchstrategie***
Flag_C01	Mehrere unterschiedliche Rechnungen für dieselbe Ware	Suche nach Rechnungen für dasselbe Produkt, die denselben Lieferanten und denselben Genehmiger haben und die innerhalb einer bestimmten Zeit (Variable: ABSTAND_RECHNUNGEN) erstellt wurden.
Flag_C02	Doppelte Angaben	Suche nach Bestellungen, die an verschiedene Lieferanten gehen, jedoch dieselbe Anschrift haben.
Flag_C03	Es wird der exakt selbe Einkaufswert gezahlt, jedoch an zwei verschiedene Lieferanten	Suche nach Rechnungen, die exakt gleiche Rechnungsbeträge haben, aber an verschiedene Lieferanten ausgezahlt wurden (innerhalb von 14 Tagen).
Flag_C04	Die selbe Rechnungsnummer mit zwei verschiedenen Belegnummern	Suche nach einer zweiten Rechnung mit selber Rechnungsnummer im selben Geschäftsjahr vom selben Lieferanten.
Flag_C05	Same-Same-Same Test	Gleiche Person, bezahlt den gleichen Lieferanten, am gleichen Tag, denselben Betrag.
Flag_C06	Same-Same-Different Test	Andere Person, bezahlt dem gleichen Lieferanten, am gleichen Tag, denselben Betrag.
Flag_C07	Gleiche Rechnungsnummer, gleicher Lieferant, anderer Betrag	Rechnungen mit der gleichen Referenzrechnungsnummer, selber Lieferant, aber der Rechnungsbetrag unterscheidet sich.

Flag_B10	Postfach als einzige Anschrift des Lieferanten oder Fehlende Kontaktdaten des Lieferanten	Suche alle Instanzen, bei denen in den Lieferantenstammdaten die Straße, Postleitzahl und Ort fehlen.
Flag_B20	Lieferanteninformationen stimmen mit Informationen eines Mitarbeiters überein (Anschrift, Bankdaten usw.)	Vergleiche die Materialstammsätze der Mitarbeiter mit denen der Lieferanten. Prüfe dabei, ob die Straße, Postleitzahl und der Mandant identisch sind.
Flag_D07	Häufige Zahlungen des gleichen (runden) Betrages an einen Lieferanten	Erstelle eine Tabelle mit Lieferanten und Mitarbeitern, die runde Beträge haben und zähle wie oft ein runder Betrag bestellt wurde. Ein Betrag ist rund, wenn er beim Auf- und Abrunden gleich ist.

Tabelle 33: Implementierung Red Flags doppelte Bezahlung

Quelle: Eigene Ergebnisse

Variablename	Beschreibung	Standard	Quelle
Abstand Rechnungen	Grenze ab wann zwei Rechnungen für das gleiche Produkt signifikant sind.	2	

Tabelle 34: Variablen für Flags im Bereich doppelte Bezahlung

Quelle: Eigene Darstellung, tlw. basierend auf (Gradischnig, 2015)

Bei Flag_C04 sollen Rechnungsnummern nicht doppelt vergeben werden, damit eine eindeutige Zuordnung möglich ist. Rechnungen können jedoch mutwillig doppelt in das System eingegeben werden, mit der Hoffnung, dass beide bezahlt werden (Lanza & Wells, 2003). Auf der Gleichheit der Referenzrechnungsnummern basiert das in *Anhang H: Implementierung Fraud Patterns* gezeigte Skript.

7.2.5.5 Pass-Through

In dem Schema Pass-Through kauft ein Komplize eine Ware oder Dienstleistung von einem Lieferanten ein und verkauft diese mit einem Zuschlag weiter. Die in der Literatur identifizierten Red Flags wurden entsprechend bei den zuvor beschriebenen Patterns implementiert, sodass sie an dieser Stelle wiederverwendet werden. Die Implementierung und Auswahl der Red Flags wird in Tabelle 35 beschrieben.

FlagId	*Red Flag*	*Textuelle Suchstrategie*
Flag_F01	Ungewöhnlich hohe Vorräte kombiniert mit entsprechenden Einkäufen von bestimmten Lieferanten (unnötig hohe/steigende Lagerbestände)	Erstelle eine Tabelle mit Einkaufsmengen für Waren pro Monat. Suche Bestellungen, bei denen im Vergleich zum Vormonat/Vorjahr/Vorjahresmonat eine dreifache Menge an Waren gekauft wurde.
Flag_F02	Höhere Einkaufsvolumina, die nicht mit höherer Geschäftsaktivität oder höherem Vorrat einhergehen (steigende Ausgaben für Waren und Dienstleistungen)	Erstelle eine Liste der monatlichen Bestellsummen und vergleiche diese mit den monatlichen Bestellsummen bei einem Lieferanten. Steigt der Anteil der Bestellsummen bei einem Lieferanten rasant an, so schlägt das Red Flag an.
Flag_F03	große Budgetabweichungen	Die Abteilung gibt über den Monat/Jahr gesehen mehr Geld aus als ihm Vorjahre(Monat). Summiere alle Bestellung einer Abteilung/Einkäufergruppe/Einkäufer über den Monat und vergleiche dies mit dem Vormonat. Erstelle hierfür eine Liste aller Nettobestellungen eines Mitarbeiters

		pro Monat. Vergleiche diese mit den Bestellungen des Vormonats. Wenn der Wert über dem zuvor definierten SPENDING_THRESHOLD liegt, so kommt es zu einer großen Budgetabweichung.
Flag_F04	Bestellsummen sind knapp unter dem Betrag, bei dem eine Autorisierung der Ausgaben erforderlich ist	Addiere alle Bestellpositionen, die zu einer Bestellung gehören und prüfe ob die Summe der Nettowerte zwischen 10-0.01 Währungseinheiten von ORDER_THRESHOLD_STAGE1 oder ORDER_THRESHOLD_STAGE2 liegen.
Flag_F05	Überbezahlung der bezogenen Produkte oder Dienstleistungen (Einkäufe sind über dem Marktpreis)	Erstelle eine Liste mit Durchschnittspreisen aller Materialien und suche anschließend Bestellungen, bei denen der Materialpreis weit vom Durchschnitt abweicht (Standardvarianz > Z_THRESHOLD).
Flag_F06	Hohe Einkaufsvolumina bei neuem bzw. unautorisierten Lieferanten	Suche alle Lieferanten, die eine Woche vor der Bestellung angelegt wurden und bei denen das Bestellvolumen höher als ORDER_THRESHOLD_STAGE2 ist.
Flag_C04	Die selbe Rechnungsnummer mit zwei verschiedenen Belegnummern	Suche nach einer zweiten Rechnung mit selber Rechnungsnummer im selben Geschäftsjahr vom selben Lieferanten.
Flag_C05	Same-Same-Same Test	Gleiche Person, bezahlt den gleichen Lieferanten, am gleichen Tag, denselben Betrag
Flag_C06	Same-Same-Different Test	Andere Person, bezahlt dem gleichen Lieferanten, am gleichen Tag, denselben Betrag

Tabelle 35: Implementierung Red Flags Pass Through

Quelle: Eigene Darstellung

7.2.5.6 Unbeteiligter Lieferant

Bei dem Schema unbeteiligter Lieferant werden Waren von einem rechtmäßigen Lieferanten eingekauft. Ein Mitarbeiter sorgt anschließend dafür, dass die korrekte Rechnung „versehentlich“ überbezahlt oder doppelt bezahlt wird. Vom rechtmäßigen Lieferanten wird „aufgrund eines Fehlers“ eine Rückzahlung gefordert, dem der Lieferant entsprechend nachgeht. Bevor das Geld das empfangene Unternehmen erreicht, wird die Zahlung abgefangen (Wells, 2013). Die entsprechenden Red Flags und ihre Implementierungsstrategie sind in Tabelle 36 dargestellt.

FlagId	***Red Flag***	***Textuelle Suchstrategie***
Flag_G01	Rückgaben von Waren	Suche nach allen Transaktionen, bei denen Ware storniert wird und ein Warenausgang existiert.
Flag_G02	Suspekte Anschrift des Lieferanten: gleiche Adresse wie ein anderer Lieferant	Vergleiche die Materialstammsätze der Mitarbeiter mit denen der Lieferanten. Prüfe dabei, ob die Straße, Postleitzahl und der Mandant identisch sind.
Flag_G03	Lieferantenrechnung ist höher als Bestellbetrag	Vergleich den Betrag der Rechnung mit dem der Bestellung (in der gleichen Währung). Suche nach nicht übereinstimmenden Werten. Ist der Rechnungsbetrag höher, so schlägt Flag_A02a an.
Flag_G05	Überbezahlung der bezogenen Produkte oder Dienstleistungen (Einkäufe sind über dem Marktpreis)	Erstelle eine Liste mit Durchschnittspreisen aller Materialien und suche anschließend Bestellungen, bei denen der Materialpreis weit vom Durchschnitt abweicht (Standardvarianz > Z_THRESHOLD).

Flag_G06	Rechnung außerhalb von normalen Arbeitszeiten erfasst	Wähle alle Rechnungen, bei denen die Erstelluhrzeit nach 20 Uhr und vor 6 Uhr liegt.]
Flag_G07	Mehrere unterschiedliche Rechnungen für dieselbe Ware	Suche nach Rechnungen für dasselbe Produkt, die denselben Lieferanten und denselben Genehmiger haben und die innerhalb einer bestimmten Zeit (Variable: ABSTAND_RECHNUNGEN) erstellt wurden.
Flag_G08	Hohe Einkaufsvolumina bei neuem bzw. unautorisierten Lieferanten	Suche alle Lieferanten aus, die eine Woche vor der Bestellung angelegt wurden und bei denen das Bestellvolumen höher als ORDER_THRESHOLD_STAGE2 ist.
Flag_G09	Es wird der exakt selbe Einkaufswert gezahlt, jedoch an zwei verschiedene Lieferanten	Suche nach exakt gleichen Rechnungsbeträgen und prüfe, ob diese an verschiedene Lieferanten gehen.
Flag_A04	Kurzfristige Änderungen der Lieferantenstammdaten	Suche nach Änderungen, bei denen sich die Kontonummer oder Bankleitzahl geändert hat.

Tabelle 36: Implementierung Red Flags unbeteiligter Lieferant
Quelle: Eigene Darstellung

7.2.5.7 Rechnungsmanipulation

Bei der Rechnungsmanipulation werden legitime Transaktionen so manipuliert, dass die Zahlung auf das Konto des Täters oder seinem Komplizen landet. Dabei muss der Mitarbeiter die Berechtigung haben Stammdaten des Lieferanten (v.a. seine Kontonummer) zu verändern. Nach der Überweisung versucht der Täter meist seine Spuren zu verwischen, indem er bspw. Kontonummernänderungen rückgängig macht oder den Lieferanten komplett löscht. Wells (2011) teilt Rechnungsmanipulation in fünf Bereiche ein: (1) Scheck Fälschung; (2) Gefälschte Auszahlung; (3) Änderung des Empfängers; (4) Gefälschte Rechnung und (5) Selbst ausgestellte Rechnung. In dieser Dissertation werden keine physischen Dokumente untersucht und nur im ERP System erkennbare Red Flags betrachtet. Tabelle 37 zeigt alle identifizierten Red Flags mit ihrer Suchstrategie.

FlagId	***Red Flag***	***Textuelle Suchstrategie***
Flag_A01	Große Budgetabweichungen (Die Abteilung gibt über den Monat oder das Jahr gesehen mehr Geld aus, als im vorherigen Monat oder Jahr)	Erstelle eine Liste aller Nettobestellungen eines Mitarbeiters pro Monat. Vergleiche diese mit den Bestellungen des Vormonats bzw. Vorjahres. Wenn die Abweichung höher als SPENDING_THRESHOLD ist, so kommt es zu einer großen Budgetabweichung.
Flag_A02a	Lieferantenrechnung ist höher als Bestellbetrag	Vergleich den Betrag der Rechnung mit dem der Bestellung (in der gleichen Währung). Suche nach nicht übereinstimmenden Werten. Ist der Rechnungsbetrag höher, so schlägt Flag_A02a an. Umgekehrt schlägt Flag_A02b an.
Flag_A02b	Bestellbetrag ist höher als Rechnung	
Flag_A03	Anpassungen der Verbindlichkeiten (in der Kreditorenbuchhaltung)	Suche nach Änderungskennzeichen bei der Rechnung in den Änderungstabellen (CDHDR und CDPOS).
Flag_A04a	Lieferantenstammsatz wird für die Bezahlung geändert	Suche in den Änderungstabellen (CDHDR und CDPOS) nach Änderungen von Kontonummer oder Bankleitzahl bei einem Lieferanten.

Flag_A04b	Lieferantenstammsatz wird für die Bezahlung geändert	Die Kontonummer wird im Vergleich zu Flag_A4a wieder vom selben Benutzer innerhalb eines bestimmten Zeitraums zurück geändert.
Flag_A05	Es wird ein Zahlungsempfänger eingetragen der einen sehr ähnlichen Namen wie ein anderer hat	Verwende Zahlungsempfänger mit dem Levenshtein Algorithmus, um ähnlich klingende Namen zu identifizieren.
Flag_A06	Ändern der Währung zwischen Einkauf und Bezahlung, um etwaige Umrechnungsdifferenzen auszunutzen	Es sollen Rechnungen identifiziert werden, die eine andere Währung als die Währungseinheit in der Bestellung haben.
Flag_A07	Doppelte Angaben (Eine Anschrift wird von mehreren Lieferanten verwendet)	Erstelle eine Liste mit Lieferanten, die die gleiche Lieferantennummer und den gleichen Namen haben, bei denen die Adressdaten jedoch unterschiedlich sind. Suche anschließend nach Bestellungen bei diesen Lieferanten.
Flag_A08	Verdopplung und Umleitung einer Rechnung	Suche nach Rechnungen, die die gleichen Rechnungsnummern und den gleichen Rechnungsbetrag haben, bei denen aber verschiedene Lieferanten beteiligt sind.
Flag_A09	Gleiche Rechnungsnummer, gleicher Lieferant anderen Betrag	Suche nach Rechnungen, die die gleiche Rechnungsnummer haben und denselben Lieferanten haben, bei denen aber ein anderer Rechnungsbetrag vorliegt.
Flag_A10	Mehrere Änderungen des Bestellwerts	Suche nach Änderung des Bestellwerts in den Änderungstabellen (CDHDR und CDPOS).
Flag_A11	Lieferanten ohne Bankkonto und mit Cash Bezahlung	Suche nach allen Lieferanten, bei denen keine Bankleitzahl vorhanden ist.

Tabelle 37: Variablen für Flags im Bereich Rechnungsmanipulation

Quelle: Eigene Darstellung

Die dazugehörigen durch den Auditor einstellbaren Werte sind in Tabelle 38 dargestellt.

Variablenname	Beschreibung	Standard	Quelle
SPENDING_THRESHOLD	Vergleich der Ausgaben von Vormonat. Grenze ab wann eine Erhöhung signifikant ist	2 (doppelt)	(Singh et al., 2011)

Tabelle 38: Variablen für Flags im Bereich Rechnungsmanipulation

Quelle: Eigene Darstellung

An dieser Stelle soll kurz auf Besonderheiten bei der Implementierung eingegangen werden. Bei Flag_A05 wird nach ähnlich klingenden Wörtern gesucht, die durch den Levenshtein Algorithmus identifiziert werden. Dieser berechnet die Übereinstimmung zweier Eingabewerte anhand der benötigten Veränderungen, um von dem einen auf den anderen Eingabewert zu gelangen (Myka & Güntzer, 1996). Soundex hingegen verwendet ein phonetisches Verfahren, welches ähnlich klingende Buchstaben miteinander vergleicht. Eine Implementierung des Levenshtein Algorithmus ist in Hatchett (2014) dargestellt und dient hier als Grundlage der Implementierung des Flags.

7.2.5.8 Private Einkäufe

Private Einkäufe sind Einkäufe auf Kosten des Unternehmens, die für den privaten Gebrauch bestimmt sind. Dabei kann der Täter die Einkäufe entweder behalten, auf sekundäre Tauschbörsen veräußern oder eine Rücklieferung veranlassen, um die Erstattung einzustreichen. Auch hier werden einige der entsprechenden Red Flags wiederverwendet. Eine Übersicht zeigt Tabelle 39.

FlagId	***Red Flag***	***Textuelle Suchstrategie***
Flag_H01	Rechnungseingang, obwohl die Bestellanforderung geblockt wurde	Suche nach allen Bestellanforderungen, zu denen ein Rechnungseingang existiert, aber die Bestellanforderung blockiert ist (das Feld BLCKD nicht leer ist).
Flag_H02	Rechnungseingang, obwohl die Bestellanforderung nicht genehmigt wurde	Suche nach Rechnungen, bei denen das Genehmigungsfeld der Bestellanforderung leer ist, obwohl die Rechnungssumme über der genehmigungspflichtigen Grenze liegt.
Flag_H03	Rechnungen, Eingangsbestätigungen und Bestelldokumente nicht übereinstimmend	Suche nach Rechnungen, bei denen die Rechnungssumme und –menge nicht mit der Bestellsumme und –menge übereinstimmt.
Flag_B04	Ungewöhnliche Genehmigungen	Erstelle eine Liste von Mitarbeitern, die an einem Tag überdurchschnittlich viele Bestellungen durchgeführt haben. Berechne hierzu die Durchschnittsbuchungen pro Tag im letzten Jahr. Das Red Flag schlägt an, wenn fünf Buchungen mehr als durchschnittlich durchgeführt werden.
Flag_B11	Unklarer Bestellgrund oder wenige Details über die erhaltene Dienstleistung	Suche nach allen Bestellungen, bei denen das eingekaufte Material nicht mit einem Materialstamm verknüpft ist oder die Material bzw. Dienstleistungsbeschreibung unter einem Grenzwert (THRESHOLD_MATTXT = Anzahl der Zeichen des Materialkurztextes) liegt.
Flag_B12	Bestellsummen sind knapp unter dem Betrag, bei dem eine Autorisierung der Ausgaben erforderlich ist	Addiere alle Bestellpositionen, die zu einer Bestellung gehören und prüfe ob die Summe der Nettowerte zwischen 10-0.01 Währungseinheiten von ORDER_THRESHOLD_STAGE1 oder ORDER_THRESHOLD_STAGE2 liegen.
Flag_B22	Keine oder falsche Mitarbeiter-ID in der Rechnung vorhanden (Lieferant ohne Steuernummer)	Erstelle eine Hilfstabelle, die alle Lieferanten enthält, bei denen die Umsatzsteuer-Identifikationsnummer oder Steuernummer fehlt. Suche anschließend alle Instanzen, bei denen Bestellungen bei diesem Lieferanten vorhanden sind.
Flag_C05	Same-Same-Same Test	Gleiche Person, bezahlt den gleichen Lieferanten, am gleichen Tag, denselben Betrag.
Flag_C06	Same-Same-Different Test	Andere Person, bezahlt dem gleichen Lieferanten, am gleichen Tag, denselben Betrag.
Flag_D02	Überbezahlung der bezogenen Produkte oder Dienstleistungen (Einkäufe sind über dem Marktpreis)	Erstelle eine Liste mit Durchschnittspreisen aller Materialien und suche anschließend Bestellungen, bei denen der Materialpreis weit vom Durchschnitt abweicht (Standardvarianz > Z_THRESHOLD).

Flag_D06	Mehrere kleine Bestellungen desselben Produkts (ein Einkauf wird in mehrere Teilkäufe unterteilt um den Genehmigungsprozess zu umgehen)	Erstelle eine Tabelle mit Bestellungen eines Tages und des gleichen Mitarbeiters, des gleichen Materials oder Lieferanten. Summiere diese auf und prüfe, ob diese über der Freigabegrenze liegen.

Tabelle 39: Implementierung Red Flags Private Einkäufe
Quelle: Eigene Darstellung

7.2.6 Abgleich der Implementierung mit identifizierten Anforderungen

Abschließend wird geprüft, in wieweit die zuvor identifizierten Anforderungen an den Prototyp umgesetzt werden können:

- Identifikation von Prozessabweichungen. Dabei sollen auffällige Kombinationen von Nutzerverhalten erkannt und Prozessabweichungen analysiert werden.

Auffällige Kombinationen von Nutzerverhalten werden durch die Implementierung der aus der Literatur identifizierten Red Flags und Fraud Patterns erkannt. Prozessabweichungen können im Process Explorer von Celonis analysiert werden. Hierzu wurden die Daten des ERP Systems in ein Process Mining lesbares Format gebracht, indem Fall-, Aktivitäts- und Prozesstabellen erstellt wurden.

- Benutzeroberfläche: Die Benutzeroberfläche sollte wie bei Singh et al. (2013) modular aufgebaut sein. Diese haben in ihrer Umfrage gezeigt, dass ein modularer Aufbau von Auditoren bevorzugt wird. Ein Dashboard soll eine Übersicht anzeigen, während weitere Informationen auf Tabs aufgeteilt werden.

Die Benutzeroberfläche wird im Kapitel 7.4 separat erstellt.

- Zusätzliche Informationen: Process Mining sollte mit zusätzlichen Informationen angereichert werden. Dies sind bestenfalls Informationen aus dem SAP System.

Celonis Process Mining ermöglicht die Darstellung weiterer Daten in der Benutzeroberfläche. Neben der reinen Prozessdarstellung werden auch zugehörige Red Flags und Fraud Patterns angezeigt. In Kapitel 7.4 werden Anforderungen zur Anzeige weiterer Informationen im Dashboard gesammelt und diese entsprechend implementiert.

- Datenanalysen sind ein wichtiger Bestandteil des Audits. Deshalb sollen im gesamten Auditprozess Daten analysiert werden.

Im gesamten Auditprozess werden Daten aus einem ERP System in einer graphischen Benutzeroberfläche analysiert.

- Datenextraktion sollte ein kleiner Bestandteil der Analyse sein und möglichst wenig Zeit in Anspruch nehmen.

Sind die Quelldaten in einer SAP HANA Datenbank gespeichert, so ist keine Datenextraktion notwendig. Daten werden standardmäßig bei einem SAP ERP on HANA oder bei einer S/4 HANA in der unterliegenden HANA Datenbank gesichert. Lediglich die entsprechenden Fall-, Aktivitäts- und Prozesstabellen müssen erstellt werden. Hierzu werden die Informationen aus

den Tabellen des Quellsystems in die entsprechenden Tabellen kopiert. Das Skript zur Erkennung von Red Flags und Fraud Patterns kann direkt auf der HANA Datenbank ausgeführt werden, benötigt jedoch Rechte auf die entsprechenden Datenbanktabellen.

- Regionale Besonderheiten, wie bspw. verschiedene Zeichensatztabellen oder unterschiedliche Währungen, sollen berücksichtigt werden.

Es wird die entsprechende Währung aus dem SAP ERP System angezeigt. Eine Währungsumrechnung ist nicht implementiert. Eine Zeichensatztabelle kann im Celonis Process Mining Prototyp nur pro Tabelle definiert werden.

- Auditoren sollen auf das Tool von überall in der Welt zugreifen können, ohne zusätzliche Software installieren zu müssen.

Celonis Process Mining ist in einem Webbrowser lauffähig. Dadurch ist bei einer Client Server Installation ein weltweiter Zugriff auf die Daten möglich, ohne zusätzliche Tools zu installieren. Auch die SAP HANA Datenbank ist über den Webbrowser erreichbar und Datenbankabfragen und –manipulationen können dort durchgeführt werden

- Zugriff auf die Daten einer bestimmten Entität sollen nur autorisierten Auditoren (Auditoren, die dieses Audit durchführen) gegeben werden.

Celonis hat ein Berechtigungskonzept implementiert, welches den Zugriff auf bestimmte Analysen nur berechtigten Personen ermöglicht. Es wird das Autorisierungskonzept von Celonis Process Mining übernommen.

- Komplexe Analysen auf großen Datenvolumen sollen in angemessener Zeit durchgeführt werden können.

Die Suche nach Red Flags wird auf Datenbankebene durchgeführt. Durch die Verwendung einer In-Memory Datenbank wird eine „angemessene“ Zeit erreicht. Die Nutzung des Fuzzy Mining Algorithmus ermöglicht die performante Rekonstruktion der Prozessinstanzen.

- Die Ergebnisse der Analyse sollen graphisch dargestellt werden, so dass Auditoren wirtschaftskriminelle Handlungen ohne IT Erfahrung erkennen.

Ein Dashboard wird in Kapitel 7.4 implementiert und ermöglicht die Erkennung von wirtschaftskriminellen Handlungen ohne IT Erfahrung.

- Bei großer Datenbasis sollen nur die wahrscheinlichsten Fälle dargestellt werden, um die Datenbasis für den Auditor zu reduzieren.

Die Datenbasis kann nach jeglicher Tabelle oder Prozessabweichung gefiltert werden. Mögliche Filteroptionen sind beispielsweise Prozessinstanzen mit den meisten Red Flags, Prozessinstanzen mit angeschlagenen Fraud Patterns, Prozessabweichungen usw. Durch die Filterung reduziert sich die Datenbasis für den Auditor.

- Ergebnisse der Analyse sollen in einer Art dargestellt werden, die es ohne zusätzlichen Aufwand erlaubt in den Auditbericht übernommen zu werden.

Ein Export der entsprechenden Analyse in ein PDF Format wird von Celonis Process Mining unterstützt und hier verwendet.

7.3 Investigative Ebene

In der investigativen Ebene werden Konsequenzen für wirtschaftskriminelle Taten verhängt. Daher wird an dieser Stelle ein kleiner Überblick über die gesetzliche Regelung von Fraud gegeben. Allerdings ist es nur ein kleiner Ausblick und hat keinen Anspruch auf Vollständigkeit. Dies wird den Rechtswissenschaften überlassen.

Die rechtliche Grundlage bei Fraud in Deutschland bildet hierbei das Strafgesetzbuch (StGB). Die hier vorgestellten Gesetzte sind nach der Auswahl von Deling (2005) und Odenthal (2009)

- Diebstahl (§§ 242 – 244, 247 und 248a StGB)
- Betrug (§§ 263-265 StGB)
- Untreue (§ 266)
- Unterschlagung (§§246 - 247 StGB)
- Urkundenfälschung (§§ 267-268, 271-275, 277-279 und 281 StGB)

Eine Übersicht über Gesetze in Amerika gibt Albrecht et al. (2012). Wenn ein Täter überführt wird, droht ihm eine Gefängnis- und/oder Geldstrafe. Jedoch muss zunächst seine Schuld bewiesen werden.

7.4 Dashboard des Prototyps

Um explorative Analysen zur Identifikation von wirtschaftskriminellem Verhalten zu ermöglichen, wird ein Dashboard auf Basis von Celonis Process Mining erstellt. Zunächst wird ein low-fidelity Prototyp entwickelt, um eine Grundlage zum besseres Verständnis des möglichen Dashboards zu schaffen. Mit Hilfe der Thinking Aloud Methode werden zwei Auditoren und sieben Teilnehmer des White Collar Hacking Contests gebeten, bestimmte Aufgaben mit dem Prototypen zu lösen und währenddessen ihre Gedanken laut auszusprechen. Diese werden anschließend befragt, welche Informationen ihnen zur Beantwortung der Aufgaben fehlen. Auf Basis dieser Informationen werden Anforderungen für den high-fidelity Prototypen entwickelt. Der low-fidelity Prototyp soll im Folgenden kurz beschrieben werden. Hierfür werden zunächst aus der Literatur Anforderungen und typische Designelemente abgeleitet.

7.4.1 Anforderungen an das Dashboard des Prototyps

Für die Erstellung eines Dashboards zur Identifikation von wirtschaftskriminellem Verhalten gibt es kaum Publikationen, die Anforderungen hierzu beschreiben. Ausnahmen bilden hier Rozinat (2014) und die Implementierung von Singh, Best, and Mula (2013), aus denen folgende Anforderungen übernommen werden:

- Die Präsentation der Informationen sollte auf mehrere Fenstern/Tabs verteilt werden.

- Daten sollen dem Benutzer möglichst ansprechend angeboten werden. Dabei sollte dieser weder zu viele, noch zu wenige Informationen erhalten.
- Für die Datenanalyse sollte eine Übersichtsdarstellung und ein Drilldown möglich sein.
- Ein Dashboard sollte eine high-level Übersicht über die Aktivitäten im System anzeigen.
- Kuchen- und Balkendiagramme eignen sich, um Zusammenhänge darzustellen

Da diese Anforderungen teilweise wenig präzise sind, werden zusätzlich Visualisierungsempfehlungen aus der Visualisierungsliteratur entnommen. Dementsprechend sind mehrere Einflussfaktoren für die Art und Struktur der Daten zu nennen. Im Folgenden wird basierend auf Schumann and Müller (2000) die wichtigsten Visualisierungsmöglichkeiten und die typische Verwendung aufgezeigt. Der Fokus richtet sich hier auf die im Celonis System enthaltenen Visualisierungsmöglichkeiten:

Punktediagramm: Verwendung zur Darstellung von relativen Positionen. Diese eignen sich insbesondere dazu, etwaige Korrelationen zwischen einer abhängigen und einer unabhängigen Variable zu erkennen. Bilden sich im Falle von quantitativen Daten monoton steigende oder fallende Linien heraus, so spricht das für eine lineare Korrelation.

Linien- und Kurvendiagramme: Diese repräsentieren quantitative Größen als Positionen einer gemeinsamen, quantitativen Skala. Zusätzlich werden benachbarte Punkte durch Linien- bzw. Kurvensegmente miteinander verbunden. Durch diese Interpolation werden Trends und lokale Strukturen in den Daten, wie auch die allgemeine Verteilung deutlicher und prägnanter dargestellt. Datenpunkte, die durch Linien und Kurvenabschnitte miteinander verbunden sind, werden somit zusätzlich wirkungsvoll gruppiert. Linien- und Kurvendiagramme können also ebenfalls zur Visualisierung von zusammenhängender Variablen genutzt werden, um eine Korrelation festzustellen.

Säulen- und Balkendiagramme: Wenn die abhängige Variable nominaler oder diskreter Natur ist und die unabhängige Variable quantitativ, so können auf der waagerechten Achse des Koordinatensystems die unabhängigen Variablen und auf der senkrechten Achse die zugehörigen abhängigen Größen abgetragen werden. Bei der Verwendung von Säulendiagrammen gibt es Regeln, die beachtet werden sollten. So sollte im Fall der Abbildung von nominalen unabhängigen Variablen auf die Abszisse die waagerechte Achse nicht dargestellt werden, um dem Eindruck vorzubeugen, dass die auf der waagerechten Achse aufgetragenen Variablen in einer Ordnungsrelation zueinanderstehen.

Histogramme: Histogramme stellen eine spezielle Form der Säulendiagramme dar. Anders als das Säulen- und Balkendiagramm, zeigt ein Histogramm nicht die Datenwerte selbst, sondern ihre Häufigkeit und Verteilung. Im Fall von quantitativen Daten erfolgt hierzu eine Klasseneinteilung des Wertebereiches, und dementsprechend werden die Häufigkeiten in diesen Klassen bestimmt. Histogramme können somit auch als eine indirekte Visualisierungstechnik bezeichnet werden. Sie werden üblicherweise als ein verbundenes Säulendiagramm dargestellt, bei dem die Klassenintervalle auf die Abszisse und die Klassenhäufigkeiten auf die Ordinate abgebildet werden.

Kreisdiagramme: Ein Kreisdiagramm, oft auch als Tortendiagramm bezeichnet, ist ähnlich wie ein Säulendiagramm zur Darstellung quantitativer Merkmale über einer nominalen, unabhängigen Variablen geeignet. Das Kreisdiagramm verwendet jedoch statt eines rechtwinkligen Koordinatensystems einen Kreis als Bezugssystem, an dem die Größen der verschiedenen Merkmale durch unterschiedlich gefärbte oder texturierte Abschnitte dargestellt werden. Diese Darstellungsform ist jedoch nur dann geeignet, wenn das Diagramm in einer ausreichenden Größe präsentiert werden kann, da bei kleinen Kreisen der Vergleich von Flächenanteilen sehr schwierig ist. Außerdem sollte die Anzahl der zu visualisierenden Variablen und ihrer Größen fünf bis sechs nicht überschreiten. Kreisdiagramme eignen sich dazu, einzelne Datenwerte im Kontext der Gesamtpopulation herauszustellen. Einzelne Kreissegmente können dabei hervorgehoben werden, um den entsprechenden Datenwert besonders zu betonen.

Tabelle: Eine Datenmenge in Tabellenform besteht aus Spalten und Zeilen. Dabei sind die einzelnen Spalten den Variablen der Datenmenge zugeordnet, und in den Zeilen stehen die erhobenen Werte für jede Variable. Üblicherweise enthalten in Tabellenform dargestellte Daten maximal eine unabhängige Variable, die meist implizit durch die Zeilenzahl gegeben ist.

Farben werden an dieser Stelle nicht betrachtet, da diese von Celonis vorgegeben und damit nicht auswählbar sind. Nachdem die gängigen Visualisierungsmöglichkeiten dargestellt werden, wird zunächst ein low-fidelity Prototyp erstellt. Dieser soll als Grundlage dienen, um fehlende Informationen und schwieriges Handling im nächsten Schritt mithilfe der Thinking Aloud Methode zu identifizieren.

7.4.2 Low-fidelity Prototyp

Der low-fidelity Prototyp ermöglicht den Erstellungsaufwand zu reduzieren und eine zügige Evaluation von Designentscheidungen durchzuführen. Der Prototyp ist modular in mehreren Tabs aufgebaut. Alle Designelemente sind interaktiv und können gefiltert werden, wobei das Setzen eines Filters eine Auswirkung auf alle Daten in allen Tabs hat. Diese werden im Folgenden vorgestellt.

1. Prozessübersicht allgemein

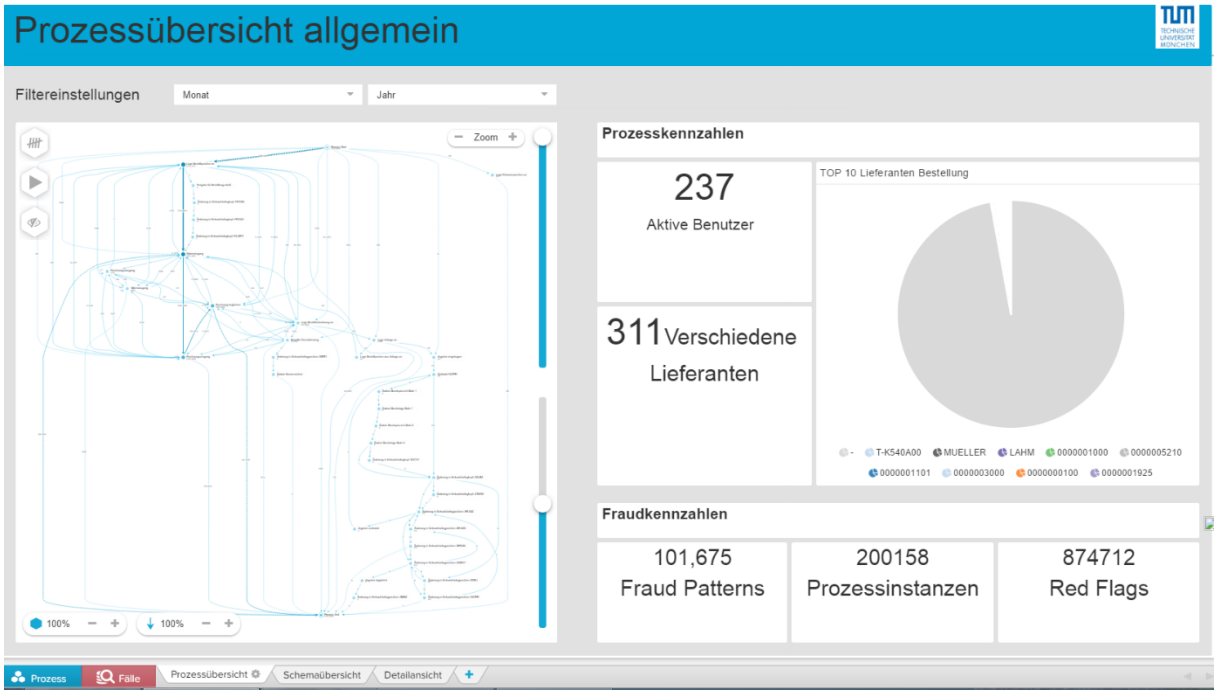


Abbildung 7-9: Low-fidelity Prototyp – Prozesssicht allgemein

Quelle: Screenshot Celonis Process Mining

Der Tab ‚Prozessübersicht allgemein' zeigt eine Übersicht über den Prozess und allgemeine Prozesskennzahlen (vergl. Abbildung 7-9). Ziel der Prozessübersicht ist einen ersten und allgemeinen Eindruck von dem entsprechenden Prozess zu bekommen. Auf der linken Seite des Tabs ist ein Prozessexplorer eingebettet, der auf Basis der Daten aus dem Quellsystem den Ist-Prozess darstellt. Dabei kann sowohl die Anzahl der Verbindungen, sowie die Anzahl der Knoten angepasst werden, um den Detaillierungsgrad der Prozessanzeige einzustellen. Diese Funktion ist vor allem hilfreich, wenn von der Norm abweichende Prozessinstanzen identifiziert werden sollen. Auf der rechten Seite sind einige Prozesskennzahlen dargestellt, wie die Anzahl der verschiedenen Benutzer des SAP Systems (Mitarbeiter), die Anzahl der Lieferanten und die Top10 aller Lieferanten nach Bestellvolumen. Zusätzlich werden im rechten unteren Teil bereits einige Fraudkennzahlen genannt, wie die Anzahl der gefundenen Fraud Patterns, die Gesamtanzahl der Prozessinstanzen und die Anzahl der gefundenen Red Flags. Im oberen Bereich des Tabs ist es möglich nach Transaktionen aus einem bestimmten Jahr und/oder Monat zu filtern.

2. Fraudübersicht allgemein

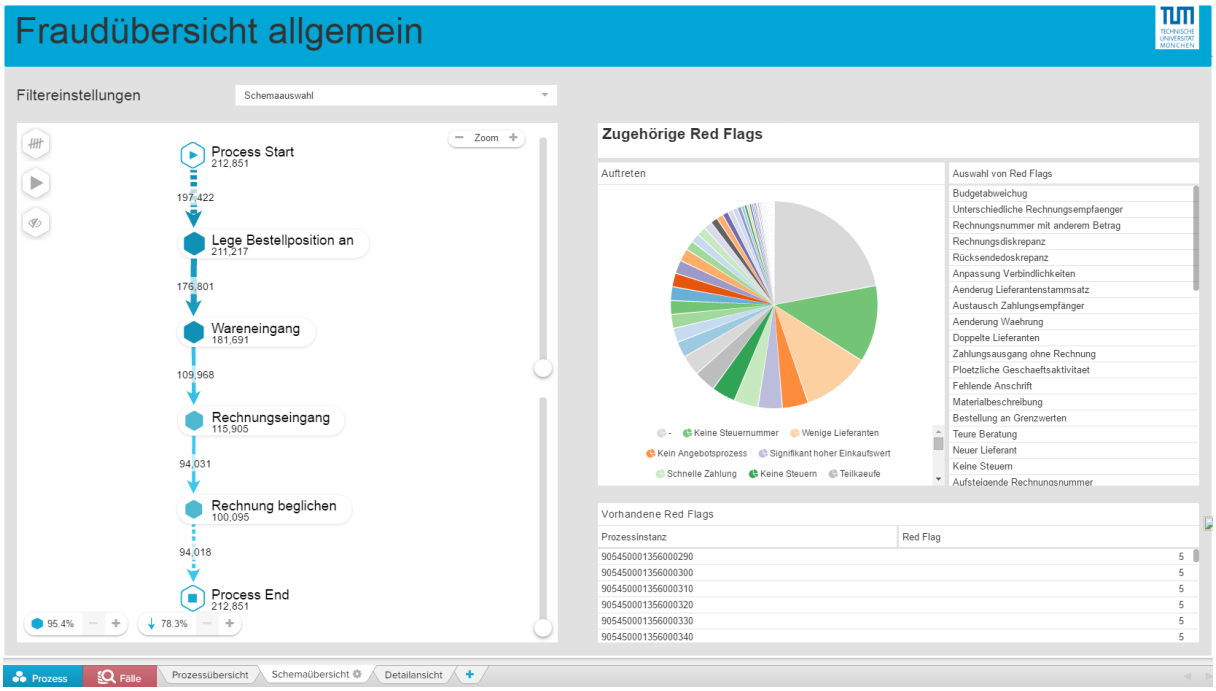


Abbildung 7-10: Low-fidelity Prototyp - Schemaübersicht

Quelle: Screenshot Celonis Process Mining

In dem zweiten Tab ‚Schemaübersicht allgemein' wird eine Übersicht über die Red Flags und Fraud Patterns angezeigt (vergl. Abbildung 7-10). Wie bereits in der Prozessübersicht ist auf der linken Seite der Prozessexplorer vorhanden, der den Ist-Prozess darstellt. Auf der rechten Seite sind Kennzahlen zu den identifizierten Red Flags und Fraud Patterns vorhanden. So werden beispielsweise die identifizierten Red Flags und ihre Häufigkeit des Auftretens in einem Kreisdiagramm dargestellt. Der Fraud Auditor hat so die Möglichkeit die Schwachpunkte in diesem Prozess zu erkennen. Des Weiteren wird eine Tabelle mit auffälligen Prozessinstanzen und der Anzahl der darin entdeckten Red Flags dargestellt. Der Auditor hat hier die Möglichkeit nach Prozessinstanzen mit einer hohen Anzahl von Red Flags zu filtern, um diese im nächsten Schritt detaillierter zu analysieren. Zusätzlich kann der Auditor nach den zuvor identifizierten Fraud Patterns filtern, indem er aus einer Drop-Down Liste danach filtert. Nur Prozessinstanzen bei denen dieses Fraud Pattern vorkommt werden angezeigt.

3. Detailexplorer

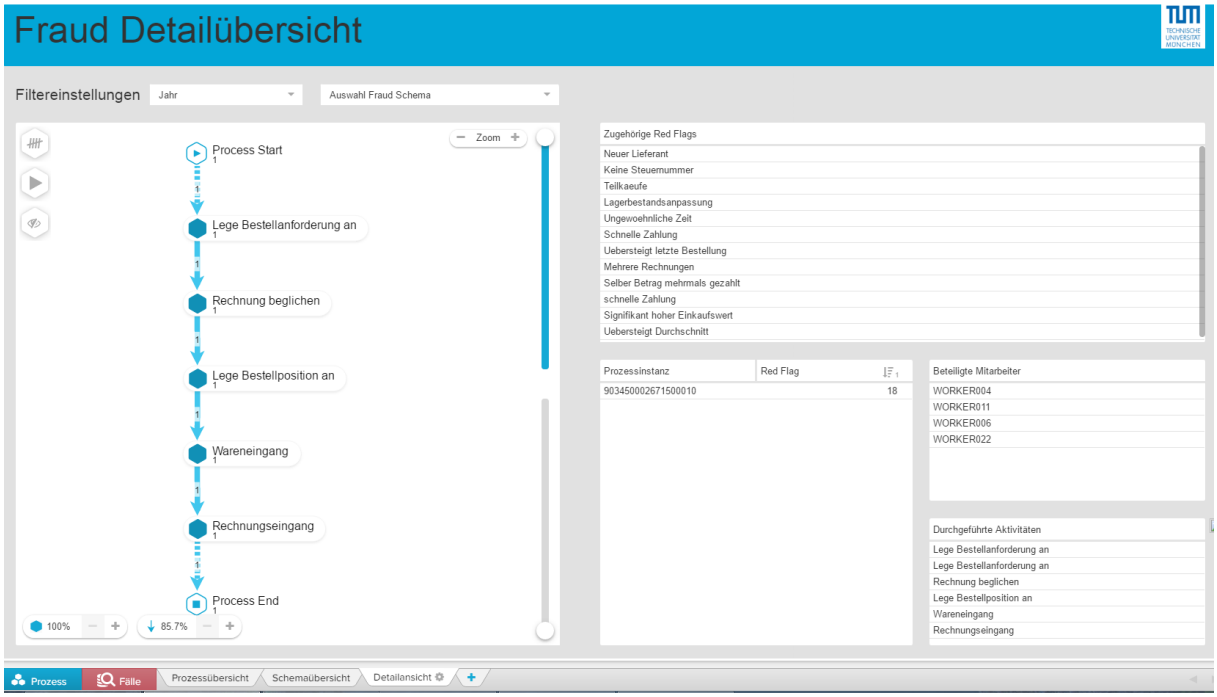


Abbildung 7-11: Low-fidelity Prototyp: Detailexplorer

Quelle: Screenshot Celonis Process Mining

Der Detailexplorer hilft vor allem für die detaillierte Analyse von einzelnen sehr auffälligen Prozessinstanzen, nach denen zuvor gefiltert wird. Wie in Abbildung 7-11 dargestellt, wird die auffällige Prozessinstanz im Prozessexplorer dargestellt. Auf der rechten Seite werden die entsprechenden identifizierten Red Flags, die beteiligten Mitarbeiter und durchgeführte Aktivitäten dargestellt.

Um diesen Prototyp zu verbessern, wird die Thinking Aloud Methode verwendet. Diese wird im Folgenden vorgestellt:

Thinking Aloud Methode

Die Thinking Aloud Methode ist eine der am häufigsten verwendeten Methoden zum Testen der Benutzbarkeit eines Systems. Lewis & Rieman (1994) und Newell & Simon (1972) beschreiben das Vorgehen dieser Methode, die auch von der Human Computer Interaction Community adaptiert wurde. Bei der Methode werden Testpersonen Aufgaben gestellt, die sie mit dem entsprechenden System durchführen sollen. Dabei werden sie gebeten laut auszusprechen, was sie währenddessen denken, tun oder fühlen. Gleichzeitig wird beobachtet, wie die Probanden die Aufgabe versuchen zu lösen (bspw. durch Bildschirmaufzeichnungen und Mouse-Tracking). So kann Verstanden werden, welche Aspekte des Produkts die Probanden erfreut, frustriert oder verwundert. Auf Basis dieser Erkenntnisse können Produkte korrigiert oder verbessert werden. Es gibt zwei typische Arten der Thinking Aloud Methode:

Parallele Thinking Aloud Methode: Diese Art der Ausführung wird am häufigsten angewandt. Hierbei bearbeitet der Teilnehmer die ihm gestellten Aufgaben und beschreibt gleichzeitig seine

Gedanken und Emotionen. Basierend auf der Personalität des Probanden und der Komplexität der Aufgabe, muss der Proband ggf. öfters daran erinnert werden seine Gedanken laut auszusprechen, während er die Aufgabe bewältigt. Menschen können gleichzeitig eine Aufgabe lösen und darüber sprechen, ohne das Ergebnis der Aufgabe zu verfälschen (Ericsson, & Simon, 1993).

Retrospektive Thinking Aloud Methode: Hierbei werden die Teilnehmer zunächst gebeten leise eine Aufgabe zu lösen. Dabei wird ihre Aufgabenlösung entweder auf Video oder die Mausbewegungen auf dem Bildschirm aufgezeichnet. Anschließend wird ihnen das entsprechende Video vorgespielt und sie werden gebeten ihre Gedanken und Gefühle zu äußern. Diese Methode kann weiterführende Einsichten in die Absichten, Strategien und Gedanken der Probanden zeigen (Guan, Lee, Cuddihy & Ramey, 2006).

In dieser Dissertation wird die parallele Thinking Aloud Methode gewählt. Ziel ist es zunächst zu verstehen, ob einfache Testaufgaben intuitiv durch die Teilnehmer mit dem Prototyp durchgeführt werden können. Zusätzlich sollen Verbesserungsmöglichkeiten und fehlende Informationen (Anforderungen) identifiziert werden. Der Befragte wird ausdrücklich gebeten seine Schritte, Gedanken und Kritiken laut zu äußern. Die zu beantwortenden Aufgaben sind in *Anhang F: Ergebnisse der Thinking Aloud Methode* dargestellt. Zusätzlich werden die Teilnehmer befragt, welche Informationen zur Fraud Detektion diese vermissen und welche Verbesserungsvorschläge diese haben. Daraus werden Anforderungen für den high-fidelity Prototypen abgeleitet. Insgesamt wurden sieben Teilnehmer des White Collar Hacking Contest[35], sowie zwei professionelle Fraud Auditoren befragt.

7.4.3 Anforderung für den high-fidelity Prototypen

Aus der Thinking Aloud Methode hat sich zunächst ergeben, dass die Teilnehmer mehrere Sichten (Tabs) wünschen. Die erforderlichen Informationen belaufen sich auf Informationen zum allgemeinen Prozess (Prozesssicht), zu den entsprechenden Fraud Schemata (Schemasicht), den beteiligten Mitarbeitern (Mitarbeitersicht), der Lieferanten (Lieferantensicht) und Produkten (Produktsicht). Deshalb werden die Informationen auf insgesamt fünf Sichten verteilt. Eine Zusammenfassung weiterer Anforderungen und eine mögliche Darstellungsform sind in Tabellen 40-43 dargestellt. Eine Ausführliche Beschreibung ist in *Anhang F: Ergebnisse der Thinking Aloud Methode* dargestellt.

[35] Für Informationen zum White Collar Hacking Contest vergl. Kapitel Forschungsinstrument8.3.1

Prozesssicht

Anforderung	Beschreibung	Darstellungsoption
Proz_01	Darstellung der Anzahl von Prozessinstanzen	Kennzahl
Proz_02a	Darstellung der Top 10 Lieferanten mit der höchten Bestellsumme	Kreisdiagramm
Proz_02b	Darstellung der Top 10 Materialien, für die die Bestellsumme am höchsten ist	Kreisdiagramm
Proz_03a	Darstellung der Anzahl von aktiven Mitarbeitern	Kennzahl
Proz_03b	Darstellung der Anzahl bestellter Materialien	Kennzahl
Proz_03c	Darstellung der Anzahl von verschiedenen Lieferanten	Kennzahl
Proz_03d	Darstellung des gesamten Rechnungsbetrags aller Rechnungen	Kennzahl
Proz_03e	Darstellung der Anzahl eingegangener Rechnungen	Kennzahl
Proz_04	Darstellung des aktiven Mandanten/Buchungskreis	Dropdown-Liste oder Tabelle
Proz_05a	Darstellung der Anzahl von Fraud Patterns	Kennzahl
Proz_05b	Darstellung der erwarteten Schadenssumme pro Fraud Pattern	Tabelle
Proz_06a	Darstellung der Anzahl von Red Flags	Kennzahl
Proz_06b	Darstellung der Schadenssumme pro Red Flag	Tabelle

Tabelle 40: Anforderungen Prozesssicht

Quelle: Eigene Darstellung

Schemaansicht

Anforderung	Beschreibung	Darstellungsoption
Schem_01	Darstellung der dentifizierten Red Flags	Tabelle
Schem_02	Filtermöglichkeit nach Fraud Patterns	Tabelle
Schem_03a	Filtermöglichkeit nach Red Flags	Tabelle: Sortiermöglichkeit nach Top 10 Prozessinstanzen mit der höchsten Anzahl Red Flags und dem höchsten Verkaufsvolumen
Schem_03b	Darstellung der Top 10 Transaktionen (nach Anzahl Red Flags/ nach Transaktionsvolumen)	
Schem_03c	Darstellung von verdächtigen Prozessinstanzen und der Anzahl von Red Flags	
Schem_03d	Darstellung der Anzahl von Fraud Patterns	Balkendiagramm
Schem_04a	Darstellung einer Übersicht über die aufgetretenen Fraud Patterns	Balkendiagramm
Schem_04b	Darstellung einer Übersicht über die aufgetretenen Red Flags	Kreisdiagramm
Schem_05	Genaue Beschreibung der Red Flags	Tabelle
Schem_06	Darstellung der Red Flags und Fraud Patterns in Diagrammen	Tabelle
Schem_07	Zeitlicher Verlauf der Red Flags	kann nicht abgebildet werden

Tabelle 41: Anforderungen an Schemaansicht

Quelle: Eigene Darstellung

Mitarbeitersicht

Anforderung	Beschreibung	Darstellungsoption
Mitarb_01	Darstellung von beteiligten Mitarbeitern (pseudonymisiert)	Tabelle
Mitarb_02	Die Art des Users (Dialog vs. Systembenutzer) sollte erkennbar sein	nicht möglich
Mitarb_03	Es sollte ersichtlich werden zu welcher Einkäufergruppe der Mitarbeiter gehört	Tabelle
Mitarb_04	Darstellung der Anzahl von beteiligten Mitarbeitern (Sollte die gesamte Prozessinstanz von nur einem Mitarbeiter durchgeführt werden, handelt es sich um einen Red Flag).	Tabelle
Mitarb_05	Darstellung der Anzahl von Vorgängen pro Mitarbeiter	Kreisdiagramm
Mitarb_06	Darstellung eines sozialen Netzwerks von Mitarbeitern, um Kooperation zu erkennen	nicht möglich
Mitarb_07	Darstellen der beteiligten Mitarbeiter pro Bestellung/ Bestellanforderung/ Wareneingang	Tabelle für jeden Prozessschritt (Bestellanforderung, Wareneingang, mögliche Änderungen, Bezahlung)

Tabelle 42: Anforderungen Mitarbeitersicht
Quelle: Eigene Darstellung

Lieferantensicht

Anforderung	Beschreibung	Darstellungsoption
Lief_01	Darstellung des Banklandes und des operierenden Landes (Markierung wenn diese beiden Werte voneinander abweichen)	Tabelle: Lieferantenland vs. Bankland (keine farbliche Markierung bei Unterschied möglich)
Lief_02	Darstellung des „Fraud“-Volumens im Verhältnis zum allgemeinen Einkaufsvolumen	Kreisdiagramm
Lief_03	Darstellung des Einkaufsvolumens pro Lieferant	Bubble Chart (Lieferant vs. Bestellpreis)
Lief_04	Darstellung des Volumens und der Anzahl von Einkäufen pro Lieferant	Tabelle
Lief_4a	Darstellung der Anzahl der Einkäufe bei einem Lieferanten	Kreisdiagramm
Lief_4b	Darstellung der Einkaufsvolumina pro Lieferant	Kreisdiagramm
Lief_05	Distanz zum Warenempfänger soll dargestellt werden	Nicht mit Celonis realisierbar
Lief_06	Darstellung der Anzahl von Lieferanten pro Land	Kreisdiagramm
Lief_07	Schlafende und wieder aktive Lieferanten	Red Flag
Lief_08	Anzahl der Red Flags pro Lieferant	Kreisdiagramm

Lief_09	Bestellvolumen/ bestellte Ware pro Lieferant	Tabelle

Tabelle 43: Anforderungen Lieferantensicht
Quelle: Eigene Darstellung

Materialsicht

Anforderung	Beschreibung	Darstellungsoption
Mat_01	Darstellung welche Materialien gekauft wird, sowie die Mengen und die Einheit (Stück, Palette usw.)	Tabelle
Mat_02a	Darstellung wie häufig ein Material gekauft wird	Kreisdiagramm
Mat_02b	Darstellung wie häufig eine Materialgruppe gekauft wurde	Kreisdiagramm
Mat_03a	Darstellung des Preises aller Bestellungen Pro Material	Kreisdiagramm
Mat_03b	Darstellung des Preises aller Bestellungen Pro Materialgruppe	Kreisdiagramm
Mat_04	Falls möglich: Darstellung ob es sich um ein verderbliches Material handelt	leider passendes Feld in SAP Tabellen nicht gefunden
Mat_05	Darstellung, ob es sich um ein Commodity-Produkt oder Spezialmaterial handelt	Keine Aufteilung zwischen Commodity und Spezialmaterial in SAP Tabellen; Deshalb Aufteilung Material oder Dienstleistung
Mat_06	Darstellung der Anzahl von Dienstleistungen im Vergleich zu Produkten	Kreisdiagramm
Mat_07	Logistikeinkäufe	keine Möglichkeit gefunden
Mat_08	Darstellung des zeitl. Verlaufs des Einkaufsvolumens pro Produkt	Zeitreihe

Tabelle 44: Anforderungen Materialsicht
Quelle: Eigene Darstellung

Zusätzliche werden noch folgende allgemeine Anforderungen genannt:

- Trennzeichen in den Zahlen sind Notwendig
- Anschauliche Graphen (Kreisdiagramm, Bar Chart usw.)
- Filterung nach Fraud Patterns und Red Flags muss möglich sein
- kleinere Schriftart verwenden
- Beibehaltung der Aufteilung nach Sichten aus dem low-fidelity Prototyp
- Prozessdiagramm beibehalten

Die hier genannten Anforderungen werden entsprechend für den high-fidelity Prototyp verwendet.

7.4.4 High-fidelity Prototyp

Der high-fidelity Prototyp setzt die identifizierten Anforderungen des ersten Prototyps um. So werden fünf Sichten erstellt, in denen Kennzahlen und Diagramme verwendet werden. Wird in einer Sicht nach einer bestimmten Information gefiltert, gelten die Filter ebenfalls auf allen weiteren Reitern und Tabellen. Man kann also beispielsweise nach einem bestimmten Fraud Pattern filtern und anschließend die Prozessinstanz aus Material-, Mitarbeiter- und Lieferantensicht betrachten. Die einzelnen Sichten werden im Folgenden kurz vorgestellt.

<u>Prozesssicht</u>

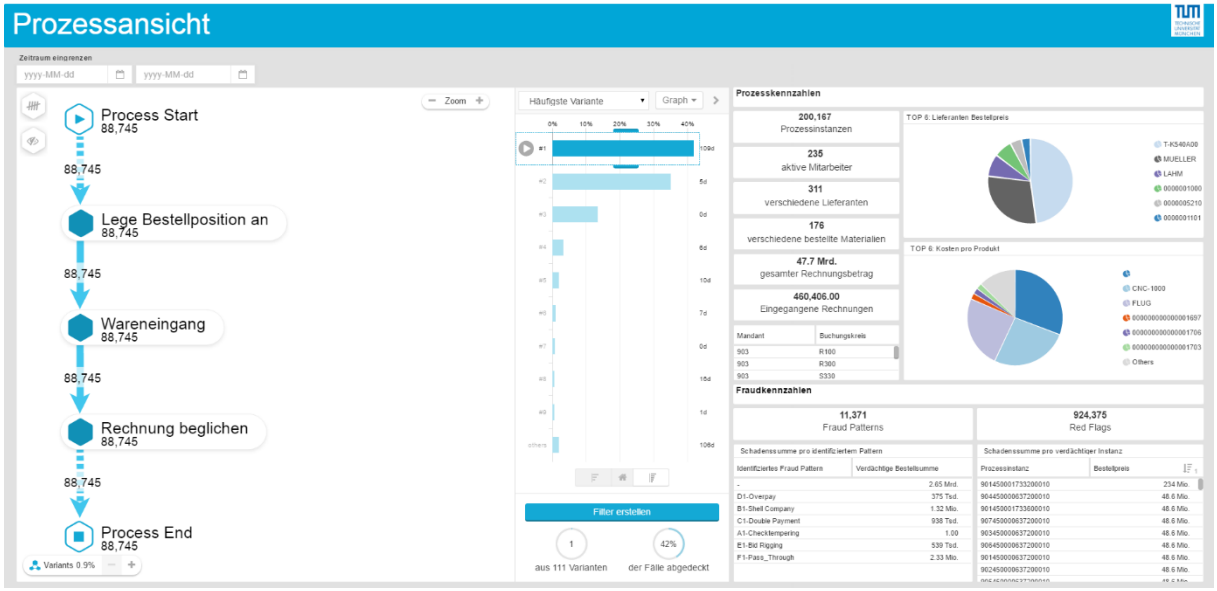


Abbildung 7-12: High-fidelity Prototyp – Prozesssicht

Quelle: Screenshot Celonis Process Mining

Das Herzstück dieser Sicht ist der Fallexplorer, wie in Abbildung 8-12 auf der linken Seite dargestellt. Dieser stellt alle möglichen Prozessvarianten dar.

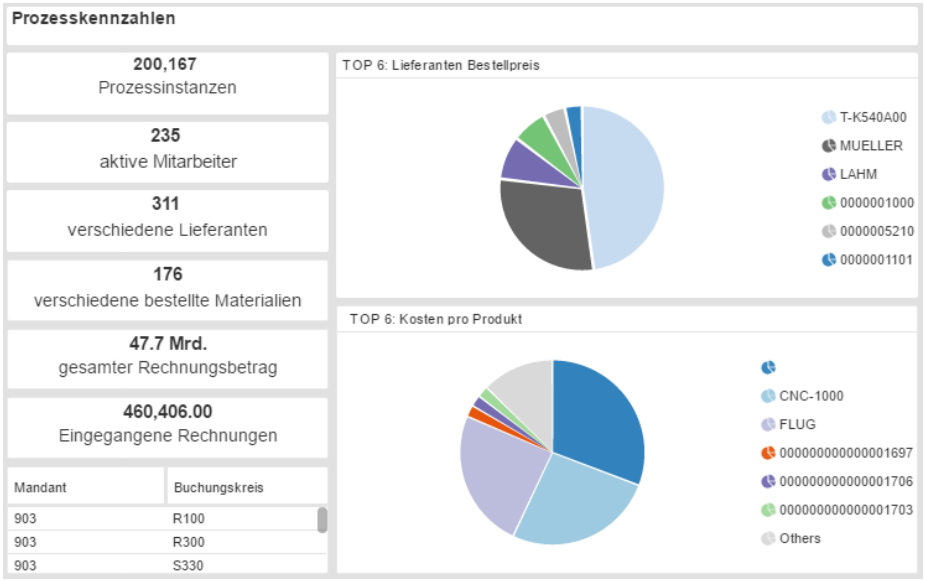


Abbildung 7-13: High-fidelity Prototyp: Prozesskennzahlen

Quelle: Screenshot Celonis Process Mining

So können beispielsweise die häufigsten oder die seltensten Prozessvarianten identifiziert werden und nach diesen gefiltert werden. Besonders seltene und abweichende Prozessinstanzen sind für den Fraud Investigator von besonderer Bedeutung, da sich Fraud oft in abweichenden Prozessinstanzen verbirgt. Auch eine Animation des exakten Verlaufs ist im Fallexplorer möglich. Zusätzlich kann in dieser Sicht nach besonders langandauernden und besonders schnellen Prozessdurchläufen gefiltert werden, um so möglicherweise Hinweise für Fraud zu erhalten. Auch gibt es die Möglichkeit den Datensatz nach einem bestimmten Zeitraum zu filtern.

Die Prozesskennzahlen, wie in Abbildung 7-13 dargestellt, geben eine Übersicht über den zu untersuchenden Prozess. Dafür wird die Anzahl der insgesamt im Datensatz identifizierten Prozessinstanzen (Anforderung: Proz_01), die Anzahl der verschiedenen aktiven und am Prozess beteiligten Mitarbeitern (Anforderung Proz_03a), die Anzahl der verschiedenen Lieferanten (Anforderung Proz_03c) und die Anzahl der bestellten Materialien bzw. Dienstleistungen (Anforderung Proz_3b) angezeigt. Zusätzlich wird der gesamte Rechnungsbetrag in der Hauswährung in diesem Zeitraum dargestellt (Anforderung Proz_03d), sowie die Anzahl der eingegangenen Rechnungen (Anforderung Proz_03e). Die Anzeige des aktiven Mandanten und des Buchungskreises (Anforderung Proz_04), sowie die Anzeige der Top 6 Lieferanten nach Bestellpreis (Anforderung Proz_02a) und nach dem teuersten Produkt (Anforderung Proz_02b) komplettieren die Sicht.

Zusätzlich werden einige wichtige Fraud Kennzahlen dargestellt, wie die Anzahl der identifizierten Fraud Patterns und Red Flags (Anforderung Proz_05a, Proz_06a). Die Übersicht über die mögliche Schadenssumme pro Fraud Pattern bzw. pro Fraud Instanz (Anforderung Proz_05b, Proz_06b) wird dargestellt. So kann beispielsweise bei dem Fraud Pattern

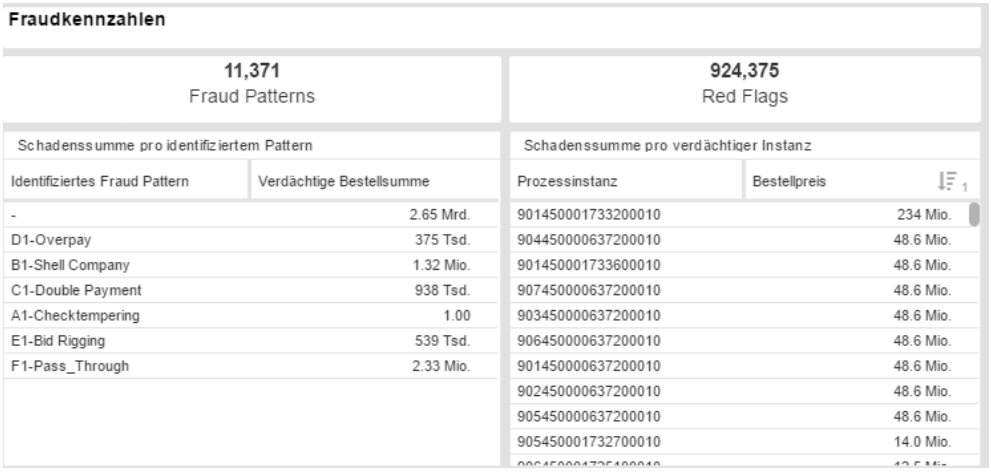


Abbildung 7-14: High-fidelity Prototyp: Fraudkennzahlen

Quelle: Screenshot Celonis Process Mining

‚Scheinfirma' in Abbildung 7-14 ein Betrag von 1,32 Millionen in der Hauswährung durch Fraud aus dem Unternehmen geflossen sein. Der Fraud Investigator kann nach allen vorkommenden Instanzen mit dem entsprechenden Fraud Pattern „Scheinfirma" filtern, um nach konkreten Hinweisen für den Verdacht zu suchen.

Schemasicht

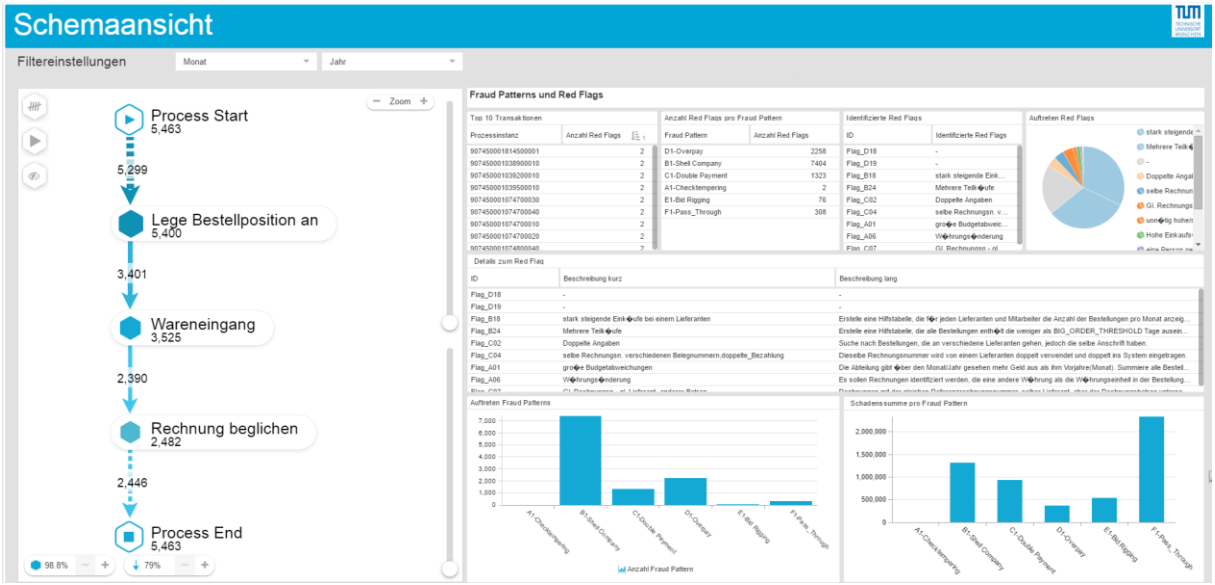


Abbildung 7-15: High-fidelity Prototyp – Schamaansicht

Quelle: Screenshot Celonis Process Mining

Die Schemasicht (Abbildung 7-15) zeigt Details zu den vorhandenen Fraud Schemata. Auf der linken Seite ist die Prozessinstanz dargestellt, wobei der Ist-Prozess mit allen Abweichungen visualisiert ist (Anforderung Schem_3c). Hier wird die am häufigsten durchlaufene Prozessinstanz visualisiert. Über zwei Schieberegler kann der Detaillierungsgrad eingestellt werden und so weitere Prozessverbindungen und Prozessaktivitäten angezeigt werden. Auf der rechten Seite sind aufgekommene Red Flags und Fraud Patterns dargestellt. Ziel dieser Tabelle ist eine Übersicht über Prozessinstanz und Anzahl der Red Flags zu geben, sowie die Möglichkeit zur Filterung nach bestimmten Fraud Patterns oder Prozessinstanzen mit besonders hoher Red Flag Anzahl. Alle vorhandenen Sichten werden entsprechend der hier ausgewählten Filtereigenschaften aktualisiert.

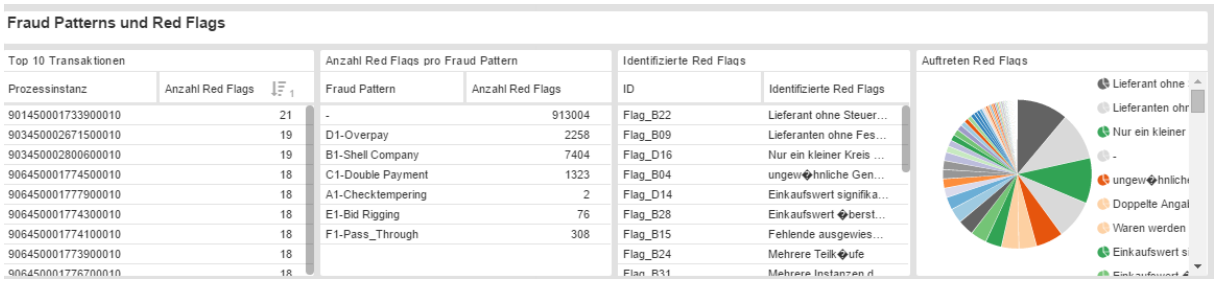


Abbildung 7-16: High-fidelity Prototyp - Fraud Patterns und Red Flags

Quelle: Screenshot Celonis Process Mining

Die oberste Reihe in Abbildung 7-16 zeigt einige Kennzahlen bezüglich Fraud Patterns und Red Flags an. In der Tabelle ‚Top 10 Transaktionen' werden die Prozessinstanzen mit den meisten identifizierten Red Flags dargestellt (Anforderung Schem_3b). Eine Studie von Albrecht and Romney (1986) hat einen positiven Zusammenhang zwischen der Anzahl von Red Flags in einer Prozessinstanz und der Wahrscheinlichkeit für Fraud gezeigt. In dieser Tabelle könnte der Auditor beispielsweise nach der ersten Prozessinstanz ‚90145000173390010' durch Doppelklick filtern. Mit 21 identifizierten Red Flags hat diese die höchste Anzahl an Red Flags in dem Datensatz und ist dadurch sehr auffällig. Alle Diagramme und Tabellen in allen Tabs werden so angepasst, dass sie nur Informationen bezüglich der gefilterten Prozessinstanz anzeigen.

Die Tabelle ‚Anzahl Red Flags pro Fraud Pattern' ermöglicht das Filtern nach Fraud Patterns (Anforderung Schem_02) und stellt die Anzahl der Red Flags pro Fraud Pattern dar. Eine weitere Tabelle ‚Identifizierte Red Flags' zeigt die identifizierten Red Flags an (Anforderung Schem_01). Besonders interessant wird diese Tabelle, wenn nach einem bestimmten Fraud Pattern oder nach einer Prozessinstanz gefiltert wird. Dann werden in dieser Tabelle nur die Red Flags angezeigt, die genau bei dieser bestimmten Prozessinstanz aufgetreten sind. Das Kuchendiagramm ‚Auftreten Red Flags' zeigt die Häufigkeitsverteilung der aufgetretenen Red Flags an (Anforderung Schem_4b). In diesem Beispiel wird klar, dass das Red Flag ‚Lieferant ohne Steuernummer' am häufigsten in diesem Datensatz aufgetreten ist. Der Auditor kann

durch einen Doppelklick nach den entsprechenden häufigen Red Flags filtern (Anforderung Schem_3a).

Details zum Red Flag

ID	Beschreibung kurz	Beschreibung lang
Flag_B22	Lieferant ohne Steuernummer	Erstelle eine Hilfstabelle, die alle Lieferanten enth€lt, bei denen die Steuernummer, Umsatzsteuer-Identifikations…
Flag_B09	Lieferanten ohne Festnetz oder nur Anrufbeantw.	Suche alle Instanzen, bei denen die Telefonnummer im Lieferantenstammsatz fehlt
Flag_D16	Nur ein kleiner Kreis an Lieferanten wird benutzt	Mitarbeiter benutzt f€r seine Bestellungen nur sehr wenige Lieferanten pro Produkt.
Flag_B04	ungew€hnliche Genehmigungen	Erstelle eine Tabelle die Personen mit €berdurchschnittlicher Anzahl an Bestellungen pro Arbeitstag (mehr als 5…
Flag_D14	Einkaufswert signifikant ueber letztem	Zahlen die den Durchschnitt der sonstigen Zahlungen €berschreiten
Flag_B28	Einkaufswert €bersteigt den letzten signifikant	Zun€chst wird eine Tabelle mit der Bestellsumme pro Bestellung erstellt. Suche in dieser Tabelle alle zuvorkom…
Flag_B15	Fehlende ausgewiesene Steuer auf Rechnung	Auf dem Belegkopf der Eingangsrechnung entspricht der Steuerbetrag in Belegw€hrung mit Vorzeichen = 0 (Ke…
Flag_B24	Mehrere Teilk€ufe	Erstelle eine Hilfstabelle, die alle Bestellungen enth€lt die weniger als BIG_ORDER_THRESHOLD Tage ausein…
Flag_B31	Mehrere Instanzen desselben Lieferanten	Suche alle Instanzen, bei denen eine Bestellung zu einem Lieferanten existiert, bei dem der Name, das Land, Po…

Abbildung 7-17: High-fidelity Prototyp - detaillierte Beschreibung der Red Flags

Quelle: Screenshot Celonis Process Mining

Detaillierte Informationen über die vorhandenen Red Flags stellt die Tabelle in Abbildung 7-17 dar (Anforderung Schem_5) und beinhaltet eine kurze und eine lange Beschreibung der Red Flags. Für den Auditor ist besonders wichtig, dass er das entsprechende Red Flag eindeutig versteht und somit richtige Schlüsse zieht.

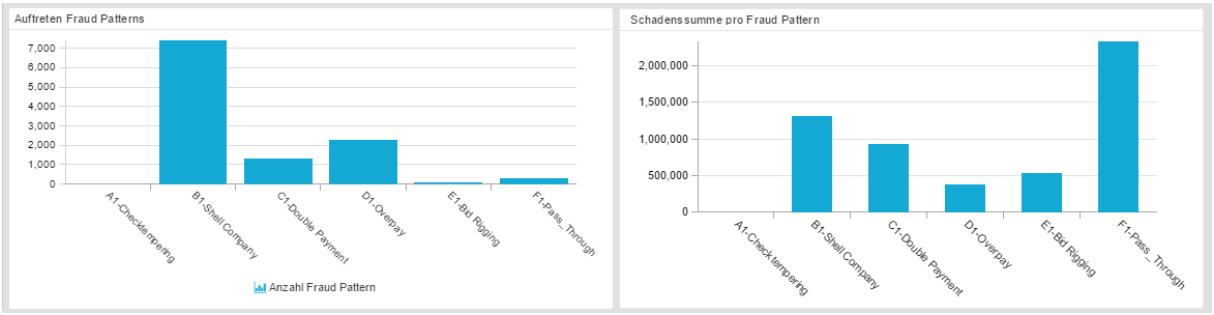


Abbildung 7-18: High-fidelity Prototyp - Verteilung der Fraud Patterns

Quelle: Screenshot Celonis Process Mining

Im unteren Bereich der Schemasicht sind zwei Diagramme dargestellt, die die Verteilung der Fraud Patterns beschreiben (vergl. hierzu Abbildung 7-18). Das Diagramm ‚Auftreten Fraud Patterns' zeigt die Häufigkeit der aufgetretenen Fraud Patterns an (Anforderung Schem_3d). In dieser Abbildung ist das Fraud Pattern Scheinfirma am häufigsten aufgetreten, während Rechnungsfälschung überhaupt nicht identifiziert wurde. Das zweite Diagramm ‚Schadenssumme pro Fraud Pattern' zeigt den wahrscheinlichen Verlust pro Fraud Pattern (Anforderung Schem_4a). So ist beispielsweise ersichtlich, dass Scheinfirma zwar häufig auftritt, allerdings die Gesamtschadenssumme dabei eher gering ist. Pass-Through Fraud kommt in diesem Datensatz recht gering vor, ist aber durch eine hohe Schadenssumme gekennzeichnet.

Die Anforderung Red Flags und Fraud Patterns in Diagrammen darzustellen ist insgesamt nachgekommen (Anforderung Schem_06). Lediglich der zeitliche Verlauf der Red Flags kann in dieser Implementierung nicht nachgekommen werden, da die Red Flags kein Datumsfeld besitzen (Anforderung Schem_07).

Mitarbeitersicht

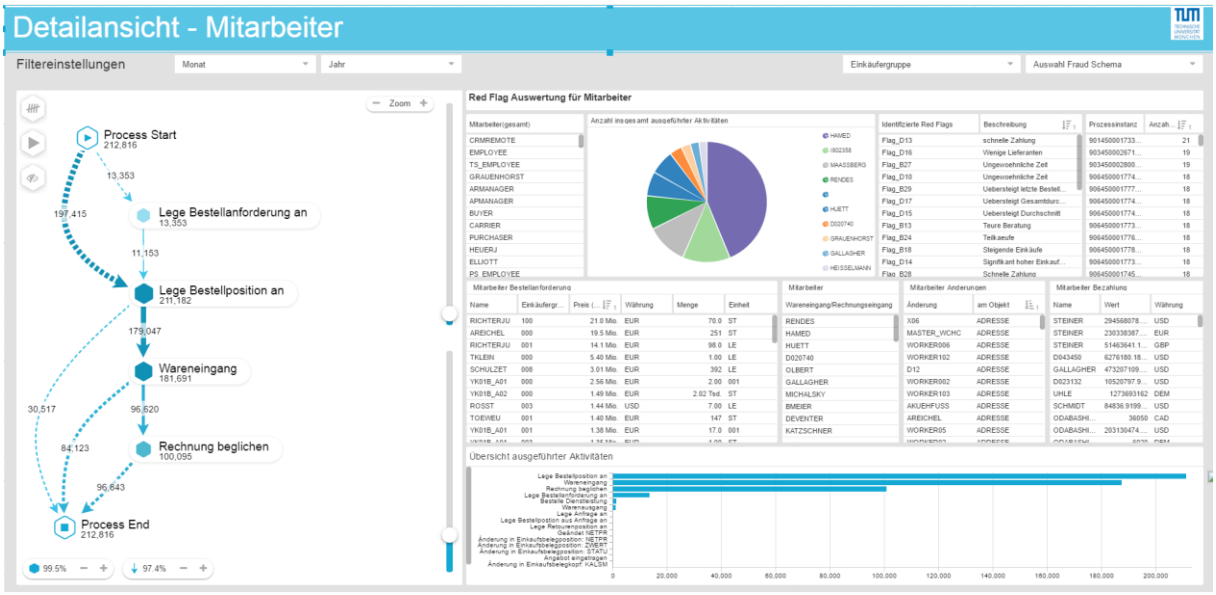


Abbildung 7-19: High-fidelity Prototyp – Mitarbeitersicht

Quelle: Screenshot Celonis Process Mining

Die Mitarbeitersicht, wie in Abbildung 7-19 gezeigt, enthält ebenfalls den Prozessexplorer. Der Fokus dieser Sicht liegt auf Informationen zu den beteiligten Mitarbeitern. Bei Filterung nach bestimmten auffälligen Prozessinstanzen können in dieser Sicht die beteiligten Mitarbeiter analysiert werden.

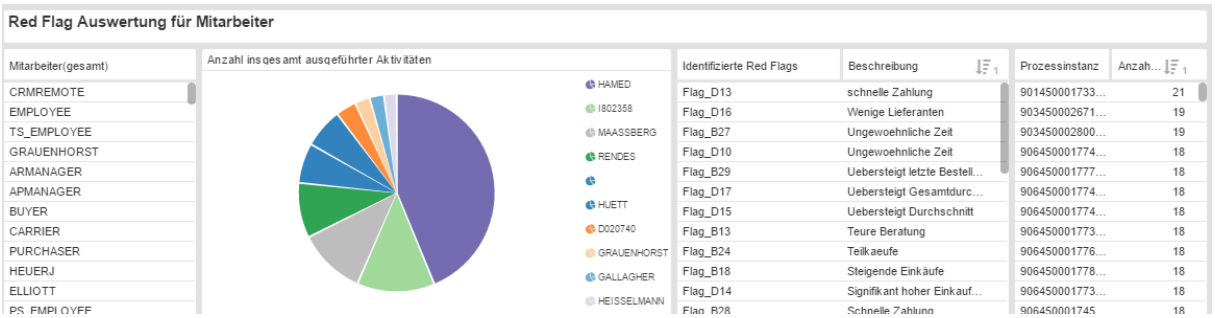
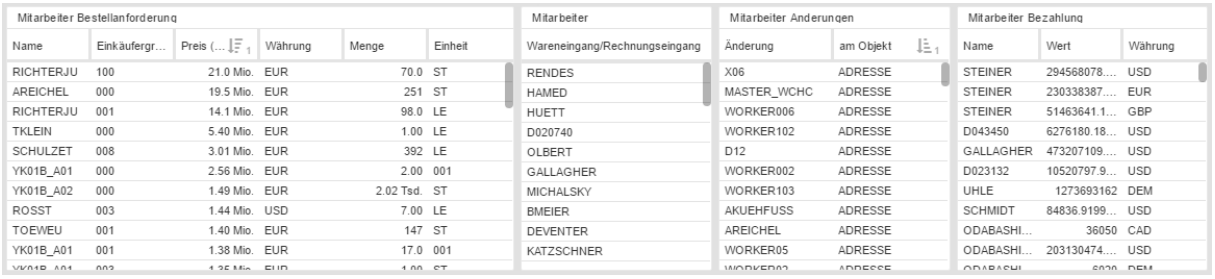


Abbildung 7-20: High-fidelity Prototyp- Red Flags Auswertung für Mitarbeiter

Quelle: Screenshot Celonis Process Mining

Abbildung 7-20 zeigt eine vergrößerte Ansicht des oberen rechten Teils der Mitarbeitersicht. In der Tabelle ‚Mitarbeiter gesamt' werden alle am Einkaufsprozess beteiligten Mitarbeiter angezeigt (Anforderung Mitarb_01). Bei Filterung auf eine bestimmte Prozessinstanz werden nur die daran beteiligten Mitarbeiter sichtbar (Anforderung Mitarb_04). Ein Kreisdiagramm ‚Anzahl insgesamt ausgeführter Aktivitäten' zeigt die Anzahl der ausgeführten Aktivitäten pro Benutzer an (Anforderung Mitarb_05). Auch wird die Anzahl der Vorgänge, die von einem Mitarbeiter erledigt werden, dargestellt. Daneben werden die identifizierten Red Flags und die Anzahl von Red Flags pro Prozessinstanz dargestellt.



Mitarbeiter Bestellanforderung

Name	Einkäufergr…	Preis (…	Währung	Menge	Einheit
RICHTERJU	100	21.0 Mio.	EUR	70.0	ST
AREICHEL	000	19.5 Mio.	EUR	251	ST
RICHTERJU	001	14.1 Mio.	EUR	98.0	LE
TKLEIN	000	5.40 Mio.	EUR	1.00	LE
SCHULZET	008	3.01 Mio.	EUR	392	LE
YK01B_A01	000	2.56 Mio.	EUR	2.00	001
YK01B_A02	000	1.49 Mio.	EUR	2.02 Tsd.	ST
ROSST	003	1.44 Mio.	USD	7.00	LE
TOEWEU	001	1.40 Mio.	EUR	147	ST
YK01B_A01	001	1.38 Mio.	EUR	17.0	001

Mitarbeiter

Wareneingang/Rechnungseingang
RENDES
HAMED
HUETT
D020740
OLBERT
GALLAGHER
MICHALSKY
BMEIER
DEVENTER
KATZSCHNER

Mitarbeiter Änderungen

Änderung	am Objekt
X06	ADRESSE
MASTER_WCHC	ADRESSE
WORKER006	ADRESSE
WORKER102	ADRESSE
D12	ADRESSE
WORKER002	ADRESSE
WORKER103	ADRESSE
AKUEHFUSS	ADRESSE
AREICHEL	ADRESSE
WORKER05	ADRESSE

Mitarbeiter Bezahlung

Name	Wert	Währung
STEINER	294568078.…	USD
STEINER	230338387.…	EUR
STEINER	51463641.1…	GBP
D043450	6276180.18…	USD
GALLAGHER	473207109.…	USD
D023132	10520797.9…	USD
UHLE	1273693162	DEM
SCHMIDT	84836.9199…	USD
ODABASHI…	36050	CAD
ODABASHI…	203130474.…	USD

Abbildung 7-21: High-fidelity Prototyp - Detailansicht Mitarbeiter

Quelle: Screenshot Celonis Process Mining

Die zweite Reihe der Mitarbeitersicht zeigt die beteiligten Mitarbeiter entlang des Einkaufsprozesses, sprich welche Mitarbeiter an der Bestellanforderung, Bestellung, Zahlung usw. beteiligt sind (vergl. Abbildung 7-21). Besonders interessant ist diese Übersicht, wenn nach einer auffälligen Prozessinstanz gefiltert wurde. In der ersten Tabelle ‚Mitarbeiter Bestellanforderung' werden die beteiligten Mitarbeiter der Bestellanforderung und Bestellung angezeigt. Dazu gehören auch Informationen zur Einkäufergruppe, Preis aller Bestellungen, Währung, Menge und Mengeneinheit (Anforderung Mitarb_03). In einer weiteren Tabelle ‚Waren- und Rechnungseingang' werden die Benutzer angezeigt, die den Waren- bzw. Rechnungseingang in das SAP ERP System eingetragen hat. Eine weitere Tabelle ‚Mitarbeiter Änderungen' zeigt ob es Änderungen an den Objekten gab und ggf. welcher Mitarbeiter diese Änderung durchgeführt hat. So wird beispielsweise angezeigt, wenn ein Mitarbeiter die Adresse oder Kontonummer des Lieferanten verändert hat. Die letzte Tabelle ‚Mitarbeiter Bezahlung' zeigt die für die Bezahlung verantwortlichen Mitarbeiter an (Anforderung Mitarb_07). Hier wird die Anforderung umgesetzt, dass die Einkäufergruppe, Einkaufsvolumen und Menge dargestellt werden soll.

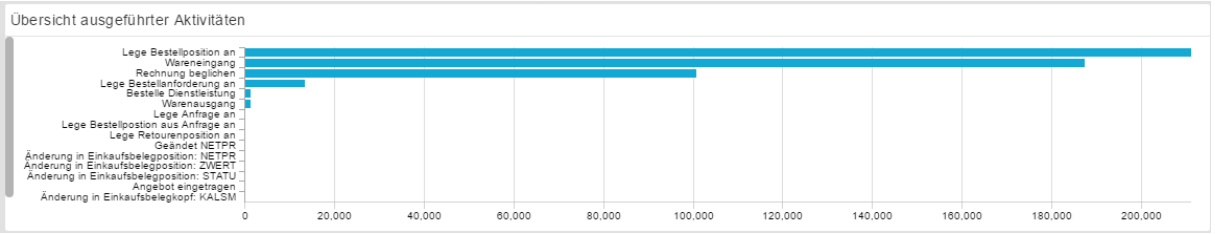


Abbildung 7-22: High-fidelity Prototyp: Übersicht der ausgeführten Aktivitäten

Quelle: Screenshot Celonis Process Mining

Im unteren Abschnitt der Mitarbeitersicht werden die einzelnen Aktivitäten im Verhältnis zur Häufigkeit ihres Auftretens im Datensatz gesetzt (Anforderung Mitarb_05). Einige Anforderungen können nicht umgesetzt werden. Die Art des Users (Dialog vs. Systembenutzer) kann nicht aus den entsprechend extrahierten Tabellen entnommen werden (Anforderung Mitarb_02). Zusätzlich kann kein soziales Netzwerk der Mitarbeiter dargestellt werden (Anforderung Mitarb_06), da dies mit der verwendeten Version von Celonis nicht möglich ist.

Lieferantensicht:

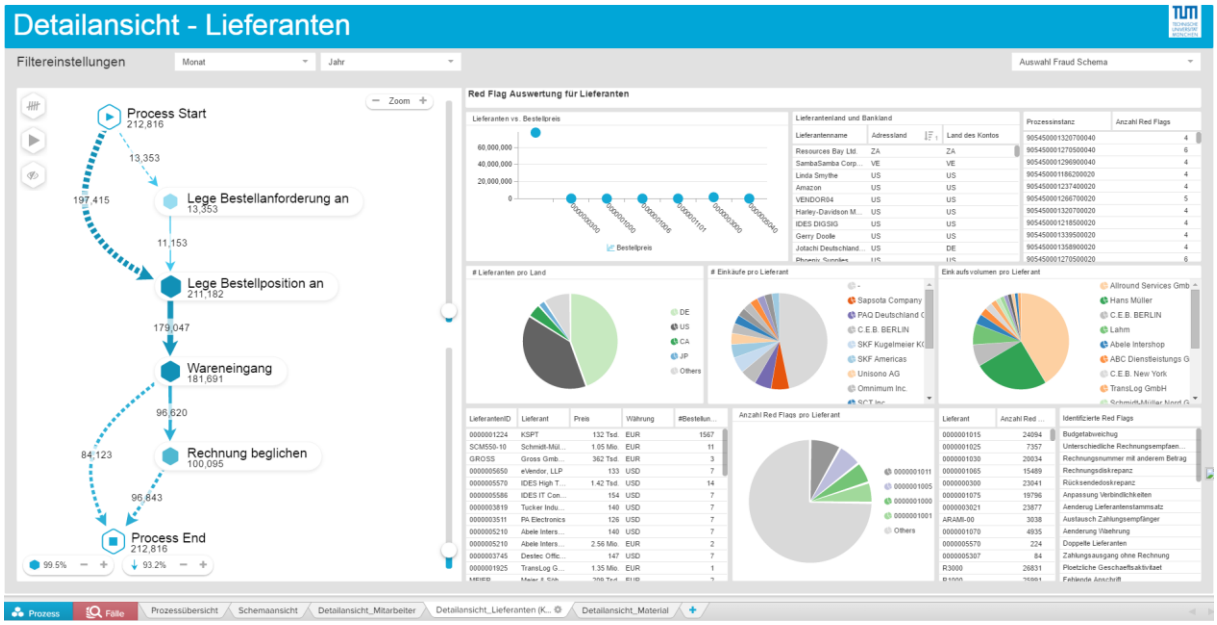


Abbildung 7-23: High-fidelity Prototyp – Lieferantensicht

Quelle: Screenshot Celonis Process Mining

Die Lieferantensicht stellt die relevanten Informationen bezüglich des Lieferanten im Einkaufsprozess dar. Wie in allen anderen Sichten stellt der linke Teil des Dashboards den Prozessexplorer dar. Der rechte Teil wird im Folgenden näher erläutert.

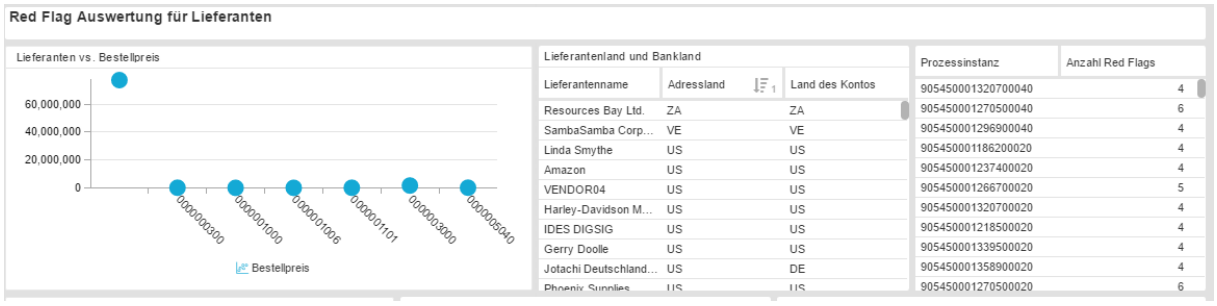


Abbildung 7-24: High-fidelity Prototyp- Red Flag Auswertung für Lieferanten

Quelle: Screenshot Celonis Process Mining

Auf der obersten Ebene der Lieferantensicht (vergl. Abbildung 7-24) ist ein Streudiagramm zu sehen, welches die Verteilung der Lieferanten anhand ihres Verkaufsvolumens anzeigt. So können Ausreißer identifiziert werden, wie beispielsweise sehr hohe Einkaufsvolumina bei einem Lieferanten (Anforderung Lief_03). Die Tabelle ‚Lieferantenland und Bankenland' zeigt den Sitz des Lieferanten (Land) und das Land, in dem sein Konto liegt (Anforderung Lief_01). Interessant ist diese Tabelle, wenn die Länder voneinander abweichen. Der Anforderung ‚Abweichungen von Adressland und Land des Kontos farbig zu markieren' kann nicht nachgegangen werden, da es in der verwendeten Celonis Version keine Möglichkeit gibt

einzelne Zeilen nach einer Wenn-Bedingung farblich zu markieren. Die letzte Tabelle zeigt die Prozessinstanz mit der Anzahl der identifizierten Red Flags an.

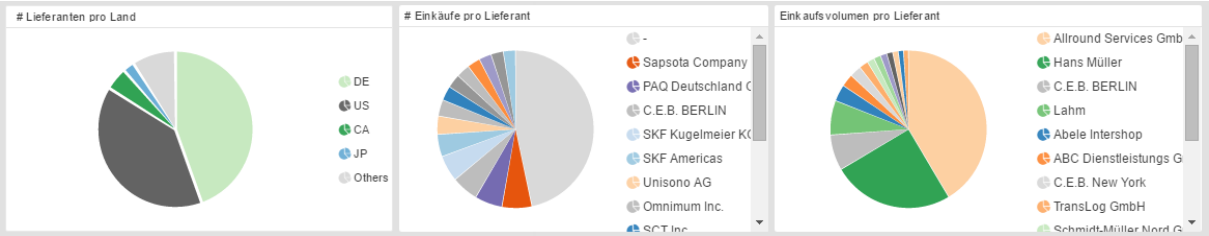


Abbildung 7-25: High- fidelity Prototyp - Kennzahlen Lieferanten

Quelle: Screenshot Celonis Process Mining

Die mittlere Reihe der Lieferantensicht zeigt einige Kennzahlen in Kreisdiagrammen an (vergl. Abbildung 7-25). Das erste Kreisdiagramm ‚#Lieferanten pro Land' zeigt die Anzahl der Lieferanten pro Land an (Anforderung Lief_06), das zweite Diagramm ‚#Einkäufe pro Lieferant' die Anzahl der Einkäufe pro Lieferant (Anforderung Lief_04a) und das dritte Diagramm ‚Einkaufsvolumen pro Lieferant' das Einkaufsvolumen pro Lieferant (Anforderung Lief_04b). Die Anforderung das auffällige Einkaufsvolumen im Vergleich zum gesamten Einkaufsvolumen darzustellen (Anforderung Lief_02) kann nicht nachgegangen werden, da keine Möglichkeit gefunden wurde das Verhältnis in Celonis auszurechnen.

Die unterste Ebene der Lieferantensicht zeigt einige grundlegende Informationen zum Lieferanten (vergl. Abbildung 7-26). Die erste Tabelle stellt allgemeine Informationen zum Lieferanten dar, wie die ID, den Namen des Lieferanten, die gesamte Bestellsumme bei diesem Lieferanten, die Währung der Bestellungen und die Anzahl aller Bestellungen bei diesem Lieferanten (Anforderung Lief_09). Durch den Jahres- und Monatsfilter kann die Anzahl und der Preis entsprechend gefiltert werden. Das mittlere Kreisdiagramm ‚Anzahl Red Flags pro Lieferant' zeigt die Anzahl der Red Flags pro Lieferant (Anforderung Lief_08) und hilft bei der Identifikation von Lieferanten mit den meisten aufgetretenen Red Flags. Die rechten beiden Tabellen zeigen die Anzahl von Red Flags pro Lieferant und die ID und Beschreibung der identifizierten Red Flags.

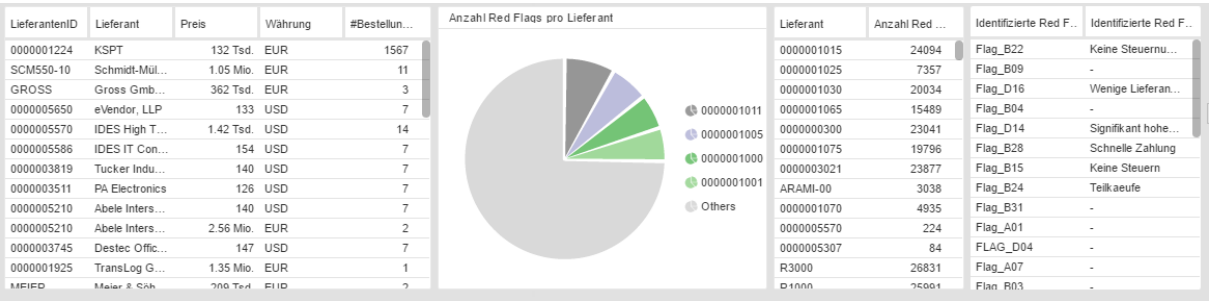


Abbildung 7-26: High-fidelity Prototyp - Grundlegende Informationen zum Lieferanten

Quelle: Screenshot Celonis Process Mining

Die Anforderung ‚die Distanz zwischen dem Besteller und dem Lieferanten darzustellen' (Anforderung Lief_05), um die Sinnhaftigkeit beim Bezug entfernter Ware zu bewerten, kann nicht nachgegangen werden, da SAP und Celonis Tabellen keine Distanzangaben haben. Die Anforderungen Lief_07 wird als Red Flag implementiert

Materialsicht

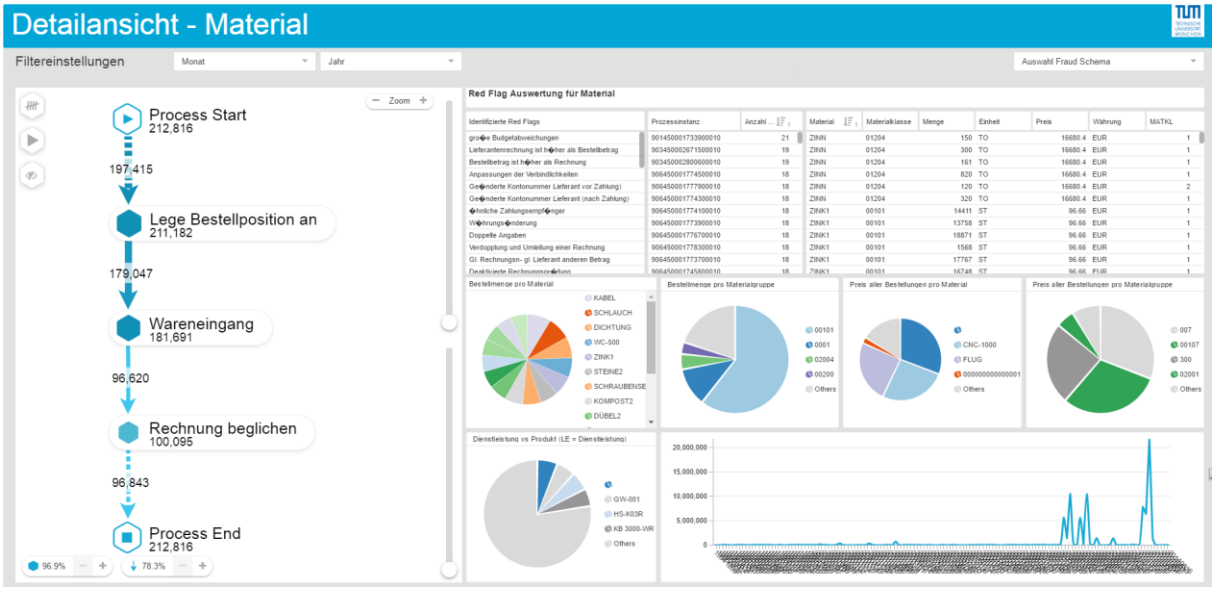
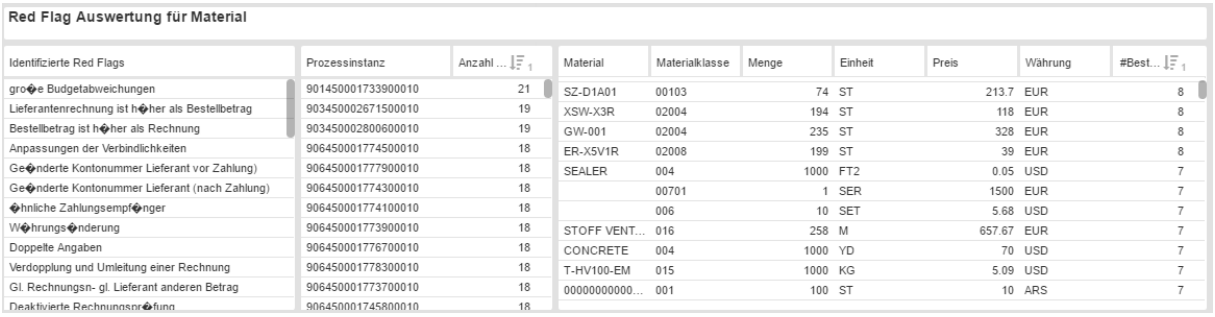


Abbildung 7-27: High-fidelity Prototyp – Materialsicht

Quelle: Screenshot Celonis Process Mining

Die Materialsicht stellt detaillierte Informationen zu den gekauften Materialien und Dienstleistungen dar. Im Folgenden werden die entsprechenden Teile gesondert beschrieben. In der obersten Reihe der Materialsicht (vergl. Abbildung 7-28) werden die identifizierten Red Flags tabellarisch dargestellt. Die zweite Tabelle zeigt die Prozessinstanz mit der entsprechenden Anzahl an Red Flags. Die rechte Tabelle zeigt allgemeine Informationen über das Material, wie die ID, eine Beschreibung, die Materialklasse, die Bestellmenge und Bestelleinheit (Stück, Paletten, Leistungseinheit…), sowie die Bestellsumme und Währung (Anforderung Mat_01).



Red Flag Auswertung für Material

Identifizierte Red Flags	Prozessinstanz	Anzahl …
gro€e Budgetabweichungen	90145000173390010	21
Lieferantenrechnung ist h€her als Bestellbetrag	90345000267150010	19
Bestellbetrag ist h€her als Rechnung	90345000280060010	19
Anpassungen der Verbindlichkeiten	90645000177450010	18
Ge€nderte Kontonummer Lieferant vor Zahlung)	90645000177790010	18
Ge€nderte Kontonummer Lieferant (nach Zahlung)	90645000177430010	18
€hnliche Zahlungsempf€nger	90645000177410010	18
W€hrungs€nderung	90645000177390010	18
Doppelte Angaben	90645000177670010	18
Verdopplung und Umleitung einer Rechnung	90645000177830010	18
Gl. Rechnungsn- gl. Lieferant anderen Betrag	90645000177370010	18
Deaktivierte Rechnungspr€fung	90645000174580010	18

Material	Materialklasse	Menge	Einheit	Preis	Währung	#Best…
SZ-D1A01	00103	74	ST	213.7	EUR	8
XSW-X3R	02004	194	ST	118	EUR	8
GW-001	02004	235	ST	328	EUR	8
ER-X5V1R	02008	199	ST	39	EUR	8
SEALER	004	1000	FT2	0.05	USD	7
	00701	1	SER	1500	EUR	7
	006	10	SET	5.68	USD	7
STOFF VENT…	016	258	M	657.67	EUR	7
CONCRETE	004	1000	YD	70	USD	7
T-HV100-EM	015	1000	KG	5.09	USD	7
00000000000…	001	100	ST	10	ARS	7

Abbildung 7-28: High-fidelity Prototyp - Red Flag Auswertung Material

Quelle: Screenshot Celonis Process Mining

Die zweite Reihe der Materialsicht beinhaltet einige Kreisdiagramme (vergl. Abbildung 7-29). Das erste und zweite Kreisdiagramm ‚Bestellmenge pro Material' und ‚Bestellmenge pro Materialgruppe' zeigen die Bestellmenge pro Material bzw. pro Materialgruppe (Anforderung Mat_02a, Mat_02b). Hier erkennt ein Auditor, wie häufig Materialien bezogen werden. Die Diagramme ‚Preis aller Bestellungen pro Material' und ‚Preis aller Bestellungen pro Materialgruppe' zeigen entsprechende die Preise an (Anforderung Mat_03a, Mat_03b). Bei ungewöhnlich hohen Preisen kann der Auditor diese im Detail betrachten und danach filtern.

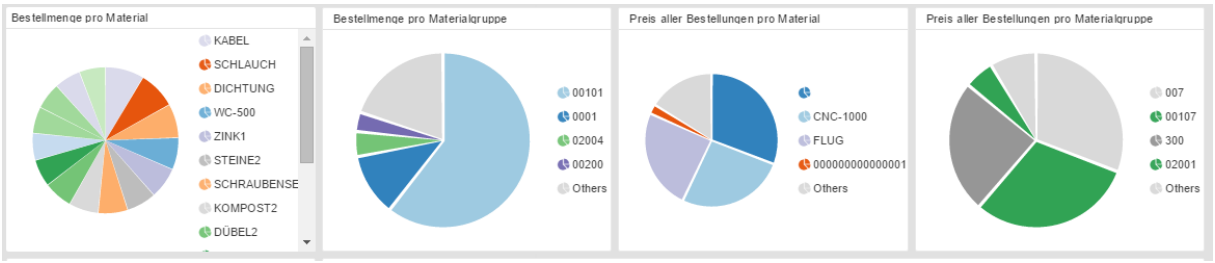


Abbildung 7-29: High-fidelity Prototyp- Kreisdiagramme Material

Quelle: Screenshot Celonis Process Mining

Auf der untersten Ebene der Materialsicht werden zwei Diagramme dargestellt (vergl. Abbildung 7-30). Das erste Diagramm ‚Dienstleistung vs. Produkt' stellt die Anzahl der bestellten Dienstleistungen in Relation zu den bestellten Materialien dar. Diese Unterscheidung ist hilfreich, da Dienstleistungen aufgrund ihres immateriellen Charakters von großer Bedeutung in der Fraud Identifikation sind. Ein Auditor kann beispielsweise in diesem Diagramm nach Dienstleistungen filtern und alle Diagramme aktualisieren sich entsprechend (Anforderung Mat_06). Ein Liniendiagramm zeigt den zeitlichen Verlauf der Bestellpreise (Anforderung Mat_08). So können rasant steigende Einkäufe eines bestimmten Materials oder Dienstleistung identifiziert werden. Auch können die Daten eines bestimmten Peak-Bereichs selektiert werden.

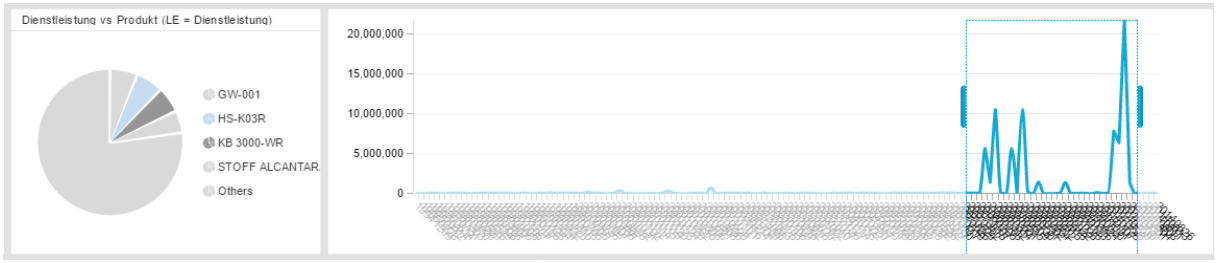


Abbildung 7-30: High-fidelity Prototyp - Verlauf der Bestellpreise

Quelle: Screenshot Celonis Process Mining

Auch hier können einige Anforderungen nicht erfüllt werden. In den vorhandenen SAP Tabellen sind keine Hinweise auf die Verderblichkeit der Materialien vorhanden (Anforderung Mat_04), so dass diese Unterscheidung nicht vorgenommen wird. Die Unterscheidung zwischen Commodity und Spezialmaterial kann nicht getroffen werden (Anforderung Mat_05), da jedes Unternehmen Commodity anders definiert und ebenfalls keine Unterscheidung in den SAP Tabellen vorhanden ist. Auch die Anforderung Logistikeinkäufe darzustellen kann nicht erfüllt werden, da die entsprechenden Felder ebenfalls nicht im Datensatz identifiziert wurden (Anforderung Mat_08).

7.5 Zusammenfassung der Ergebnisse

In diesem Kapitel wird das zuvor identifizierte Vorgehen nach Albrecht et al. (2012) und Bozkaya et al. (2009) auf den Einkaufsprozess angewendet. Zunächst werden in der analytischen Ebene mögliche Red Flags identifiziert und in das Kategorisierungsschema des ACFE Baumes eingeordnet, um so Fraud Patterns abzuleiten. Insgesamt werden acht Fraud Patterns im Einkaufsprozess identifiziert, die konkret folgende sind: Kickback Fraud, Angebotsmanipulation, Scheinfirma, Doppelte Bezahlung, Pass-Through, unbeteiligter Lieferant, Rechnungsmanipulation und private Einkäufe. Die entsprechenden Fraud Patterns werden durch Experteninterviews validiert, wobei zehn Experten mit folgenden Positionen im Unternehmen befragt werden: Audit Director, Audit Manager, Procurement Engineer, Internal Audit Leitung, Strategischer Einkauf, SCM Procurement Governance und Senior Data Analyst. Ihre Aufgabe ist es Red Flags als irrelevant, relevant oder besonders relevant für das entsprechende Fraud Pattern einzustufen. Zusätzlich sollen diese fehlende Fraud Patterns und Red Flags ergänzen. Basierend auf diesen Ergebnissen werden die Fraud Patterns angepasst.

Auf technischer Ebene wird der Prototyp implementiert. Zunächst werden Informationen aus den entsprechenden SAP Tabellen in das für Celonis Process Mining notwendige Format gebracht. Hierzu werden Fall-, Aktivitäts- und Prozesstabellen erstellt und entsprechend durch den ETL Prozess befüllt. Der Einkaufsprozess kann anschließend mit dem Prozessexplorer analysiert werden. Um die Analyse von wirtschaftskriminellem Verhalten zu ermöglichen, werden Prozessinstanzen mit vorkommenden Red Flags verknüpft. Dazu wird eine externe Datenstruktur aufgebaut, die einfach im Celonis PM Tool angebunden werden kann. Diese sieht die Erweiterung der Fall-, Aktivitäts- und Prozesstabellen um vier weitere Tabellen vor, in denen die identifizierten Red Flags und Fraud Patterns gespeichert werden und die die Anzeige aufgetretener Red Flags entlang der Prozessinstanz im Dashboard ermöglicht. Zur Identifikation der Red Flags wird ein SQL Skript auf Datenbankebene implementiert. Die Celonis-eigene Abfragesprache PQL hat sich als nicht mächtig genug für die Identifikation von Red Flags erwiesen.

Um explorative Analysen zur Identifikation von wirtschaftskriminellem Verhalten zu ermöglichen, wird ein Dashboard auf Basis von Celonis PM erstellt. Zunächst werden Anforderungen aus der Literatur in einem low-fidelity Prototyp umgesetzt. Mit Hilfe der Thinking Aloud Methode werden zwei Auditoren und sieben Teilnehmer des White Collar Hacking Contests gebeten, bestimmte Aufgaben mit dem Prototypen zu lösen und währenddessen ihre Gedanken laut auszusprechen. Diese werden zusätzlich befragt, welche Informationen ihnen zur Beantwortung der Aufgaben fehlen. Auf Basis dieser Informationen werden Anforderungen für den high-fidelity Prototypen entwickelt. Der high-fidelity Prototyp besteht aus fünf Sichten, die konkret folgende sind: Prozesssicht, Schemasicht, Mitarbeitersicht, Lieferantensicht und Materialsicht. Im Dashboard sind alle verwendeten Tabellen und Diagramme interaktiv. Aus jedem Objekt kann ein Filter gesetzt werden, der entsprechend alle anderen Tabellen in jeder Sicht aktualisiert. So kann beispielsweise nach auffälligen Prozessinstanzen, nach bestimmten Fraud Patterns oder nach Prozessinstanzen mit einer hohen Anzahl von aufgetretenen Red Flags gefiltert werden.

8 Evaluation

Der hier vorgestellte Prototyp soll als nächstes evaluiert werden. Dazu werden zunächst einige Methoden der Evaluation zusammengefasst, bevor der Prototyp auf verschiedene Datensätze angewendet wird.

8.1 Methode zur Evaluation

Neben der Entwicklung des Artefaktes ist die zweite Aktivität der gestaltungsorientierten Forschung die Evaluation, welche sich mit der systematischen Bewertung der entwickelten Artefakte beschäftigt (March & Smith, 1995). Das Evaluationsergebnis hilft ein besseres Problemverständnis zu erlangen und die Qualität des Artefaktes zu verbessern (Hevner et al., 2004). Die betrachteten Bewertungsdimensionen sind dabei die Nützlichkeit, die Qualität und die Effizienz bei der Lösung der adressierten Problemstellung (Hevner et al., 2004). Dabei gibt es verschiedene Methoden, die zur Evaluation des Prototyps verwendet werden können (Hevner et al., 2004). Diese werden in Tabelle 45 dargestellt. Die Methoden werden gemäß ihrer zugrundeliegenden Vorgehensweise in beobachtend, analytisch, experimentell, testend und beschreibend aufgeteilt:

Art	Methode	Beschreibung
Beobachtend	Fallstudie	Untersuchung des Artefakts im jeweiligen Geschäftsumfeld
	Feldstudie	Beobachtung der Nutzung des Artefakts in Projekten
Analytisch	Statische Analyse	Untersuchung der Struktur des Artefakts
	Architekturanalyse	Untersuchung der Integrationsfähigkeit des Artefakts in technische Infrastruktur
	Optimierung	Demonstration der Optimalität des Artefakts für den Zweck oder Aufzeigen der Grenzen der Optimierung
	Dynamische Analyse	Untersuchung des Laufzeitverhaltens des Artefakts
Experimentell	Kontrolliertes Experiment	Untersuchung von Artefakteigenschaften unter kontrollierten Bedingungen
	Simulation	Ausführen des Artefakts unter Nutzung nicht-realer Daten
Testend	Funktionale Tests	Verwendung der Schnittstellen des Artefakts, um Fehler zu finden (Black Box Tests)
	Strukturelle Tests	Testen der inneren Funktionsweise des Artefakts, um Fehler zu finden (White Box Test)
Beschreibend	Experteninterview	Begründung der Nützlichkeit des Artefakts durch Informationen aus der Wissensbasis

Szenario	Erstellung von Verwendungsszenarios, um die Nützlichkeit des Artefakts zu zeigen

Tabelle 45: Methoden zur Evaluation

Quelle: Eigene Darstellung basierend auf Hevner et al., (2004)

Zunächst erscheinen funktionale Tests sinnvoll, da hierdurch die funktionalen Anforderungen an das Artefakt getestet werden können. Dazu werden in einem ersten Schritt Daten künstlich mit Hilfe eines Datengenerators erstellt. Der Prototyp soll anschließend die im Generator implementierten wirtschaftskriminellen Handlungen identifizieren. Um die Funktionsfähigkeit auch bei nicht selbst implementierte Fraud Cases zu prüfen, wird im zweiten Schritt ein kontrolliertes Experiment durchgeführt, der so genannte White Collar Hacking Contest (WCHC). Im WCHC begehen die Teilnehmer zunächst Fraud in einem fiktiven Unternehmen in einem SAP ERP System und identifizieren nach einem Datentausch den Fraud der anderen Teilnehmer. Die hierbei entstandenen Datensätze werden mit dem Prototypen analysiert und entsprechend mit den jeweiligen Präsentationen der Teilnehmer ausgewertet.

Als letztes werden Fallstudien in zwei Unternehmen durchgeführt, bei denen der Prototyp auf reale Datensätze angewendet wird. Beide Datensätze wurden bereits von professionellen Fraud Investigatoren hinsichtlich Fraud untersucht. Ohne dieses Wissen wird zunächst Fraud identifiziert und anschließend mit den professionellen Ergebnissen verglichen.

8.2 Evaluation mit einem synthetischen Datensatz

Zur Evaluation des Prototyps mit einem synthetischen Datensatz wird zunächst erklärt, wie der Datengenerator implementiert wird. Anschließend wird dargestellt, wie der Prototyp Fraud aufdeckt.

8.2.1 Fraud Datengenerierung

Aus Sicherheitsgründen sind wenige Unternehmen bereit echte Datensätze an Forscher weiterzureichen, vor allem, wenn diese Fraud im Datensatz vermuten (Yannikos et al., 2011). Aus diesem Grund werden zunächst synthetische Daten generiert. Hierfür wird ein Datengenerator[36] entwickelt, der normale und fraudulente Daten im SAP ERP Einkaufsprozess erstellt. Auf Basis dieser Daten kann anschließend der Prototyp validiert werden. Der Vorteil synthetisch hergestellter Daten ist, dass die Anzahl und Art des enthaltenen Frauds bereits im Voraus bekannt ist. Daraus können Metriken wie die falsch-positiv oder richtig-positiv Rate berechnet werden. Im Folgenden wird die Implementierung des Datengenerierungstools kurz dargestellt.

Das Datengenerierungstool ist mit Hilfe der SAP-internen Programmiersprache ABAP entwickelt und verwendet neben Automatisierungstechniken Application Programming Interfaces (BAPIs) und Batch Input Maps. Es generiert Daten im SAP Einkaufsprozess.

[36] Vergleich hierzu Baader, Meyer, Wagner, and Krcmar (2016) und Wagner (2014)

8.2.1.1 Ähnliche Ansätze der Datengenerierung aus der Literatur

Zunächst sollen hier vergleichbare Ansätze aus der Literatur zur synthetischen Generierung von Datensätzen diskutiert werden. Synthetische Nutzerdaten können als Daten definiert werden, die durch einen simulierten Nutzer, der simulierte Aktionen in einem künstlichen Umfeld durchführt erzeugt werden (Barse et al., 2003). Man unterscheidet grundsätzlich zwischen zwei Annährungsweisen für die Datengenerierung: die analytische und die konstruktive Vorgehensweise.

Der analytische Ansatz basiert auf die Extrapolation von historischen Nutzerdaten. Dabei besteht es aus fünf Phasen (Barse et al., 2003): (1) Datensammlung, (2) Analyse von historischen Daten um Parameter zu identifizieren, (3) Nutzerprofile erstellen (4) Nutzer- und (5) Systemverhalten modellieren. Der Vorteil des analytischen Ansatzes ist die Datenauthentizität. Der Nachteil ist die Abhängigkeit des synthetischen Datensatzes von der Datenqualität des Beispieldatensatzes. Einige Beispiele dieses Ansatzes im Kontext der Fraud Erkennung sind von Lundin, Kvarnström & Jonsson (2002) oder Barse et al. (2003). In der verwandten Disziplin des Intrusion Detection sind die Arbeiten von Muthukrishnan, Chandrasekaran & Upadhyaya (2004), Greenberg (1988) oder Schonlau (1998) interessant.

Der konstruktive Ansatz modelliert Benutzerverhalten basierend auf Expertenwissen. Zunächst werden Benutzerverhalten basierend auf verschiedenen Abstraktionslevel innerhalb eines Systems definiert. Anschließend wird ein dreischichtiger stochastischer Nutzersimulator als Markov Prozessketten erstellt und generiert (Yannikos et al., 2011). Der Vorteil dieses Verfahrens ist, dass das Nutzerverhalten basierend auf bestimmten Anforderungen hin modelliert werden kann. Der größte Nachteil ist die mathematische Komplexität dieses Ansatzes. Der konstruktive Ansatz wird unter anderem von Yannikos et al. (2011) im Bereich Fraud Detektion verwendet.

Das Datengenerierungstool folgt dem konstruktiven Ansatz, da der Datensatz möglichst viele Fraud Szenarien enthalten soll. Ein sehr ähnlicher Ansatz wird von Islam et al. (2010) vorgestellt. Diese simulieren Benutzerverhalten im Einkaufsprozess eines SAP ERP Systems, indem sie die entsprechenden SAP Tabellen mit zufälligen Daten durch einen Zufallsgenerator befüllen (Islam et al., 2010). Ihre Benutzersimulation basiert auf keinem Modellierungsansatz. Im Vergleich zu diesem Ansatz wird in dieser Arbeit die in der Literatur identifizierten Fraudschemata als Basis gewählt.

8.2.1.2 Anforderungen für die Datengenerierung

Um einen möglichst realistischen Datensatz zu generieren, werden zunächst Anforderungen an den Datensatz aus der Literatur erhoben. Diese sind größtenteils aus Publikationen zur synthetischen Datengenerierung für Fraud Daten entnommen und sollen hier kurz beschrieben werden.

- Die Generierung eines ausreichend großen Datensatzes um die Skalierbarkeit des Fraud Entdeckungsverfahrens testen zu können ist notwendig (Griffin, 2012; A. Islam et al., 2011).

- Fraudulente und normale Daten sollen im Datensatz enthalten sein (Barse et al., 2003).
- Eine graphische Benutzeroberflächse ist notwendig, um das Verhältnis der zu generierenden Fraud Szenarien in Relation zu normalen Daten darstellen zu können.
- Der beteiligte Benutzer in einer Transaktion oder in einem Simulationslauf sollte identifizierbar sein (Mercuri, 2003).
- Normales Verhalten sollte möglichst nah an der Realität modelliert werden. Dieses beeinflusst laut einer Studie von Maxion und Tan (2000) die Erkennungsrate von Fraud Algorithmen.
- Zufällige Generierungen von Parametern durch den Prozessverlauf sind notwendig, wie beispielsweise die Anzahl der bestellten Waren oder das Bestelldatum.
- Ein Indikator sollte vorhanden sein, der für jede Transaktion anzeigt, ob es sich um Fraud oder keinen Fraud handelt (Lundin et al., 2002).
- Möglichst viele realistische Fraud Szenarien sollen im Datensatz inkludiert sein.
- Die Anzahl und Verteilung der fraudulente Aktivitäten sollte so realitätsnah wie möglich sein.

Um also normales und fraudulentes Verhalten zu implementieren, wird zunächst der ‚Standard Einkaufsprozess', sowie die in der Literatur identifizierten Fraudschemata implementiert. Da sich für jedes identifizierte Schema noch leichte Abweichungen darstellen lassen, wird im Folgenden ein kurzer Überblick über die exakte Implementierung der Fraudschemata gegeben.

- Ausnutzung eines Rahmenvertrags

Um regelmäßig Geschäfte mit einem Geschäftspartner durchzuführen, werden oft Rahmenverträge geschlossen. Hierfür wird häufig im Einkaufsprozess auf die Verwendung eines Freigabemechanismus verzichtet (Bönner et al., 2011). Unternehmen profitieren häufig von diesen Rahmenverträgen, da zum einen die Einkaufsabteilung entlastet wird und zum anderen durch größere Einkaufsvolumen Vorteile in den Vertragskonditionen ausgehandelt werden. Fehlende Kontrollmaßnahmen im RV-Management bieten allerdings zahlreiche Möglichkeiten für betrügerisches Verhalten. Zum Beispiel können nicht mehr gültige Rahmenverträge genutzt werden, um den Freigabe-Mechanismus zu umgehen. Es kann sich entweder durch Abrufe aus bereits ausgeschöpften oder bereits abgelaufenen Rahmenverträgen manifestieren (Bönner, Riedl, & Wenig, 2011). Deshalb ist dieses implementierte Szenario dem Pattern „Persönliche Einkäufe" unterzuordnen, da diese Rahmenverträge für den Einkauf von Waren für den persönlichen Gebrauch oder Weiterverkauf verwendet werden können. Im SAP ERP können Rahmenverträge als Mengen- oder als Wertverträge angelegt werden, je nachdem wodurch die Begrenzung der abrufbaren Quantität festgelegt wird (SAP, 2014). Der Einfachheit halber werden nur Mengenkontrakte betrachtet. Ebenso wird „unwirtschaftliche" Rahmenvertragsverwendung, z.B. günstigere Preise bei Einzelbestellung, aufgrund der hohen Modellierungskomplexität, nicht betrachtet. Das Datengenerationstool simuliert die Verletzung eines Mengenkontrakts.

- Rechnung ohne Bezug zur Bestellung

Im Normalfall wird der Bestellprozess dadurch in Gang gesetzt, dass von einem Mitarbeiter einer Fachabteilung ein Bedarf festgestellt wird (Bönner et al., 2011). Der Mitarbeiter erstellt

eine Bestellanforderung, später wird im Einkauf die Bestellung angelegt. Finden diese Arbeitsschritte nicht oder nicht innerhalb des SAP ERP Systems statt, so kommt es beim Erhalt der Rechnung zum Phänomen „Rechnung ohne Bezug“. Derartige Rechnungen sind sehr risikoreich, da im Zuge der Rechnungsanerkennung innerhalb des SAP-Systems keine ausreichende Prüfung auf inhaltliche Korrektheit möglich ist (Bönner et al., 2011). Weder können die Mengen- und Preisangaben der einzelnen Rechnungspositionen auf Richtigkeit geprüft werden, noch die Einhaltung der vereinbarten Zahlungsbedingungen oder die korrekte Kontierung der Ausgabe (Bönner et al., 2011). Im Grunde ist nicht einmal klar, ob die berechnete Ware überhaupt bestellt oder geliefert wurde. Dieses Problem tritt verstärkt bei Dienstleistungen durch ihren immateriellen Charakter auf (Bönner et al., 2011).

Insgesamt gibt es folgende drei Möglichkeiten:

- Fehlende Bestellanforderung: Zwar existiert eine korrekte Bestellung auf die sich die Rechnung bezieht, jedoch wurde hierzu keine Bestellanforderung angelegt. Somit ist unklar, aufgrund welchen Bedarfs die Bestellung erfolgte.

- Fehlende Bestellung: Die Rechnung referenziert keine Bestellung, ein Wareneingang hat jedoch stattgefunden.

- Fehlender Wareneingang: Die Rechnung referenziert weder einen Bestell-Beleg noch eine Wareneingangs-Buchung. Es ist somit unklar, ob die berechnete Leistung überhaupt erbracht wurde (Bönner et al., 2011)

Dieses Szenario kann zu dem Fraud Pattern “Scheinfirma” zugeordnet werden, da es fehlende Bestellungen, Bestellanforderungen oder Wareneingang simuliert. Alle drei Arten wurden implementiert.

- CpD Transaktion

Das Kürzel „CpD“ steht für „Conto pro Diverse“ (Bönner et al., 2011). Dies bezeichnet ein Konto, welches nicht genau einer Person oder Organisation zugeordnet ist, sondern als anonymes Sammelkonto fungiert. Im Bereich des Einkaufsprozesses sind hierbei immer Lieferanten-Konten gemeint. CpD-Konten kommen immer dann zur Anwendung, wenn Transaktionen mit einem einmaligen Geschäftspartner abgeschlossen werden sollen, für den sich die Anlage eines dedizierten Stammsatzes nicht lohnt (Bönner et al., 2011). Die CpD-Lieferanten-Konten können für eine unbestimmte Anzahl an Kreditoren genutzt werden. Da in dem Konto keine näheren Lieferantendaten (z.B. Anschrift, Kontoverbindung) enthalten sind, müssen diese bei einer Kaufabwicklung immer manuell in die entsprechenden Belege eingegeben werden (Bönner et al., 2011). Dies beeinträchtigt die Transparenz einer derartigen Transaktion erheblich, da die eigentliche Kunden-Lieferanten-Beziehung nicht mehr klar erkennbar im System abgebildet ist (Bönner et al., 2011). Eine CpD-Transaktion könnte beispielsweise dazu genutzt werden, einen Kauf mit einem Lieferanten abzuwickeln, zu dem im System eine Lieferantensperre gesetzt ist (Bönner et al., 2011). Durch die Nutzung des CpD Kontos können verschiedene wirtschaftskriminelle Handlungen ausgeführt werden. Beispielsweise kann es dem Fraud Pattern „Private Einkäufe“ zugeordnet werden, da dieses anonyme Konto für Einkäufe des eigenen Bedarfs verwendet werden kann. Ebenfalls kann das

Konto aber auch für eine „Scheinfirma“ verwendet werden, da diese nicht in den Stammdaten des Unternehmens gespeichert werden muss. Die Stammdaten eines Unternehmens sind meist besonders vor Änderungen gesichert.

- Manuelle Zahlung

Normalerweise werden alle Bezahlungen durch einen automatischen Zahlungslauf im SAP ERP System durchgeführt. Als alternative Möglichkeit kann die Zahlung auch manuell durchgeführt werden. Als manuelle Zahlung bezeichnet man alle Zahlungsverfahren, die nicht auf den automatischen Zahlungslauf basieren (Bönner et al., 2011). Hierunter fällt auch die Situation, dass eine Zahlung in einem Fremdsystem durchgeführt wird und nachträglich in der Buchhaltung des SAP ERP Systems erfasst werden muss (Bönner et al., 2011). Ein automatischer Zahlungslauf kann grundsätzlich nur durchgeführt werden, wenn die Rechnung korrekt eingebucht wird, die Bankverbindung des Kreditors im System vorhanden ist, das Rechnungsanerkennungsverfahren abgeschlossen ist und keine Zahlsperre vorliegt (Bönner et al., 2011). Manuelle Zahlungen sind auch unabhängig von diesen Bedingungen möglich und stellen daher ein Risiko dar, da sie zur Umgehung der Prüfungsverfahren missbraucht werden können. Zudem besteht das Risiko, dass Skonto-Fristen irrtümlicherweise nicht genützt werden. Durch die manuelle Zahlung wird ein Geldabfluss in der Firma rein buchhalterisch im System erfasst. Eine Informations-Übernahme aus Belegen ist nicht möglich (Bönner et al., 2011). Zur Durchführung der Buchung stehen mehrere Möglichkeiten zur Verfügung. Beispielsweise wird die manuelle Zahlung als reine Belegbuchung im Hauptbuch betrachtet, die mittels der Transaktion FB01 durchgeführt wird (Bönner et al., 2011). Hieraus resultiert eine offene Zahlung, der keine Verbindlichkeit im Kreditoren-Nebenbuch zugrunde liegt. Der Bezug zum Rechnungseingang muss manuell hergestellt werden. Dies geschieht durch die Auszifferung von Rechnung und Zahlung mittels der Transaktion F-44 (Clearing) (Singh, 2012). Manuelle Zahlungen werden vor allem in dem Fraud Pattern „Doppelte Bezahlung“ verwendet, da die Bezahlung zunächst automatisiert und zusätzlich manuell bezahlt werden kann. Auch kann diese bei dem Fraud Pattern „Unbeteiligter Lieferant“ vorkommen.

- Nicht referenzierter Fraud

Das Szenario nicht-referenzierter Fraud ist der manuellen Zahlung sehr ähnlich, da Zahlungen ohne Bezug manuell durchgeführt werden können (Bönner et al., 2011). Der Unterschied liegt jedoch in der Reihenfolge der Prozess-Schritte, da hier die Zahlung vor dem Eingang der Rechnung erfolgt. Ähnlich wie bei manueller Zahlung lässt sich dieses Szenario zu mehreren Fraud Patterns zuordnen.

- Doppelte Bezahlung

Bei der doppelten Bezahlung wird eine Ware oder eine Dienstleistung doppelt bezahlt. Für eine doppelte Zahlung gibt es verschiedene Ursachen. Beispielsweise kann eine Rechnung mehrfach eingegangen sein. Dabei wird diese einmal mit Bezug zur Bestellung und einmal ohne Bestellbezug im System angelegt und bezahlt. Auch kann eine Rechnung versehentlich oder beabsichtigt mehrfach erfasst werden, beispielsweise, wenn diese einem Mahnschreiben beiliegt. Die Zweiterfassung einer Rechnung kann ebenfalls für ein Duplikat der Kreditoren-

Stammdaten durchgeführt werden oder innerhalb eines anderen Buchungskreises. Diese doppelte Zahlung kann dem Pattern „Doppelte Zahlung“ zugeordnet werden.

- Rechnungsmanipulation

In diesem Schema ist die Absicht des Täters eine Zahlung an einen Kreditor so umzuleiten, dass diese auf das eigene Konto oder das eines Komplizen gebucht wird (Islam et al., 2010). Deshalb werden die Kreditoren-Stammdaten vor der Durchführung der Zahlung modifiziert. Anschließend werden die Änderungen wieder Rückgängig gemacht, um Spuren zu verschleiern. Dieses Fraud Schema kann dem Pattern „Rechnungsmanipulation“ zugeordnet werden.

- Falsche Rechnung

Bei diesem Fraud-Fall wird im Zuge des Rechnungseingangs eine Rechnung mit preislich überhöhten Positionen gebucht (Islam et al., 2010). Das SAP-System reagiert bei entsprechender Konfiguration auf ein derartiges Vorkommnis mit einer Rechnungssperre (SAP, 2013b). Diese wird von einem betrügerischen Anwender wieder gelöst. Bei der Durchführung des Zahlungslaufs wird ein überhöhter Geldbetrag an den Lieferanten überwiesen. Der interne Komplize erhält einen Anteil (eine Kickback-Zahlung) des zu hoch entrichteten Preises. Dieses Fraud Szenario kann zu dem Fraud Pattern „Kickback“ zugeordnet werden, da eine überhöhte Zahlung durchgeführt wird.

- Unterschlagung

Das Ziel des Betrügers bei Unterschlagung ist Firmeneigentum zu entwenden, z.B. indem auf Kosten der Firma private Bestellungen über das Firmensystem abgewickelt werden (Islam et al., 2010). Die technische Möglichkeit dazu entsteht häufig aufgrund fehlender oder fehlerhafter Berechtigungszuteilung für die am Einkaufsprozess beteiligten Personen. Ein eindeutiges Indiz für eine Unterschlagungshandlung ist die Abwicklung des gesamten Bestellprozesses (Bestellanforderung, Bestellung und Freigaben) durch denselben Anwender (Islam et al., 2010). Die Erstellung einer Bestellanforderung muss hierbei nicht zwingend erfolgen, da der Anwender in dem Szenario die Kontrolle über das Freigabeverfahren zur Bestellung besitzt. Dieses Szenario ist dem Pattern „Private Einkäufe“ zugeordnet.

- Fingierter Kauf

Das Ziel beim Fraud-Szenario „Fingierter Kauf“ ist, den Erwerb einer Ware durch die Firma vorzutäuschen und hierdurch einen Zahlungsfluss an einen kooperierenden Lieferanten zu verursachen (Islam et al., 2010). Hierbei kommt eine Zahlung ohne tatsächliche Leistungserbringung oder ohne Lieferung von Waren zustande. Dies kann dem Fraud Pattern „Rechnungsmanipulation“ zugeordnet werden. Zwei Varianten dieses Szenarios sind dabei denkbar. In der ersten legt ein bösartiger Mitarbeiter eine Bestellung an und bucht zu dieser den Rechnungseingang, wobei ein Wareneingang nicht stattfindet (Islam et al., 2010). Damit die Rechnung trotzdem im Zahlungslauf berücksichtigt wird, muss der Mitarbeiter diese freigeben (dieser Schritt ist bei Islam et al. (2010) nicht erwähnt, in der Praxis jedoch notwendig). In der zweiten Variante des Szenarios fingiert der betrügerische Anwender zu einer ursprünglich

korrekten Bestellung einen Wareneingang und bucht darauf eine Rechnung. Im Zahlungslauf wird nun eine niemals eingegangene Ware bezahlt. Beiden Varianten gemeinsam ist der Versuch, einen in der Realität nicht korrekt abgewickelten Kauf vorzutäuschen.

8.2.1.3 Umsetzung der Datengenerierung

Im Folgenden soll die Implementierung des Datengenerierungstools dargestellt werden. Hierfür wird ein SAP ERP 6.06 IDES System verwendet. Vorteil des IDES Systems ist die vorhandenen Daten und Customizing Einstellungen. Zunächst werden typischen SAP Artefakte zur möglichen Implementierung beschrieben. Das Ziel des Datengenerators ist dabei die bereits beschriebenen Fraud Szenarien, sowie normales Verhalten zu implementieren. In unserem Modell sind die Szenarien aus diskreten atomaren Schritten aufgebaut, die entweder Dokumente im SAP ERP System erstellen oder ändern. Insgesamt gibt es zwei Möglichkeiten Prozessschritte zu implementieren: die Nutzung von Business Application Programming Interfaces (BAPI)-Aufrufen oder von Batch Input Maps (BDC) (Wegelin & Englbrecht, 2009).

BAPIs sind remotefähige RFC Funktionsbausteine und Teil der Service-Orientierten Architektur von SAP. Man kann sich diese als API für die Modifikation von Geschäftsobjekten vorstellen, weshalb sie sich einfach für diesen Fall verwenden lassen. Allerdings gibt es nicht für alle Prozessschritte eine entsprechende BAPI. Beispielsweise existiert keine BAPI für die automatisierten Zahlungsläufe oder das Ausziffern von Buchungen. Für diese Prozessschritte wird deshalb eine Batch Input Map verwendet. Eine Batch Input Map kann als die Aufnahme einer SAP Dynpro Ausführung, gekapselt in einem Funktionsmodul, verstanden werden und kann mit benutzerspezifische Inputparameter gefüllt werden. Die Nutzung von BAPIs ist komfortabler und robuster. Dennoch finden bei beiden Varianten dieselben Prüfungen wie bei einer normalen SAP ERP Transaktion über die Benutzeroberfläche statt. Auch werden die identischen Dokumente und Tabelleneinträge erstellt.

Die Architektur des Datengenerators enthält vier Ebenen. Die unterste Ebene modelliert einzelne Nutzeraktionen des SAP Einkaufprozesses. Einzelne Schritte des Einkaufsprozesses werden implementiert, wie die Erstellung einer Bestellanforderung, einer Bestellung oder die Bezahlung. Diese Schicht besteht aus 14 ABAP Objektklassen, die die zuvor genannten BAPIs oder BDC Calls in einer perform_step() Methode kapseln. Neben dem BAPI oder BDC Funktionsaufruf enthält die perform_step() Methode auch Logik für die Inputparameter und Fehlerbehandlung. Die Ausführung jeder Transkation wird durch den Aufruf der Methode getriggert und hat zur Folge, dass ein SAP Dokument erstellt oder geändert wird. Die IDs der erstellten Dokumente werden als Outputparameter zurückgegeben. Tabelle 46 zeigt eine Übersicht über die verschiedenen Prozessschritte und die verwendeten BAPI oder BDC aufrufe.

Prozess Schritte	**BAPI oder BDC**
Erstellung Bestellanforderung	BAPI_REQUISITION_CREATE
Freigabe Bestellanforderung	BAPI_REQUISITION_RELEASE_GEN
Erstellung Bestellung	BAPI_PO_CREATE1
Freigabe Bestellung	BAPI_PO_RELEASE
Erstellung Wareneingangsdokument	BAPI_GOODSMVT_CREATE

Erstellung einer eingehenden Rechnung (Dokument)	BAPI_INCOMINGINVOICE_CREATE
Erstellung einer eingehenden Rechnung (Dokument) (ohne Referenz zur Bestellung)	BAPI_ACC_DOCUMENT_POST
Freigabe blockierter Rechnung	BAPI_INCOMINGINVOICE_RELEASE
Änderung der Bankdetails des Kreditors	BDC for transaction XK02
Automatischer Zahlungslauf	BDC for transaction F110
Manuelle Bezahlung	BDC for transaction FB01
Ausziffern	BDC for transaction F-44

Tabelle 46: Verwendete BAPIs und BDCs in den implementierten Prozessschritten
Quelle: Eigene Darstellung

Die zweite Schicht modelliert normales und wirtschaftskriminelles Verhalten, indem die einzelnen Aktionen (Prozessschritte) der darunterliegenden Schicht verkettet werden. Für jedes wirtschaftskriminelle Szenario und für das normale Verhalten wird jeweils eine ABAP Objektklasse erstellt. Diese kann durch die Methode perform_scenario() aufgerufen werden. Zwischen den einzelnen Schritten des Szenarios müssen Input und Output Daten transferiert werden, um sicherzustellen, dass jeder Prozessschritt auf den Output des vorhergehenden Prozessschrittes basiert. Deshalb werden als Input Daten jedes Prozessschrittes die Output Daten des vorhergehenden Schrittes verwendet (bzw. in der dritten Schicht zufällig generiert). Eine Anforderung an den Generator ist die Indikation der einzelnen Prozessschritte. Deshalb zeigt ein Flag an, ob es sich bei einer Transaktion um Fraud handelt oder nicht. Die gespeicherten Informationen dieser Schicht sind der Prozessschritt, das Flag (Fraud oder kein Fraud), Input und Output Parameter jedes Prozessschrittes und falls vorhanden etwaige Fehlermeldungen.

Die dritte Schicht der Architektur führt eine zufällige Anzahl an Fraud und normalen Prozessinstanzen aus, indem es Szenarien aus der zweiten Schicht instanziiert und ihre perform_scenario() Methode aufruft. Neben der Ausführung der Szenarien beinhaltet die dritte Schicht einen Zufallsgenerator für die Erstellung bestimmter Parameter bei der Prozessausführung. Zunächst wird die Art des Szenarios über einen Zufallsgenerator bestimmt. Diese Information ist für die Generierung der Input Parameter wichtig und basiert auf der diskreten Wahrscheinlichkeitsverteilung, die in der GUI ausgewählt werden kann. Im zweiten Zufallsgenerierungsschritt werden die Parameter für die Szenarien ausgewählt. Jedes Szenario benötigt (auch abhängig von den Prozessschritten) eine Anzahl an numerischen und nicht numerischen Parametern, wie beispielsweise Materialnummer, Anzahl der bestellten Materialen, Preisvariationen in der Rechnung, Datum und Zeit der Ausführung und die ID des Verkäufers. Die Auswahl von konsistenten und eindeutigen Parametern ist eine der komplexesten Anforderungen, da beispielsweise nicht alle Materialien in jeder Organisationseinheit bestellt werden können. Auch kann nicht jeder Nutzer in einer bestimmten Organisationseinheit einkaufen.

Die vierte Schicht des Datengenerierungstools ist die Benutzeroberfläche, die als SAP Dynpro Transaktion entwickelt wird. Durch die Benutzerschnittstelle können Benutzer neue

Datengenerierungsläufe starten, die Anzahl der zu generierenden Prozessinstanzen bestimmen und eine diskrete Wahrscheinlichkeitsverteilung, die die Häufigkeit der verschiedenen

Fraud Szenarien bestimmt, auswählen. Abbildung 8-1 zeigt einen Screenshot der graphischen Benutzerschnittstelle zur Konfiguration der verschiedenen Fraud Szenarien.

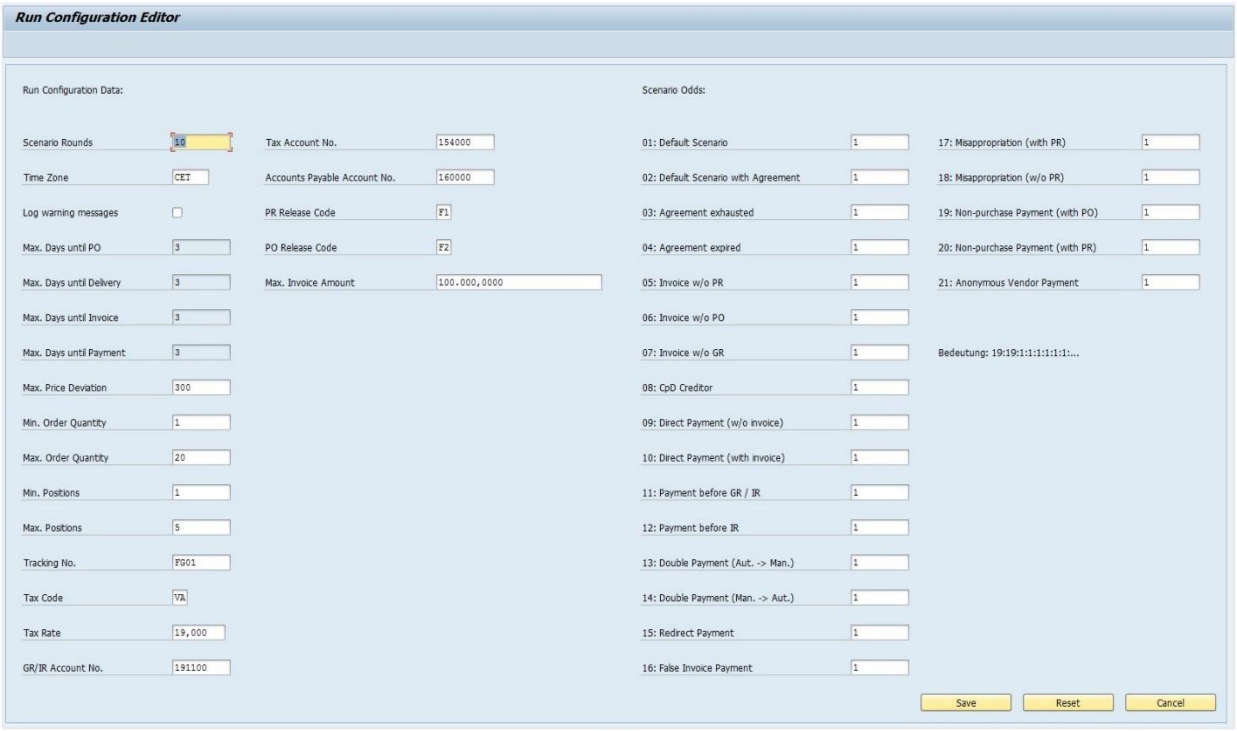


Abbildung 8-1: Konfigurationseditor des Fraud Datengenerators
Quelle: Eigene Darstellung (Screenshot aus SAP ERP System)

Zusätzlich kann der Benutzer im Konfigurationseditor bereits laufende Transaktionen stoppen und Informationen über abgebrochene Durchläufe in Form von Fehlermeldungen ansehen. Der Datengenerator wird objektorientiert entwickelt und kann einfach erweitert werden, indem weitere Prozessschritte oder neue Fraud Szenarien hinzugefügt werden. Neben den zentralen Klassen für die Prozessschritte und Szenarien-Implementierung werden auch vom SAP ERP angebotene Hilfsklassen verwendet, um Datenbankzugriff, Logging, Fehlerbehandlungen und Datentransfer zwischen den verschiedenen Prozessschritten zu ermöglichen.

8.2.2 Fraud Erkennung

Zur Fraud Erkennung wird der in der zweiten Forschungsfrage implementierte Prototyp parametrisiert, indem einige Schwellwerte für die Berechnung der Fraud Flags gesetzt und Fraud Patterns definiert werden. Eine detaillierte Beschreibung der beiden Initiationsschritte wird im Folgenden beschrieben. Zunächst wird kurz dargestellt, wie die Daten aus der Quelldatenbank in die Zieldatenbank geladen werden.

8.2.2.1 Übertragung der Daten in die HANA

Um die Daten analysieren zu können, müssen diese zunächst aus dem SAP ERP System in die SAP HANA Datenbank übertragen werden. Hierzu wird das Tool SAP Data Services Designer verwendet. Zunächst werden über die ODBC Schnittstelle allgemeine Verbindungen zum SAP ERP System und zur SAP HANA Datenbank hergestellt. Anschließend müssen die Meta-Daten der Tabellen repliziert werden, indem für jede Tabelle ein Batch Job erstellt wird. Bei der Ausführung des Batch Jobs werden die Daten aus dem ERP System in die SAP HANA Datenbank transferiert. Ein beispielhafter Batch Job für die Tabelle MKPF ist in Abbildung 8-2 dargestellt. Analog wird für jede notwendige Tabelle ein entsprechender Batch Job erstellt und ausgeführt.

Abbildung 8-2: ETL Prozess für Tabelle MKPF

Quelle: Eigene Darstellung (Screenshot aus Business Objects Data Services Designer)

8.2.2.2 Parametrisierung des Prototyps

Bevor der Prototyp verwendet werden kann, müssen einige Parameter für das entsprechende Unternehmen eingestellt werden. Diese werden, falls vorhanden, aus den jeweiligen Publikationen entnommen. Falls keine Angaben gefunden werden, werden Annahmen getroffen. Im produktiven Einsatz des Prototyps soll der Fraud Investigator die Parametrisierung des Prototyps vornehmen. Dabei gibt er unternehmenstypische Richtlinien und Grenzwerte an, wie beispielsweise die Grenze ab welchem Wert eine Bestellung einer Freigabe bedarf. Die hier vorgenommenen Grenzwerte sind in Tabelle 47 abgebildet.

Variablenname	Beschreibung	Verwendet	Quelle
ABSTAND_RECHNUNG	Grenze innerhalb wann zwei Rechnungen für ein Produkt erstellt werden als signifikant gilt.	2 Tage	
BIDDING_DURATION_THRESHOLD	Wie lange sollte eine Angebotsphase mindestens dauern	5 Tage	Wells 2011
BIDDING_PARTICIPANTS_THRESHOLD	Wie viele Teilnehmer muss eine Anfrage mindestens haben	3 Teilnehmer	
BIDDING_THRESHOLD	Ab welcher Summe muss eine Anfrage ausgelöst werden.	25.000 €	
BIG_ORDER_THRESHOLD	Grenze ab wann eine Erhöhung der Rechnungssumme im Vergleich zum Vormonat signifikant ist	2.00 (doppelt)	(Singh et al., 2011)
FAST_ORDER_THRESHOLD	Ab wann gilt die Bestellung als "eilig"	1 Tag	
FAVOURITE_VENDOR_THRESHOLD	Welchen Anteil muss der Mitarbeiter bei einem Lieferanten haben, damit dieser sein Favorit ist.	0.75 (75%)	

MIN_ORDER_COUNT	Wie viele Bestellungen müssen bereits bei einem Lieferanten durchgeführt worden sein, um als favorisierter Lieferant zu gelten	10 Bestellungen	
NO_KNOWN_VENDOR	Wie hoch darf die Bestellsumme maximal sein, damit ein Lieferant keinen Stammsatz benötigt	5000.00	
ORDER_THRESHOLD	Grenze ab wann eine Erhöhung signifikant ist	2 (doppelt)	(Singh et al., 2011)
ORDER_THRESHOLD_STAGE1	Grenze für erste Genehmigungsstufe	500.00 €	
ORDER_THRESHOLD_STAGE2	Grenze für zweite Genehmigungsstufe	5000.00 €	
SERVICE_THRESHOLD_DOWN	Kleine Dienstleistungsaufträge die normalerweise ohne zusätzliche Genehmigung durchgeführt werden können	500.00 €	
SERVICE_THRESHOLD_UPPER	Sehr große Dienstleistungsaufträge	5000.00 €	
SPENDING_THRESHOLD	Vergleich der Ausgaben von Vormonat. Grenze ab wann eine Erhöhung signifikant ist	2 (doppelt)	(Singh et al., 2011)
STANDARDABWEICHUNG	Standardabweichung für stets gleiche Beträge	10	
THRESHOLD_MATTXT	Ab wann ist der Materialtext zu kurz	6 Zeichen	
TIME_THRESHOLD	Ab wie vielen Jahren ohne Geschäftsaktivität mit Lieferant ist eine erneute Aktivität suspekt.	1 Jahr	(Wells, 2002)
UNCOMMON_TIME	Zeit, in der eine Geschäftsaktivität eher ungewöhnlich ist (bspw. Nachts)	21:00-5:00 Uhr	
UPPER_LENGTH_THRESHOLD	Mindestanzahl an Buchstaben für einen Lieferant	3 Buchstaben	
VENDOR_COUNT_THRESHOLD	Wie viele Lieferanten sollten für ein Produkt vorhanden sein	3 Lieferanten	
Z_THRESHOLD	Signifikanz für Z-Wert	3	(Albrecht et al., 2012)

Tabelle 47: Verwendete Einstellungen der Variablen

Quelle: Eigene Darstellung

Zusätzlich werden die wichtigsten Red Flags pro Fraud Patterns festgelegt, wobei der Prototyp nach dem parallelen Auftreten dieser Red Flags sucht. Bei der parallelen Suche nach allen Red Flags pro Fraud Pattern ist die Ergebnismenge meist null und kein Fraud Pattern schlägt an. Die hier ausgewählten Kombinationen sind beispielhafter Natur. In der Praxis wird dieser Schritt dem Auditor überlassen. Tabelle 48 zeigt zu jeder Auswahl die Anzahl der gefundenen Fraud Patterns im Datensatz.

Fraud Pattern	Gewählte Kombination	# Fraud Patterns
Kickback	Flag_D01, Flag_D12	0
	Flag_D01, Flag_D05	0
	Flag_D01, Flag_D06	0
	Flag_D11, Flag_D17	0
Angebotsmanipulation	Flag_E01, Flag_E06	0
	Flag_E03, Flag_E06	0
	Flag_E04, Flag_E16	0
	Flag_E04, Flag_E09	0
	Flag_E06, Flag_E07	0
Scheinfirma	Flag_B01, Flag_B10	0
	Flag_B09, Flag_B13	0
	Flag_B12, Flag_B13	0
	Flag_B15, Flag_B16	0
	Flag_B01, Flag_B09	94
Doppelte Zahlung	Flag_C01, Flag_C02	318
	Flag_C01, Flag_C03	848
	Flag_C01, Flag_C02, Flag_C03	0
	Flag_C02, Flag_C03	6
	Flag_C01, Flag_C07	64
Pass-Through	Flag_F01, Flag_F02	0
	Flag_F01, Flag_F03	0
	Flag_F02, Flag_F05,	0
	Flag_F02, Flag_F03	0
	Flag_F02, Flag_F03, Flag_F04	0
Unbeteiligter Lieferant	Flag_G01, Flag_G02	0
	Flag_G01, Flag_G03	0
	Flag_G02, Flag_G03,	0
	Flag_G03	0
Rechnungsmanipulation	Flag_A01, Flag_A02	0
	Flag_A03, Flag_A04	0
	Flag_A04, Flag_A06	0
	Flag_A04, Flag_A08	0
	Flag_A04, Flag_A09	0

Tabelle 48: Red Flag Kombinationen für Fraud Patterns
Quelle: Eigene Darstellung

8.2.2.3 Ergebnisse

Zunächst wird an dieser Stelle der Datensatz allgemein und anschließend die identifizierten Fraud Szenarien beschrieben.

8.2.2.3.1 Allgemeine Beschreibung des Datensatzes

Der Datensatz enthält insgesamt 216.401 Prozessinstanzen, darunter auch die bereits im SAP System vorhandenen Beispieldaten (IDES- Daten). Insgesamt sind 241 aktive Mitarbeiter am Einkaufsprozess beteiligt. Diese nehmen 1063 verschiedene Materialien von 318 Lieferanten entgegen. Insgesamt beinhaltet der Datensatz ein Rechnungsvolumen von 5,15 Milliarden € verteilt auf 69.388 Rechnungen. Es werden 924 Fraud Patterns und 1.057.124 Red Flags mit der oben genannten Instanziierung des Prototyps identifiziert. Diese sollen im Folgenden näher analysiert werden.

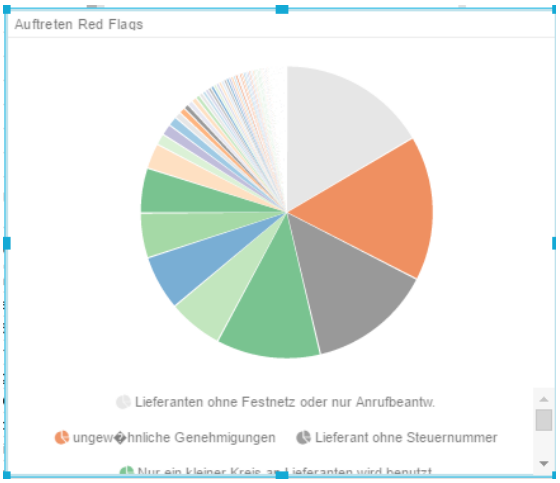


Abbildung 8-3:Verteilung der Häufigkeit der einzelnen Red Flags

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Abbildung 8-3 zeigt die Häufigkeitsverteilung der einzelnen Red Flags. Am häufigsten treten die Red Flags *‚Lieferant ohne Festnetz oder nur Anrufbeantworter‘, ‚ungewöhnliche Genehmigungen‘* und *‚Lieferant ohne Steuernummer‘* auf. Diese Red Flags können mit der schlechten Datenqualität im IDES Datensatz erklärt werden. Bei der Erstellung der Lieferanten werden oft nur die Minimalangaben befüllt. Deshalb kommt es häufig zu fehlenden Steuernummern und Telefonnummern. Auch Genehmigungen werden oft nicht modelliert. Hinzu kommt eine Besonderheit des generierten Datensatzes - innerhalb kurzer Zeit werden sehr viele Daten generiert. Deshalb schlagen beispielsweise Red Flags wie *‚Umsätze bei schlafenden Verkäufern steigen rapide an‘* oder *‚Einkaufsvolumen übersteigt den letzten*

signifikant‘ häufig an. Red Flags mit einer zeitlichen Dimension müssen in diesem Datensatz kritisch betrachtet werden.

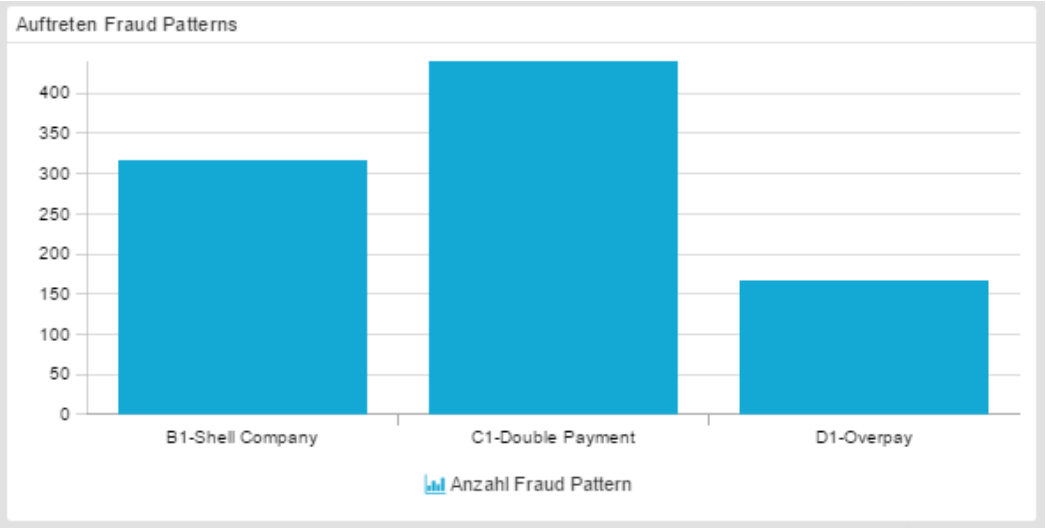


Abbildung 8-4: Aufgetretene Fraud Patterns

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Mit der in Kapitel 8.2.2.2 genannten Konfiguration können drei Fraud Patterns identifiziert werden. Das Fraud Pattern ‚*Doppelte Bezahlung‘* wird am häufigsten im Datensatz erkannt, gefolgt von ‚*Scheinfirma‘* und ‚*Überbezahlung‘* (vergl. Abbildung 8-4). Der verursachte Schaden ist allerdings bei Scheinfirmen mit insgesamt 19.900 € mit Abstand am höchsten (vergl. Abbildung 8-5).

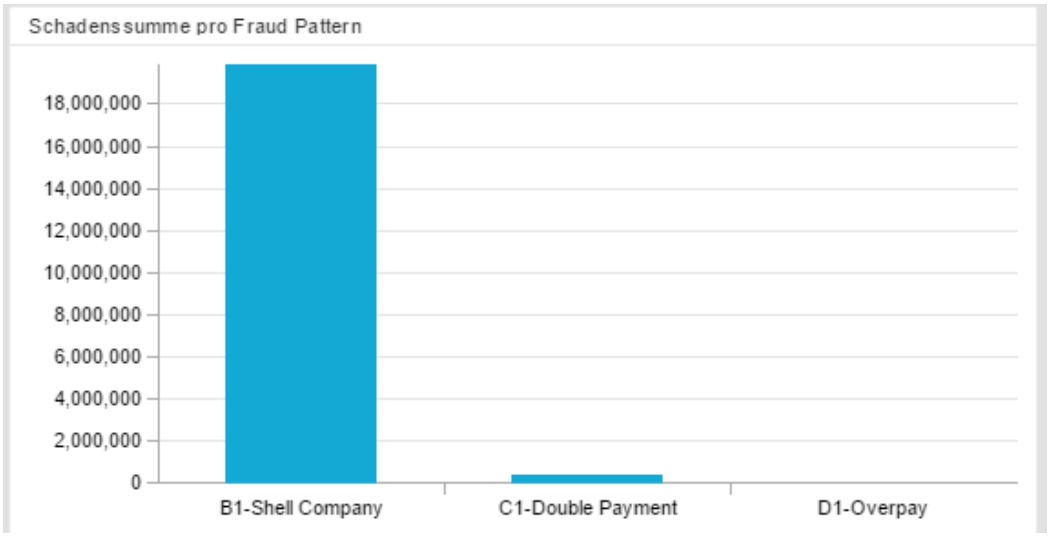


Abbildung 8-5: Identifizierte Fraud Patterns inklusive Schadenssumme

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Zusätzlich werden auffällige Prozessinstanzen mit dem höchsten Verlust oder mit der höchsten Anzahl von Red Flags identifiziert. In Abbildung 8-6 erkennt man beispielsweise, dass die Prozessinstanz 9004500006372 sechs Red Flags mit einem Nettopreis von 48.6 Mio € aufweist.

Da die mögliche Schadenssumme sehr hoch ist, kann sich der Analyst systematisch durch die einzelnen Prozessinstanzen durcharbeiten.

Top 10 Transaktionen

Prozessinstanz	Anzahl Red F...	NettoPreis
9004500006372...	6	48.6 Mio.
9004500007721...	15	14.3 Mio.
9004500017251...	11	13.8 Mio.
9004500017266...	10	12.5 Mio.
9004500006374...	12	10.7 Mio.
9004500006374...	12	7.80 Mio.
9004500017250...	9	7.54 Mio.
9004500006374...	12	7.20 Mio.
9004500004870	14	7.00 Mio

Abbildung 8-6:Top Fraudverdächtige Transaktionen mit dem höchsten Nettoverlust
Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Im Folgenden sollen die Daten mithilfe des Prototyps systematisch analysiert werden, um mögliche Frauds zu identifizieren. Der Vorteil eines synthetisch generierten Datensatzes ist, dass jeder Fraud als solcher gekennzeichnet ist und so ein Vergleich möglich ist. Deshalb soll an dieser Stelle auf die generierten Datensätze gefiltert werden. Mit dieser Filtereinstellung bleiben 191.366 Prozessinstanzen übrig, an denen insgesamt 39 verschiedenen aktive Mitarbeiter beteiligt sind. Der Rechnungsbetrag reduziert sich auf 4,47 Mio € verteilt auf knapp unter 70 Tsd. Rechnungen.

8.2.2.3.2 Identifikation von Fraud Patterns

Zunächst sollen die angeschlagenen Fraud Patterns im Detail untersucht werden. *‚Kickback Fraud‘* wird nicht im Datensatz identifiziert. Dies kann als positiv eingestuft werden, da der Datengenerator keinen Kickback-Fraud generiert hat. Auch bei *‚Angebotsmanipulation‘* handelt es sich um ein Fraud Pattern, welches nicht im generierten Datensatz vorhanden ist und welches nicht angeschlagen ist.

Das Fraud Pattern *‚Scheinfirma‘* wird im Datensatz identifiziert. Die Kombination von Flag_B01 (*plötzliche Geschäftsaktivitäten mit alten „schlafenden“ Lieferanten*) und Flag_B09 (*Lieferanten ohne Festnetzanschluss oder nur mit Anrufbeantworter*) hat 19 Lieferanten hervorgebracht, die als Scheinfirma in Verdacht stehen. Diese werden im Folgenden näher analysiert.

Lieferantenland und Bankland

Lieferantenname	Adressland	Land des Kontos
Jotachi Deutschland...	US	DE
SMP	US	DE
SKF Americas	US	DE
Gusswerk US	US	DE
AluCast	US	DE
SEC System SA	FR	DE
Sunny Electronics G...	DE	DE
SKF Kugelmeier KG...	DE	DE
Wollner AG	DE	DE
PAQ Deutschland G...	DE	DE
Grosshandel-Baden...	DE	DE
KBB Schwarze Pum...	DE	DE

Abbildung 8-7: Lieferanten und Bankenland

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Zunächst fällt bei einigen dieser Lieferanten auf, dass ihr Adressland nicht mit dem Land des Bankkontos übereinstimmt (vergl. Abbildung 8-7). Die verdächtigen Lieferanten sollen durch Filterungen systematisch betrachtet werden.

Zunächst wird auf den Lieferanten ‚Jotachi‘ gefiltert. Dieser ist ein PC Lieferant, bei dem das Unternhemen diverse Kabel und Netzwerkkarten gekauft hat. Filtert man nach allen Prozessinstanzen dieses Lieferanten, so ergeben sich einige Ungereimtheiten. Bei vier Prozessinstanzen beginnt der Prozessablauf mit dem Schritt „Rechnung beglichen“, in einem Fall sogar doppelt. Anschließend wird eine Bestellanforderung und Bestellung angelegt, wobei der Wareneingang fehlt. Da es sich nicht um eine Dienstleistung handelt, ist das Fehlen des Wareneinganges kritisch zu sehen. Zusätzlich kommen bei diesem Lieferanten 51 Prozessinstanzen vor, bei denen nur eine Rechnungen beglichen wird, ohne jegliche Bestellanforderung, Bestellung, Waren- oder Rechnungseingang (vergl Abbildung 8-8). Vergleicht man die Prozessinstanzen mit dem Output des Generators, so handelt es sich hier tatsächlich um Fraud.

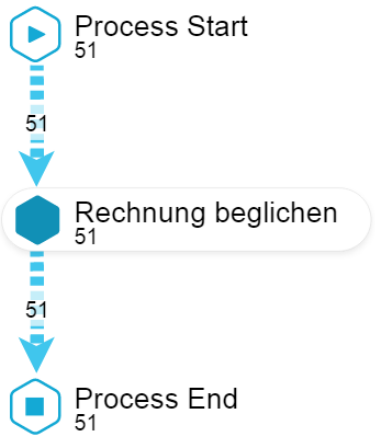


Abbildung 8-8:Prozessinstanzen die lediglich eine Rechnung begleichen

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Das Unternehmen ‚SMP' wird ebenfalls genauer betrachtet, da hier auch interessante Prozessdurchläufe identifiziert werden. In zwei Fällen wird nur die Rechnung beglichen, ohne Bestellung, Waren- oder Dienstleistungseingang. Bei beiden Rechnungen ist der Mitarbeiter ‚MASSBERG' als einziger Mitarbeiter beteiligt. Es ist auffällig, dass dieser Mitarbeiter als einziger auch an der Zahlung der Rechnung bei dem zuvor analysierten Lieferanten ‚Jotachi' beteiligt ist. Auch hier gilt wieder, dass dieser Mitarbeiter und der beteiligte Lieferant ‚SMP' genauer untersucht werden sollten.

Der Lieferant ‚AluCast' hat in 35 Fällen eine eigenartige Reihenfolge der Prozessausführung. Meist begleicht dieser zuerst eine Rechnung und bekommt anschließend Ware (Vorauskasse). In zwei Fällen begleicht das Unternehmen eine Rechnung ohne Wareneingang. Auch hier ist wieder der Mitarbeiter ‚MASSBERG' als einziger involviert. Die Vermutung liegt nahe, dass dieser Mitarbeiter häufig an Rechnungen ohne Bestellung und Wareneingang beteiligt ist. Filtert man also nach dem Mitarbeiter ‚MASSBERG' (vergl. Abbildung 8-9), erkannt man, dass er nur an 106 Prozessinstanzen beteiligt ist. Alle Prozessinstanzen weisen das Muster Begleichung einer Rechnung ohne Bestellungen oder Wareneingang auf.

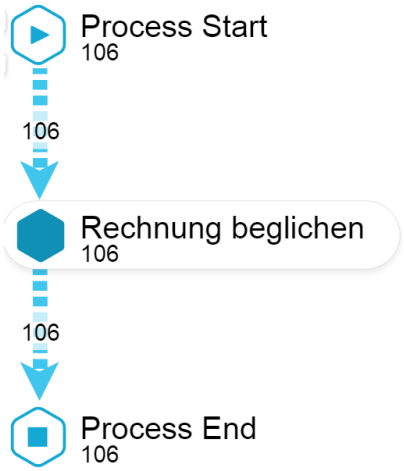


Abbildung 8-9: Prozessinstanzen des Lieferanten ‚Massberg'

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Der Mitarbeiter ‚MASSBERG' ist der einzige im Datensatz, bei dem Rechnungen ohne Wareneingag beglichen werden. Aus diesem Grund ist dies ein sehr verdächtigter Mitarbeiter. Vergleicht man die 106 Prozessinstanzen mit dem Output des Datengenerators, so handelt es sich hierbei tatsächlich um Fraud.

Die restlichen als Scheinfirma identifizierten Lieferanten weisen keine weiteren Hinweise auf Fraud auf. Teilweise ist die Reihenfolge der ausgeführten Transaktionen etwas merkwürdig, da beispielsweise zuerst der Wareneingang durchgeführt wird und anschließend die Bestellung. Allerdings wird dies nicht zwangsläufig als Fraud eingestuft, da die Ware angekommen ist. Es ist anzunehmen, dass die hohe Anzahl an identifizierten Fraud Patterns hier aufgrund der schlechten Datenqualität der Masterdaten zustande gekommen ist.

Das Fraud Pattern *‚doppelte Zahlung'* hat gleich mehrere Prozessinstanzen als verdächtig eingestuft. Bei insgesamt 124 Prozessinstanzen wird eine Rechnung mehrfach bezahlt (vergl. Abbildung 8-10).

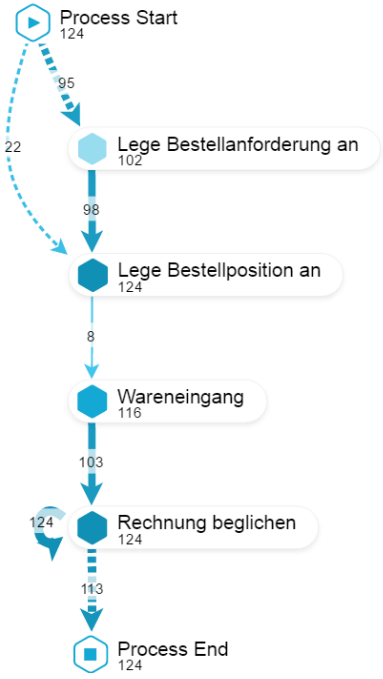


Abbildung 8-10: Transaktionen mit doppelter Zahlung

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Bei einigen dieser Prozessinstanzen wird die Ware nicht geliefert, die Rechnung aber doppelt beglichen. Vergleicht man diese 124 Prozessinstanzen mit dem tatsächlichen Fraud-Vorkommen des Datengenerators, so handelt es sich hierbei tatsächlich um Fraud. Der Prototyp unterscheidet allerdings nicht, ob Zahlungen manuell oder mit dem Zahlungslauf durchgeführt werden. Diese Unterscheidung ist allerdings hilfreich, da mit der manuellen Zahlung gesperrte Rechnungen trotzdem bezahlt werden können. Deshalb sollte diese Unterscheidung zusätzlich im Prototyp aufgenommen werden.

Das Fraud Pattern *‚Pass-Through'* wird nicht im Datensatz identifiziert. Da im generierten Datensatz nur zufällige Preise angenommen werden, exisitiert dieses Schema auch nicht. Die

Fraud Patterns *‚unbeteiligter Lieferant‘* und *‚private Einkäufe‘* werden ebenfalls nicht identifiziert und sind nicht im Datengenerator implementiert.

Das Fraud Pattern *‚Rechnungsmanipulation‘* ist angeschlagen, da das Red Flag Flag_A04 (*geänderte Kontoinformationen vor Zahlung*) besonders häufig vorkommt. Bei der Implementierung dieses Red Flags wurde keine zeitliche Komponente betrachtet. Lediglich die Änderung einer Kontonummer löst das entsprechende Red Flag aus. Da sich Kontonummern aber ändern ist das per se kein Fraud. Deshalb soll die Implementierung des Red Flags so angepasst werden, dass zusätzlich eine zeitliche Dimension beachtet wird. Logisch soll das Red Flag nur anschlagen, wenn die Kontonummernänderung zwischen Rechnungseingangsdatum und dem Skontodatum liegt. Dadurch wird erwartet, dass dieses Red Flag weniger häufig auftritt und die Trefferquote höher ist. Trotz dieser Anpassung ist das Vorkommen dieses Red Flags noch sehr hoch. Dies kann mit der Natur des Datengenerators erklärt werden. Da die Daten an einem Tag künstlich generiert werden, werden auch alle Änderungen innerhalb dieses Tages durchgeführt. Dennoch muss genannt werden, dass alle durch den Datengenerator erstellten Rechnungsmanipulationsfälle identifiziert wurden.

8.2.2.3.3 Fraud Detektion durch Analyse der Top 10 Prozessinstanzen

Als nächstes sollen Prozessinstanzen mit einer hohen Anzahl an Red Flags identifiziert werden. Albrecht et al. (2012) haben einen positiven Zusammenhang zwischen der Anzahl der identifizierten Red Flags und dem tatsächlichen Vorkommen von Fraud identifiziert. Der Prototyp zeigt eine Tabelle mit den *‚Top 10 Transaktionen‘* an. Dabei kann nach den Top 10 Transaktionen mit der höchsten Anzahl an Red Flags und der höchsten Schadenssumme sortiert werden. Durch die Filtermöglichkeit können systematisch diese Prozessinstanzen analysiert werden. Im generierten Datensatz sind die Preise zufällig gewählt, so dass nur die Prozessinstanzen mit den meisten Red Flags analysiert werden. Diese sind in Abbildung 8-11 dargestellt:

Top 10 Transaktionen

Prozessinstanz	↓ 1	NettoPreis
900450002106500010	18	180e-3
900450002106500030	18	2.70
900450002079500020	18	9.18
900450002046200010	17	323
900450002079500040	16	160e-3
900450002078900010	16	160e-3
900450002046100010	16	304
900450002079500030	16	8.16
900450002067300030	16	1.52 Tsd.
900450002069700030	16	2.40

Abbildung 8-11: Top Transaktionen mit den meisten identifizierten Red Flags

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Diese sollen nun einzeln betrachtet werden, indem auf jede verdächtige Prozessinstanz gefiltert wird. Prozessinstanz 9004500210650010 und 9004500210650030 gehören zur selben Prozessausführung und weisen 18 Red Flags auf.

Abbildung 8-12:Prozessdiagramm einer Prozessinstanz mit 18 identifizierten Red Flags

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Der Prozessablauf ist in Abbildung 8-12 zu sehen und weist einige Unregelmäßigkeiten auf. So wird die Rechnung zuerst beglichen und anschließend die Bestellanforderung und Bestellposition angelegt. Die Änderungen im Einkaufsbelegkopf sind mit der Freigabestrategie zu erklären und stellen somit keine Besonderheit dar. Abbildung 8-13 stellt die identifizierten Red Flags für diese Prozessinstanz dar. Vor allem die Red Flags ‚*mehrere Rechnungen für*

dieselbe Ware' und *‚Änderung der Kontonummer vor Überweisung'* sind sehr auffällig. Das Fraud Pattern *‚Rechnungsmanipulation'* ist ebenfalls angeschlagen.

Details zum Red Flag

ID	Beschreibung kurz	Beschreibung lang
Flag_F02	unn&#65533;tig hohe/steigende Lagerbest&#65533;nde	Lagerbestand ist im Vergleich zum Vormonat/Vorjahr/Vorjahresmonat absolut oder Prozentual gestiegen
Flag_D04	rasant steigende Eink&#65533;ufe bei einem Lieferanten	Prozentualer Anteil am gesamten Einkauf zum Vormonat/Vorjahr/Vorjahresmonat. Absolute Zahl an K&#65533;ufen im Vergleich zum Vormonat…
Flag_C01	mehrere Rechnungen f&#65533;r dieselbe Ware	Suche nach Rechnungen, die das selbe Produkt haben, den selben Lieferanten, den selben Genehmiger haben und innerhalb einer bes…
Flag_D07	Zahlung gleichen Betrages an einen Lieferanten	Betr&#65533;ge &#65533;hneln sich sehr stark und sind die meiste Zeit rund.
Flag_D10	Zahlung au&#65533;erhalb der Gesch&#65533;ftszeit	Suche nach Transaktionen in einem bestimmten Zeitraum (eg. 18 Uhr - 6 Uhr)
Flag_B27	Rechnungen- die sehr schnell beglichen werden	Suche alle Eintr&#65533;ge, bei denen der Abstand zwischen der Erfassung und Bezahlung einer Rechnung zwischen 0 und der h&#65533;ffte der ge…
Flag_B25	Rechnungen mit stets gleichen Rechnungsbetr&#65533;gen	Erstelle eine Hilfstabelle, die alle Eink&#65533;ufe beinhaltet, bei denen der auf- und abgerundete Betrag der Bestellung gleich ist. Z&#65533;hleanschl…
Flag_D13	Rechnungen die sehr schnell beglichen wurden	Verstrichene Zeit zwischen Lieferung und Zahlung unter einem bestimmten Threshold. Hier k&#65533;nnen Beispielsweise bekannte Skontogr…
Flag_D16	Nur ein kleiner Kreis an Lieferanten wird benutzt	Mitarbeiter benutzt f&#65533;r seine Bestellungen nur sehr wenige Lieferanten pro Produkt.
Flag_B09	Lieferanten ohne Festnetz oder nur Anrufbeantw.	Suche alle Instanzen, bei denen die Telefonnummer im Lieferantenstammsatz fehlt

Abbildung 8-13: Identifizierte Red Flags

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Aus Mitarbeitersicht ist auffällig, dass nur drei Mitarbeiter am Prozess beteiligt sind, wobei der User ‚WAGNERC' mit 75% aller durchgeführten Aktivitäten besonders aktiv und damit besonders auffällig ist (vergl. Abbildung 7-14).

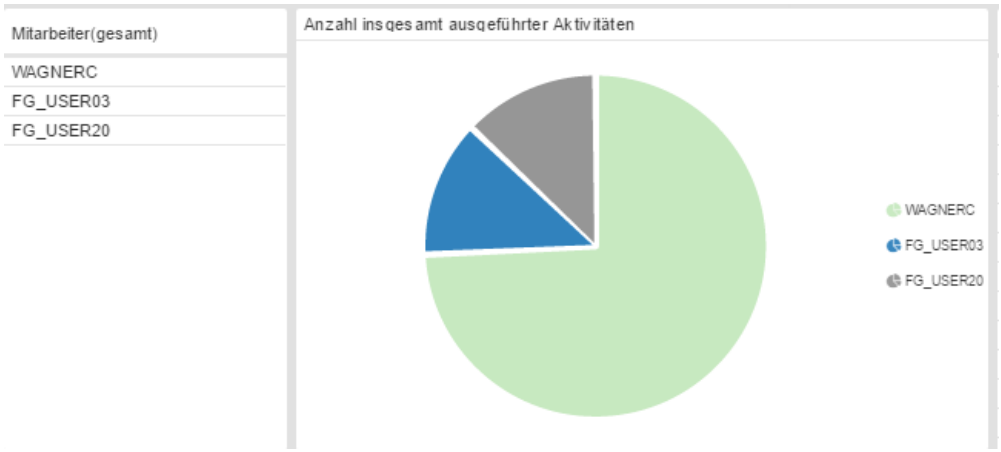


Abbildung 8-14: Mitarbeiter beteiligt an der Prozessinstanz

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Aus Lieferantensicht fällt auf, dass der zugehörige Lieferant ‚SEC Systems SA' seinen Sitz in Frankreich hat, jedoch ein Konto in Deutschland angibt. Insgesamt sind bei diesem Lieferanten 36 Red Flags aufgetreten. Aufgrund der Hinweise kann hier Rechnungsmanipulation oder Scheinfirma angenommen werden. Für die Rechnungsmanipulation spricht, dass die Kontonummer des Lieferanten vor der Überweisung geändert wurde. Auf Scheinfirma deuten Hinweise, wie die *‚plötzlich steigenden Rechnungen bei einem Lieferanten'* oder *‚Lieferant ohne Festnetznummer oder nur mit Anrufbeantworter'* hin. Dies kann aber an den schlecht gepflegten Masterdaten im IDES Beispieldatensatz liegen, wodurch Rechnungsmanipulation wahrscheinlicher ist. Vergleicht man die Ergebnisse mit dem Output des Fraud Generators, handelt es sich hierbei um Rechnungsmanipulation.

Die zweite Prozessinstanz mit sehr vielen Red Flags ist 900450002079500020 (ebenfalls 9004500207950040 und 900450002079500030). Die Prozessinstanz startet mit dem Schritt ‚Rechnung beglichen' und der Wareneingang fehlt komplett. Das Fraud Pattern *‚Rechnungsmanipulation'* schlägt an. Der gesamte Prozessablauf wird durch zwei Mitarbeiter

durchgeführt. Auffälligkeiten bei den bestellten Materialien oder dem Lieferanten sind nicht vorhanden. Von den angeschlagenen Red Flags sind besonders auf folgende hinzuweisen: ‚*Kein Wareneingang'* (obwohl es sich nicht um eine Dienstleistung handelt), ‚*Zahlung* stets *gleichen Betrags an Lieferanten'* und ‚*steigende Ausgaben für Waren'*. An dieser Stelle wird also Rechnung ohne Wareneingang vermutet. Vergleicht man die Ergebnisse mit dem Output des Datengenerators, handelt es sich hierbei tatsächlich um ‚Rechnung ohne Leistung oder Warenlieferung'.

Bei Prozessinstanz 900450002046200010 werden 17 Red Flags erkannt. Dabei wird das Fraud Pattern *‚doppelte Zahlung'* erkannt, da es mehrere Rechnungen für dieselbe Ware gibt. Auch wird der Freigabeprozess nicht durchgeführt. Aus Mitarbeitersicht sind nur zwei Mitarbeiter an dieser Prozessinstanz beteiligt. Zum Lieferanten und Material sind keine Besonderheiten zu nennen. Beim Vergleich mit dem Output des Datengenerators handelt es sich tatsächlich um eine *‚doppelte Zahlung'*.

Prozessinstanz 900450002078900010 hat mit 16 Red Flags die nächsthöchste Anzahl von Red Flags. Bei dieser Prozessinstanz schlägt das Fraud Pattern *‚Rechnungsmanipulation'* an. Aus Mitarbeitersicht ist zu erkennen, dass nur drei Mitarbeiter am gesamten Einkaufsprozess beteiligt sind. Beim Lieferanten ist auffällig, dass er eine französische Adresse hat, jedoch das Bankkonto in Deutschland liegt. Bei dem Material sind keine Auffälligkeiten zu sehen. Es handelt sich bei diesem Fraud Case tatsächlich um *‚Rechnungsmanipulation'*, wenn man die Prozessinstanz mit dem Output des Fraud Generators vergleicht.

Mit 16 Red Flags hat die Transaktion 900450002046100010 eine hohe Anzahl von Red Flags. Filtert man speziell nach dieser Prozessinstanz, werden einige Auffälligkeiten deutlich. Ein Fraud Pattern schlägt nicht an. Jedoch ist erkenntlich, dass zuerst die Rechnung beglichen und anschließend die Bestellanforderung und Bestellposition angelegt wird. Ein Wareneingang ist nicht vorhanden. In den Red Flags wird allerdings deutlich, dass es mehrere Rechnungen zu einer Ware gab und die Ware zusätzlich zu ungewöhnlichen Zeiten bezahlt wurde. Es wird vermutet, dass es sich hierbei um Rechnungen ohne Lieferung der Ware handelt. Dieser Verdacht bestätigt sich.

Die Prozessinstanzen 900450002067300030 und 900450002069700030 weisen mit 16 Stück eine hohe Anzahl an Red Flags auf. Das Fraud Pattern ‚*Rechnungsmanipulation'* schlägt bei beiden an. Aus Material- und Lieferantensicht sind keine besonderen Vorkommnisse ersichtlich. Es wird davon ausgegangen, dass es sich in diesem Fall um ‚*Rechnungsmanipulation'* handelt. Vergleicht man dieses Ergebnis mit dem Output des Fraud Generators, so bestätigt sich der Verdacht.

8.2.2.3.4 Fraud Detektion durch Prozessabweichung

Zusätzlich sollen Prozessinstanzen identifiziert werden, bei denen es zu ungewöhnlichen Abweichungen im Prozessablauf kommt. Diese sind beispielsweise doppelte Bezahlungen, Bezahlungen ohne Wareneingang oder fehlende Genehmigungen. Durch das Filtern auf diese Prozessinstanzen werden zusätzlich die dazugehörigen Red Flags und Fraud Patterns angezeigt. Diese Prozessabweichungen werden im Folgenden vorgestellt.

1) Zahlung einer Rechnung ohne Wareneingang

Zunächst wird nach Prozessinstanzen ohne Wareneingang, jedoch mit Begleichung der Rechnung gefiltert. Dabei handelt es sich entweder um Dienstleistungen oder aber um Rechnungen ohne gelieferten Waren. Die Anwendung dieser Filterregel zeigt, dass 647 Prozessinstanzen davon betroffen sind (Abbildung 8-15).

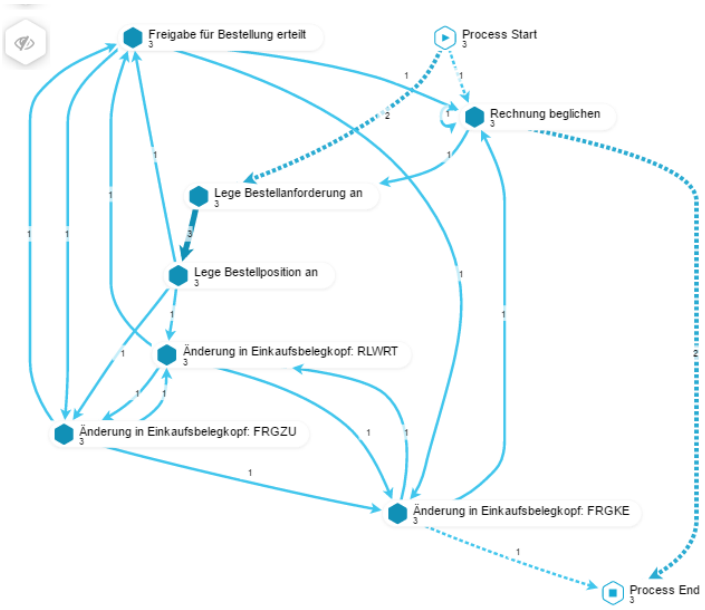


Abbildung 8-15: Prozesssicht (bezahlte Rechnung ohne Wareneingang)
Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

In 34 Prozessinstanzen wird zuerst die Rechnung beglichen und anschließend die Bestellposition angelegt und freigegeben. Dies kann in der Praxis ein dringender Einkauf sein, bei dem die Formalien und die Genehmigung erst im zweiten Schritt durchgeführt werden. Allerdings kann es auch ein Hinweis auf Fraud sein, weshalb an dieser Stelle neben der Prozessinstanz auch die aufgetretenen Red Flags beachtet werden. Innerhalb dieser Prozessinstanzen werden zwei Fraud Patterns identifiziert. Bei drei Prozessinstanzen schlägt der Prototyp auf das Pattern *‚Scheinfirma‘* an. Dabei wird die Bestellung vom selben Mitarbeiter genehmigt, der auch den Lieferanten erstellt hat. Zusätzlich sind die Einkaufsvolumina bei diesen neu erstellten Lieferanten sehr hoch. Eine genaue Untersuchung der beteiligten Mitarbeiter und Lieferanten ist an dieser Stelle notwendig. Bei weiteren drei Prozessinstanzen identifiziert der Prototyp eine *‚doppelte Bezahlung‘*. Hierbei werden mehrere Rechnungen erstellt, obwohl eine Ware nie geliefert wird. Eine Rechnung wird sogar doppelt beglichen. Da allerdings bei diesem Lieferanten nur zwei Transaktionen im Gesamtwert von 10€ vorhanden sind, übersteigen die Investigationskosten in einem normalen Unternehmen den Schaden. Dennoch sollte bei einer weiteren Kooperation mit diesem Lieferanten Vorsicht geboten sein.

2) Doppelte Zahlung einer Rechnung

Anschließend werden Fälle mit einer doppelten Zahlung einer Rechnung untersucht. Hierfür wird im Prozessexplorer nach Prozessinstanzen gefiltert, die doppelt durch den Schritt ‚Rechnung beglichen' führen. Wie in Abbildung 8-16 zu sehen, ist dies insgesamt in 124 Fällen geschehen.

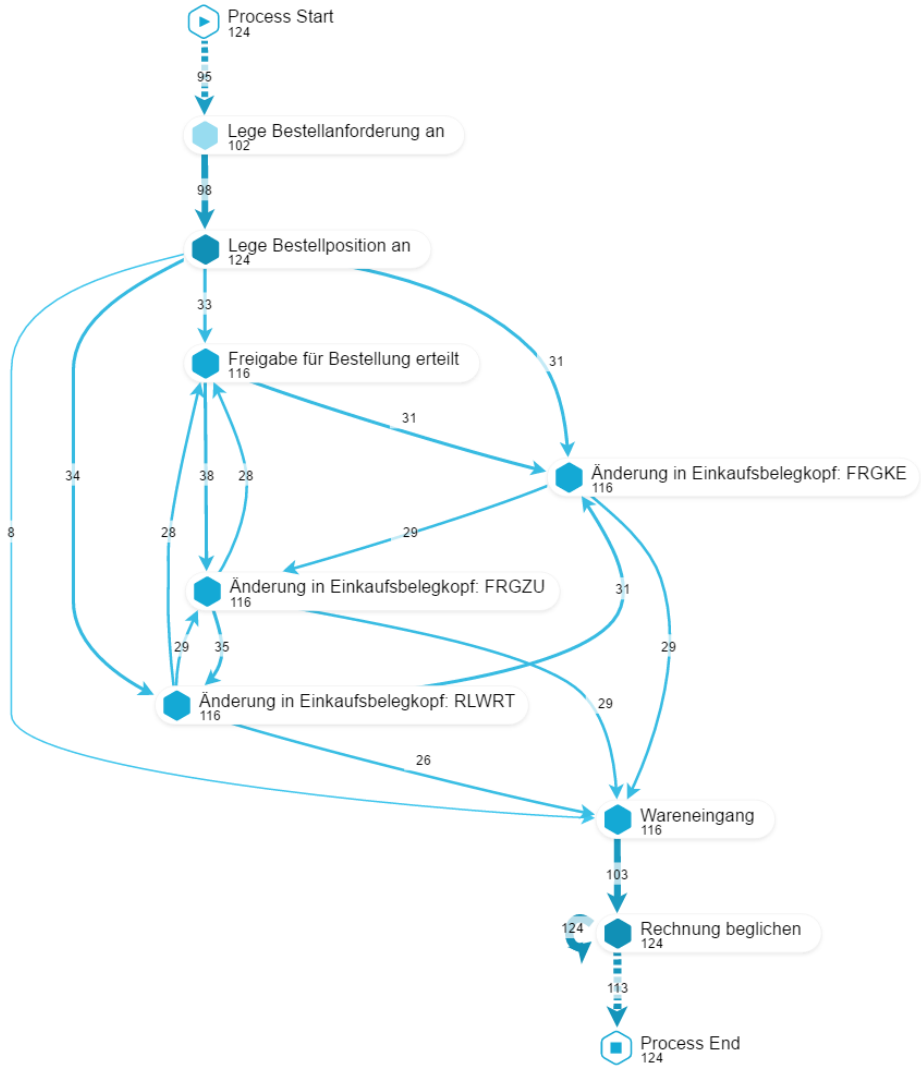


Abbildung 8-16: Prozessdarstellung doppelte Begleichung der Rechnung

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Der Prototyp unterscheidet nicht zwischen manueller Zahlung und Zahlung durch den automatischen Zahlungslauf. Die Fraud Patterns ‚*doppelte Zahlung*' und ‚*Rechnungsmanipulation*' sind angeschlagen. Da im Abschnitt ‚doppelte Zahlung' ausführlich darauf eingegangen wurde, wird dieser Fall nicht weiter analysiert.

3) Rechnung beglichen

Eine weitere Auffälligkeit in diesem Datensatz ist, dass 601 Rechnungen ohne jeglichen Bezug zur bestellten oder gelieferten Ware oder Dienstleistung vorhanden sind (vergl. Abbildung 7-17).

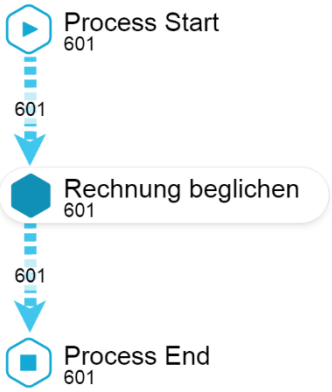


Abbildung 8-17: Prozessdarstellung Rechnung beglichen ohne Waren oder Dienstleistungseingang
Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Für Rechnungen ohne Bezug kann es mehrere Gründe geben. Beispielsweise kann in einem externen System die Kaufabwicklung durchgeführt werden und lediglich die buchhalterischen Schritte im SAP ERP System abgebildet werden. Bei allen 601 Prozessinstanzen werden allerdings zwei Besonderheiten identifiziert: *‚Mehrere Rechnungen für eine Dienstleistung/Ware‘* und *‚Rechnungsmanipulation‘*. Es wird also kurz vor der Bezahlung die Bankinformationen geändert. Analysiert man die unterschiedlichen Sichten, stellt sich heraus, dass der Mitarbeiter ‚Rendes‘ etwa 80 Prozent der Rechnungen beglichen hat. Filtert man also allein nach diesem Nutzer, so stellt sich heraus, dass er Rechnungen von insg. 1,1 Mio. € beglichen hat. Bei allen fehlt die Bestellanforderung und Bestellung, teilweise sogar der Wareneingang. Auffällig ist auch, dass nur zwei Lieferanten bei den 480 Prozessinstanzen dieses Mitarbeiters beteiligt sind. Diese sind neben ‘Sapsota Company Limited’ auch ‘Abbot Supplies Inc.’ Als Fraud Pattern hat nur das Pattern *‚Doppelte Zahlung‘* angeschlagen. Als Red Flags haben *‚ungewöhnliche Genehmigungen‘*, *‚Zahlung des gleichen Betrags an mehrere Lieferanten‘* oder der *‚Same-Same Different Test‘* angeschlagen. Bei dem Same-Same-Different Test zahlen zwei Personen dem gleichen Lieferanten am gleichen Tag denselben Betrag. Dies scheint allerdings kein geplanter Fraud Case zu sein, da die Prozessinstanzen nicht als Fraud im Datengenerator markiert sind. Es wird vermutet, dass der Fraud Generator an dieser Stelle einen Fehler geworfen hat und damit die Ausführung der Prozessinstanz unterbrochen hat.

8.2.2.4 Zusammenfassung und Interpretation der Ergebnisse

Insgesamt kann man den Datensatz durch Filterung auf drei verschiedene Arten untersuchen: Analyse der identifizierten Fraud Patterns, Analyse der Prozessinstanzen mit den meisten Red Flags und Analyse von Prozessabweichungen. Zusätzlich könnte man auch Lieferanten oder Mitarbeiter mit den meisten Red Flags detailliert untersuchen. Dies wird allerdings an dieser

Stelle nicht verfolgt, da die Daten künstlich generiert werden und Mitarbeiter, Lieferanten und Material zufällig gewählt werden.

Durch jede der beschriebenen Analysen werden wirtschaftskriminelle Handlungen identifiziert. Alle Fraud Fälle mit Prozessabweichungen wurden erkannt. Dazu gehören Rechnung ohne Bestellanforderung oder Bestellung, sowie Rechnung ohne Wareneingang, Zahlung ohne Rechnung und Zahlung vor Rechnungs- oder Wareneingang. Auch die aus der Literatur abgeleiteten Fraud Patterns haben zuverlässig die versteckten Fraud Cases identifiziert. Die Ergebnisse des generierten Datensatzes sind in Tabelle 49 dargestellt.

Synthetischer Datensatz	191.366 Prozessinstanzen 392 versteckte Fraud Szenarien	
	Identifiziert	Nicht Identifiziert
	316	76

Tabelle 49: Ergebnisse Fraud Analyse synthetischer Datensatz
Quelle: Eigene Darstellung

Von den insgesamt 392 generierten Fraudfällen wurden im künstlichen Datensatz 316 identifiziert und 76 nicht identifiziert. Um die Qualität des Prototyps mit anderen Ergebnissen vergleichbar zu machen, wird die sogenannte Wahrheitsmatrix (Konfusionsmatrix) verwendet. Diese ist aus dem Bereich des Data Minings bekannt (Witten & Frank, 2005) und findet auch im Bereich Fraud Detektion Verwendung (Phua et al., 2010).

	Fraud im Datensatz vorhanden	**Fraud nicht im Datensatz vorhanden**
Fraud vom Prototypen identifiziert	Richtig-positiv: (rp/(rp+fn))= 80,06%	Falsch-positiv: (fp/(rn+fp))= 0,17%
Fraud nicht vom Prototypen identifiziert	Falsch-negative (fn/(rp+fn))= 19,38%	Richtig-negativ: (rn/(rn+fp)) = 99,83%

Tabelle 50: Wahrheitsmatrix synthetischer Datensatz
Quelle: Eigene Darstellung

Dabei wurden als Berechnungsgrundlage folgende Werte angenommen:

- Richtig Positiv (rp): 316 (Summe aus den korrekt identifizierten Werten im Datensatz)
- Falsch Negativ (fn): 76 (Nicht identifizierter Fraud im Datensatz)
- Falsch Positiv (fp): 318 (Identifizierter Fraud, den es aber nicht gab)
- Richtig Negativ (rn): 190.246 (Alle analysierten Prozessinstanzen, bei denen kein Fraud vorkommt)

Die recht hohe falsch-positiv Rate hängt vor allem mit dem implementierten Red Flag *„Änderung einer Kontonummer“* zusammen. Dabei wird dieses Red Flag erkannt, sobald sich die Kontonummer eines Lieferanten ändert und anschließend eine Zahlung auf dieses Konto

erfolgt. Dabei wird keine zeitliche Dimension betrachtet. Die hohe falsch-positiv Rate kann auch damit erklärt werden, dass die Daten an nur einem Tag generiert wurden. Dadurch schlagen sämtliche Red Flags mit Zeitbezug an, wie *‚plötzliche Aktivität bei schlafenden Lieferanten‘* oder *‚stark steigende Einkäufe bei neuem Lieferanten‘.*

Durch diese erste Iteration des Design Science Zyklus wird noch Verbesserungspotenzial bei der Implementierung des Prototyps identifiziert. Im Einzelnen sind folgende Verbesserungsanforderungen an den Prototypen aus der ersten Iterationsrunde entstanden:

1) Die prototypische Implementierung macht keinen Unterschied zwischen einer manuellen Zahlung und einer Zahlung durch den automatischen Zahlungslauf. Eine Unterscheidung ist aber sinnvoll, da vor allem gesperrte Zahlungen manuell bezahlt werden können. In der Prozessübersicht soll deshalb eine Unterscheidung eingefügt werden.
2) Ausschöpfung eines abgelaufenen Rahmenvertrags wird nicht erkannt. Dieser Red Flag soll zu dem Fraud Pattern ‚*Private Einkäufe‘* hinzugefügt werden.
3) Die Ausschöpfung eines CpD (Conto pro Diverse) Kontos wird nicht angezeigt. Dies kann aber dahingehend ausgenutzt werden, dass nicht autorisierte oder gesperrte Lieferanten bezahlt werden. Ein zusätzliches Red Flag *‚Nutzung des CpD Kontos‘* soll dem Fraud Pattern *‚Scheinfirma‘* hinzugefügt werden.
4) Bei dem Red Flag *‚Änderung der Kontonummer‘* wird keine zeitliche Einschränkung angegeben und soll hinzugefügt werden.

Diese vier Aspekte werden zu dem Prototyp hinzugefügt. Bei der Untersuchung von synthetisch erstellten Daten kann der Vorwurf der fehlenden Validität entstehen, da selbst definierte Fraud Cases identifiziert werden. Deshalb wird in einem zweiten Schritt die Evaluation mit einem semi-synthetischen Datensatz durchgeführt.

8.3 Evaluation mit semi-synthetischen Daten (White Collar Hacking Contest)

Als nächstes wird die Analyse mit Daten des White-Collar Hacking Contests durchgeführt. Eine genaue Beschreibung des Wettbewerbs wird im Kapitel 8.3.1 vorgestellt. Anschließend werden die Daten mit dem zuvor erstellten Prototyp ausgewertet und mit den Präsentationen der Teilnehmer verglichen.

8.3.1 Forschungsinstrument

Für die hier durchgeführte Evaluation der Daten werden mehrere Datensätze aus dem White-Collar Hacking Contest der Technischen Universität München genutzt. Die Veranstaltung White-Collar Hacking Contest (WCHC) ist ein rundenbasierter Wettbewerb mit dem Ziel praxisorientiert Fraud Investigationen durchzuführen. Dabei werden die Teilnehmer des Wettbewerbs in einzelne Teams aufgeteilt. Die Teams nehmen zuerst die Rolle des Fraudsters (Wirtschaftskriminellen) ein. Dabei ist ihre Aufgabe Geld möglichst unbemerkt aus dem Unternehmen zu entwenden (Fraud zu begehen). Hierfür erhält jedes Team einen SAP Mandanten, in dem es einen oder mehrere Fraud Cases implementieren kann. Anschließend

nehmen die einzelnen Teams die Rolle des forensischen Prüfers ein. Hierfür erhalten die Teilnehmer einen Datenbankabzug eines gegnerischen Teams, welchen sie auf Spuren für Fraud analysieren. Der Gewinner des Wettbewerbs hat möglichst viel Geld unentdeckt entwendet und möglichst viele Fraud Cases der gegnerischen Teams identifiziert.

Das Konzept der Veranstaltung wurde von Dr. Michael Schermann an der Technischen Universität München entwickelt[37], wofür er 2011 den Ernst Otto Fischer-Lehrpreis erhielt. Der Contest wurde insgesamt drei Mal an der Technischen Universität München durchgeführt. Verschiedene Praxispartner standen den Teilnehmern bei der Auswahl von Fraud Cases als Coaches beratend zur Seite und waren Teil der Jury für die Ermittlung des Siegerteams. So wurde der Contest 2011 von KPMG unterstützt. Im Jahr 2014 wurde der Wettbewerb in Kooperation mit der Hochschule Heilbronn und den Auditing Abteilungen der Unternehmen Siemens, BMW, T-Systems und WTS durchgeführt. Im Jahre 2015 wurde der WCHC in Kooperation mit dem Studiengang Fraud Detektion der DeMontfort University und dem Process Mining Unternehmen Celonis durchgeführt.

Bei jeder Ausführung des WCHC wurden in drei Runden zunächst Fraud Cases versteckt und anschließend die Fälle der gegnerischen Teams analysiert. Die erste Runde diente jeweils zum Verstehen des SAP Systems, des Einkaufsprozesses und Fraud allgemein. Deshalb wurde entsprechend jedem Team ein Fraud Case zugeordnet, welches es implementieren sollte. Da hierbei noch keine interessanten Fraud Cases zu Stande kamen, werden die Daten aus der ersten Runde nicht in dieser Dissertation analysiert. In der zweiten und dritten Runde konnten die Teilnehmer eigene Ideen einbringen und Fraud begehen. Um die implementierten Fraud Szenarien möglichst realitätsnah zu gestalten, wurde jedem Team ein professioneller Coach (ein Praxispartner) zur Seite gestellt. In persönlichen und telefonischen Absprachen tauschten sich Teilnehmer und Coaches über Ideen und interessante Fraud Cases aus dem Berufsalltag aus. Dadurch konnte sichergestellt werden, dass sich im Datensatz sehr realitätsnahe und interessante Fraud Cases befinden. Um den Wettbewerb möglichst realitätsnah zu gestalten, wurden den Teilnehmern ein Datengenerationstool zur Verfügung gestellt. Dies ermöglichte den normalen Einkaufsprozess zu simulieren und erschwerte den Gegnern somit die Identifikation der Fraud Cases.

Bei jedem Wettbewerb wurde jeweils ein SAP ERP 6.04 System mit mehreren Mandanten verwendet. Im Jahr 2011 und 2014 wurde das Schulungssystem der SAP mit einem IDES Datensatz verwendet, während 2015 das Schulungssystem der SAP University Competence Centers verwendet wurde (GBI). Diese Schulungssysteme waren deshalb nötig, da bereits Master- und Bewegungsdaten erhalten sind (Beispieldaten), sowie bereits Customizing Einstellungen getroffen sind. An den Standardeinstellungen wurden keine Änderungen durchgeführt.

Für diese Arbeit werden die Daten aus 2014 und 2015 ausgewertet, um den implementierten Prototypen zu evaluieren. Die Daten aus dem Jahre 2011 können nicht verwendet werden, da wichtige Spalten und Tabellen nicht gesichert wurden. Die jeweiligen Datensätze aus den Runden 2 und 3 werden mit dem entwickelten Prototyp analysiert. Die Ergebnisse werden mit

[37] Für Details vergl. Schermann & Boss (2014).

den tatsächlich implementierten Fraud Cases verglichen. Da die Autorin als Dozentin an der TUM die Veranstaltung begleitet hat, liegen ihr die Daten aus beiden Jahren vor.

8.3.2 Parametrisierung des Prototyps

Für die Parametrisierung des Prototyps sind zwei Aspekte erforderlich. Zum einen müssen die Grenzwerte definiert werden und zum anderen die Kombination von Red Flags zu einem Fraud Pattern ausgewählt werden. Tabelle 51 zeigt eine Übersicht über die entsprechenden Kombinationen von Red Flags mit den dazugehörigen Anzahl der Treffer im Datensatz. Für die unternehmenstypischen Richtlinien und Grenzwerte (wie beispielsweise die Grenze ab wie viel € eine Bestellung einer Freigabe bedarf) werden die Werte analog zur synthetisch generierten Datensatz verwendet und sind in Tabelle 47 zusammengefasst.

Kickback Fraud

Kombinationen Red Flags	Runde 2 2014	Runde 3 2014	Runde 2 2015	Runde 3 2015
Flag_D01, Flag_D12	0	0	0	0
Flag_D01, Flag_D05	0	392	0	0
Flag_D01, Flag_D06	0	0	0	0
Flag_D11, Flag_D17	0	40	0	0
Flag_D02, Flag_D03	0	774	0	0

Angebotsmanipulation

Kombinationen Red Flags	Runde 2 2014	Runde 3 2014	Runde 2 2015	Runde 3 2015
Flag_E01, Flag_E06	0	0	0	0
Flag_E03, Flag_E06	1	2	0	0
Flag_E04, Flag_E16	0	0	0	0
Flag_E04, Flag_E09	0	0	0	0

Scheinfirma

Kombinationen Red Flags	Runde 2 2014	Runde 3 2014	Runde 2 2015	Runde 3 2015
Flag_B01, Flag_B10	0	49	0	0
Flag_B09, Flag_B13	0	72	0	0
Flag_B12, Flag_B13	0	0	0	0
Flag_B15, Flag_B16	0	182	0	0
Flag_B01, Flag_B09	7	2462	10	288

Doppelte Zahlung

Kombinationen Red Flags	Runde 2 2014	Runde 3 2014	Runde 2 2015	Runde 3 2015
Flag_C01, Flag_C02	0	2660	0	0
Flag_C01, Flag_C03	0	7317	0	0
Flag_C01, Flag_C02, Flag_C03	0	0	0	0
Flag_C02, Flag_C03	0	42	0	0
Flag_C01, Flag_C07	0	546	0	0

Pass Through

Kombinationen Red Flags	Runde 2 2014	Runde 3 2014	Runde 2 2015	Runde 3 2015
Flag_F01, Flag_F02	0	1106	0	0

	Flag_F01, Flag_F03	0	0	0	0
	Flag_F02, Flag_F05,	0	774	0	0
	Flag_F02, Flag_F03	0	0	0	0
	Flag_F02, Flag_F03, Flag_F04	0	0	0	0
unbeteiligter Lieferant	**Kombinationen Red Flags**	**Runde 2 2014**	**Runde 3 2014**	**Runde 2 2015**	**Runde 3 2015**
	Flag_G01, Flag_G02	0	0	0	0
	Flag_G01, Flag_G03	0	0	1	0
	Flag_G02, Flag_G03,	0	116	0	0
	Flag_G03	0	5527	0	2
Rechnungsmanipulation	**Kombinationen Red Flags**	**Runde 2 2014**	**Runde 3 2014**	**Runde 2 2015**	**Runde 3 2015**
	Flag_A01, Flag_A02	0	0	0	0
	Flag_A03, Flag_A04	0	0	0	0
	Flag_A04, Flag_A06	0	0	0	0
	Flag_A04, Flag_A08	0	0	0	0
	Flag_A04, Flag_A09	0	0	0	0
	Flag_A04	0	142367	0	0
Private Einkäufe	**Kombinationen Red Flags**	**Runde 2 2014**	**Runde 3 2014**	**Runde 2 2015**	**Runde 3 2015**
	Flag_H01, Flag_H02	0	0	0	0
	Flag_H02, Flag_H05	0	0	0	0
	Flag_H03, Flag_H08,	0	36	0	0
	Flag_H04, Flag_H05	0	2	0	0

Tabelle 51: Red Flag Kombinationen für Fraud Patterns (WCHC)
Quelle: Eigene Darstellung

8.3.3 Evaluation mit den Daten des WCHC 2014 (IDES)

Es sollen nun die Daten der einzelnen Gruppen mit dem Fraud Detektion Prototypen analysiert werden. Hierzu werden zunächst die Daten aus jeder Runde in die Datenbank SAP HANA geladen. Anschließend werden die Skripte zur Erstellung der notwendigen Tabellen für Celonis Process Mining, sowie für die Suche nach Red Flags und Fraud Patterns ausgeführt. Anschließend wird der Datensatz jeder Runde analysiert und mit dem tatsächlichen Fraud verglichen. Das Laden der Daten in die Datenbank und die Initialisierung des Prototyps erfolgen analog zum Kapitel 8.2.2.1 und werden hier nicht erneut dargestellt. Die Ergebnisse aus jedem Mandanten werden im Folgenden vorgestellt.

8.3.3.1 Evaluation mit Daten aus WCHC Runde 2

Da beim WCHC jedes Team einen eigenen Mandanten zur Implementierung von Fraud erhalten hat, werden an dieser Stelle die identifizierten Besonderheiten in jedem Mandanten zusammengefasst.

Im Mandanten **902** ist zunächst ersichtlich, dass es zu Änderungen der Kontonummern (Bankdaten) bei vielen Lieferanten gab, bevor Transaktion durchgeführt wurden.

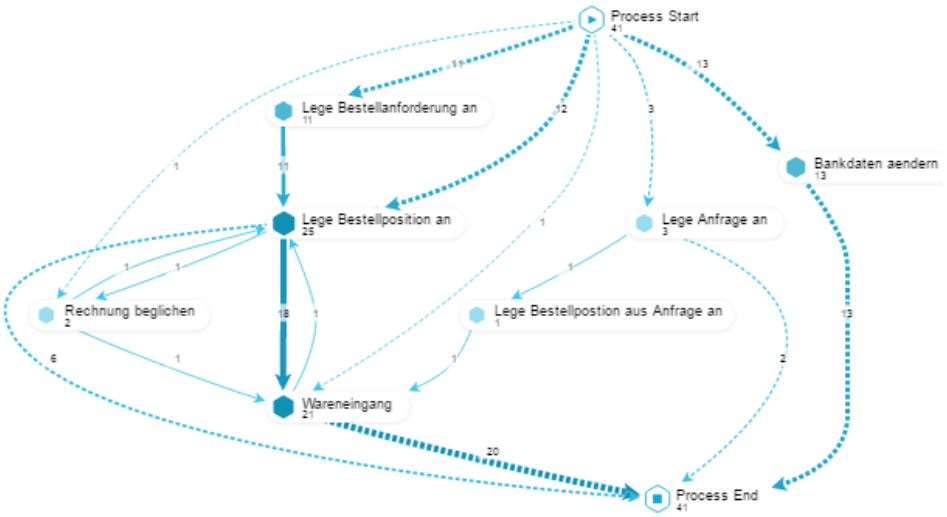


Abbildung 8-18: Prozessansicht Mandant 907
Quelle: Eigene Darstellung (Screenshot Celonis Process Mining)

Untersucht man diesen Sachverhalt genauer, so sieht man, dass neue IBAN und BICS eingeführt werden. Da es im Jahr 2014 in Deutschland zu einer Umstellung von Kontonummer und Bankleitzahl hin zu IBAN und BIC kam, so ist dieser Sachverhalt an dieser Stelle nicht weiter verwunderlich und stellt somit zunächst keinen Fraud dar. Dennoch ist auffällig, dass eine Achterbahn (warum braucht ein Fahrradunternehmen eine Achterbahn?) noch über Kontonummer und Bankleitzahl gekauft wird. Diese wird allerdings vor dem Kauf der Achterbahn verändert, so dass hier der Fraud vermutet wird.

Im Mandanten **905** ist auffällig, dass meist nur Dienstleistungen bestellt werden. Dabei ist eine Dienstleistung mit dem Namen „Sonderreinigung“ im Wert von 13.250 € vorhanden. Hierfür wird ein neuer Lieferant „Chemieteufel GmbH“ erstellt und die Sonderreinigung bestellt. Bei dieser Bestellung handelt es sich um die einzige Bestellung bei diesem neuen Lieferanten. Es gibt trotz der hohen Summe kein Ausschreibungsverfahren, keine Bestellanforderung und kein Genehmigungsverfahren. Es wird deshalb angenommen, dass diese Dienstleistung nie (oder nicht im abgerechneten Umfang) durchgeführt wird. Typische Red Flags, wie ‚*fehlende Angaben bei dem Lieferanten*‘ sind vorhanden, können aber aufgrund der generell nicht sorgfältig erstellten Masterdaten entstanden sein. Zusätzlich ist in diesem Mandanten auffällig, dass alle Waren und Dienstleistungen ohne MwSt. eingekauft werden. Dies kann auf die Unerfahrenheit der Teilnehmer zurückgeführt werden. Es wird vermutet, dass das Unternehmen ‚Chemieteufel GmbH‘ eine Scheinfirma ist und die Sonderreinigung nicht in vollem Ausmaß durchgeführt wird.

Im Mandanten **907** werden Flachdichtungen und Sechskantschrauben gekauft. Insgesamt wird der Wareneingang gebucht und die Rechnung beglichen, allerdings im nächsten Schritt von dem Benutzer Namens ‚Schacht‘ wieder zurückgesendet. Die Rechnung wird allerdings nie storniert. Deshalb wird vermutet, dass ein Komplize beim Lieferanten ‚C.E.B. Berlin & Max‘ die Zahlung für die stornierte Ware annimmt und mit dem Benutzer ‚Schacht‘ teilt.

Im Mandanten **904** wird ebenfalls eine Ware zurückgesendet, ohne die Rechnung zu stornieren. Weitere Hinweise sind nicht erkennbar. Es wird der gleiche Fraud wie im Mandanten 907 vermutet.

Im Mandanten **906** ist das Fraud Pattern *‚Angebotsmanipulation‘* angeschlagen. Filtert man alle Daten nach diesem Fraud Pattern, entsteht eine Prozessinstanz wie in Abbildung 8-19 dargestellt.

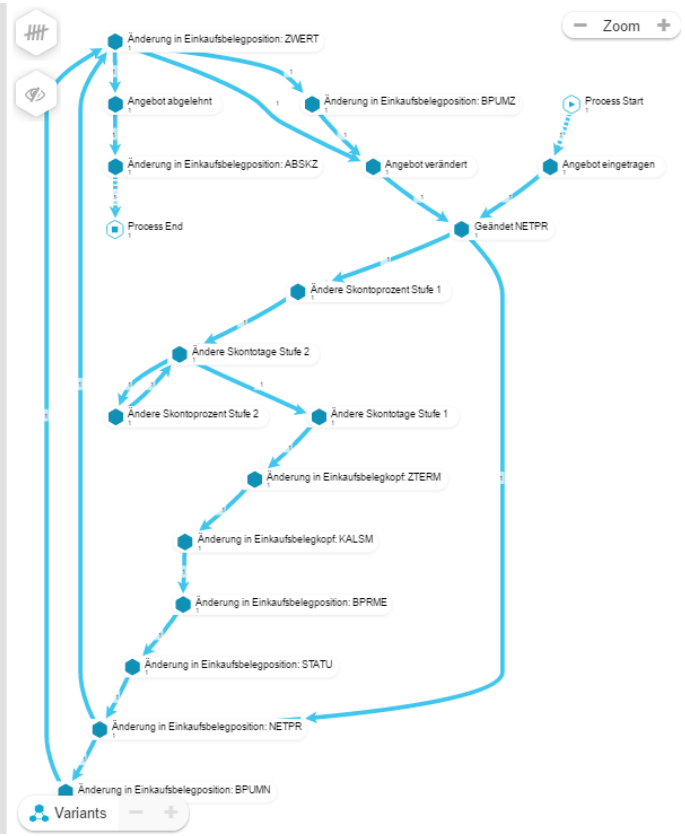


Abbildung 8-19: Prozessinstanz für das Fraud Pattern Angebotsmanipulation
Quelle: Eigene Darstellung (Screenshot Celonis Process Mining)

In dieser Prozessinstanz sind insgesamt elf Red Flags aufgefallen. Dazu zählen beispielsweise die *‚starke zeitliche Begrenzung der Angebotsabgabe‘* und die *‚nah beieinanderliegenden Ausschreibungsangebote‘*. Diese sind eher mit dem Charakter des Wettbewerbs zu erklären. Allerdings gibt es auch Red Flags, die sehr verdächtig sind. Dazu gehört, dass *‚bestehende Preise bei einem neuen Angebot fallen‘*, *‚ein Mitarbeiter die Lieferantenerstellung und Bestellung bei diesem Lieferanten durchführt‘* oder *‚Lieferanten die Möglichkeit haben nachträglich ihr Angebot aufzustocken‘*. Bei dieser Ausschreibung von Computer-Chips haben die Unternehmen ‚Mikron‘, ‚Infinion‘ und ‚AMD‘ teilgenommen (Achtung, hierbei handelt es sich um ein fiktives Beispiel der Wettbewerbsteilnehmer). Trotz der Ausschreibung wird der teuerste Bieter ausgewählt. Somit wird der Verdacht der Angebotsmanipulation geäußert.

Im Mandanten **901** ist zunächst auffällig, dass es viele Änderungen an den Währungskursen gibt. Besonders ist dabei der Umrechnungskurs von € in Haitianische Gourde aufgefallen. Es werden nach der Währungskursanpassung 26 Bestellungen bei dem Unternehmen ‚Maliga

Marvel Global Association‘ in Haiti durchgeführt. Vergleicht man den Wechselkurs mit dem aktuellen Währungskurs, so werden anstatt 26.901 € umgerechnet 242.111 € überwiesen. Es wird davon ausgegangen, dass es sich hierbei um Fraud handelt.

Im Mandant **903** ist zunächst auffällig, dass es insgesamt nur acht bestellte Materialien gibt (Metall, verdrilltes Kabel, Mount, Farbe, Grundierung, Washer und einen Basis Motor). Besonders auffällig ist, dass der Benutzer namens ‚WORKER02‘ die gesamte Prozesskette für den Kauf eines Motors durchführt. Andere Mitarbeiter sind in dieser Prozessinstanz nicht beteiligt. Zusätzlich ist der Motor *sehr knapp unter der Genehmigungsgrenze* (Kosten: 49.999€; Genehmigungsgrenze: 50.000 €). Diese Bestellung hat den höchsten Wert in diesem Mandanten. Ein Logistikunternehmen ‚Translog GmbH Stuttgart‘ ist der Lieferant dieses Motors. Dabei stellt sich die Frage, warum ein Logistikunternehmen Maschinen verkauft? Dieser Sachverhalt gilt als auffällig für Fraud. Vermutlich wird der Basis Motor nicht geliefert.

8.3.3.2 Vergleichende Analyse Runde 2

In diesem Bereich sollen die identifizierten Fraud Cases mit den von den Teilnehmern begangenen Fraud Cases verglichen werden. Als Grundlage zur Auswertung werden die Präsentationen der jeweiligen Teilnehmer verwendet, in der die Teilnehmer ihre Fraud Idee und Umsetzung detailliert beschreiben.

902	Umstellung IBAN/BIC	Im Zuge der Umstellung auf IBAN und BIC werden alle Konten entsprechend korrekt geändert. Jedoch werden auch die alten Bankdaten (Kontonummer und Bankleitzahl) geändert. Eine Rechnung wird entsprechend mit den alten Bankdaten durchgeführt.	Ja
905	Sonderreinigung	Eine Sonderreinigung für einen ausgelaufenen Tank wird ad-hoc bestellt. Diese wird allerdings nie geliefert.	Ja
907	Rückgaben	Flachdichtungen werden eingekauft. Diese werden teilweise wieder zurückgesendet, ohne aber die Rechnung zu stornieren.	Ja
904	verschrottete Ware	Ware wird gekauft, jedoch “versehentlich“ vom Gabelstapelfahrer zerstört. In Wirklichkeit wird die Ware jedoch auf Internetplattformen für gebrauchte Ware verkauft. Im SAP System wird diese als verschrottet angegeben.	Nein
906	Ausschreibungs-fraud	In einem Ausschreibungsverfahren werden verschiedene Computerchips verglichen. Es wird letztlich die teuerste Ware bei gleicher Qualität ausgewählter. Der Chiphersteller zahlt dem	Ja

		Komplizen im Unternehmen eine Ausgleichzahlung für die Auswahl.	
901	Wechselkursmanipulation	Der Wechselkurs zwischen Euro und Yen wird verändert. Anschließend wird eine Bestellung in Japan durchgeführt und die Rechnung entsprechend mit dem manipulierten Wechselkurs bezahlt. Die Überbezahlung wird zwischen Fraudster und Komplize aufgeteilt.	Nein
901	Wechselkursmanipulation II	Der Wechselkurs zwischen Euro und Yen wird verändert. Es wird gewartet, bis der Komplize eine Rechnung sendet, um diese anschließend mit dem gefälschten Wechselkurs zu bezahlen.	Nein
901	Wechselkursmanipulation III	Eine bisher nicht im System eingetragene Währung (HTG) wird hinzugefügt, allerdings mit einem falschen Währungskurs. Anschließend werden Waren aus Haiti bestellt und entsprechend bezahlt.	Ja
903	Zu hohe Rechnungen	Für die Lieferung von Motoren werden zu hohe Kosten in Rechnung gestellt. Die Überbezahlung wird zwischen den Fraudstern und den Komplizen im anderen Unternehmen aufgeteilt.	Tlw.

Tabelle 52: Gegenüberstellung tatsächliche Fraudschemata und identifizierte
Quelle: Eigene Darstellung

Die Fraud Cases ‚Umstellung IBAN/BIC', ‚Sonderreinigung' und ‚Rückgaben' können vor allem mit der Visualisierung der jeweiligen Prozessinstanz leicht identifiziert werden. Der Fraud Case ‚verschrotteten Ware' wird nicht erkannt. In der Praxis stellt dieser Fraud ein Risiko dar. Der Gabelstapelfahrer riskiert bei wiederholten unachtsamen Verhalten seine Arbeitsstelle. Zusätzlich sind die Fernseher oft im neuen Zustand vor dem Fall in der Verpackung durch Styropor oder ähnlichen Dämmmaterialien geschützt. Dadurch ist es fraglich, ob die Fernseher tatsächlich durch einen Sturz vom Gabelstapler zerbrechen. Auch das Weiterverkaufen der verschrotteten Ware stellt ein Risiko dar, da der Verkaufshändler leicht überführt werden kann (Anhand der eindeutigen ID der Fernseher).

Das Fraud Pattern ‚Angebotsmanipulation' identifiziert erfolgreich den versuchten Fraud mit Computer Chips. Allerdings kann man nicht immer von Fraud ausgehen, wenn das teuerste Angebot ausgewählt wird. In diesem Fall kommt es zu weiteren Unstimmigkeiten (bspw. die Möglichkeit nachträglich das Angebot aufzubessern), so dass der Fraud identifiziert wird.

Eine Wechselkursmanipulation im Mandant 901 wird festgestellt und als auffällig markiert. Weitere Wechselkursänderungen werden zwar im Prototypen erkannt, aber nicht im Detail analysiert.

Im Mandanten 903 wird fälschlicherweise angenommen, dass das Produkt namens ‚Motor' nicht geliefert, jedoch trotzdem bezahlt wird. Tatsächlich werden zu hohe Kosten für den Motor berechnet. Eine manuelle Untersuchung des Lagers hätte die Annahme widerlegen können (die im Rahmen dieses Wettbewerbs nicht möglich ist). Dennoch ist diese Transaktion sehr auffällig (Kosten sind knapp unter Genehmigungsgrenze, nur ein Mitarbeiter ist für den gesamten Prozessablauf verantwortlich, warum verkauft ein Logistikunternehmen Motoren). Aus diesem Grund wäre der Fraud an dieser Stelle bei einer genauen Untersuchung des Workers02 und des Lieferanten aufgefallen.

8.3.3.3 Evaluation mit Daten aus WCHC Runde 3

Der Datensatz enthält 212.816 Prozessinstanzen und 235 an der Prozessausführung beteiligte Mitarbeiter. Es werden 176 verschiedene Materialien und Dienstleistungen von 311 verschiedenen Lieferanten bestellt. Dabei werden 460.406 Rechnungen mit einem Gesamtrechnungsbetrag von 47,7 Milliarden € bezahlt. Der Fraud Prototyp identifiziert 11.371 Fraud Patterns und 924.375 Red Flags. Der mögliche Schaden beläuft sich auf 2,65 Mrd. €. Eine detaillierte Analyse erfolgt aufgrund der vordefinierten Fraud Patterns, den auffälligsten Prozessinstanzen und möglicher Prozessabweichungen. Anschließend werden die Ergebnisse mit der Dokumentation aus dem Wettbewerb verglichen. Genehmigungen werden an dieser Stelle nicht betrachtet, da diese der Einfachheit halber nicht durch die Teilnehmer realisiert wurden.

Zunächst soll der Mandant **901** analysiert werden. Auffällig ist sofort eine Prozessinstanz, bei der 4500€ für Transportkosten ausgegeben werden. Dabei wird die Rechnung beglichen, bevor die Dienstleistung erbracht wird. Auffällig ist neben der hohen Summe für Lieferkosten auch, dass der Lieferant eine natürliche Person und kein Unternehmen ist. Weitere Dienstleistungen oder Transporte werden bei dieser Person nicht bestellt. Auch das Fraud Pattern *‚Scheinfirma'* schlägt bei dieser Person an, da die Adresse identisch zu der eines anderen Lieferanten ist und der Lieferant einzig eine Postfachanschrift hat. Zusätzlich wird der Lieferant vom selben

Mitarbeiter genehmigt, wie auch angelegt. Eine genaue Überprüfung dieser Person mit Verdacht auf Scheinfirma ist daher wünschenswert.

Abbildung 8-20: Prozesssicht Rechnung vor Dienstleistungserbringung beglichen
Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Eine weitere sehr hohe Dienstleistungsposition in diesem Mandanten tritt für die Reparatur einer neuen Pumpe auf. Auch hier wird zunächst die Rechnung beglichen und im nächsten Schritt die Dienstleistung bestellt. Fraglich ist, warum bei einer neuen Pumpe sofort Reparaturkosten in Höhe von 17,5 Tsd. € anfallen und ob diese nicht unter die Gewährleistungspflicht des Lieferanten fallen. Es könnte sich bei den Reparaturkosten um Einbaukosten (den die Teilnehmer falsch deklariert haben) handeln. Dennoch bedarf es einer genauen Prüfung dieser Reparaturkosten. Eine weitere Auffälligkeit im Datensatz ist, dass vermeintlich Commodity Materialien aus den Fidschis importiert werden. So werden Kugellager, Kabelbäume, Katalysatoren, Hauptplatinen und Aluminium im Gesamteinkaufswert von 942 Tsd. € bestellt. Beteiligt sind die beiden Unternehmen ‚Jamuna ltd.' und ‚Kaopeng AG'. Zu hinterfragen ist an dieser Stelle, ob es nicht preisgünstiger wäre Commodity Materialien im eigenen Land zu bestellen um Lieferkosten zu sparen. Hier muss nicht unbedingt Fraud vorliegen. Eine Wirtschaftlichkeitsprüfung wäre aber sinnvoll. Zusätzlich wird erkenntlich, dass 73% aller Bestellungen Flüge sind. Dabei werden Kosten von 19,5 Millionen € für 300 Flüge veranschlagt. Diese Flüge werden alle bei dem Unternehmen ‚Hans Müller' eingekauft. Selbst wenn Hans Müller ein Reisebüro ist, ist es doch sehr unwahrscheinlich oder zumindest unwirtschaftlich durchschnittlich etwa 65.000 € pro Flug zu zahlen. Weiterhin werden noch drei Fraud Patterns erkannt. Zunächst wird das Pattern *Scheinfirma* erkannt. Neben dem zuvor benannten Lieferanten ‚Hans Müller' ist auch das

Unternehmen ‚SUESS' aufgefallen. Bei diesem Lieferanten werden für 1,51 Mio. € Tablet PCs bestellt. Fast die gesamte Prozessaktivität wird durch den Mitarbeiter ‚PSEIBOLDT' durchgeführt. Hier wird aufgrund der hohen Summe für die Tablet PCs und der Ausführung des gesamten Prozesses durch einen Mitarbeiter die genaue Prüfung dieses Falls empfohlen.

Im Mandanten **902** ist das Fraud Pattern *‚Angebotsmanipulation'* angeschlagen. Bei einer Ausschreibung werden nachträgliche Änderungen des Angebots akzeptiert. Auch ist die Ausschreibung stark geteilt und jede Ausschreibung knapp unter der Genehmigungsgrenze. Insgesamt werden nur wenige Angebote abgegeben und als ein neues Angebot hinzukommt, fallen die bestehenden Preise. Diese Anzeichen sprechen deutlich für einen Angebotsmanipulationsfraud. Der gesamte Prozessablauf wird durch einen einzigen Mitarbeiter im Unternehmen durchgeführt, so dass hier der Fraud vermutet wird.

Im Mandanten **903** gibt es Hinweise auf eine *‚Scheinfirma'*. So werden 57t Zinn bei einem neuen Lieferanten gekauft. Die Zahlung wird auf ein Konto einer Privatperson getätigt und nicht auf ein Firmenkonto. Jede Zinn-Bestellung überschreitet die vorherige um ein Vielfaches. Die Ausgaben für Zinn steigen ebenfalls erheblich, wie in Abbildung 8-21 dargestellt ist.

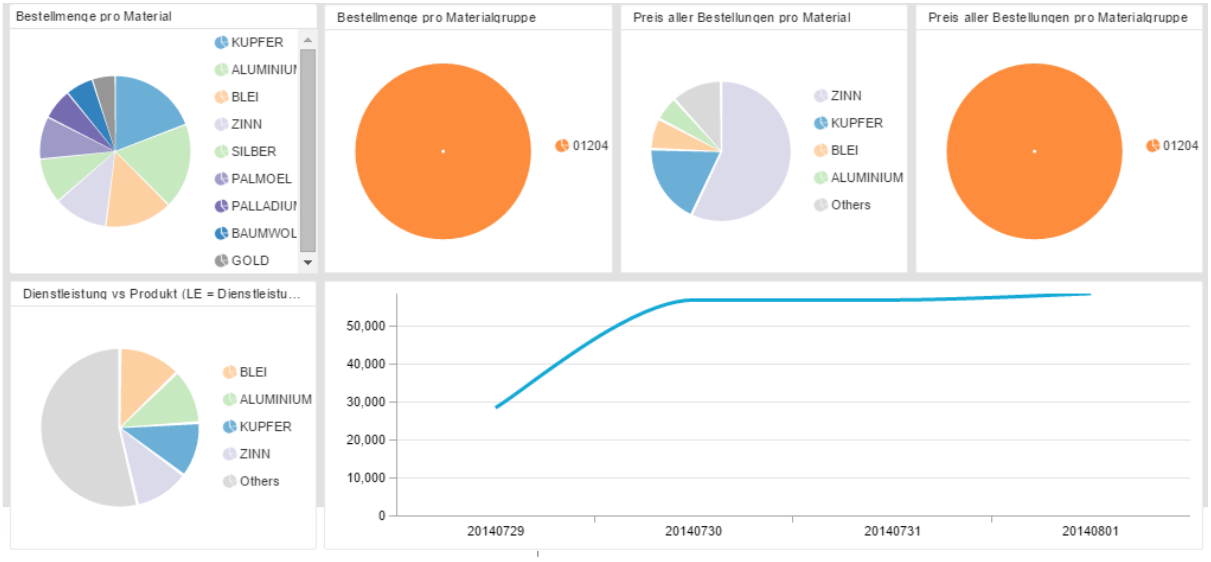


Abbildung 8-21: Steigende Ausgaben für Zinn

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Man erkennt in Abbildung 8-21 neben den steigenden Kosten für Zinn auch, dass die Ausgaben für Zinn überdurchschnittlich hoch sind (Preis aller Bestellungen pro Material). Deshalb wird eine Scheinfirma vermutet, die nicht in vollem Umfang oder Überteuert Zinn anbietet.

Im Mandanten **904** ist eigenartig, dass das Unternehmen IDES 650 kg Uran kauft. Zunächst stellt sich die Frage, wie und warum ein Unternehmen Uran in diesen Mengen kaufen kann. Bei der Filterung nach allen involvierten Daten erkennt man, dass Uran nach dem Einkauf wieder Veräußert wird (Warenausgang). Der gesamte Prozess wird nur durch den Mitarbeiter ‚X06' durchgeführt. Diese Tatsache bedarf einer genaueren Analyse durch entsprechende Interviews mit den beteiligten Mitarbeitern und dem Lieferanten ‚C.E.B Berlin'. Bei diesem Lieferanten werden sonst Fernseher, SSDs und Monitore gekauft. Zusätzlich wird in diesem Mandanten deutlich, dass besonders hohe Kosten für die Leistung Headhunter und Beratung angefallen sind (vergl. Abbildung 8-22). Entweder hat dieses Unternehmen ein massives Problem mit der Einstellung neuer Mitarbeiter, oder aber es handelt hierbei um Fraud.

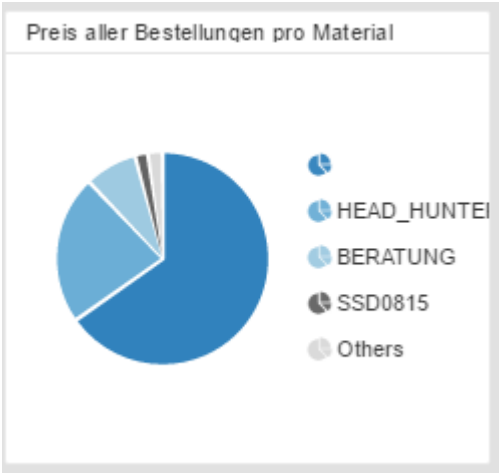


Abbildung 8-22: Hohe Kosten für Headhunter Dienstleistungen
Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Im Mandanten **905** werden die Fraud Patterns *‚Scheinfirma'* und *‚unbeteiligter Lieferant'* erkannt. Bei Scheinfirma ist auffällig, dass alle Prozessschritte nur durch den Mitarbeiter ‚YK1B_A02' durchgeführt werden. Interessant ist auch, dass bei einer Bestellung ein ‚BMW 760 Li' für 689.075€ von dem Lieferanten ‚Ultralight' gekauft wird. Bei so hohen Anschaffungskosten wäre eine Anschaffung direkt beim Hersteller sinnvoll. Detaillierte Interviews mit dem Lieferanten und dem entsprechenden Mitarbeiter erscheinen hier notwendig. Derselbe Mitarbeiter ist auch alleiniger Ausführer des Einkaufsprozesses bei dem zweiten Fraud Pattern unbeteiligter Lieferant. Auch hier wird wieder ein teures Auto (Mercedes Benz) für 1.168.067 € vom Lieferanten ‚Abele Intershop' bezogen und eine Rechnung doppelt beglichen. Diese Prozessinstanz hat mit insgesamt 17 die meisten Red Flags in diesem Mandanten. Auch hier wird die genaue Prüfung von Abele Intershop und dem Mitarbeiter YK1B_A02 empfohlen.

Im Mandanten **906** wird das Pattern *‚Kickback Fraud‘* erkannt. Dabei werden Zahlungen weit über den Marktdurchschnitt für Gabelstapler ausgegeben. Insgesamt werden 408.596 Gabelstapler gekauft und teilweise doppelt bezahlt. Für die Anschaffung von 408.596 Gabelstapler würde man eine Ausschreibung und eine Angebotseinholungsphase erwarten. Diese fehlen allerdings. Es werden beispielsweise 2500 Gabelstapler für 20.000€ das Stück eingekauft. Der Wareneingangsbeleg fehlt, die Rechnung wird aber doppelt beglichen. Alle Bestellvorgänge werden von nur drei Mitarbeitern durchgeführt. Auffällig ist aus Lieferantensicht, dass der Lieferant die gleiche Adresse wie ein anderer hat. Bei 142 Bestellungen wird kein Wareneingang verzeichnet, obwohl die Rechnung beglichen wird. In sieben Fällen wird die Rechnung sogar doppelt bezahlt. Dieser Sachverhalt ist in Abbildung 8-23 dargestellt. Das Pattern ‚Kickback Fraud‘ schlägt auch beim Einkauf von Schweißmaschinen und Klimaanlagen an, da erheblich höhere Ausgaben als im Durchschnitt verzeichnet werden können. Aufgrund der unzureichenden Vergleichsdatenlage aufgrund der Datengenerierung im Wettbewerb, wird diesem Pattern nicht weiter nachgegangen.

Abbildung 8-23: Prozesssicht Rechnung ohne Wareneingang

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Im Mandanten **907** besteht der Verdacht auf *‚doppelte Zahlungen‘*, wobei mehrere Rechnungen für dieselbe Ware im System vorhanden sind. Bei diesen Rechnungen fällt auf, dass die Lieferantenrechnung höher als der Bestellbetrag ist. Dabei wird die gesamte Prozessinstanz lediglich von dem Mitarbeiter ‚KUEHFUSS‘ durchgeführt Diese Rechnungen werden allerdings nie bezahlt. Wenn kein Geld das Unternehmen verlässt, handelt es sich streng genommen nicht um Fraud. Zusätzlich fällt in diesem Mandanten auf, dass in sechs Fällen lediglich eine Rechnung ohne Bezug zur Bestellanforderung oder Bestellung beglichen wird. Alle Zahlungen gehen an den Lieferanten ‚C.E.B. Berlin‘, bei dem Stilllegung und Geometriechecks bestellt werden. Auffällig ist hierbei, dass der Stammsatz auf Deutsch und auf Englisch existiert und mit beiden eingekauft wird, wobei insgesamt 401 Tsd. € an den entsprechenden Lieferanten bezahlt werden. Trotz der hohen Kosten für diese Dienstleistungen wird keine Ausschreibung durchgeführt. Außerdem ist es merkwürdig, dass die Bestellung von

dem Administrator mit SAP-All Rechten angelegt wird, ohne das eine Genehmigung vorliegt. Deshalb ist an dieser Stelle ein Interview mit dem Lieferanten ‚C.E.B. Berlin' sinnvoll.

8.3.3.4 Vergleichende Analyse Runde 3

Es werden nun die identifizierten Fraud Cases mit den von den Teilnehmern des Wettbewerbs beschriebenen Fraud Cases verglichen. Dabei wird geprüft, ob diese Fraud Cases identifiziert wurden. Die Ergebnisse sind in Tabelle 53 zusammengestellt.

Mandant	**Fraud Typ**	**Beschreibung**	**Identifiziert?**
901	Überteuerte Laptops bei einer Scheinfirma	Es werden 1500 Tablets bei einem Scheinlieferanten zu einem überhöhten Preis bestellt.	Ja
	Zusätzliche Lieferkosten	Motorblöcke werden eingekauft. Zusätzlich werden noch Lieferkosten zu den Motorblöcken addiert, die eigentlich im Lieferpreis enthalten sind.	Nein
	Defekte Lieferung	Bei einer Lieferung werden als defekt angegebene Pumpen geliefert. Diese werden auf Kosten des IDES Unternehmens von einer Scheinfirma „repariert". Die Bezahlung für die nicht erbrachte Leistung wird zwischen der Scheinfirma und dem Auftrag gebenden Mitarbeiter geteilt.	Ja
902	Piraten Fraud	Das Unternehmen IDES hat Zinn aus Jeddah (Saudi-Arabien) gekauft. Auf dem Transportweg nach Hamburg sind häufig Piraten unterwegs, weshalb eine Piratenpauschale hinzugefügt wird. Tatsächlich wird aber die Route über Südafrika gewählt, wo keine Piraten vorkommen. Die zusätzlichen Kosten werden durch den Einkauf eines teuren Gemäldes durch den Fraudster eingenommen.	Nein
903	Transportkosten-fraud	Es werden für bestellte Autoscheinwerfer höhere Transportkosten pro Stück berechnet. Da insgesamt 70.468 Stück bestellt werden, wird so eine erhebliche Summe aus dem Unternehmen geschaffen.	Nein
	Angebotsmanipulationsfraud	Computer Chips werden in einer Ausschreibung bestellt. Nach der Angebotsphase wird das	Ja

		teuerste Angebot ausgewählt, obwohl alle Computerchips gleichwertig sind.	
	F&E Extrakosten	Bei einer Bestellung werden für Sensoren neue Anforderungen erhoben. Damit der Lieferant diesen Anforderungen nachgehen kann, wird für einen bestimmten Zeitraum eine zusätzliche F&E Kostenpauschale bei der Bestellung des Produktes vereinbart. Nach dieser Zeit soll der normale Preis bezahlt werden. Jedoch wird auch nach dieser Periode die zusätzlich R&D Pauschale erhoben und zwischen den Tätern aufgeteilt.	Nein
904	Personalabwerber	Bei diesem Fraud Fall wird ein Personalabwerber engagiert. Bevor die Zahlung auf das Konto des Personalers getätigt wird, wird seine Kontonummer geändert und die Überweisung auf das Konto eines Komplizen durchgeführt. Durch einen Fehler der Teilnehmer wird die Kontonummer nie im System geändert und kann somit nicht identifiziert werden.	ungültig
905	Gold Fraud	Gold wird eingekauft und entsprechend versteuert. Da aber nach deutschem Recht Anlagegold nicht versteuert wird (da es eine Währung ist), konnten die zu viel eingenommenen Gelder vom Finanzamt unbemerkt zurückgefordert werden.	Nein
906	Schlechte Qualität	Kabelstränge mit einer schlechten Qualität werden eingekauft. Dabei handelt es sich nicht um A-Ware (sondern um B-Ware) die aber zum Preis von A-Ware verkauft wird.	Nein
907	Fallende Preise nicht berücksichtigt	Für das Material 100-100 Casings werden die Preise gesenkt. Das Unternehmen IDES zahlt weiterhin den vollen Preis, so dass die Preisdifferenz zwischen dem Lieferanten und dem internen Einkäufer aufgeteilt wird.	Tlw.

Tabelle 53: Gegenüberstellung tatsächliche Fraudschemata und identifizierte
Quelle: Eigene Darstellung

Es werden bereits viele Fraudfälle erkannt. Dennoch gibt es an dieser Stelle Verbesserungspotential. Zunächst werden Fraud Cases, die Lieferkosten enthalten, nicht erkannt. Deshalb sollten Red Flags, die Unregelmäßigkeiten bei Lieferkosten entdecken

hinzugefügt werden. Zusätzlich reagiert das Pattern Kickback Fraud nicht zuverlässig. Eine mögliche Erklärung liegt in der Natur der Daten. Da der Wettbewerb zeitlich begrenzt ist und das SAP System vor und nach dem Wettbewerb nicht produktiv verwendet wird, kommt es hier zu Unregelmäßigkeiten, wie beispielsweise plötzlich steigende Ausgaben für einige Produkte oder bei einigen Lieferanten.

Auch müssen einige Red Flags bei der Suche nach Fraud ignoriert werden, da die Daten des Wettbewerbs einige Auffälligkeiten aufweisen. Dazu gehören Red Flags bezogen auf unvollständige Daten, Genehmigungen oder zeitliche Aspekte. Der Gold Fraud mit falsch berechneten Steuersätzen wurde nicht erkannt. In diesem Fall wäre das Finanzamt am Fraud beteiligt. Eine Beteiligung des Finanzamtes wäre zwar möglich aber erscheint eher unwahrscheinlich.

Das Fraud Case mit gelieferter B-Ware statt A-Ware wurde nicht erkannt. Mangelhafte Qualität ist insgesamt schwierig zu identifizieren, da diese oft erst bei der Benutzung festgestellt werden kann. Oft werden Materialien stichprobenartig geprüft. Allerdings können so keine Langzeitschäden oder schnellerer Verschleiß identifiziert werden. Noch schwieriger erscheint schlechte Dienstleistungsqualität erkennbar zu sein. Aus Sicht des Lieferanten ist dieser Fraud Case allerdings gefährlich, da er bei gleichbleibender schlechter Qualität ggf. ausgewechselt wird. Dennoch handelt es sich um einen durchaus realistischer Fraud Fall, der identifiziert werden sollte.

8.3.4 Evaluation mit den Daten des WCHC 2015 (GBI)

Als nächstes soll der Prototyp mit den Daten des White Collar Hacking Contests 2015 ausgewertet werden.

8.3.4.1 Evaluation mit Daten aus WCHC Runde 2

Der GBI Datensatz in der zweiten Runde des White Collar Hacking Contests 2015 enthält 18.517 Prozessinstanzen mit 30 aktiven Mitarbeitern und 26 verschiedenen Lieferanten. Es werden insgesamt 13 verschiedene Materialien im Gesamtwert von 34,84 Tsd. € aufgeteilt auf 36 Rechnungen eingekauft. Insgesamt werden in dem Datensatz 18 Fraud Patterns (*Scheinfirma* und *unbeteiligter Lieferant*) und 10.721 Red Flags identifiziert.

Im Mandanten **713** wird das Fraud Pattern *‚Scheinfirma‘* erkannt. Interessant in der dazugehörigen Prozessinstanz ist, dass der gesamte Bestellprozess lediglich von dem Mitarbeiter ‚KOENIG‘ durchgeführt wird. Dabei werden Helme im Wert von 125 € bestellt. Die Gesamtsumme ist insgesamt gering, so dass eine Untersuchung dieses Lieferanten nur bei einem regelmäßigen Verdacht sinnvoll wäre. Die gefundenen Anzeichen für einen Scheinlieferanten sind: *Lieferant ohne Steuernummer, mehrere Instanzen desselben Lieferanten, plötzliche Aktivitäten in nicht aktiven Konten* und *Lieferant ohne Festnetz oder nur Anrufbeantworter*. Alle hier genannten Red Flags können auch auf die schlechte Datenqualität und Unerfahrenheit der Wettbewerbsteilnehmer hindeuten. Dennoch erscheint eine Untersuchung des Lieferanten ‚Olympic Protective Gear‘ und des Nutzers ‚KOENIG‘ als

sinnvoll. Weitere Fraud Patterns sind nicht aufgetreten. Streng genommen werden keine Rechnungen in diesem Mandanten bezahlt, wodurch kein Fraud vorkommt (vergl. Abbildung 8-24). Dennoch wird von einer geplanten Bezahlung der Rechnungen ausgegangen.

Abbildung 8-24: Zahlung ist in allen Prozessinstanzen nicht vorgekommen
Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Auffällig in der Prozessgraphik ist eine Prozessinstanz, bei der zuerst der Wareneingang und anschließend die Bestellung angelegt wurde. Per se ist dies kein Fraud und kann auf eine dringliche Anfrage hindeuten. Es handelt sich hierbei allerdings um eine „Mannstunde Fundament ausheben", also eine Leistungseinheit bei der die Eile und die Leistung an sich stutzig macht. Dabei wird bei dem Lieferanten ‚Jevgeni Bronshtein' der Firma ‚BAUJ' eingekauft. Bei Filterung auf diese Firma erkennt man, dass diese nur für das Fundament zuständig ist. Auffällig erscheint hier, dass für jeden Posten zur Erbauung der Lagerhalle eine eigenständige Firma beauftragt wird, wie Abbildung 8-25 zeigt.

Material
Grundstück
Lagerhalle 1000qm entwerfen
Entwurf Lagerhalle
Grundstück 2500qm
Baugenehmigung Lager Heidelberg
Gutachten Grundstück
Catering pro Person
Mannstunde Fundament ausheben
Mannstunde Gelände räumen
Fundament giessen

Abbildung 8-25: Materialien für den Bau einer Lagerhalle
Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Filtert man ausschließlich nach für den Bau der Lagerhalle benötigten Materialien, so erkennt man alle beteiligten Lieferanten und ihre entsprechende Anzahl an Red Flags (vergl. Abbildung 8-26). Es fällt auf, dass jeder Lieferant sehr viele Red Flags aufweist. Vor allem die beteiligten Lieferanten ‚BAUJ' und ‚ARCH' sollten durch die hohe Anzahl von Red Flags genau untersucht werden. Es wird davon ausgegangen, dass die entsprechende Dienstleistung für den Bau der Lagerhalle nicht oder nicht im vollen Umfang durchgeführte wurde.

Lieferant	Anza...
ARCH	16.0
IMMO1	7.00
MUSTERBAU	7.00
BAUG	6.00
BAUJ	6.00
BAUT	6.00
LAH	5.00
0000125000	3.00

Abbildung 8-26: Materialien und Red Flags

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Im Mandanten **714** wird das Fraud Pattern *‚Scheinfirma‘* identifiziert. Dabei sind Red Flags enthalten, wie *‚plötzliche Aktivitäten in nicht aktiven Konten‘* und *‚Lieferanten ohne Festnetz oder nur Anrufbeantworter‘.* Auch hier können die Fehler auf unsaubere Daten hinweisen. Die Lieferung von Mittagessen ist hier auffällig, da eines der Mittagessen nicht geliefert wird (vergl. Abbildung 8-27).

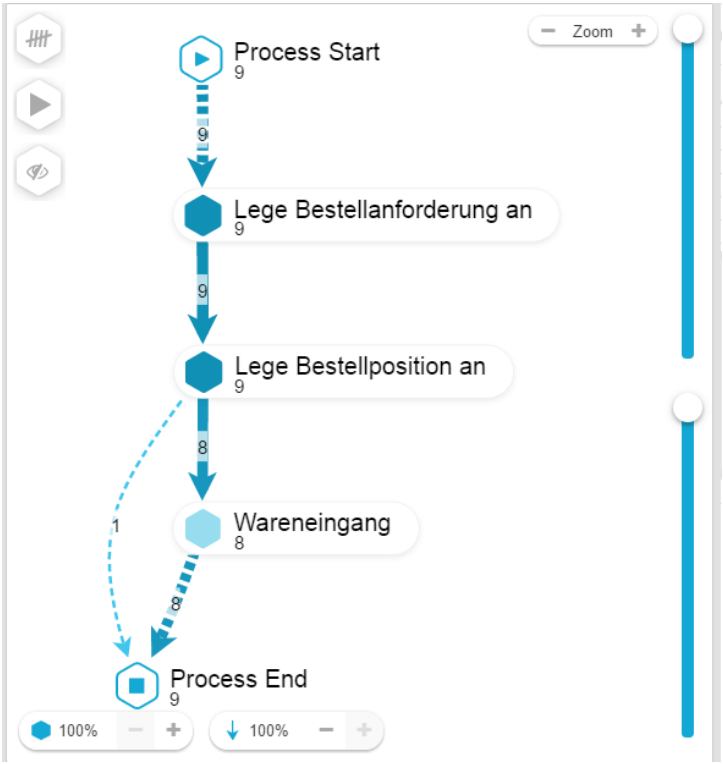


Abbildung 8-27:Prozessdiagramm Mittagessen

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Des Weiteren ist auffällig, dass die Bestellmenge über die Zeit kontinuierlich wächst (vergl. Abbildung 8-28). Es ist zu prüfen, ob die steigende Anzahl der Mittagessen mit einem Anstieg der Mitarbeiteranzahl zusammenhängt. Es können auch andere Gründe, wie spezielle Events, für den starken Anstieg existieren. Sollte dies nicht der Fall sein, so kann davon ausgegangen werden, dass sich Freunde und Familie der Mitarbeiter am Essen beteiligen oder das Essen anderweitig veräußert wird. Die Transaktionen mit den Mittagessen weisen die meisten Red Flags auf, so dass ein Deal mit dem Lieferanten der Mittagessen vermutet wird. Eine genaue Prüfung ist hier sinnvoll.

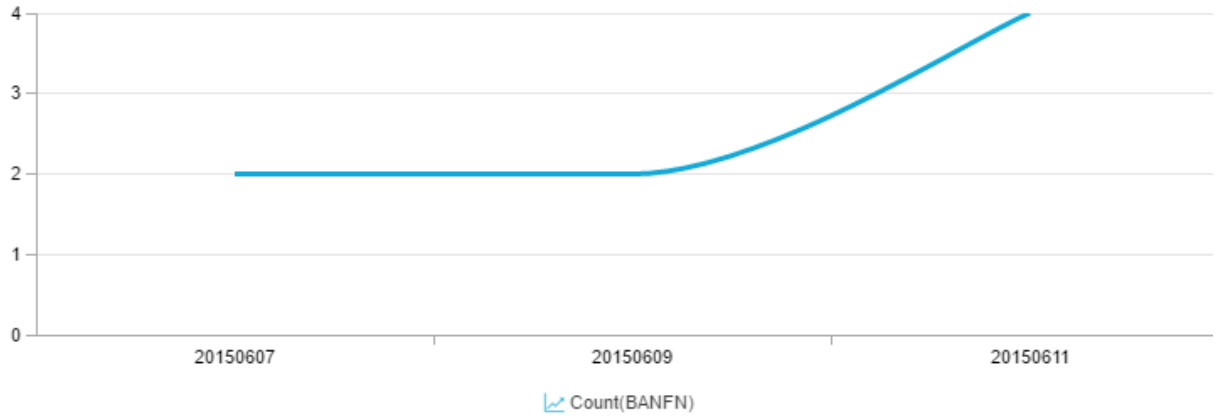


Abbildung 8-28: Steigende Transaktionen bei Mittagessen

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Im Mandanten **715** ist zunächst auffällig, dass das Fraud Pattern *‚unbeteiligter Lieferant‘* anschlägt. Dabei werden von dem User ‚GBI_006‘ Waren angenommen, die anschließend wieder storniert werden. Trotzdem wird die Rechnung für diese Fahrräder bezahlt. Deshalb wird an dieser Stelle Fraud vermutet. Eine weitere Auffälligkeit in diesem Mandanten ist die Existenz von zwei Lieferanten mit demselben Namen, jedoch unterschiedlicher IDs. Dabei handelt es sich um die ‚Firma Boomtown Tire & Wheel‘ mit den IDs 102006 und 102013. Bei beiden Unternehmen werden Materialien eingekauft, wie Abbildung 8-29 zeigt.

EBELN	LIFNR	TXZ01	MENGE	NETPR
4500000003	102013	Lock Washer 5 mm	13.200.000	0.05
4500000004	102006	Lock Washer 5 mm	13.200.000	0.05
4500000003	102013	Pedal Assembly	3.300.000	44.46
4500000004	102006	Pedal Assembly	3.600.000	44.20
4500000003	102013	Touring Frame-Black	3.300.000	200.89
4500000004	102006	Touring Frame-Black	3.600.000	199.89
4500000003	102013	Touring Handle Bar	3.300.000	24.85
4500000004	102006	Touring Handle Bar	3.600.000	24.70
4500000003	102013	Touring Seat Kit	3.300.000	49.80
4500000004	102006	Touring Seat Kit	3.600.000	49.50

Abbildung 8-29: Materialien mit Menge und Preis Abbildung

Quelle: Eigene Darstellung

Da bei beiden Lieferanten exakt dieselbe Ware mit exakt derselben Menge und exakt dem selben Preis bestellt wird, wird an dieser Stelle Fraud vermutet. Es wird angenommen, dass die doppelt erhaltene Ware veräußert wird und der Gewinn einbehalten wird.

Im Mandanten **716** kommt es zu Auffälligkeiten im Prozessablauf. In drei Prozessinstanzen werden Waren (Sattelstützen) gekauft und wieder zurückgesendet. Anschließend wird die Rechnung versendet und die Rechnungssumme angepasst. Da die Rechnungssumme allerdings mit der Bestellsumme übereinstimmt, handelt es sich hierbei nicht um Fraud. In einem Fall wird der Nettopreis nach der Bestellung doppelt geändert. Anschließend wird auch in der Lieferung der Nettopreis verändert. Nach dem Erhalt der Rechnung wird die Ware wieder zurückgesendet und die Rechnung annulliert. Auch hier wird kein Fraud vermutet. In einem weiteren Fall wird zunächst die Ware geliefert und anschließend der Preis für die Ware angepasst. Die Rechnungssumme ist höher als die Bestellsumme und sollte geprüft werden. Eine weitere Auffälligkeit ist eine Lieferung von Sattelstützen in einer größeren Anzahl, als in der Bestellung angegeben. Es kann eine nicht dokumentierte Änderung im Bestellwunsch gegeben haben, es kann ein Fehler aufgetreten sein oder es handelt sich um Fraud. In einem Fall wird eine Rechnung ohne Erhalt der Ware bezahlt, die näher betrachtet werden sollte.

8.3.4.2 Vergleichende Analyse Runde 2

Aus den Präsentationen der eigentlichen Teilnehmer geht hervor, welchen Fraud Fall diese tatsächlich durchgeführt haben. Es wird der Fraud Fall kurz zusammengefasst und anschließend bewertet in wieweit dieser durch den Prototyp identifiziert wird.

Mandant	**Fraud Typ**	**Beschreibung**	**Identifiziert?**
713	Überhöhte Arbeitszeit	Ein neues Lagerhaus soll gebaut werden. Ein Komplize des Fraudsters hat bei den Arbeiten an der Geländeräumung geholfen. Dieser hat jedoch mehr Stunden berechnet, als er tatsächlich benötigt hat.	Tlw.
714	Essensfraud	Durch eine Gesundheitsinitiative der GBI werden Mittagessen für die Mitarbeiter zu einem reduzierten Preis angeboten. Jedoch werden große Mengen der Mittagessen bestellt, so dass einige der Essensrationen anschließend durch die Fraudster veräußert werden.	Ja
715	Kommission Fraud	Für Einsparungen im Produktionsprozess bezahlt die Firma GBI den beteiligten Mitarbeitern Boni. Deshalb manipulieren die Täter die Preise für die Fahrräder leicht, so dass eine höhere Summe in Rechnung gestellt werden kann. Anschließend „verhandeln“ die Täter die Preise neu und erhalten den Bonus für die Einsparung.	Tlw.

716	Verspätete Zahlungen	Der Mitarbeiter verspätet die Zahlung einer Rechnung absichtlich, damit seinem Unternehmen kein Skonto gewährt wird. Da sein Komplize Mitarbeiter des Lieferanten ist, wird das Skonto trotz Verzögerung gewährt. Dieses wird aber direkt auf das Konto des Mitarbeiters überwiesen und zwischen den beiden Tätern geteilt.	Nein

Tabelle 54: Gegenüberstellung tatsächliche Fraudschemata und identifizierte
Quelle: Eigene Darstellung

Im Mandanten 713 wurden mehr Stunden als durchgeführt berechnet. Die Unstimmigkeit in der Stundenanzahl (18 Stunden) wurde nicht erkannt. Jedoch war dieser Lieferant insgesamt sehr auffällig, so dass eine zusätzliche Kontrolle empfohlen wurde. Ein Fraud Pattern zur Erkennung von Abrechnung nicht geleisteter Arbeitsstunden ist nur schwer möglich. Es gibt keine Vergleichswerte für die Dauer einer Dienstleistung. Auch arbeitet jeder Handwerker unterschiedlich schnell, wodurch wieder Unstimmigkeiten entstehen können.

Im Mandanten 714 wird der Fraud identifiziert. Die hohe Anzahl der Mittagessen und vor allem die rasant steigende Anzahl von Käufen haben den Fraud verraten. Dieser Fraud Case scheint aber schwer realisierbar. Der Verkauf von Mittagessen an Dritte ist nicht einfach, da es sich um schnell verderbliche Ware handelt. Es wäre nur möglich das Mittagessen in unmittelbarer Nähe und nur unmittelbar nach dem Erhalt der Ware weiterzuverkaufen. Der Verkaufswert, bzw. die Gewinnspanne pro Mittagessen, ist ebenfalls verhältnismäßig gering. Die Gefahr der Aufdeckung im Vergleich zum Gewinn macht diesen Fraud Case in der Praxis wenig attraktiv.

Im Mandanten 715 wurden die leichten Preisanstiege festgestellt, jedoch kein Fraud dahinter vermutet. Insgesamt wurde der Fraud also nicht identifiziert. Es ist schwierig sinkende Kosten, die manuell erhöht wurden zu erkennen. Erkannt wird allerdings ein zurückgesendetes Kettenschloss, welches trotzdem bezahlt wurde. Die Teilnehmer des Wettbewerbs haben dies als Fehler deklariert.

Im Mandanten 716 wird der entsprechende Fraud Fall nicht identifiziert. Es wirkt eigenartig, dass ein Mitarbeiter des Lieferanten das Skonto nach dem Erhalt der vollständigen und verspäteten Zahlung gesondert auf ein Konto überweisen kann. Dadurch wird der Fraud Fall in der Realität nicht als realistisch angesehen und kann durch die Audit Abteilung des Lieferanten einfach identifiziert werden.

8.3.4.3 Evaluation mit Daten aus WCHC Runde 3

Der Datensatz aus Runde drei enthält 142.584 Prozessinstanzen. Insgesamt werden zwei Fraud Patterns identifiziert – *‚Scheinfirma‘* und *‚unbeteiligter Lieferant‘*. Dabei werden 290 Fraud Patterns und 1295 Red Flags identifiziert. Materialien (36 verschiedene) im Gesamtwert von 17,2 Mrd. € werden bestellt, wobei die größten Ausgaben bei Robotern, Fährrädern und Nickel liegen. Eine verdächtige Prozessinstanz mit 35,2 Millionen € Bestellpreis fällt sofort ins Auge.

Es wird der Mandant 700 und die beiden Buchungskreise US00 und DE00 verwendet. In dieser Runde wird im Gegensatz zu den bisherigen Runden nur in einem SAP Mandanten Fraud begangen. Deshalb wird hier nach Fraud Patterns, Instanzen mit einer hohen Anzahl von Red Flags und Prozessabweichungen gesucht.

Zunächst sollen die beiden Fraud Patterns näher betrachtet werden. Das Fraud Pattern *‚unbeteiligter Lieferant‘* kommt doppelt im Datensatz vor. Bei beiden Instanzen wird die Rechnung doppelt bezahlt und eine Gutschrift erstellt. Eine der beiden Bestellanforderung ist mit 1,4 Mio. USD sehr hoch (Abbildung 8-30).

Mitarbeiter Bestellanforderung

Name	Einkäuferg...	Preis ...	Währung	Menge	Einheit
GBI-065	N00	1.40 Mio.	USD	2.00	EA
GBI-010	N00	2.00 Tsd.	USD	150	ST

Abbildung 8-30: Mitarbeiter Bestellanforderung

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Analysiert man diese Prozessinstanz im Detail, erkennt man, dass die gesamte Prozessinstanz einzig vom Mitarbeiter ‚GBI-065‘ durchgeführt wird. Es werden vom Lieferanten ‚iRobot Deluxe‘ zwei ‚robotics manufacturing e-bikes deluxe‘ geliefert. Scheinbar handelt es sich um Herstellungsroboter. Bei einer solch hohen Summe ist es aber auffällig, dass an der gesamten Prozessinstanz nur ein Mitarbeiter beteiligt ist und keine Ausschreibung durchgeführt wird. Deshalb ist eine Analyse dieses Lieferanten von besonderer Bedeutung.

Das Fraud Pattern *‚Scheinfirma‘* kommt deutlich häufiger im Datensatz vor. Bei Filterung auf das entsprechende Pattern erkennt man im Prozessexplorer, dass in keiner Prozessinstanz Ware bezahlt wird (Abbildung 8-31).

Abbildung 8-31:Scheinfirma Abbildung

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Es wird hier davon ausgegangen, dass die Rechnungen beglichen werden, um dem Verdacht der Scheinfirma weiter nachzugehen. Bei allen 144 Prozessinstanzen werden Offroad Helme, Knieschoner, Rahmen aus Carbon und ein Panasonic Fernseher TX-85XW944 gekauft. Die Käufe von Knieschonern und den Rahmen zeigen eine Reihe von Auffälligkeiten, wie bspw. die Ausführung der gesamten Prozessinstanz durch nur einen Mitarbeiter (GBI-760). Aufgetretene Red Flags sind *‚keine Genehmigung‘*, *‚dringende Aufträge‘*, *‚keine Steuernummer‘*, *‚mehrere Instanzen desselben Lieferanten‘*, *‚fehlende Adressdaten‘* und *‚plötzliche Aktivitäten bei einem schlafenden Lieferanten‘*. Es werden insgesamt 1000 Carbon Rahmen zu je 17 Tsd. € gekauft. Durch die hohen Kosten pro Rahmen und den beschriebenen Auffälligkeiten bei diesem Lieferanten ‚Burgmeister‘, ist eine detaillierte Analyse notwendig.

Als nächste werden Prozessinstanzen mit den meisten identifizierten Red Flags analysiert. Die Transaktion mit der größten Anzahl identifizierter Red Flags ist der Einkauf bei ‚iRobot Deluxe‘. Da dieser Fall bereits bei dem Fraud Schema *‚Unbeteiligter Lieferant‘* analysiert wurde, wird er an dieser Stelle nicht erneut betrachtet.

Weitere auffällige Prozessinstanzen sind bei dem Lieferanten ‚Devinci' aufgetreten. Bei diesem Lieferanten werden 150 Fahrradrahmen für jeweils 2000€ pro Stück eingekauft. Der hohe Preis pro Rahmen lässt sich durch das Material Carbon der Rahmen erklären. Angeschlagene Red Flags sind *‚Lieferantenrechnung höher ist als die Bestellsumme', ‚Steuer auf der Rechnung fehlt', ‚mehrere Rechnungen für dieselbe Ware'* und *‚Unstimmigkeiten bezüglich der Angebotsausschreibung'*, da nur sehr wenige Lieferanten bei der Ausschreibung geboten haben. Aus diesen Gründen sollte der Lieferant ‚Devinci' genau geprüft werden.

Eine weitere Auffälligkeit in diesem Datensatz ist eine Prozessinstanz mit 15 identifizierten Red Flags. Dabei werden Schrauben im Wert von 8,60 € gekauft. Erstaunlich hierbei ist allerdings, dass Transportkosten von ebenfalls 8,60 € hinzukommen. Möglich ist, dass die Lieferkosten bereits im Kaufpreis enthalten sind und nicht extra berechnet werden müssen. Ein Hinweis hierfür ist, dass der Lieferant als ‚unwichtig' im Materialtext gekennzeichnet ist. Auffällig ist auch, dass der gesamte Prozessdurchlauf von nur einem Mitarbeiter ‚GBI-753' durchgeführt wird. Der Gesamtbetrag für Fraud ist sehr gering. Trotzdem wird hier von einem Fraud ausgegangen, bei dem stets kleine Summen abgeschöpft werden, die sich über die Jahre summieren. Wenn man von monatlichen Kosten von 8,60 € für nicht erbrachte Lieferungen ausgeht, summiert sich der Schaden auf 103,20 € pro Jahr.

Eine weitere auffallende Transaktion mit 13 Red Flags ist ein Einkauf von Pedale bei dem Händler ‚MP Peter Mayer'. Hier fällt zunächst auf, dass bei dem Materialtext ‚Laptop17' steht, während es sich um Pedale handelt (vergl. Abbildung 8-32). Auch die Anschrift des Lieferanten ist mehrfach im System vorhanden. Stutzig macht die große Menge von 100.000 Stück zu 17,50€/Stück bei einem bisher unbekannten Lieferanten. Bei so hohen Ausgaben wäre eine Ausschreibung notwendig. Bei dem Lieferanten Namens ‚Peter Mayer' suggeriert es ein eher kleines Unternehmen bei dem eine hohe Anzahl von Waren gekauft wird. Auch ist der Prozessverlauf äußert merkwürdig. So werden 10.000 Pedale (oder Laptops) bestellt, jedoch nur ein Teil hiervon bezahlt. Es wird empfohlen das Unternehmen ‚MP Peter Mayer' genau zu untersuchen.

Material ID	Materialtext	...	Menge	Einheit	Preis	Währung	#Bestell...
PEDALE_STRG	Laptop17"	U...	10000	ST	17.5	USD	1

Abbildung 8-32: Transaktion mit 13 Red Flags

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Eine weitere Auffälligkeit ist, dass fünf Tonnen Kupfer gekauft werden. Dabei werden wieder Piratenkosten einberechnet. Deshalb wird vermutet, dass der Fraud Case aus dem WCHC 2014 wiederholt wird. Als Lieferant gilt hier ‚Metinvest'.

Weiterhin auffällig ist die Bestellung von zwei Schwertransporten für eine Statue für die Firmenzentrale. Eine Fahrradskulptur im Wert von 970.000USD wird gekauft, wobei zwei Schwertransporte für jeweils 30.000 USD beauftragt werden. Zunächst stellt sich die Frage, warum zwei Transporte für eine Skulptur bestellt werden. Interessant ist auch, dass die beiden Transportunternehmen sehr ähnliche Namen haben: ‚TRANSBIG' und ‚TRANSBIG2'. Es wird angenommen, dass der Lieferant entweder doppelt im Stammsatz gepflegt ist, oder aber

einer der beiden Lieferanten eine Scheinfirma ist. Deshalb wird an dieser Stelle der Fraud vermutet.

Auch auffällig sind Lizenzkosten für ein Rahmendesign. Dabei wird pro Rahmen 500 € für das Design bezahlt. Bei insgesamt 10.000 gekauften Rahmen entsteht ein Gesamtbetrag von 5 Mio. € für Design, was an dieser Stelle etwas hoch wirkt. Selbst wenn dies kein Fraud sein sollte, so sind die Ausgaben etwas hoch und es müsste mit dem Lieferanten neu verhandelt werden. Auch ist auffällig, dass die gesamte Transaktion lediglich durch den Mitarbeiter ‚GBI-982' durchgeführt wird.

Im Prozessexplorer fallen 200 Prozessinstanzen auf, bei denen der Wareneingang fehlt (vergl. Abbildung 8-33). Eine detaillierte Untersuchung ist sinnvoll. Zum einen fallen darunter die bereits beschriebenen Transportkosten für die Bestellung von Zinn aus Jeddah. Bei weiteren 184 Prozessinstanzen werden nur Bestellungen, ohne Waren- oder Rechnungseingang angelegt, so dass von unvollständigen Prozessinstanzen ausgegangen wird, die nicht näher betrachtet werden.

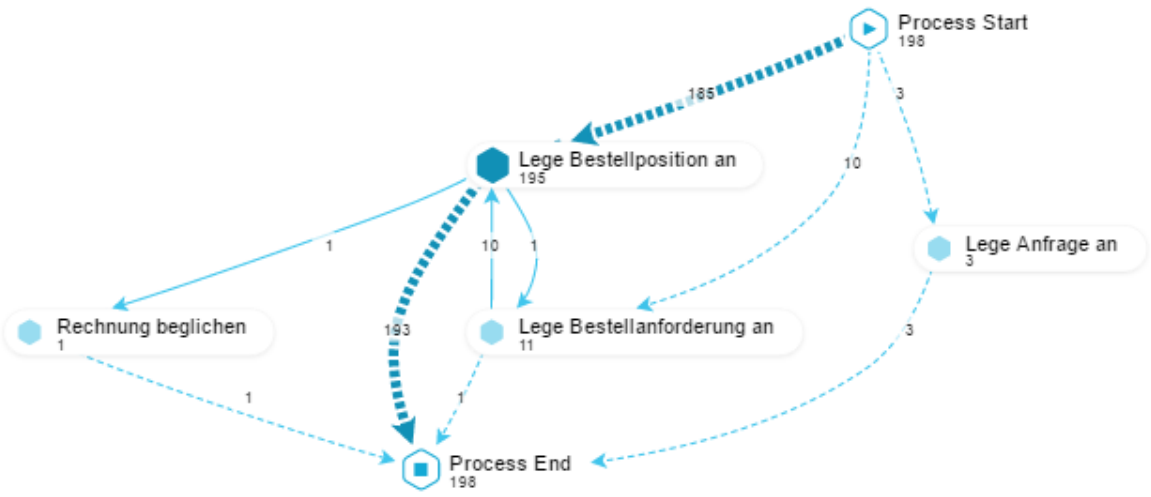


Abbildung 8-33: Prozessdiagramm Transportkosten
Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

8.3.4.4 Vergleichende Analyse Runde 3

Es werden nun die identifizierten Fraud Cases mit den von den Teilnehmern des Wettbewerbs beschriebenen Fraud Cases verglichen. Die Ergebnisse sind in Tabelle 55 zusammengestellt.

#	**Fraud Name**	**Beschreibung**	**Identifiziert?**
1	Angebotsmanipulationsfraud	Es werden nach einem Ausschreibungsprozess Fahrradrahmen gekauft. Die angeblich "qualitativ	Ja

		hochwertigeren" Rahmen des Anbieters ‚Divici' werden trotz des überhöhten Angebots gekauft. Der Täter im GBI Unternehmen stellt sicher, dass das teure Produkt ausgewählt wird. Der Komplize beim Lieferanten Divici erhält für den gut ausgehandelten Deal eine Provision, die er sich mit dem Fraudster im GBI Unternehmen teilt.	
2	Go-green Initiative	GBI Mitarbeiter erhalten für die Reduzierung von CO2 einen Bonus im Rahmen der Go-green Initiative des Unternehmens. Ein manipulierter Truck mit gefälschtem CO2 Ausstoß wird gekauft. Der Mitarbeiter erhält den Bonus und teilte sich diesen mit dem Lieferanten.	Nein
3	Pre-payment Fraud	Pedale für neue Fahrräder werden gekauft und bezahlt. Jedoch muss der Lieferant Peter Mayer Insolvenz anmelden, so dass die bereits bezahlten Pedale nicht geliefert werden.	Ja
4	Schlechte Konditionen	Der beteiligte Lieferant bietet gute Kaufkonditionen bei einer zeitigen Bezahlung der Rechnung. Der Mitarbeiter handelt mit seinem Chef aus (der über die besonderen Kaufkonditionen nicht informiert ist), dass er einen Bonus bei Aushandlung eines niedrigen Preises erhält. Aufgrund des niedrigen Preises erhält der Fraudster seinen Bonus.	Nein
5	Fehlende Laptops	Insgesamt werden 10.000 Laptops bestellt, aber nur 2.000 geliefert. Die Rechnung wird für die gesamte Anzahl an Laptops beglichen.	Ja
6	Schlechte Qualität Fraud	Gelenkschoner werden gekauft, die jedoch eine schlechte Qualität aufweisen. Der Qualitätsmanager des GBI Unternehmens erhält eine einmalige Zahlung, um bei der Qualitätsprüfung keine Mängel "festzustellen".	Nein
7	Kauf eines teuren Roboters	Zwei Produktionsroboter werden gekauft. Zwei Angebote von verschiedenen Lieferanten werden eingeholt, wobei das teurere ausgewählt wird.	Ja
8	Griech. E	Der Buchstabe "E" sieht im griechischen identisch aus, wie das lateinische „E". Im Datensatz sind zwei Datensätze mit Verkaufskonditionen für das Material REIFEN enthalten - mit griechischem E und mit lateinischem E. Beide weisen unterschiedliche Stückkosten auf. Für eine Bestellung wird das teure Produkt REIFEN mit dem griechischen E gewählt.	Nein

9	Überteuerte Produkte	Ein Mitarbeiter des Lieferanten “Burgmeister” verkauft einem Komplizen im GBI Unternehmen Fernseher zu einem überhöhten Preis und beide teilen sich anschließend den Gewinn.	Nein
10	Schlechte Qualität Fraud	Minderwertige Fahrradrahmen werden zum Preis der hochwertigen Fahrradrahmen eingekauft.	Nein
11	Doppelte Berechnung der Transportkosten	Eine neue Statue für das Hauptquartier wird gekauft, wobei die Transportkosten im Preis inkludiert sind. Trotzdem werden die Transportkosten separat berechnet.	Ja
12	Manipulierte Wechselkursraten	Durch den Krieg in der Ukraine und dem Ölproblem sind die Wechselkurse für UAH und RUB deutlich gefallen und anschließend wieder gestiegen. Der Fraudster nutzt die Situation aus und ändert die Rate beim Fall manuell. Der Anstieg wird nicht im System erfasst.	Nein
13	Nicht erhaltener Discount	Ein Discount von 10% wird mit dem Unternehmen BIKEMASTER vereinbart. Ein Mitarbeiter der GBI veranlasst die Zahlung des Gesamtbetrags ohne den Discount. Die Differenz wird zwischen dem Fraudster und dem Komplizen aufgeteilt.	Nein
14	Transportkosten	Schrauben werden von Atlanta nach Hamburg geliefert. Allerdings werden für eine 8000 km lange Strecke 9000 km abgerechnet.	Ja
15	Piraten Fraud Revival	Kupfer wird aus Jeddah bestellt. Es werden Extrakosten für Piraten berechnet, obwohl es in dieser Gegend keine Piraten gibt.	Ja

Tabelle 55: Gegenüberstellung tatsächliche Fraudschemata und identifizierte
Quelle: Eigene Darstellung

In der dritten Runde des WCHC werden bereits Fraud Cases mit Transportkosten identifiziert. Ein großes Problem bei der Fraud Detektion stellt aber weiterhin die schlechte Qualität von Waren und Dienstleistungen dar. Minderwertige oder gefälschte Ware, die zu marktdurchschnittlichen Preisen verkauft wird, wird nicht erkannt. Ein möglicher Hinweis auf diese Art von Fraud wären überdurchschnittlich schnelle Abschreibungen oder Beschwerden der Mitarbeiter. Als Anhaltspunkt im SAP System können Lagerzahlen verglichen werden. Dennoch kann ein solcher Fraud nicht effizient erkannt werden.

Bei der Angebotsmanipulation (vergl. Nummer 1 in Tabelle 55) scheint zunächst eigenartig, dass das entsprechende Fraud Pattern nicht anschlägt. Ein detaillierter Blick in die Daten zeigt aber den Grund hierfür auf. Die Teilnehmer des White Collar Hacking Contests haben gar keine Ausschreibung im eigentlichen Sinn erstellt, sondern lediglich mehrere Preisanfragen zu

Unternehmen gesendet. Streng genommen gab es keine Ausschreibung, so dass das Pattern diese auch nicht identifizieren konnte.

Auch eine Analyse der Stammdaten wird nicht durchgeführt. Der griechische E Fall kann nur durch einen Abgleich auf Ähnlichkeiten der Stammdaten identifiziert werden. Hierzu gibt es im SAP ERP System einen Report, der dies durchführt. Sowohl im IDES, wie auch im GBI System ist dieser standardmäßig ausgeschaltet.

Fraud Fälle mit gefälschten Wechselkursen manuell sind schwierig zu identifizieren. So müsste jede Änderung des Wechselkurses manuell auf die Richtigkeit überprüft werden.

8.3.5 Zusammenfassung und Interpretation der Ergebnisse

Der Prototyp wird im zweiten Zyklus von Design Science im Rahmen des White Collar Hacking Contests auf unterschiedlichen SAP ERP Systemen (IDES und GBI) mit unterschiedlichen Customizing Einstellungen angewendet. Dabei haben die Teilnehmer des Wettbewerbs Fraud Cases im SAP ERP System implementiert. Die dabei entstandenen Datensätze werden mit Hilfe des Prototyps analysiert.

Im IDES Datensatz werden von den versteckten Fraud Cases 8 Identifiziert, 9 nicht identifiziert und 3 teilweise identifiziert.

IDES Datensatz (Runde 2 und 3 WCHC)	3.215 Prozessinstanzen Runde 2 212.816 Prozessinstanzen Runde 3	
Identifiziert	Nicht Identifiziert	Tlw. Identifiziert
8	9	3

Tabelle 56: Ergebnisse Fraud Analyse IDES Datensatz
Quelle: Eigene Darstellung

Im GBI Datensatz wurden 13 identifiziert, 9 nicht identifiziert und 2 teilweise identifiziert.

GBI Datensatz (Runde 2 und 3 WCHC)	18.517 Prozessinstanzen Runde 2 142.584 Prozessinstanzen Runde 3	
Identifiziert	Nicht Identifiziert	Tlw. Identifiziert
13	9	2

Tabelle 57: Ergebnisse Fraud Analyse GBI Datensatz
Quelle: Eigene Darstellung

Insgesamt werden also im Wettbewerbsdatensatz 21 von 44 Fraud Cases identifiziert. Der Datensatz beinhaltet eine Fraud Rate von 0,02%. An dieser Stelle wird wieder eine Wahrheitsmatrix erstellt:

	Fraud im Datensatz vorhanden	**Fraud nicht im Datensatz vorhanden**
Fraud vom Prototypen identifiziert	Richtig-positiv: (rp/(rp+fn))= 53,84%	Falsch-positiv: (fp/(rn+fp))= 0,003%
Fraud nicht vom Prototypen identifiziert	Falsch-negative (fn/(rp+fn))= 46,15%	Richtig-negativ: (rn/(rn+fp)) = 99,99%

Tabelle 58: Wahrheitsmatrix WCHC
Quelle: Eigene Darstellung

Dabei werden als Berechnungsgrundlage folgende Werte angenommen:

- Richtig Positiv (rp): 21 (Summe aus den korrekt identifizierten Werten im IDES und GBI Datensatz)
- Falsch Negativ (fn): 18 (Nicht identifizierter Fraud im IDES und GBI Datensatz)
- Falsch Positiv (fp): 12 (Identifizierter Fraud, den es aber nicht gab)
- Richtig Negativ (rn): 377.088 (Alle analysierten Prozessinstanzen, bei denen kein Fraud vorkommt)

Eine solche Wahrheitsmatrix lässt sich mit echten Daten schwer nachbilden, da in einem Unternehmen die gesamte Anzahl an Fraud unbekannt ist. Es gibt allerdings einige Studien, die ebenfalls Wahrheitsmatrizen angeben. So hat im Bereich von Abrechnungsfraud Barse et al. (2003) Neuronale Netzwerke verwendet, um Fraud zu identifizieren. In ihrem synthetisch erzeugten Datensatz haben sie eine richtig-positiv Rate von 26,6% erreicht und eine falsch-positiv Rate von 0,8%. Anschließend haben sie ihren Algorithmus auf einen echten Datensatz angewendet, bei dem sie eine richtig-positive Rate von 4,9% und eine falsch-positiv Rate von 6,5% erreichen. Verglichen mit diesen Ergebnissen schlägt sich der Prototyp in beiden Bereichen besser. Allerdings sind diese Raten auch sehr stark vom vorhandenen Fraud abhängig.

Bezerra & Wainer (2008a) analysieren Prozesskennende Informationssysteme nach Fraud mit einem Anomaliendetektionsalgorithmus. Ihre richtig-positiv Rate liegt bei 99,9% mit einer falsch-positiv Rate von 57,4%. Verglichen mit ihren Ergebnissen zeigt der Prototyp deutlich schlechtere Erkennungsraten. Die falsch-positiv Rate des Prototyps ist in beiden Evaluationen deutlich geringer. Die richtig-positiv Rate kann durch weitere Fraud Patterns und Red Flags verbessert werden. Eine so hohe falsch-positiv Rate mit über 50% bei Bezerra & Wainer (2008a) führt dazu, dass die Analysten durch die hohe Anzahl (Flut) an Falschinformationen überfordert sind (Chandola et al., 2009).

Die hier verwendeten Daten haben einige Limitationen, die so nicht in der realen Welt vorkommen. So kommt es bei beiden Datensätzen zu sehr kurzen Zeitspannen, in denen das System verwendet wird. Dies führt zwangsläufig zu einigen Red Flags, wie plötzlicher Anstieg von Bestellungen bei schlafenden oder neuen Lieferanten, ungewöhnliche Transaktionen oder schnell aktiv werdende neue Lieferanten. Es wäre möglich den Prototypen sehr feingranular einzustellen, was aber für reale Unternehmen unrealistisch ist. Auch lassen sich einige Phänomene nur anhand der Daten des Wettbewerbs erklären. Beispielsweise werden oft nicht

verpflichtende Felder, wie Telefonnummer des Lieferanten, aus Zeitgründen bei Erstellung eines neuen Lieferanten leer gelassen. Auch fehlen oft Mehrwertsteuersätze bei den Transaktionen, die im echten Unternehmen ausgewiesen werden müssen. Die so entstandenen Red Flags werden hier ignoriert.

Trotzdem müssen auch in der zweiten Runde Verbesserungen am Prototypen durchgeführt werden. Red Flags zur Identifikation von Transportfraud sollen hinzugefügt werden. So werden zum einen Transporte in der Prozessgraphik dargestellt, sowie das Red Flag *‚Transportkosten über dem Durchschnitt‘* hinzugefügt. Die Aufnahme des Transports in der Prozessgrafik ermöglicht die einfache Analyse von doppelter Ausführung eines Transports. Auch sollen Änderungen von Wechselkursen als Prozessschritt aufgenommen werden, um zukünftig Wechselkursfrauds zu erkennen.

8.4 Evaluation mit echten Datensätze zweier Unternehmen

Nachdem der implementierte Prototyp mit synthetischen und semi-synthetischen Datensätzen evaluiert wurde, soll als nächstes die Evaluation mit realen Datensätzen zweier Unternehmen durchgeführt werden. Dabei wird ein Datensatz von einem Wirtschaftsprüfungsunternehmen und von einer Audit Abteilung eines großen Konzerns zur Verfügung gestellt. Beide Datensätze wurden zuvor von professionellen Auditoren analysiert. Die Ergebnisse des Prototyps werden nach der Auswertung mit den Ergebnissen der Auditoren verglichen und beschrieben.

8.4.1 Fallstudie Unternehmen Alpha

Der Prototyp wird anhand von Daten eines großen Unternehmens (hier genannt Alpha) aus dem Bereich Verkehrs- und Fahrzeugtechnik validiert, welche von einem Wirtschaftsprüfungsunternehmen zur Verfügung gestellt werden. Diese stammen aus dem Financial Accounting (FI) und Material Management (MM) des SAP ERP Systems. Insgesamt wird eine Datenmenge in der Größe von ca. 127 GB bereitgestellt. Genauere Informationen über das zu analysierende Unternehmen werden aus Gründen der Geheimhaltung nicht bekannt gegeben. Zusätzlich haben die Daten das Wirtschaftsprüfungsunternehmen nicht verlassen. Es wurde nur ein lokaler Zugang zu einer MS SQL Datenbank mit den darin enthaltenen Daten gewährleistet wird. Um den Prototypen mit Hilfe des Datensatzes validieren zu können, kommt die Werkstudentin Kerstin Gottelt[38] des Wirtschaftsprüfungsunternehmens zum Einsatz. Diese hat im Rahmen eines interdisziplinären Projektes (IDP) bei der Autorin dieser Dissertation die Aufgabe der Evaluation des Prototyps mit Hilfe der Daten des Wirtschaftsprüfungsunternehmens erhalten. Grund hierfür ist ihr Zugang zu den Daten des Wirtschaftsprüfungsunternehmens vor Ort. Zunächst muss sichergestellt werden, dass die Studentin den Prototypen versteht und den Umgang damit sicher beherrscht. Dazu erhält sie ein Training und steht im permanenten Austausch und unter Anleitung der Autorin. Die Ergebnisse der Auswertung werden im zweiten Schritt mit dem Audit Bericht des Unternehmens verglichen. Der Betreuer auf Seiten des Wirtschaftsprüfungsunternehmens hat den Datensatz im Rahmen seiner Tätigkeit zuvor geprüft, sowie bei der Initiierung des Prototyps und bei dem

[38] Vergleich Gottelt (2016)

Vergleich mit dem Audit Bericht unterstützt. Zunächst beschreibt dieser sein eigenes Vorgehen zur Analyse des Datensatzes. Das Wirtschaftsprüfungsunternehmen verwendet für die Datenanalyse Red Flags und Celonis Process Mining. Die Red Flags sind eine Eigenimplementation, während Celonis PM zur Darstellung des Prozesses eingesetzt wird. Daten erhält das Wirtschaftsprüfungsunternehmen von ihren Mandanten. Die Identifikation von Fraud ist eine untergeordnete Aufgabe des Wirtschaftsprüfungsunternehmens. Primär werden Compliance Richtlinien mit oben genannten Maßnahmen überprüft, im Audit Bericht festgehalten und dann mit dem Kunden besprochen.

8.4.1.1 Parametrisierung des Prototyps

Um den Prototypen zu initialisieren, werden zunächst Interviews mit verantwortlichen Auditoren des Wirtschaftsprüfungsunternehmens geführt. Dabei werden die Threshold Values und die wichtigsten Red Flags pro Fraud Patterns identifiziert. Die Ergebnisse sind in Tabelle 59 und Tabelle 60 zusammengefasst.

Variablenname	**Beschreibung**	**Verwendet**
ABSTAND_RECHNUNG	Grenze innerhalb wann zwei Rechnungen für ein Produkt erstellt werden signifikant sind.	2 Tage
BIDDING_DURATION_THRESHOLD	Wie lange sollte eine Angebotsphase mindestens dauern	5 Tage
BIDDING_PAPRTICIPANTS_THRESHOLD	Wie viele Teilnehmer muss eine Anfrage mindestens haben	3 Teilnemer
BIDDING_THRESHOLD	Ab welcher Summe muss eine Anfrage ausgelöst werden	25 000 €
BIG_ORDER_THRESHOLD	Grenze ab wann eine Erhöhung der Rechnungssumme im Vergleich zum Vormonat signifikant ist	2 (doppelt)
FAST_ORDER_THRESHOLD	Ab wann gilt die Bestellung als "eilig"	1 Tag
FAVOURITE_VENDOR_THRESHOLD	Welchen Anteil muss der Mitarbeiter bei einem Lieferanten haben, damit dieser sein Favorit ist	0,75 (75%)
MIN_ORDER_COUNT	Wie viele Bestellungen müssen bereits bei einem Lieferanten durchgeführt worden sein, um für einen übermäßigen Bezug von Waren bei einem Lieferanten relevant zu sein	10 Bestellungen
NO_KNOWN_VENDOR	Wie hoch darf die Bestellsumme maximal sein, damit ein Lieferant keinen Stammsatz benötigt	5000 €
ORDER_THRESHOLD	Grenze ab wann eine Erhöhung signifikant ist	2 (doppelt)
ORDER_THRESHOLD_STAGE1	Grenze für erste Genehmigungsstufe	500 €
ORDER_THRESHOLD_STAGE2	Grenze für zweite Genehmigungsstufe	5000 €
SERVICE_THRESHOLD_DOWN	Kleine Dienstleistungsaufträge die normalerweise ohne zusätzliche Genehmigung durchgeführt werden können	500 €
SERVICE_THRESHOLD_UPPER	Sehr große Dienstleistungsaufträge	5000 €
SPENDING_THRESHOLD	Vergleich der Ausgaben von Vormonat. Grenze ab wann eine Erhöhung signifikant ist	2 (doppelt)

STANDARDABWEICHUNG	Standardabweichung für stets gleiche Beträge	10
THRESHOLD_MATTXT	Ab wann ist der Materialtext zu kurz	6 Zeichen
TIME_THRESHOLD	Ab wie vielen Jahren ohne Geschäftsaktivität mit Lieferant ist eine erneute Aktivität suspekt.	1 Jahr
UNCOMMON_TIME	Zeit, in der eine Geschäftsaktivität eher ungewöhnlich ist (bspw. Nachts)	21:00-05:00 Uhr
UPPER_LENGTH_THRESHOLD	Mindestanzahl an Buchstaben für einen Lieferant	3 Zeichen
VENDOR_COUNT_THRESHOLD	Wie viele Lieferanten sollten für ein Produkt vorhanden sein	3 Lieferanten
Z_THRESHOLD	Signifikanz für Z-Wert	3

Tabelle 59: Threshold Values Unternehmen Alpha

Quelle: Eigene Darstellung

Fraud Schema	Signifikante Red Flags
Kickback	Flag_D01, Flag_D02, Flag_D12
Bid Rigging	Flag_D02, Flag_E11
Scheinfirma	Flag_B01, Flag_B10, Flag_B14
Doppelte Bezahlung	Flag_C05, Flag_C06
Pass Through	Flag_F02
Unbeteiligter Lieferant	Flag_G06, Glag_G07
Rechnungsmanipulation	Flag_A04, Flag_A05, Flag_A06
Private Einkäufe	Flag_H01, Flag_H06

Tabelle 60: Auswahl der Red Flags pro Fraud Pattern (Unternehmen Alpha)

Quelle: Eigene Darstellung

Bei der Initialisierung des Prototyps sind einige Besonderheiten im Datensatz aufgetreten, so dass dieser teilweise angepasst werden muss. Zunächst muss die SQL Implementierung leicht verändert werden, da sich die Befehle zwischen MS SQL und SAP HANA SQL unterscheiden. Die Aktivität „Leistungserfassung“ und „Dienstleistung abnehmen“ kann nicht abgebildet werden, da die notwendige Tabelle „ESSR“ (SAP Services) nicht bereitgestellt werden kann. Außerdem fehlen in einigen Tabellen Einträge, die durch „Dummy“-Werte ersetzt werden. Konkret werden folgende Werte ersetzt:

- “00:00:00” als Uhrzeit für die Bestellanforderungen (EBAN_UZEIT)
- “0000-00-00” als Änderungszeit der Positionen (CDPOS_UDATE)

In der Änderungstabelle CDHDR wird der Benutzer als „EventUser” und nicht wie üblich als „USERNAME” gespeichert. Dies muss entsprechend angepasst werden. Die Red Flags zur Angebotsausschreibung E01, E05, E06, E08, E09 und E13 müssen weggelassen werden, da das Feld “EKKO_SUBMI” nicht ausgefüllt ist. In diesem Feld werden die Bieter einer Ausschreibung gespeichert. Da die Bieter aus Anonymisierungsgründen im Datensatz gelöscht werden, können entsprechende Felder nicht betrachtet werden. In den Lieferantenmasterdaten werden keine Telefonnummern gespeichert (Spalte LFA1_TELF1 ist leer), so dass die Red Flags B09 und B21 weggelassen werden müssen. Das Red Flag D12 wird so angepasst, dass

die Adresse nicht weiter über den Abgleich von Postleitzahl (KNA1_PSTLZ) und Straße (KNA1_STRAS) bestimmt wird, da beide Felder aus Datenschutzgründen fehlen. Stattdessen wird nur nach dem Ort (KNA1_ORT) verglichen, wodurch dieses Red Flag vermutlich häufiger vorkommt und dadurch mehrere falsch-positive Werte liefert.

8.4.1.2 Ergebnisse

Insgesamt sind im Datensatz 547.835 Prozessinstanzen vorhanden. Daran sind 546 Mitarbeiter und 2.855 Lieferanten beteiligt. Es werden 57.242 verschiedene Waren und Dienstleistungen im Wert von 147 Mio € bestellt, die sich auf 4.472.225 Rechnungen verteilen. Die Daten liegen in einem Mandanten und zwei Buchungskreisen vor. Der Prototyp hat mit dieser genannten Kombination insgesamt 110 Fraud Patterns identifiziert, die sich auf die Patterns *Überbezahlung* (32) und *Doppelte Bezahlung* (78) verteilen. Insgesamt werden 994.222 Red Flags in diesem Datensatz gefunden. Einige Red Flags treffen sehr häufig zu. Eine Übersicht über die erhaltenen Daten sind in Abbildung 8-34 gezeigt.

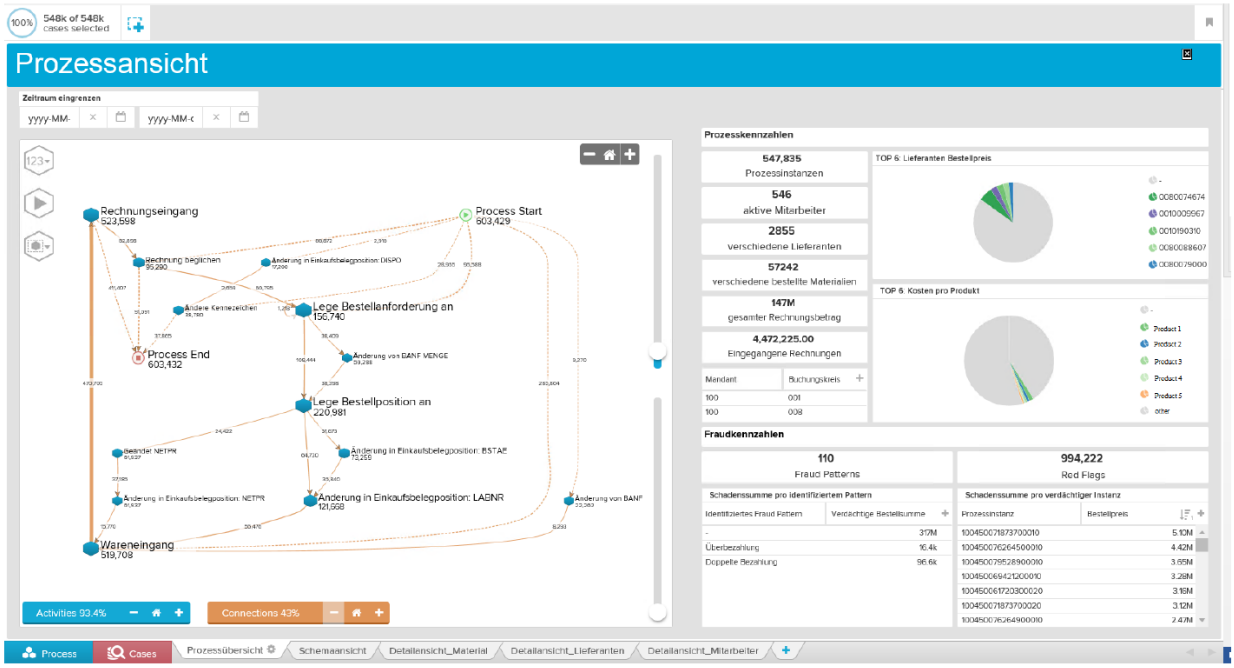


Abbildung 8-34: Prozessübersicht

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Auch hier werden wieder die Top10 Transaktionen mit den meisten identifizierten Red Flags im Detail analysiert, sowie Prozessabweichungen und Fraud Patterns. Insgesamt werden die wichtigsten Beobachtungen dargestellt.

Änderung der Lieferantenstammdaten

Zunächst ist auffällig, dass es eine hohe Anzahl an Änderungen in vielen Lieferantenstammsätzen gibt. Da der Lieferantenstammsatz recht statisch ist, ist diese Änderung zunächst auffällig, allerdings noch kein Fraud. In 31% aller Prozessinstanzen (169.000 von 548.000) kommt es zu den besagten Änderungen. Insgesamt werden die Änderungen von 199 verschiedenen Mitarbeitern durchgeführt. Setzt man dies in Bezug zu den insgesamt 546 beteiligten Mitarbeitern, so erkennt man, dass fast jeder zweite Mitarbeiter mindestens einen Lieferantenstammsatz verändert hat. Es ist sehr stark davon auszugehen, dass das ERP System keine klar definierten Zugangsrechte auf sensible Daten hat. Diese fehlende Trennung der Nutzerrechte ermöglicht das Fraud Schema Rechnungsmanipulation. Dabei ändert ein Mitarbeiter die Kontodaten eines Lieferanten auf seine Daten oder die eines Komplizen. Nach der Überweisung der Rechnung macht dieser die Änderung wieder rückgängig oder löscht den Lieferanten. Allerdings ist dieses Fraud Schema nicht im Datensatz aufgetreten. Trotzdem sollte eine angemessene Funktionstrennung implementiert werden. Dieser Zusammenhang wird in Abbildung 8-35 dargestellt.

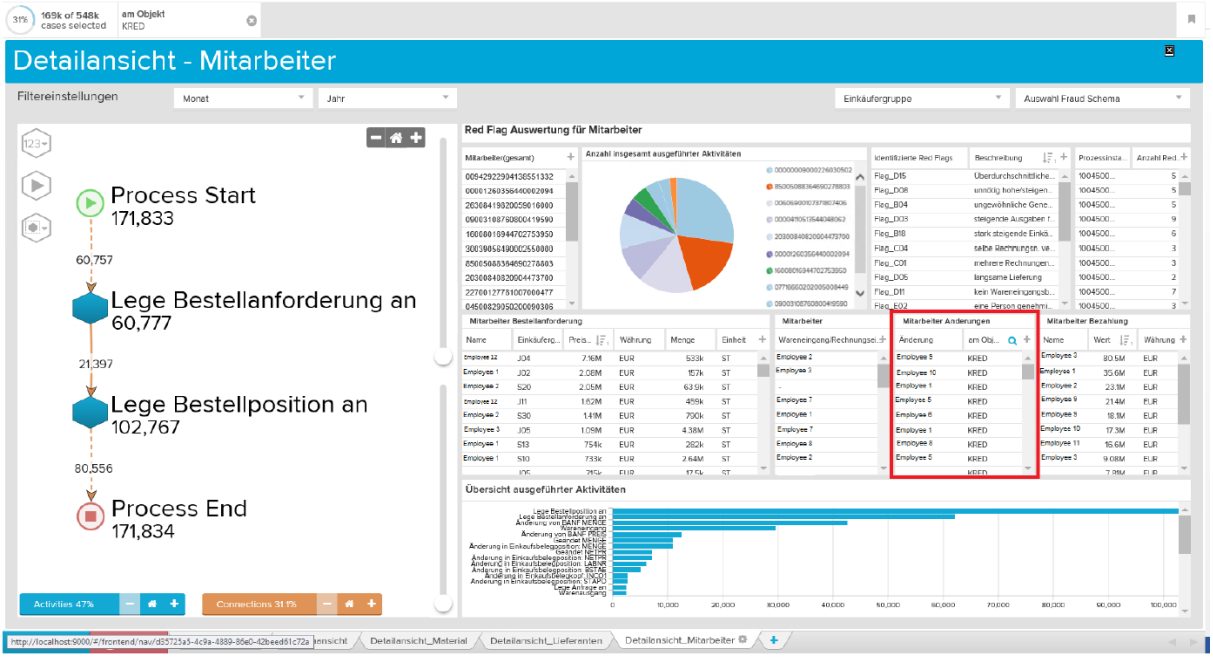


Abbildung 8-35: Detailansicht_Mitarbeiter gefiltert nach Prozessinstanzen, die Änderungen im Lieferantenstammsatz enthalten

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Zahlungen ohne Bestellanforderung und Bestellung

Desweiteren gibt es viele Zahlvorgänge ohne vorherige Bestellanforderung oder Bestellung im System. Insgesamt werden in 298.000 von 548.000 der analysierten Prozessinstanzen keine Bestellanforderung und Bestellung erstellt, wie in Abbildung 8-36 dargestellt ist. Ein Grund hierfür könnten unvollständige Prozessinstanzen sein. So könnten Bestellanforderungen und Bestellungen im Vorjahr durchgeführt worden sein und deshalb in der Stichprobe fehlen. Außerdem können diese außerhalb des ERP Systems angelegt und nicht in das System repliziert

worden sein. Eine Verfolgung dieses Ergebnisses ist an dieser Stelle nicht weiter möglich und wird deshalb nur als Beobachtung festgehalten.

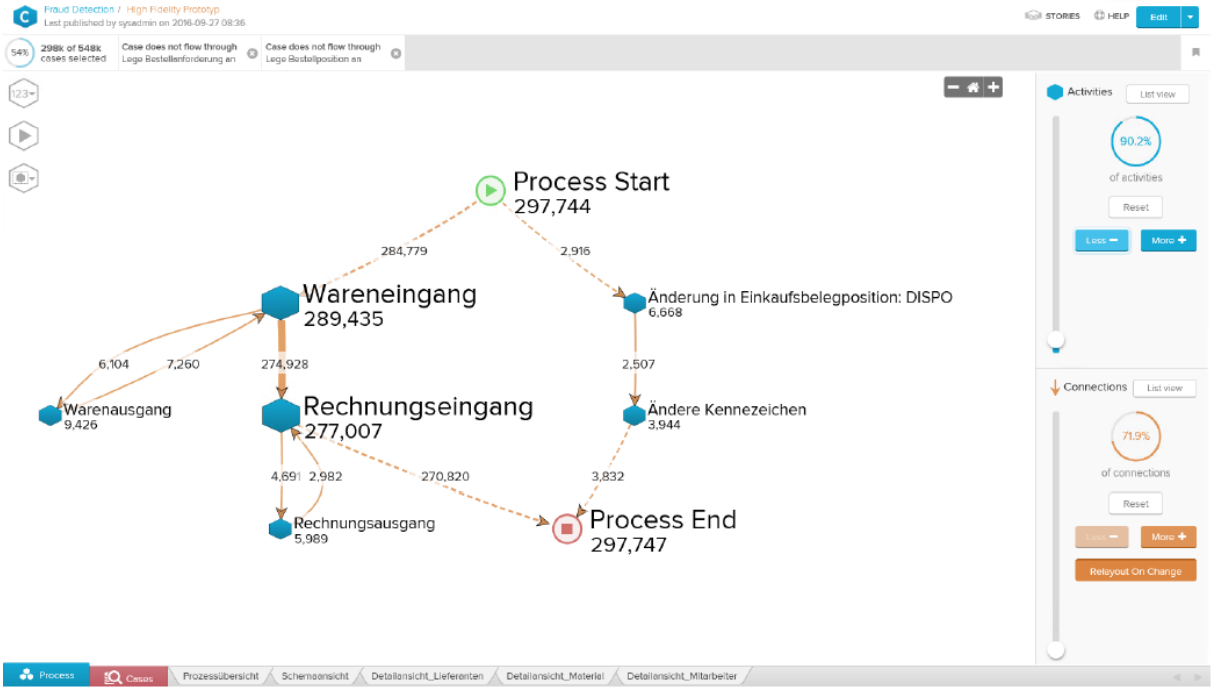


Abbildung 8-36: Prozessinstanzen ohne Bestellanforderung und Bestellung

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Als weiteres Indiz ist aufgefallen, dass oft das Red Flag „Fehlende Autorisierung" angeschlagen ist. Dabei werden keine Autorisierungsschritte im System angezeigt, obwohl die entsprechenden Schwellwerte erreicht werden. Diese fehlenden Autorisierungen sind ein Hinweis auf das fehlende Vier Augen Prinzip.

Bid Rigging (Angebotsmanipulation)

In der weiteren Betrachtung der Daten ist die Kombination folgender Red Flags besonders häufig vorgekommen:

- Flag_E02: dieselbe Person genehmigt den neuen Lieferanten und die Zahlungen an ihn
- Flag_E03: Firmen haben die Möglichkeit ihr Angebot aufzustocken
- Flag_E04: Die Angebotsphase ist sehr kurz

Alle drei Red Flags sind besonders für das Fraud Pattern Bid Rigging relevant, so dass nach diesen drei gefiltert wird. In insgesamt 6.647 Prozessinstanzen kommen (unter anderem) genau diese drei Red Flags vor, wobei 31 aktive Mitarbeiter daran beteiligt sind. Die Rechnungssumme aller dieser Instanzen beläuft sich auf etwa 60,5 Mio €. Außer dieser Kombination ist es sehr auffällig, dass der Lieferant „Vendor GmbH" (Lieferantennamen werden durch das Unternehmen Alpha aus Anonymisierungsgründen geändert) in einem sehr hohen Anteil involviert ist. Dies kann in der Detailansicht der Lieferanten betrachtet werden, wie Abbildung 8-36 zeigt:

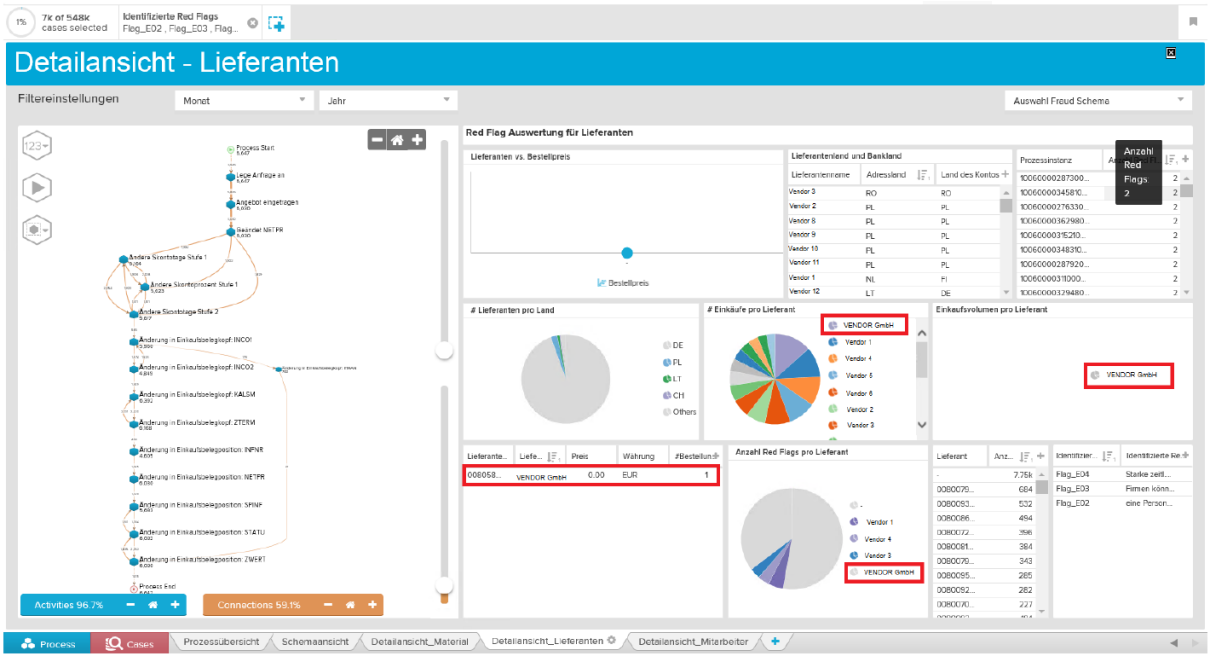


Abbildung 8-37: Detailansicht_Lieferant – gefiltert nach Red Flags E02, E03 und E04

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Um diesen Sachverhalt näher zu analysieren, wird nach dem Lieferant „Vendor GmbH“ gefiltert. Diese Auswahl enthält 144 Prozessinstanzen, wobei sich die Rechnungssumme auf 26.000 € beläuft. Zur weiteren Verfeinerung der Ergebnisse wird ein Filter auf Prozessinstanzen, bei denen die Angebotsfrist nachträglich verändert wird, gesetzt. Dies führt zu 19 Prozessinstanzen. Zusätzlich ergibt die Filterung, dass der Mitarbeiter „Employee 12“ alle genannten Angebotsfristen verändert hat. Diese Kombination ist äußerst merkwürdig und sollte weiter beobachtet werden. Es ist anzunehmen, dass der Lieferant „Vendor GmbH“ sehr stark favorisiert wird und dieser mit „Employee 12“ kooperiert. Ob es hier außerhalb des ERP Systems zu Kickback Zahlungen kommt ist allerdings nicht ersichtlich.

Fraud Pattern „Doppelte Bezahlung“

Der ausgewählte Datensatz enthält 16 Prozessinstanzen, bei denen der Verdacht auf doppelte Bezahlungen vorliegt. Dabei sind 31 Mitarbeiter und acht verschiedene Lieferanten daran beteiligt. Diese Lieferanten haben drei verschiedene Waren im Wert von 278.000 € verteilt auf 275 Rechnungen gekauft (vergl. Abbildung 8-38).

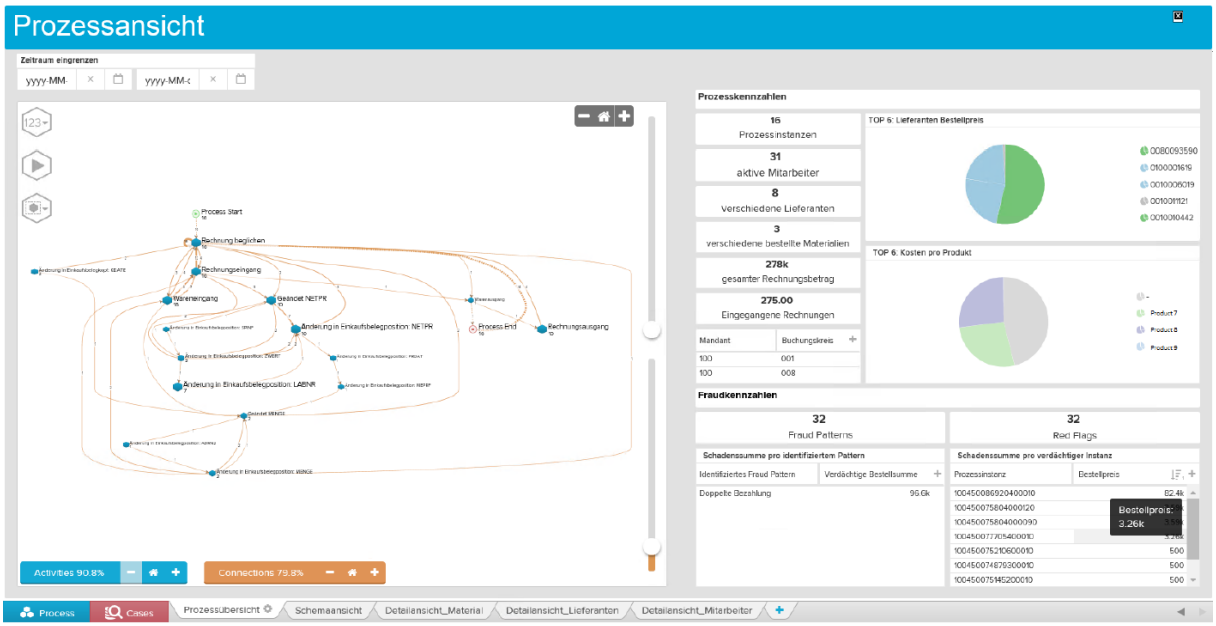


Abbildung 8-38: Prozessübersicht gefiltert nach dem Fraud Pattern Doppelte Bezahlung

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

In insgesamt 16 Prozessinstanzen wird der Prozessschritt „Rechnung beglichen“ mindestens doppelt ausgeführt. In fünf dieser 16 Prozessinstanzen wird das Red Flag ‚*Mehrere Rechnungen für dieselbe Ware*‘, in acht der 16 Prozessinstanzen ‚*Selbe Rechnung, verschiedene Belegnummer*‘ und in allen 16 Prozessinstanzen das Red Flag ‚*Selber Preis an verschiedene Lieferanten gezahlt*‘ gefunden.

In 13 der genannten Prozessinstanzen kann die doppelte Bezahlung nach genauer Betrachtung der Daten erklärt werden. So werden hierbei Teilzahlungen durchgeführt und in einer zweiten Rechnung die Restsumme beglichen. Allerdings sind drei der genannten Prozessinstanzen sehr verdächtig. Die detaillierten Ergebnisse sind in Tabelle 61 dargestellt. Alle diese doppelten Zahlungen haben gemeinsam, dass die selbe Summe für eine Rechnung mit verschiedenen Buchhaltungsbelegnummern beglichen wird. Besonders die doppelte Bezahlung P1 und P2 sind sehr auffällig, da alle vier Zahlungen an einen Lieferanten von demselben Mitarbeiter durchgeführt wurden.

Doppelte Bezahlung	**Buchungsdatum**	**Mitarbeiter**	**Rechnungsnummer**	**Lieferant**	**Summe**	**Buchhaltungsbelegnummer**
P1-1	2007-10-29	Employee 12	R0974521	0080093590	7501,49	0031089998
P1-2	2007-10-31	Employee 12	R0974521	0080093590	7501,49	0031089640
P2-1	2007-10-23	Employee 12	R0975210	0080093590	8585,37	0031089306
P2-2	2007-10-23	Employee 12	R0975210	0080093590	8585,37	0031089639
P3-1	2007-11-08	Employee 13	435442	0100001619	1957,2	0030120154
P3-2	2007-11-08	Employee 13	435442	0100001619	1957,2	0030120156

Tabelle 61: Auffällige doppelte Bezahlungen

Quelle: Eigene Darstellung

Fraud Pattern „Kickback“

Das Fraud Pattern „Kickback“ hat 26 Prozessinstanzen hervorgebracht. Insgesamt werden 78 Red Flags für die ausgewählten Prozesse identifiziert. Die entsprechenden Prozessinstanzen beinhalten 24 aktive Mitarbeiter, vier verschiedene Lieferanten und 12 verschiedene Materialien. Eine Rechnungssumme von 3,5 Mio. € verteilt auf 133 Rechnungen wird identifiziert. Abbildung 8-39 zeigt diesen Sachverhalt.

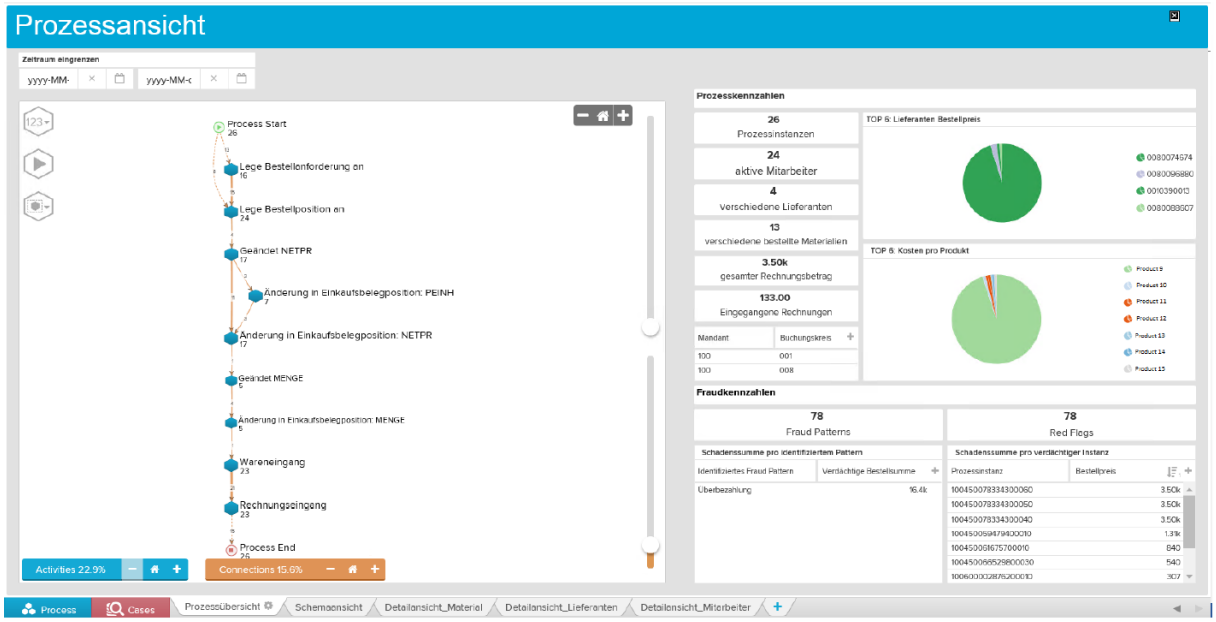


Abbildung 8-39: Prozessansicht gefiltert nach dem Fraud Pattern „Kickback“

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Wenn man allerdings einen detaillierten Blick auf die hier genannten Prozessinstanzen wirft, können diese erklärt werden. Das Red Flag ‚*Kunde ist gleichzeitig Lieferant*‘ kann darauf zurückgeführt werden, dass einige Felder leer sind und damit die leeren Felder „gleich“ sind. Zusätzlich bezieht das Unternehmen Alpha hoch spezialisierte Waren, die bestimmten Qualitätsstandards entsprechen müssen. Aus diesem Grund können nur wenige Lieferanten diese Waren liefern. Das Red Flag *‚Trend zu einem favorisierten Lieferanten‘* kann dadurch erklärt werden. Auch das Red Flag *‚Einkäufe über Marktpreisen‘* kann als unkritisch betrachtet werden, da alle Preise nicht signifikant über den Marktpreisen liegen.

Auffällige Red Flags

Als letzten Schritt sollen auch häufig genannte Red Flags analysiert werden. Besonders häufig kommen in diesem Datensatz folgende Red Flags vor

- Kunde ist gleichzeitig Lieferant
- Nur ein kleiner Kreis an Lieferanten wird gewählt
- Hohe Bestellmengen bei einem Lieferanten
- Einkaufswert signifikant über Marktwert
- Exzessive Rechnungen bei einem Lieferanten

- Große Budgetabweichungen
- Fehlende Genehmigungen

Die meisten der hier genannten Red Flags wurden bereits beschrieben und können mit der starken Spezialisierung von Alpha erklärt werden. An dieser Stelle soll vor allem auf das Red Flag *‚Fehlende Genehmigungen‘* eingegangen werden. Die Filterung nach Prozessinstanzen mit einer Genehmigung zeigt, dass in nur 2.346 von 74.172 Prozessinstanzen diese erteilt wurde, obwohl dies die Firmenrichtlinien erfordern.

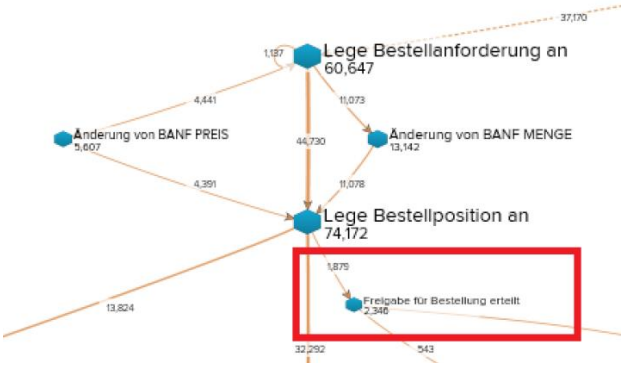


Abbildung 8-40: Prozessinstanzen mit erteilter Freigabe von Bestellungen

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

8.4.1.3 Vergleich der Ergebnisse mit Audit Bericht und Interpretation der Ergebnisse

Die hier beschriebenen Ergebnisse werden an dieser Stelle mit dem internen Audit Bericht verglichen.

Im Audit Bericht ist eine der Hauptkritiken die fehlenden Regularien und Prozessstandards im Einkaufsprozess, wie beispielsweise fehlende Bestellanforderungen. Rechnungen ohne Referenz auf Bestellungen werden bezahlt, können aber ohne diese Referenz nicht verifiziert werden. Auch der Prototyp hat viele Prozessinstanzen identifizieren, bei denen die Bestellung oder Bestellanforderung fehlt.

Ein zweiter von den Auditoren beanstandeter Punktv ist die Änderung von kritischen Daten im SAP ERP System. So werden viele unautorisierte Änderungen von Mitarbeitern des Unternehmens Alpha durchgeführt, wie beispielsweise die Änderung von Bankdaten, Lieferadressen oder das Blockieren von Lieferanten. Auch der Prototyp hat diese Schwachstelle erkannt.

Zusätzlich wird im Bericht der Genehmigungsprozess kritisiert. So besagen die Firmenrichtlinien von Alpha, dass eine Bestellanforderung abhängig von der Bestellsumme genehmigt werden muss. Dabei gibt es verschiedene Transaktionen, bei denen diese Regularien nicht eingehalten wurden. Der Prototyp hat diesen Sachverhalt ebenfalls aufgedeckt.

Auf der anderen Seite werden Unregelmäßigkeiten entdeckt, die nicht im Auditbericht vorkommen. So werden auffällige doppelte Bezahlungen und mögliche

Angebotsmanipulationen identifiziert. Eine Konfrontation mit dem zuständigen Auditor hat ergeben, dass er diese Unregelmäßigkeiten sehr plausibel und interessant findet und eine Neubewertung dieses Sachverhalts in Erwägung zieht.

Zusammenfassend kann festgestellt werden, dass sich die Erkenntnisse aus dem Auditbericht mit denen des Prototyps stark decken. Zusätzlich werden zwei sehr kritische Sachverhalte identifiziert, die nicht im Auditbericht dargestellt werden. So kommt es in mehreren Fällen zur doppelten Bezahlung und zur Angebotsmanipulation, bei der besonders ein Lieferant-Mitarbeiterpaar zu kooperieren scheint. Diese Unregelmäßigkeiten werden nicht im Auditingbericht identifiziert, sollten aber weiter überprüft werden.

Das Red Flag ‚*Kunde ist gleichzeitig Lieferant*' ist 214.222-mal in diesem Datensatz vorgekommen und durch die zugrundeliegenden Daten zu erklären. Da aus Anonymitätsgründen die Postleitzahl und Straße des Lieferanten und Kunden nicht mitgeliefert wird, wird die Gleichheit nur auf Basis des Ortes verglichen. Durch die besondere Datenlage, bedarf es keiner Änderung in der Implementierung des entsprechenden Red Flags. Ein Verbesserungsvorschlag von den zuständigen Auditoren bezüglich des Prototyps ist eine Anpassung der Prozesssicht. Im Prototyp wird für jede Modifikation eines Objektes ein eigener Prozessschritt im Dashboard angezeigt. Dadurch werden sehr viele Prozessschritte visualisiert und die Prozesssicht wirkt überladen. Als Lösung könnte Beispielsweise der Prozessschritt „Änderungen von Objekt" dargestellt werden und in einer separaten Tabelle die konkrete Änderung.

8.4.2 Fallstudie Unternehmen Beta

Bei hier genanntem Beta handelt es sich um einen großen Konzern, welcher sich auf Elektrotechnik und Elektronik spezialisiert hat. Es ist eines der größten Unternehmen in diesem Bereich und in insgesamt 190 Ländern tätig. Der Prototyp wird ebenfalls anhand von realen Daten validiert. Dabei werden insgesamt 3 GB an Daten aus dem Financial Accounting (FI) und Material Management (MM) des SAP Systems bereitgestellt. Kritische Felder, wie Mitarbeiternamen, Adressen und Produktnamen werden gehashet und nicht im Klartext übergeben. Die Daten werden in die SAP HANA Datenbank der TU München geladen. Anschließend wird der Prototyp initialisiert und die Daten ausgewertet.

Das Unternehmen Beta identifiziert Fraud mit Hilfe von Red Flags und hat zusätzlich eine Whistleblowing Hotline implementiert. Bei der Red Flag Lösung handelt es sich um eine Eigenentwicklung mit einer graphischen Weboberfläche. Die Controlling and Finance Audit Abteilung ist für die Identifikation von Fraud zuständig. Darunter geordnet ist die Controlling and Finance Analytics Abteilung. Diese ist für die Datenanalyse der jeweiligen SAP Systeme zuständig und gibt ihre Erkenntnisse in Form eines Audit Berichts an die Fraud Invest Abteilung weiter (auch eine Unterabteilung von Controlling and Finance Audit). Bei dem Bericht liegt das Hauptaugenmerk auf den auffälligen Lieferanten. Die Fraud Invest Abteilung erhält zusätzlich Informationen aus der Whistleblowing Hotline und führt diese mit den Informationen aus dem Audit Bericht zusammen. Anschließend geht diese den Auffälligkeiten in sogenannten on-site Visits vor Ort nach und führt Interviews mit den entsprechenden Lieferanten. Da der

Audit Bericht aus Datenschutzgründen nicht zur Verfügung steht, sollen die zehn verdächtigsten Lieferanten in einem Ergebnisgespräch dargestellt werden. Bei diesem werden die Ergebnisse durch die Analysten des Unternehmens Beta bewertet.

8.4.2.1 Parametrisierung des Prototyps

Um den Prototypen zu initialisieren, werden zunächst die verantwortlichen Auditoren des Unternehmens Beta interviewt. Hierzu werden die Threshold Values aus Erfahrungen der Auditoren entnommen, sowie die wichtigsten Red Flags pro Fraud Case bestimmt. Die Ergebnisse sind in Tabelle 62 und Tabelle 63 dargestellt.

Variablenname	**Beschreibung**	**Verwendet**
ABSTAND_RECHNUNG	Grenze innerhalb wann zwei Rechnungen für ein Produkt erstellt werden als signifikant gilt.	1 Tag
BIDDING_DURATION_THRESHOLD	Wie lange sollte eine Angebotsphase mindestens dauern	5 Tage
BIDDING_PAPRTICIPANTS_THRESHOLD	Wie viele Teilnehmer muss eine Anfrage mindestens haben	3 Teilnehmer
BIDDING_THRESHOLD	Ab welcher Summe muss eine Anfrage ausgelöst werden	10.000 €
BIG_ORDER_THRESHOLD	Grenze ab wann eine Erhöhung der Rechnungssumme im Vergleich zum Vormonat signifikant ist	2.00 (doppelt)
FAST_ORDER_THRESHOLD	Ab wann gilt die Bestellung als "eilig"	1 Tag
FAVOURITE_VENDOR_THRESHOLD	Welchen Anteil muss der Mitarbeiter bei einem Lieferanten haben, damit dieser sein Favorit ist	0.75 (75%)
MIN_ORDER_COUNT	Wie viele Bestellungen müssen bereits bei einem Lieferanten durchgeführt worden sein, um für einen übermäßigen Bezug von Waren bei einem Lieferanten relevant zu sein	5 Bestellungen
NO_KNOWN_VENDOR	Wie hoch darf die Bestellsumme maximal sein, damit ein Lieferant keinen Stammsatz benötigt	5000.00
ORDER_THRESHOLD	Grenze ab wann eine Erhöhung signifikant ist	2 (doppelt)
ORDER_THRESHOLD_STAGE1	Grenze für erste Genehmigungsstufe	5000.00 €
ORDER_THRESHOLD_STAGE2	Grenze für zweite Genehmigungsstufe	50000.00 €
SERVICE_THRESHOLD_DOWN	Kleine Dienstleistungsaufträge die normalerweise ohne zusätzliche Genehmigung durchgeführt werden können	500.00 €
SERVICE_THRESHOLD_UPPER	Sehr große Dienstleistungsaufträge	5000.00€
SPENDING_THRESHOLD	Vergleich der Ausgaben von Vormonat. Grenze ab wann eine Erhöhung signifikant ist	2 (doppelt)
STANDARDABWEICHUNG	Standardabweichung für stets gleiche Beträge	10
THRESHOLD_MATTXT	Ab wann ist der Materialtext zu kurz	8 Zeichen
TIME_THRESHOLD	Ab wie vielen Jahren ohne Geschäftsaktivität mit Lieferant ist eine erneute Aktivität suspekt.	1 Jahr

UNCOMMON_TIME	Zeit, in der eine Geschäftsaktivität eher ungewöhnlich ist (bspw. Nachts)	20:00-06:00 Uhr
UPPER_LENGTH_THRESHOLD	Mindestanzahl an Buchstaben für einen Lieferant	3 Zeichen
VENDOR_COUNT_THRESHOLD	Wie viele Lieferanten sollten für ein Produkt vorhanden sein	3 Lieferanten
Z_THRESHOLD	Signifikanz für Z-Wert	3

Tabelle 62: Threshold Values Unternehmen Beta

Quelle: Eigene Darstellung

Fraud Schema	Signifikante Red Flags
Kickback	Flag_D07, Flag_D09, Flag_D11
Bid Rigging	Flag_E02, Flag_E04
Scheinfirma	Flag_B08, Flag_B10
Doppelte Bezahlung	Flag_C02
Pass Through	Flag_F02
Unbeteiligter Lieferant	Flag_G06, Glag_G07
Rechnungsmanipulation	Flag_A08, Flag_A09
Private Einkäufe	Flag_H01, Flag_H06

Tabelle 63: Auswahl der Red Flags pro Fraud Pattern (Unternehmen Beta)

Quelle: Eigene Darstellung

Durch einige Besonderheiten im Datensatz müssen einige Anpassungen im Prototypen gemacht werden. Die Aktivität „Leistungserfassung“ und „Dienstleistung abnehmen“ kann nicht abgebildet werden, da die notwendige Tabelle „ESSR“ (SAP Services) nicht bereitgestellt wird. Das SAP Systems des Unternehmens steht physisch in einem europäischen Land. Die Daten werden aber in einem asiatischen Land erfasst. Dadurch kommt es bei den Zeitstempeln zu ungewöhnlichen Zeiten. Beim Laden der Daten in die Datenbank muss der Zeit- und Datumsstempel so manipuliert werden, dass die Zeitverschiebung herausgerechnet wird. In der Tabelle EKKO steht der Wert F für Normalbestellungen (anstatt A). Dies wird in der Implementierung des Prototypens angepasst.

8.4.2.2 Ergebnisse

Der Datensatz umfasst insgesamt 1.276.267 Prozessinstanzen. Dabei sind 3.872 aktive Mitarbeiter im Einkaufsprozess beteiligt. Insgesamt werden Waren im Gesamtwert von 12,8 Trillionen Euro bei 1.703 Lieferanten bestellt. Die Daten liegen in einem Mandanten und einem Buchungskreis vor. Der Prototyp hat mit dieser genannten Kombination insgesamt 80 Fraud Patterns identifiziert, die sich auf die Patterns Kickback und Pass Through verteilen. Insgesamt werden 5.741.477 Red Flags in diesem Datensatz gefunden, wobei einige signifikant häufig auftreten. Eine Übersicht über die erhaltenen Daten sind in Abbildung 8-41 dargestellt.

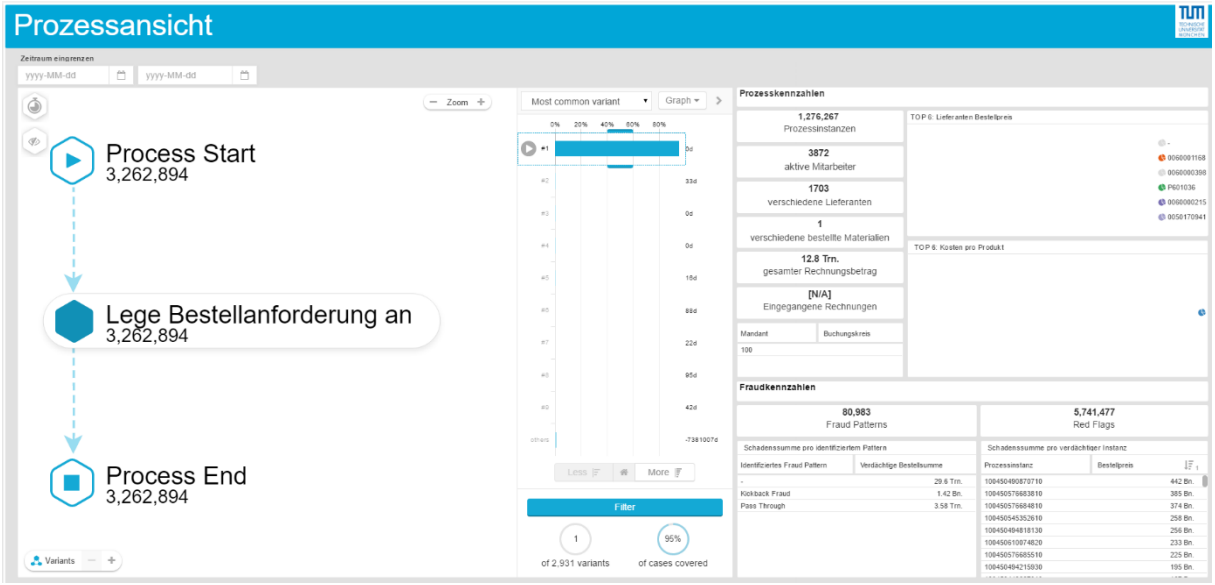


Abbildung 8-41: Übersicht über die Daten des Unternehmens Beta

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Im Unternehmen Beta ist es üblich nach verdächtigen Lieferanten zu suchen. Um also vergleichbare Ergebnisse zu ermöglichen, werden an dieser Stelle auffällige Lieferanten identifiziert.

Auffällige Lieferanten (mit einer hohen Anzahl an Red Flags)

Zunächst wird nach Lieferanten mit einer hohen Anzahl von angeschlagenen Red Flags gesucht. Dabei ist Lieferant **0060000215** sehr auffällig. Bei Filterung nach diesem Lieferanten erkennt man, dass der Prozessverlauf sehr chaotisch ist (Abbildung 8-42). Auch signifikant ist, dass es in acht Fällen zu doppelten Zahlungen kommt. Zusätzlich werden keine Wareneingänge für bestellte Waren verbucht. Von allen bestellten Waren handelt es sich bei einer um eine Dienstleistung. Leider werden die Materialtexte der Waren und Dienstleistungen aus Geheimhaltungsgründen nicht mitgeliefert. Spannend an dieser Stelle wäre, ob die beschriebene Dienstleistung zu den sonst gelieferten Waren passt. Aus den Red Flags geht hervor, dass der Wechselkurs manuell angepasst wird. Desweiteren ist bei diesem Lieferanten der Rechnungsbetrag höher ist der Bestellbetrag, keine Steuer auf der Rechnung ausgewiesen und die Einkäufe liegen über dem Marktpreis. Auch gleicht die Adresse die eines anderen Lieferanten und der Same-Same-Same Test schlägt an. Dabei hat eine Person denselben Betrag doppelt an den Lieferanten überwiesen. Auch die Bestellanforderung und Bestellung liegen zeitlich nah beieinander. Es ist möglich, dass es sich hierbei um eine Scheinfirma handelt, bei der zu überhöhten Preisen eingekauft wird. Teilweise werden Rechnungen ohne Wareneingang bezahlt und doppelte Bezahlungen getätigt. Eine detaillierte Prüfung dieses Lieferanten wird empfohlen.

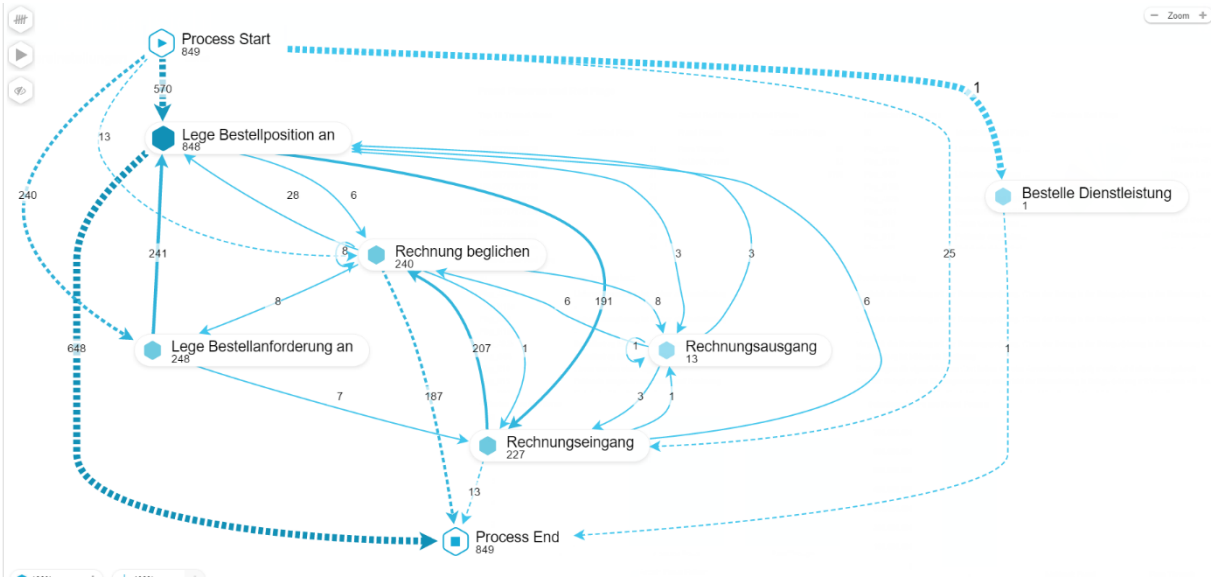


Abbildung 8-42: Prozessexplorer gefiltert auf Lieferant 0060000215

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Auch Lieferant **0060000327** wird als sehr verdächtig eingestuft. Betrachtet man die Red Flags bezüglich dieses Lieferanten, so werden Rechnungen für nicht gelieferte Waren bezahlt. Auch werden in einigen Fällen höhere Rechnungssummen als die Bestellsumme bezahlt. Dies ist sehr verwunderlich, da die meisten Unternehmen in dieser Größenordnung standardmäßig den Three Way Match im SAP System aktiviert haben. Dabei prüft das System automatisch, ob die Bestellsumme und die Bestellmenge mit der gelieferten Bestellmenge und Rechnungssumme übereinstimmt. Sollte dies nicht der Fall sein, so akzeptiert das System die Rechnung nicht.

Dennoch ist an dieser Stelle das Red Flag angeschlagen und es kam zur Zahlung von einer Rechnung, die höher als die Bestellsumme war. Sehr auffällig ist auch, dass es mehrere Instanzen dieses Lieferanten gibt, obwohl standardmäßig jeder Lieferant nur einmalig in den Stammdaten geführt wird. Auch hat der Lieferant keine Telefonnummer in den Stammdaten hinterlegt. Das Red Flag *‚fehlende Genehmigungen‘* ist bei diesem Lieferanten angeschlagen, obwohl die Bestellsumme genehmigungspflichtig gewesen wäre. Ein weiteres angeschlagenes Red Flag ist die steigende Anzahl von Käufen einhergehend mit einer Steigerung der Lagerbestände. Dies ist oft ein Hinweis auf eine Scheinfirma, da offensichtlich die gelieferten Waren nicht direkt benötigt werden, sondern gelagert werden. Betrachtet man das Zahlverhalten, so ergeben sich hier auch einige Unregelmäßigkeiten. So wird regelmäßig ein stets gleicher und runder Betrag gezahlt. Auch sind die Bestellsummen knapp unter dem Grenzwert, so dass Genehmigungsverfahren umgangen werden können. Der Same-Same-Different Test ist positiv, bei welchem zwei Personen dem gleichen Lieferanten am gleichen Tag denselben Betrag zahlen. Eine detaillierte Betrachtung dieses Lieferanten wird empfohlen.

Prozessabweichungen

Als zweiten Schritt werden Prozessabweichungen analysiert und auf dieser Basis auffällige Lieferanten identifiziert.

Zunächst wird nach Prozessinstanzen gefiltert, die nur Dienstleistungen beinhalten. Dabei ist die Prozessabweichung aus Abbildung 8-43 sehr auffällig. So sieht man hier, dass es Änderungen im Wechselkurs gibt, was zunächst ungewöhnlich ist. Außerdem sind Dienstleister oft in geographischer Nähe zum Leistungsnehmer. Die genaue Dienstleistungsbeschreibung müsste also auf Plausibilität untersucht werden.

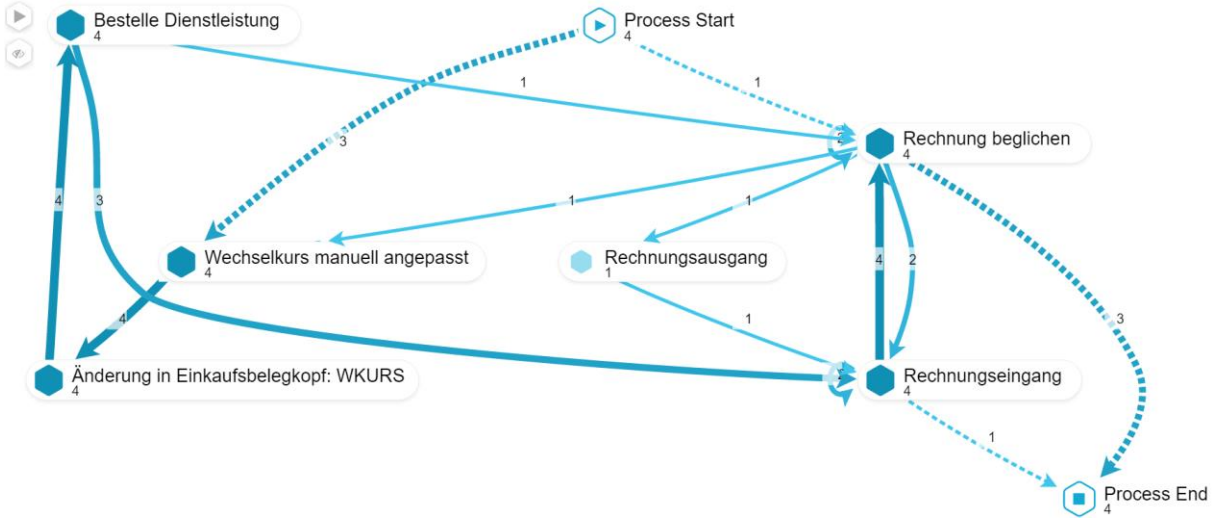


Abbildung 8-43: Auffällige Prozessinstanz Lieferanten 0050144497 und 006004640

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Bei diesem Prozess sind zwei Lieferanten beteiligt (0050144497 und 006004640). Beide Lieferanten sollen nun im Detail geprüft werden.

Bei Lieferant **0050144497** sind mehrere Instanzen desselben Lieferanten in den Stammdaten vorhanden. Möglicherweise handelt es sich um ein nicht korrekt gepflegtes Stammdatenmanagement. Auch kommt es zu Auffälligkeiten bei den Rechnungen. So werden Rechnungen bezahlt, die signifikant höher sind als die letzten Rechnungen. Es werden aber auch Rechnungen ohne Bezug zu einer Dienstleistung oder einem Wareneingang beglichen (Abbildung 8-44), dies teilweise auch doppelt. So hat auch der Same-Same-Different Test angeschlagen. Dabei wird dem Lieferanten am selben Tag von zwei Personen derselbe Betrag überwiesen. Außerdem werden diese Rechnungen sehr schnell beglichen (innerhalb eines Tages), obwohl normalerweise ein Zahlungsziel von mehreren Tagen vereinbart wird. Auch fehlen Genehmigungen, obwohl diese laut Unternehmensrichtlinien erforderlich wären. Insgesamt kam es zu rasant steigenden Einkäufen bei diesem Lieferanten. Es wird also empfohlen diesen Lieferanten aufgrund des auffälligen Zahlverhaltens weiter zu untersuchen.

Abbildung 8-44: Auffällige Prozessinstanz Lieferant 0060004640

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Auch Lieferant **0060004640** zeigt einige Auffälligkeiten. Betrachtet man die Red Flags zu diesem Lieferanten, so werden Waren ohne Genehmigungen bestellt, obwohl diese notwendig wären. Auch kommt es zu rasant steigenden Käufen bei diesem Lieferanten. Der Lieferant war für zwei Jahre inaktiv und wird plötzlich wieder reaktiviert. Dies kann ein Hinweis auf Missbrauch eines alten Lieferanten für fingierte Käufe sein. Dafür spricht auch der fehlende Wareneingang, da dieser meist von dritten Personen durchgeführt wird. Auch die Stammdaten

sind bei diesem Lieferanten nicht vollständig gepflegt. So fehlt beispielsweise die Telefonnummer. Auch hat der Same-Same-Same Test angeschlagen. So wird dem Lieferanten an einem Tag die gleiche Summe doppelt überwiesen. Aus diesen Gründen sollte dieser Lieferant ebenfalls detailliert geprüft werden.

Auffällige Lieferanten nach Fraud Patterns

Als nächstes sollen an dieser Stelle auffällige Lieferanten nach Fraud Patterns betrachtet werden. Nach genauer Betrachtung der Datenlage ist vor allem das Kickback Fraud Pattern von besonderer Bedeutung. Abbildung 8-45 zeigt dabei die auffälligsten Lieferanten bei diesem Fraud Schema. Der kritischste Lieferant ist hierbei 0060000215, der bereits detailliert betrachtet wurde.

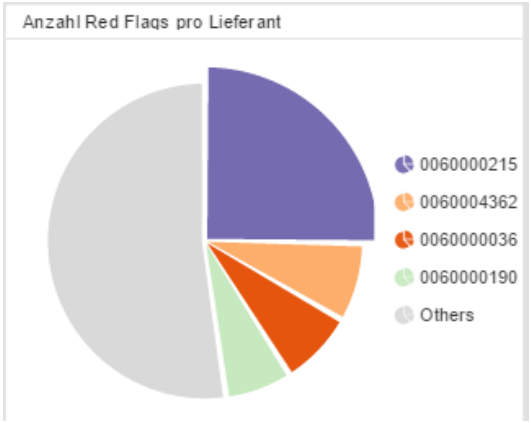


Abbildung 8-45: Auffällige Lieferanten bei Kickback Fraud
Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Lieferant **0060004362** zeigt ebenfalls eine sehr hohe Anzahl von Red Flags. Konkret sind beispielsweise keine Steuern auf seinen Rechnungen ausgewiesen. Auch werden steigende Einkäufe bei diesem Lieferanten getätigt. Denkbar wäre hierbei, dass die möglichen Täter immer mutiger werden und immer höhere Bestellungen tätigen, zumal diese Bestellungen auch mit einem Anstieg in den Lagerbeständen einhergehen. Sehr interessant ist ebenfalls, dass dieser Lieferant die gleiche Adresse wie ein anderer Lieferant hat. Entweder handelt es sich hierbei um kleine Firmen, die ihre Büros im selben Gebäude haben oder aber um eine große Firma, bei der in den Stammdaten mehrere Abteilungen als jeweilige Einzelfirma geführt werden. Letzteres würde für eine unkorrekte Stammdatenführung sprechen. Es sind aber auch Szenarien denkbar, bei denen ein Lieferant kopiert wird und somit ein gefälschter Lieferant angelegt wird. Hierfür spricht auch, dass bei diesem Lieferanten die Telefonnummer nicht gepflegt ist. Insgesamt wird dieser Lieferant sehr favorisiert, da er bei 75% der Einkäufe ausgewählt wird. Auffällig ist aber, dass Rechnungen für nicht gelieferte Waren beglichen, sowie mehrere Rechnungen für dieselbe Ware gestellt werden. Hierbei kann es sich um den Ausgleich von Kickback Zahlungen handeln. Dafür spricht auch, dass das Red Flag „Einkäufe über dem Marktpreis“ angeschlagen hat und es oft zu Rechnungen mit stets gleichen Rechnungsbeträgen kommt. Diese Auffälligkeiten sollten weiter analysiert werden.

Auch Lieferant **0060000036** zeigt viele Besonderheiten auf. Bei diesem Lieferanten werden Einkäufe über dem Marktpreis getätigt. Auch werden mehrere Rechnungen für dieselbe Ware in Rechnung gestellt, was an sich für Teilrechnungen sprechen kann. Auffällig ist aber, dass stets gleiche Beträge an diesen Lieferanten bezahlt werden. Auch werden mehrere kleine Bestellungen desselben Produktes durchgeführt. Hier könnte beispielsweise eine regelmäßige Lieferung von stets gleichen Verbrauchsmaterialien möglich sein, allerdings sind in solchen Fällen die verhandelten Preise selten über dem Marktpreis. Auch ist ungewöhnlich, dass es bei diesem Lieferanten zu steigenden Einkäufe kommt. Auch der Same-Same-Same Test hat angeschlagen. Dabei hat eine Person den Lieferanten am selben Tag doppelt bezahlt. Auch eine langsame Lieferung bei dringenden Aufträgen ist hier vorgekommen. Betrachtet man die Prozessinstanz aus Abbildung 8-46, so erkennt man, dass der Wareneingang fehlt. Durch die genannten Red Flags ist eine detaillierte Überprüfung des genannten Lieferanten sinnvoll.

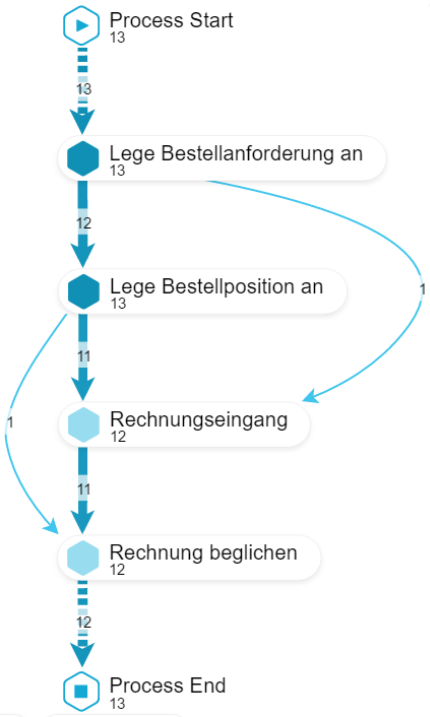


Abbildung 8-46: Auffällige Prozessinstanzen von Lieferant 0060000036

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Auch Lieferant **0060000190** zeigt einige Auffälligkeiten für Kickback Fraud. So hat dieser Lieferant keine Steuern auf Rechnungen ausgewiesen. Auch sind Einkäufe über dem Marktpreis, was ein starkes Kriterium für Kickback Fraud ist. Damit einhergehend kommt es zu steigenden Einkäufen bei diesem Lieferanten, die mit einer Erhöhung des Lagerbestandes verbunden sind. Es liegt die Vermutung nahe, dass nicht benötigte Waren bestellt und ins Lagger gebracht werden. Dafür spricht auch, dass der Einkaufswert den letzten signifikant übersteigt. Auch im Vergleich zum Vormonat gibt die Abteilung doppelt so viel Geld für Bestellungen bei diesem Lieferanten aus. Eine mögliche Erklärung könnte aber auch eine steigende Kooperation mit diesem Lieferanten sein. Verdächtig ist aber die fehlende ausgewiesene Steuer bei legalen Rechnungen. Auch hat dieser Lieferant die gleiche Adresse wie ein anderer Lieferant. Für die bestellte Ware gibt es nur einen sehr kleinen Kreis an

Lieferanten. Entweder handelt es sich um spezialisierte Ware, bei der es nicht viele Lieferanten gibt oder um einen langjährigen Partner. Möglich wäre ebenfalls, dass es sich nicht um eine ausschriebungspflichtige Bestellung handelt und somit nur wenige Lieferanten kontaktiert werden. Bei Betrachtung der Prozessinstanzen dieses Lieferanten in Abbildung 8-47 erkennt man, dass der Wareneingang nie verbucht wird. Deshalb soll dieser Lieferant kritisch im Detail analysiert werden.

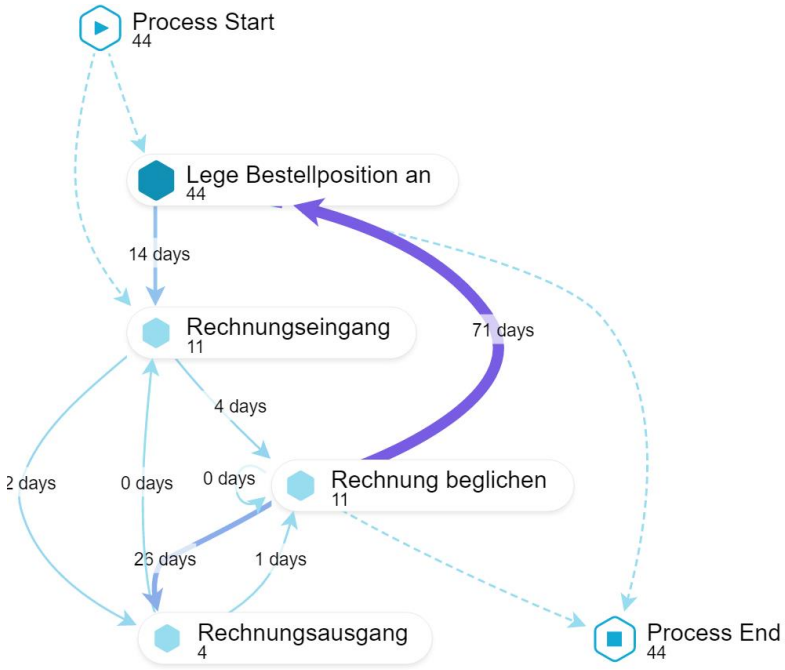


Abbildung 8-47: Auffällige Prozessinstanz Lieferant 0060000190
Quelle: Eigene Darstellung (Screenshot von Celonis Process Mining)

Prozessinstanzen mit hoher Anzahl Red Flags

Als letzter Schritt werden Prozessinstanzen mit den meisten Red Flags betrachtet. So ist der Lieferant mit der Lieferantennummer **0060003948** auffällig. Hierbei kommt es zu exzessiven und steigenden Rechnungen von diesem Lieferanten. Dabei werden aber stets meist runde Beträge überwiesen. Auch die ausgewiesenen Rechnungen sind höher als der Bestellbetrag. Ein Mitarbeiter des Unternehmens Beta bezahlt diesem Lieferanten am selben Tag die gleiche Summe doppelt (Same-Same-Same Test). Bei den Stammdaten dieses Lieferanten fehlt die Telefonnummer.

Auch der Lieferant **0050144214** ist sehr auffällig. Bei Betrachtung der Prozessinstanz in Abbildung 8-48 erkennt man, dass in 13 Fällen Rechnungen ohne Wareneingang beglichen werden. Die Einkäufe liegen meist über dem Marktpreis und die Einkaufswerte übersteigen den letzten signifikant. Beispielsweise könnte es sich um eine Scheinfirma handeln, bei der im Laufe der Zeit die Täter immer mutiger werden. Auch werden Rechnungen für nicht gelieferte Waren beglichen und der Same-Same-Same Test schlägt an. Dabei überweist ein Mitarbeiter der Firma Beta die gleiche Summe am selben Tag doppelt. An den Rechnungen ist auch auffällig, dass diese sequentiell steigend sind. Auch hat der Lieferant die gleiche Adresse wie

ein anderer Lieferant. Insgesamt sprechen diese genannten Red Flags für eine Scheinfirma oder ein Pass Through Fraud Pattern. Eine detaillierte Untersuchung dieses Lieferanten wird deshalb dringend empfohlen.

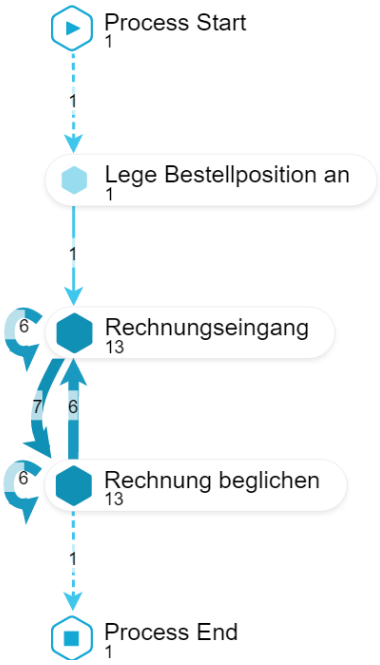


Abbildung 8-48: Auffällige Prozessinstanz für Lieferant 0050144214

Quelle: Eigene Darstellung (Screenshot aus Celonis Process Mining)

Als letzter auffälliger Lieferant soll an dieser Stelle der Lieferant **0050170867** genannt werden. Betrachtet man die Prozessinstanzen dieses Lieferanten (Abbildung 8-49) erkennt man, dass zunächst 12 Rechnungen ohne Wareneingang beglichen werden. Interessant ist hierbei auch, dass die Bestellung erst nach der Zahlung der Rechnung durchgeführt wird (allerdings nur für eine Ware). Bei allen anderen Prozessinstanzen werden nur Rechnungen beglichen ohne Bestellung oder Wareneingang. Betrachtet man die Red Flags zu diesem Lieferanten erkennt man, dass es zu doppelten Zahlungen für eine Ware kommt und mehrere Rechnungen für eine Ware gesendet werden. Auch Rechnungen für nicht gelieferte Waren sind im System vorhanden. Insgesamt erweckt dieser Lieferant den Anschein, dass es sich hierbei um eine Scheinfirma handelt, die lediglich zum Zweck der fälschlichen Abrechnungen gegründet wird. Eine detaillierte Analyse ist hierbei notwendig.

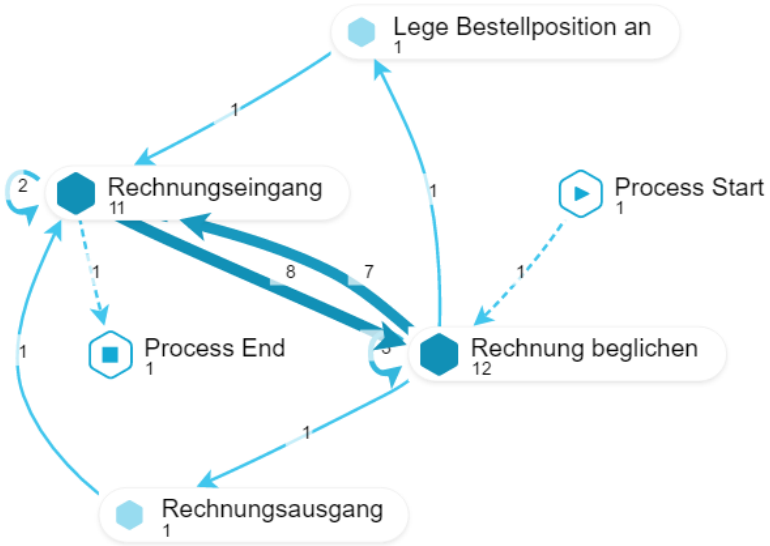


Abbildung 8-49: Auffällige Prozessinstanzen Lieferant 0050170867
Quelle: Eigene Darstellung (Screenshot Celonis Process Mining)

8.4.2.3 Vergleich der Ergebnisse mit Beta und Interpretation

Es werden die zehn auffälligsten Lieferanten identifiziert. Diese werden anschließend bei einer Ergebnispräsentation bei Unternehmen Beta vorgestellt, bei welcher der Partner Data Analytics, Direktor Operational Audit, Partner Internal Audit und zwei Data Analysten anwesend sind. Einer der beiden Data Analysten hat das entsprechende Audit für diesen Datensatz durchgeführt. In der Ergebnispräsentation der Autorin dieser Dissertation wird zunächst der Prototyp vorgestellt und anschließend die oben genannten Ergebnisse. Diese werden abschließend von den beiden Analysten bewertet. Bei dem Vergleich der Ergebnisse wird berichtet, dass alle Lieferanten mit einer führenden ‚6' nach den vorhergehenden ‚0' interne Lieferanten sind. Dabei kommt es zur internen Leistungsverrechnung, die zwischen verschiedenen Ländern des Unternehmens Beta durchgeführt werden. Da interne Leistungsverrechnung nicht Teil des Audits ist, werden diese Ergebnisse nicht im Detail betrachtet. Im Gespräch haben die Auditoren allerdings dargestellt, dass sie viele dieser Leistungsverrechnungen kritisch sehen. Allerdings ignorieren sie diese Erkenntnisse, da streng genommen kein Geld das Gesamtunternehmen verlässt. Leider wurde die Information mit den genannten Lieferanten erst bei der Abschlusspräsentation bekannt gegeben. Insgesamt sind sieben der identifizierten verdächtigen Lieferanten interne Lieferanten, womit sich häufig vorkommende Red Flags erklären lassen. Beispielsweise muss bei interner Leistungsverrechnung keine Umsatzsteuer angegeben werden, interne Lieferanten werden oft bevorzugt und oft sind interne Leistungen über dem üblichen Marktpreis. Es kann also nur noch ein Statement zu den drei verbleibenden externen Lieferanten gegeben werden. Bei Lieferant 0050144214 wird als einziges ein on-site Visit durchgeführt, welches nur bei dens verdächtigsten Lieferanten durchgeführt wird. Der Prototyp hat diesen Lieferanten ebenfalls als sehr verdächtig eingestuft. Die anderen beiden hier genannten Lieferanten haben die Analysten ebenfalls kritisiert.

Insgesamt empfinden die Analysten die Kombination aus Process Mining und Red Flags als sehr interessant. Um die Prozessinstanz zu sehen loggen sich diese aktuell in das SAP ERP System des Unternehmens ein. Die Darstellung im Dashbord empfinden sie als hilfreich und zeitsparend. Auch die Zusammenfassung von Red Flags zu Fraud Patterns sehen diese als hilfreich. Als Verbesserungsvorschläge haben sie genannt, dass der Prototyp spezifische Red Flags je Kulturkreis hervorheben könnte. So haben die Analysten ein gehäuftes Auftreten von Red Flags nach Kulturkreis beobachtet. Dies ist allerdings nicht Bestandteil dieser Dissertation und wird nicht im Prototyp implementiert. Auch wäre eine dynamische Darstellung der Red Flags interessant. So könnte beispielsweise ein Schieberegler eingebaut werden, um den zeitlichen Verlauf der Red Flags darzustellen. Diese Idee ist sehr spannend und mit dem Zeitstempel des Datensatzes darstellbar. Allerdings sind nicht alle Red Flags mit einer Zeitkomponente versehen. So können beispielsweise Red Flags wie ‚Lieferant wird immer von derselben Person erstellt und genehmigt' nur ex-post analysiert werden. Eine Aufteilung in zeitliche und ex-post Red Flags wäre nötig, um diese Funktion einzubauen. Zusätzlich ist ihnen eine Exportfunktion für den Audit Bericht und das Bookmarken von verschiedenen vorgenommenen Filterungen wichtig, um direkt auf das Ergebnis der Filterung klicken zu können (bspw. um das Ergebnis zu besprechen oder nach einer Unterbrechung die Analyse fortzuführen). Diese Funktionen sind durch Celonis implementiert und es bedarf keine Änderung im Prototyp.

Insgesamt kann festgehalten werden, dass der Prototyp bei Unternehmen Beta ebenfalls die kritischen Ergebnisse erkannt hat. Lediglich auffällige interne Leistungsverrechnungen werden erkannt, die allerdings nicht von Unternehmen Beta verfolgt werden.

9 Fazit und Ausblick

Ziel dieser Arbeit ist es den traditionellen Red Flag Ansatz (Hinweise auf wirtschaftskriminelles Verhalten) mit Process Mining zu kombinieren. Dies ermöglicht die Visualisierung des Ist-Prozesses eines Unternehmens mit den dazugehörigen Red Flags. Da eines der Hauptprobleme der Fraud Detektion die Informationsflut und eine hohe Rate von falsch-positiven Werten ist, sollen zusätzlich Red Flags zu Fraud Patterns kombiniert werden. Treten alle genannten Red Flags im Datensatz auf, so schlägt das Fraud Pattern an.

An dieser Stelle sollen zunächst die Ergebnisse der Forschungsfragen zusammengefasst werden. Anschließend soll der theoretische und praktische Beitrag zur Forschung identifiziert und Limitationen und weiterer Forschungsbedarf dargestellt werden.

Forschungsfrage 1: Welche Betrugsmöglichkeiten im Einkaufsprozess bestehen und wie können diese betrügerische Taten mithilfe von Massendatenanalysen identifiziert werden?

Zur Beantwortung der ersten Forschungsfrage werden mehrere Literaturstudien durchgeführt. Zunächst wird auf das Problem einer einheitlichen Definition von Wirtschaftskriminalität und Fraud eingegangen. Mit Hilfe einer Literaturrecherche werden die gängigsten Definitionen und Tatbestände gesammelt. Fraud, der gegen das Unternehmen gerichtet ist (auch Occupational Fraud genannt), kann dabei in die drei großen Kategorien Korruption, Vermögensschädigung und Berichtsmanipulation fallen. Die Möglichkeiten, innerhalb dieser Kategorien Fraud zu begehen, sind vielfältig. Für diese Arbeit sind jedoch nur Frauds von Interesse, die mit dem Einkaufsprozess in Verbindung stehen. Deshalb werden die gängigsten Fraud Delikte auf Basis der ACFE Klassifizierung für den Einkaufsprozess identifiziert. Zu diesen Delikten werden auf Basis der Literaturstudie Red Flags zugeordnet, womit folgende Fraud Patterns identifiziert werden: Interessenkonflikt, Kickback, Angebotsmanipulation, Scheinfirma, doppelte Bezahlung, Pass Through, Unbeteiligter Lieferant, Rechnungsmanipulation und private Einkäufe. Eine Liste mit den entsprechenden Red Flags pro Fraud Pattern ist in Tabelle 51 dargestellt. Aufgrund der Zielstellung diese Indikatoren innerhalb eines SAP-Systems zu finden, fallen einige dieser Flags wegen fehlender Erkennbarkeit aus der Betrachtung heraus. So kann beispielsweise ein veränderter Lebensstil nicht im SAP ERP System gemessen werden. Die identifizierten Red Flags pro Fraud Pattern werden anschließend durch Experteninterviews validiert.

Anschließend werden typische Fraud Detektionsverfahren aus der Literatur identifiziert. Hierzu wird eine zweite Literaturstudie durchgeführt. Das Ergebnis dieser Studie zeigt die typischen Aufdeckungsverfahren. Als fachliche Ansätze zur Identifikation von Fraud lassen sich Fraud Bewusstseinstraining, Mitarbeiteruntersuchung, Enthüllungssysteme, physische Dokumentenanalyse, Analyse von Texten, Numerische Analyse (Benfords Gesetz) und interne Kontrollen nennen. Algorithmen zur Frauderkennung lassen sich zu Statistischen, Klassifikation, Clustering oder sonstige Algorithmen zusammenfassen. Die am häufigsten in der Literatur genannten Algorithmen sind Neuronale Netzwerke, Entscheidungsbäume und Regression. Diese werden mit der recht neuen Fraud Detektionsmethode – dem Process Mining – verglichen.

Da Process Mining nicht zu den am häufigsten verwendeten Fraud Detektionsalgorithmen zählt und somit aus den Ergebnissen der zweiten Literaturstudie fällt, wird in einer dritten Literaturstudie speziell auf Fraud Detektion mit Process Mining eingegangen. Die meisten Forscher setzen Process Mining ein, um Abweichungen im Prozessablauf zu identifizieren und diese hinsichtlich Fraud zu analysieren. Typischerweise werden auch die Einhaltung von Kontrollen, wie beispielsweise die Funktionstrennung oder das Vier-Augen Prinzip, analysiert.

Forschungsfrage 2: Welche Anforderungen hinsichtlich der Gestaltung eines Prototyps für Fraud Detektion mit Hilfe von Red Flags und Process Mining ergeben sich aus der Literatur und Experteninterviews und wie lässt sich dieser Prototyp implementieren?

In der zweiten Forschungsfrage werden Anforderungen an den Prototypen gesammelt. Eine Anforderung ist zunächst die in Forschungsfrage 1 vorgestellten Fraud Patterns und die dazugehörigen Red Flags zu implementieren. Zusätzlich werden Anforderungen aus bestehenden Implementationen von Fraud Detektionstools aus Literatur und Praxis

entnommen. Singh et al. (2013) führen beispielsweise eine aufschlussreiche Befragung zu der von ihnen konzipierten Benutzeroberfläche durch. Die Aufteilung von Informationen auf mehrere Teilbereiche wird deshalb auch für diese Implementierung übernommen. Weiterhin wird der Wunsch nach zusätzlichen Informationen zum betrachteten Prozess in die Implementierung aufgenommen. Aus Unternehmensseite steht ein CIP Bericht Vorbild, bei dem das Unternehmen zunächst Anforderungen an eine Fraud Detektion Lösung und ihre Implementierung vorstellt. Das Dashboard des Prototyps orientiert sich zunächst an den vorhandenen akademischen Ansätzen für die Fraud Detektion, sowie anderer Process Mining Lösungen. Hierfür wird ein low-fidelity Prototyp erstellt und mit der Thinking Aloud Methode evaluiert. Als Ergebnis der Evaluation werden neue Anforderungen erhoben und in einem high-fidelity Prototyp umgesetzt.

Abschließend wird eine Process Mining Lösung ausgewählt, um diese Anforderungen umzusetzen. Wegen einer frei konfigurierbaren Oberfläche und einer erweiterbaren Datenbasis wird die gleichnamige Lösung der Firma Celonis gewählt. Zunächst werden die für Process Mining notwendigen Fall-, Aktivitäts- und Prozesstabellen durch ein SQL Skript erstellt. Um auch die Red Flags anzeigen zu können, wird die Datenstruktur erweitert. Die Red Flags werden auf Datenbankebene mit Hilfe von SQL-Skripten in den Daten gesucht. Zwar bietet Celonis eine SQL-ähnliche Sprache an (PQL), diese hat sich allerdings, durch den eingeschränkten Funktionsumfang, als nicht ausreichend für diesen Zweck erwiesen. Um den Prototypen auf das entsprechende Unternehmen anzupassen, muss der Prototyp zunächst durch den Auditor oder Fraud Investigator instanziiert werden. Dabei werden unternehmensspezifische Grenzwerte definiert werden, wie beispielsweise Genehmigungsstufen. Anschließend wählt der Auditor aus jedem Fraud Pattern die für ihn wichtigsten zusammengehörigen Red Flags aus. Der Prototyp sucht anschließend nach einer Kombination dieser Red Flags.

Die gewählte Implementierung des Prototyps ist offen für Erweiterungen. Neue Red Flags oder Fraud Patterns können ohne Änderungen an der Datenstruktur oder der Benutzeroberfläche hinzugefügt werden.

Forschungsfrage 3: Welche Implikationen hinsichtlich der Weiterentwicklung und Nutzung des vorgestellten Prototyps zur Fraud Detektion resultieren durch die Anwendung am Beispiel des Einkaufsprozesses?

Zur Beantwortung der dritten Forschungsfrage wird der high-fidelity Prototyp evaluiert, indem dieser auf drei verschiedene Datensätze angewendet wird. Zunächst wird ein Datengenerator implementiert, der entsprechend Fraud und prozesskonforme Daten in einem SAP ERP System generiert. Diese Daten werden anschließend mit dem in Forschungsfrage 2 entwickelten Prototypen ausgewertet.

Als Ergebnis der ersten Evaluationsstufe werden weitere Red Flags identifiziert, die zum Prototypen hinzugefügt werden. In einem zweiten Schritt wird der Prototyp auf einem Datensatz des Wettbewerbs White Collar Hacking Contest angewendet. Der White Collar Hacking Contest wurde von Michael Schermann an der TU München ins Leben gerufen und stellt einen Wettbewerb dar, bei dem die Teilnehmer zunächst Fraud in einem SAP ERP System

begehen und in einem zweiten Schritt den Fraud der Gegner identifizieren. Die dabei entstandenen Daten werden mit Hilfe des Prototyps ausgewertet. Anschließend werden die Ergebnisse in Relation zu den tatsächlich begangenen Frauds der Teilnehmer gesetzt. Als drittes werden Daten von zwei realen Unternehmen mit Hilfe des Prototyps ausgewertet. Bei Unternehmen Alpha werden alle im Auditbericht dargestellten Ergebnisse auch im Prototyp erkannt. Zusätzlich können zwei weitere sehr auffällige Frauds identifiziert werden, die mit den traditionellen Fraud Detektionsmethoden nicht identifiziert wurden. Bei Unternehmen Beta werden ebenfalls die wichtigsten Frauds erkannt. Auch werden zusätzlich Auffälligkeiten bei der internen Leistungsverrechnung erkannt, die üblicherweise nicht durch die Auditing Abteilung analysiert werden.

Eine Kombination des Ansatzes von Red Flags mit Process Mining kann dabei das bisherige Vorgehen um hilfreiche Informationen bereichern. So werden die Ist-Prozesse in einem Unternehmen mitsamt den identifizierten Red Flags visualisiert. Dabei ist es möglich nach einzelnen Red Flags, Fraud Patterns, Prozessinstanzen mit den häufigsten Vorkommnissen von Red Flags oder der höchsten Schadenssumme zu filtern. Mögliche Prozessabweichungen werden in der Prozesssicht dargestellt und können ebenfalls nach Abweichungen gefiltert werden. Der Prototyp stellt Informationen in den Sichten – Prozesssicht, Schemasicht, Material, Lieferant und Mitarbeiter – bereit. Jede Filterung wird auf alle Sichten angewendet, so dass beispielsweise bei der Auswahl einer Prozessinstanz nur die dazugehörigen Red Flags, Fraud Patterns, Mitarbeiter, Lieferanten und gekaufte Ware bzw. Dienstleistung angezeigt werden.

Um diesen Ansatz mit anderen Forschungsbeiträgen vergleichbar zu machen, wirdd eine Wahrheitsmatrix berechnet. Im Vergleich zu anderen Beiträgen erkennt man, dass die Anzahl der falsch-positiven Werte deutlich geringer ist. Allerdings ist die Erkennungsrate niedriger als bei einigen anderen Fraud Detektionsverfahren. Dem kann Abhilfe geschaffen werden, indem weitere Red Flags und Fraud Patterns zum Prototypen hinzugefügt werden. Eine Wahrheitsmatrix im realen Unternehmen ist nicht möglich, da die Anzahl der tatsächlich im Datensatz enthaltenen Frauds nicht bekannt sein kann.

Theoriebeitrag

Zunächst wird eine Literaturstudie mit im Einkaufsprozess vorkommenden Fraud Szenarien und den dazugehörigen Red Flags erstellt. Vor allem stellt interner Fraud noch eine Forschungslücke (Jans, Lybaert, & Vanhoof, 2009) dar, so dass das Ziel war diese Forschungslücke zu schließen. Zusätzlich werden verschiedene Algorithmen zur Fraud Detektion miteinander verglichen.

Der klassische Red Flag Ansatz wird mit Process Mining vereint, sowie zusammengehörige Red Flags zu Fraud Patterns kombiniert. Im Vergleich zu anderen Forschungsarbeiten kann so die falsch-positiv Rate deutlich gesenkt werden.

Zusätzlich wird ein effektiver Datengenerator realisiert. Bisherige Ansätze zur Generierung von synthetischen SAP Anwenderdaten basieren auf einen Nachbau der Benutzerinteraktionen in einem System-externen Tool (z.B. mit Java entwickelte Tools). Durch die Verwendung der von SAP bereitgestellten Technologien und Programmiersprache, können dieselben

Funktionsbausteine, wie die SAP GUI, verwendet und so die Nutzersimulation möglichst authentisch rekonstruieren werden.

Praxisbeitrag

Als Praxisbeitrag lässt sich zunächst der Prototyp zur Identifikation von Fraud im Einkaufsprozess nennen, welcher Auditoren, Mitarbeiter der internen und externen Revision oder Fraud Forensiker als graphische Hilfe zur Identifikation von Fraud dient. Dabei zeigt der Prototyp ungewöhnliche Prozessinstanzen mitsamt den darin enthaltenen Red Flags und Fraud Patterns an. Weitere Informationen über den Lieferanten, der gekauften Ware oder Dienstleistung und den zugehörigen Mitarbeiter werden angezeigt. Diese komplette Sicht auf den Fall ermöglicht es dem Fraud Investigator auf einen Blick dolose Handlungen zu identifizieren.

Zusätzlich wurde auch ein Datensimulator gebaut, da es einen Mangel am authentischen User Daten gibt (Barse et al., 2003), die wirtschaftskriminelles und regelkonformes Verhalten beinhalten. Dieser Datensatz kann in der Praxis verwendet werden, um beispielsweise Benchmarks von Fraud Detektionsmechanismen durchzuführen.

Limitation

Diese Forschung unterliegt einigen Limitationen. Zunächst wird eine deduktive Fraud Detektionsmethode angewendet. Nur bereits bekannte Red Flags und Fraud Patterns können im Datensatz erkannt werden. Dieser Ansatz kann jedoch um weitere Red Flags und Fraud Patterns ergänzt werden, um weitere wirtschaftskriminelle Taten zu identifizieren.

Bei den synthetischen und semi-synthetischen Datensätzen sind vor allem die Zeitstempel ein Problem. Das SAP System wird nur zum Zeitpunkt der Datengenerierung bzw. des White Collar Hacking Contests sehr stark beansprucht, die restliche Zeit nicht. Deshalb schlagen Red Flags mit zeitlichem Bezug an, wie beispielsweise ‚plötzlich hohe Aktivitäten eines schlafenden Lieferanten'. Bei den realen Datensätzen werden Waren und Dienstleistungen anonymisiert. So ist es beispielsweise schwierig zu deuten, ob die Dienstleistung zu der gelieferten Ware gerechtfertigt scheint. Auch werden in dem Datensatz von Alpha Daten zur Anonymisierung gelöscht. Einige Red Flags vergleichen „leere" Werte auf Gleichheit und schlagen deshalb besonders häufig an (erhöhte falsch-positiv Rate).

Eine weitere Einschränkung ist, dass der hier vorgestellte Prototyp Daten lediglich aus einem ERP Systemen entnimmt. Eine Erweiterung der Datenquellen um bspw. Kommunikationsdaten (Email, Chats usw.) wie von Islam et al. (2011) vorschlagen, würde die Genauigkeit der Algorithmen verbessern. Allerdings stellt dies auch einen tiefen Einschnitt in die Persönlichkeitsrechte der Mitarbeiter dar.

Ausblick

Diese Arbeit ist eine Erweiterung der Forschung zum Thema Fraud Detektion. Sie dient dazu einen genaueren Blick auf die Kombination aus Process Mining und Red Flags zu werfen. Eine Möglichkeit den hier vorgestellten Ansatz zu erweitern ist die Einbeziehung von weiteren Datenquellen, deren zusätzliche Informationen die Erkennungsrate verbessern könnte. Die Auswertung von Telefon- und E-Mailverkehr, wie sie zum Beispiel Islam et al. (2011) vorstellt, kann dabei helfen weitere Zusammenhänge zu finden, die sich aus den in SAP zur Verfügung stehenden Daten allein nicht ableiten lassen.

Auch kann der Einkaufsprozess noch um weitere Prozesse erweitert werden. Ein geeigneter Prozess wäre der Vertriebsprozess. So können Red Flags aus dem Einkaufsprozess mit Red Flags aus dem Vertriebsprozess im Zusammenhang betrachtet werden. So könnte das Red Flag deutliche Zunahme der Lagerbestände für ein bestimmtes Material mit einem höheren Verkauf des Endproduktes erklärt werden.

Die Architektur dieses Prototyps wird so erstellt, dass sie einfach erweiterbar ist. Die Vision ist eine zentrale, unabhängige und unternehmensübergreifende Sammelstelle von Fraud Patterns und Red Flags zu erstellen. Die Idee ist analog zum Aufbau eines Virusscanners. Jedes Unternehmen kann diese Red Flags entsprechend in ihren eigenen Fraud Detektionsstrategie aufnehmen.

Auch ist es möglich den entsprechenden Prototypen in Echtzeit zu testen. Mit der Entstehung von S4/HANA als neues ERP System der SAP AG müssen die Daten vom ERP System nicht zunächst in eine separate Datenbank extrahiert werden. Die Performanz der Datenbank ermöglicht den Prototypen auf dem produktiven System auszuprobieren und Fraud in Echtzeit zu analysieren. So soll aus den regelmäßigen ad-hoc Analysen ein kontinuierliches Verfahren werden.

Eine weitere interessante Forschungsrichtung könnte die Erstellung eines umfangreichen und technologieunabhängigen Evaluationsframeworks für die Fraud Detektionsklassifizierer. Bisher hat jede Publikation, der verschiedene Fraud Detektionsverfahren miteinander vergleicht, eigene Evaluationsdimensionen verwendet. Oft verwenden diese Autoren eigene Experimente um bspw. die Performanz oder die Genauigkeit der Verfahren zu testen. Diese Ergebnisse wären für andere Wissenschaftler relevanter, wenn sich Studien miteinander vergleichen lassen können. Deshalb wäre an dieser Stelle eine Art Standardisierung mit bestimmten Evaluationsmetriken sinnvoll.

Abschluss

Die Abwehr von Fraud ist ein Thema, dass nicht nur von Wirtschaftsprüfern, sondern auch von den Unternehmen (vor allem Geschäftsführer) selbst ernst genommen werden sollte. Die Forschung und Praxis zum Thema Fraud und Fraud Detektion hat mit der Zeit einige Methoden und Techniken hervorgebracht, die dabei helfen sollen das eigene Unternehmen zu schützen. Mit dem Einzug der Computertechnologie hat sich die Arbeit des Wirtschaftsprüfers jedoch radikal geändert. Riesige Datenmengen machen die Suche nach Fraud immer schwieriger. Der

Computer muss als Hilfsmittel anerkannt werden. Mit Hilfe von leistungsstarken in-memory Datenbanken können mittlerweile nicht nur Stichproben der Daten, sondern alle vorhandenen Datensätze ausgewertet werden. Nichts destotrotz können die gelieferten Ergebnisse nur Hinweise auf Fraud geben. Für eine tiefergehende Untersuchung sind weitere Informationen nötig. Die Informationen über die Prozessinstanz sind aber womöglich über mehrere Systeme verstreut. Je mehr Daten zentral zusammengetragen werden, desto leichter kann die Unterscheidung von legitimen und nicht legitimen Transaktionen werden. Process Mining stellt dabei eine der neuesten Möglichkeiten dar, Informationen aus einem System zu extrahieren. Das Wissen, über den IST-Prozess im Unternehmen, bietet hilfreiche Informationen über das eigene Unternehmen und die darin stattfindenden Abläufe. Diese können auch dabei helfen Fraud aufzudecken. Es ist aber wichtig zu verstehen, dass es keine Fertiglösung geben kann, da Unternehmen unterschiedlich aufgebaut sind. Indikatoren für Fraud, die in einem Unternehmen gelten, müssen nicht zwingend in derselben Ausprägung für ein anderes gelten. Trotz der Unterstützung durch moderne Technologien bleibt der Prozess der Fraud Detektion getrieben vom Wissen über das eigene Unternehmen, den Mitarbeitern und dem Unternehmensumfeld. Denn die Fraud Detektion Lösung muss individuell an die vorliegenden Gegebenheiten angepasst werden, um optimale Ergebnisse zu erzielen.

Literaturverzeichnis

Aalst, W.M.P.v.d. (2005). Business alignment: using process mining as a tool for Delta analysis and conformance testing. *Requirements Engineering, 10*(3), 2005, 198-211, https://doi.org/10.1007/s00766-005-0001-x.

Aalst, W.M.P.v.d. (2012). Process Mining. *Communications of the ACM, 55*(8), 76-83.

Aalst, W.M.P.v.d., Adriansyah, A., & Dongen, B.v. (2012). Replaying History on Process Models for Conformance Checking and Performance Analysis. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2*(2), 182-192. doi:0.1002/widm.1045

Aalst, W.M.P.v.d., & Günther, C.W. (2007). Finding Structure in Unstructured Processes: The Case for Process Mining. In T. Basten, G. Juhás, & S. Shukla (Red.), *Seventh International Conference on Application of Concurrency to System Design* (ACSD) (S. 3–12). Bratislava: IEEE. doi:10.1109/ACSD.2007.50

Aalst, W.M.P.v.d., & Medeiros, A.K.A.d. (2005). Process Mining and Security: Detecting Anomalous Process Executions and Checking Process Conformance. *Electronic Notes in Theoretical Computer Science, 121*, 3–21. doi:10.1016/j.entcs.2004.10.013

Aalst, W.M.P.v.d., Medeiros, A.K.A.d., & Weijters, A.J.M.M. (2005). Genetic Process Mining. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, G. Ciardo, & P. Darondeau (Red.), *Applications and Theory of Petri Nets* (S. 48–69). Berlin/Heidelberg, Deutschland: Springer-Verlag.

Aalst, W.M.P.v.d., Reijers, H. A., & Song, M. (2005). Discovering Social Networks from Event Logs. *Computer Supported Cooperative Work (CSCW), 14*(6), 549-593

Aalst, W.M.P.v.d., Rubin, V., Verbeek, H.M.W., Dongen, B.F., Kindler, E., & Günther, C.W. (2010). Process mining: a two-step approach to balance between underfitting and overfitting. *Software & Systems Modeling, 9*(1), 87–111. doi:10.1007/s10270-008-0106-z

Aalst, W.M.P.v.d., Dongen, B.F.v, Herbst, J., Maruster, L., Schimm, G., & Weijters, A.J. (2003). Workflow mining: A survey of issues and approaches. *Data & Knowledge Engineering, 47*(2), 237–267.

Aalst, W.M.P.v.d., Weijters, T., & Maruster, L. (2004). Workflow Mining: Discovering Process Models from Event Logs. *IEEE Transactions on Knowledge and Data Engineering, 16*(9), 1128–1142. doi:10.1109/tkde.2004.47

Aalst, W.M.P.v.d. (2011). *Process Mining: Discovery, Conformance and Enhancement of Business Processes*. Berlin/Heidelberg, Deutschland: Springer-Verlag.

Aalst, W.M.P.v.d., Beer, H.T.d., & Dongen, B.F.v. (2005). Process Mining and Verification of Properties: An Approach Based on Temporal Logic. In Meersman, R., Tari, Z., Hacid, M.-S., Mylopoulos, J., Pernici, B., Babaoglu, O., Jacobsen, H.A., Loyall, J., Kifer, M., & Spaccapietra, S.(Red.), *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE* (S. 130–147). Berlin/Heidelberg, Deutschland: Springer-Verlag.

Aalst, W.M.P.v.d., Hee, K.M.v.d., Werf, J.M.v.d., & Verdonk, M. (2010). Auditing 2.0: Using Process Mining to Support Tomorrow's Auditor. *Computer, 43*(3), 90–93. doi:10.1109/mc.2010.61

Aalst, W.M.P.v.d., & Weijters, A.J.M.M. (2005). Process Mining. In M. Dumas, W.M.P.v.d. Aalst, & A. Hofstede (Red.), *Process-Aware Information Systems* (S. 235-255). Hoboken (USA): John Wiley & Sons.

Aalst, W.M.P.v.d., Weijters, A.J.M.M., & Maruster, L. (2004). Workflow Mining: Discovering Process Models from Event Logs. *IEEE Transactions on Knowledge and Data Engineering, 16(9),* 1128-1142. doi:10.1109/TKDE.2004.47

Abbott, L.J., Park, Y., & Parker, S. (2000). The effects of audit committee activity and independence on corporate fraud. *Managerial Finance, 26*(11), 55–67.

Abbott, L.J., Parker, S., & Peters, G.F. (2001). Audit Committee Characteristics and Financial Misstatement: A Study of the Efficacy of Certain Blue Ribbon Committee Recommendations. *Convention Proceedings of the 2001 Annual Meeting of the Americal Accounting Association.*

Accorsi, R., & Stocker, T. (2012). *On the Exploitation of Process Mining for Security Audits: The Conformance Checking Case.* Paper presented at the 27th Annual ACM Symposium on Applied Computing (S.1709-1716), New York, NY, USA: ACM. doi={10.1145/2245276.2232051}

ACFE. (1996). *Report to the Nation on Occupational Fraud and Abuse*. Austin (USA) Abgerufen von http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/1996-rttn.pdf

ACFE. (2002). *Report to the Nation on Occupational Fraud and Abuse*. Austin (USA) Abgerufen von http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/2002RttN.pdf

ACFE. (2004). *Report to the Nation on Occupational Fraud and Abuse*. Austin (USA) Abgerufen von http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/2004RttN.pdf

ACFE. (2006). *Report to the Nation on Occupational Fraud and Abuse*. Austin (USA) Abgerufen von http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/2006-rttn.pdf

ACFE. (2008). *Report to the Nation on Occupational Fraud and Abuse*. Austin (USA) Abgerufen von http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/2008-rttn.pdf

ACFE. (2010). *Report to the Nation on Occupational Fraud and Abuse*. Austin (USA) Abgerufen von http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/rttn-2010.pdf

ACFE. (2011). *Fraud Examiners Manual.* Austin (USA): Association of Certified Fraud Examiners

ACFE. (2012). *Report to the Nation on Occupational Fraud and Abuse*. Austin (USA) Abgerufen von http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

ACFE. (2014). *Report to the Nation on Occupational Fraud and Abuse*. Austin (USA) Abgerufen von http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2014-report-to-nations.pdf

ACFE. (2016). *Report to the Nation on Occupational Fraud and Abuse*. Austin (USA) Abgerufen von https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

ACFE. (2018). *Report to the Nation on Occupational Fraud and Abuse*. Austin (USA) Abgerufen von https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

Agrawal, R., Gunopulos, D., & Leymann, F. (1998). Mining Process Models from Workflow Logs. In H.J. Schek, G. Alonso, F. Saltor, & I. Ramos (Red.), *Advances in Database Technology — EDBT'98* (S. 467-483): Berlin/Heidelberg: Springer-Verlag.

AICPA, The American Institute of Certified Public Accountants. (2002). Statement on Auditing Standards No. 99: Consideration of Fraud in a Financial Statement Audit, 316. Abgerufen von https://www.aicpa.org/

Al-ajwad, M. N., & Carr, L. (2016). An Open Public E-Procurement Solution to Tackle Corruption in Iraq. In 2016 International Conference for Students on Applied Engineering (ICSAE) (S. 83–88). IEEE.

Albanese, J.S. (1996). Offense-Based versus Offender-Based Definitions of White Collar Crime. In J. Helmkamp, R. Ball, & K. Townsend (Red.), *Proceedings of the Academic Workshop. Definitional Dilemma: Can and Should There Be a universal Definition of White Collar Crime?* (S. 87–93). Morgantown (USA).

Albrecht, W.S., Albrecht, C.C., & Albrecht, C.O. (2004). Fraud and corporate executives: Agency, Stewardship and Broken Trust. *Journal of Forensic Accounting, 5*, 109–130.

Albrecht, W.S., Albrecht, C.O., Albrecht, C.C., & Zimbelman, M.F. (2012). *Fraud Examination* (4 Aufl.). Mason (USA): Cengage Learning.

Albrecht, W.S., & Romney, M.B. (1986). A red-flagging management fraud: a validation. *Advances in Accounting, 3*, 323-333.

Albrecht, W.S., Romney, M.B., Cherrington, D.J., Payne, I.R., & Roe, A.J. (1982). *How to Detect and Prevent Business Fraud*. Englewood Cliffs (USA): Prentice-Hall.

Aleskerov, E., Freisleben, B., & Rao, B. (1997). CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection. In J. F. Marshall, R. J. Marks, & M. Wolf (Red.), *Proceedings of the IEEE/IAFE 1997 Conference on Computational Intelligence for Financial Engineering (CIFEr)* (S. 220–226).

Allan, T., & Zhan, J. (2010). Towards Fraud Detection Methodologies. In S. Panchanathan, S.-S. Yeo, & J. Liu (Red.), *Proceedings of the 5th International Conference on Future Information Technology* (S. 1–6). New York City, NY, USA: IEEE. doi: 10.1109/CIFER.1997.618940

Allen, A. (2007). Turning the screw on fraud. *Supply Management, 12*(22), 15.

Alles, M., Brennan, G., Kogan, A., & Vasarhelyi, M.A. (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems, 7*(2), 137-161. doi: http://dx.doi.org/10.1016/j.accinf.2005.10.004.

Anand, V., Ashforth, B.E., & Joshi, M. (2004). Business as usual: The acceptance and perpetuation of corruption in organizations. *The Academy of Management Perspectives, 18*(2), 39–53. doi:10.5465/ame.2004.13837437

ARC. (2016). Audit Innovation Award. Abgerufen von http://audit-challenge.com/?page_id=6669

Artís, M., Ayuso, M., & Guillén, M. (1999). Modelling different types of automobile insurance fraud behaviour in the Spanish market. *Insurance: Mathematics and Economics, 24*(1-2), 67–81. doi:10.1016/s0167-6687(98)00038-9

Artís, M., Ayuso, M., & Guillén, M. (2002). Detection of automobile insurance fraud with discrete choice models and misclassified claims. *Journal of Risk and Insurance, 69*(3), 325–340.

Atteslander, P. (2010). *Methoden der empirischen Sozialforschung.* (13. Aufl.), Erich Schmidt-Verlag, Berlin, Deutschland 2010.

Atwood, J. A., Robison-Cox, J. F., & Shaik, S. (2006). Estimating the Prevalence and Cost of Yield-Switching Fraud in the Federal Crop Insurance Program. *American Journal of Agricultural Economics, 88*(2), 365–381.

Avellanet, A. W. (2010). Anti-Fraud Controls: What Internal Auditors Need To Know. *Internal Auditing, 25*(1), 10–26.

Baader, G., Meyer, R., Wagner, C., & Krcmar, H. (2016). Specification and Implementation of a Data Generator to simulate Fraudulent User Behavior. In W. Abramowicz, R. Alt, &

B. Franczyk, B. (Red.), *Business Information Systems: 19th International Conference: Vol. 255. BIS 2016,*(S. 67-78) Leipzig, Deutschland: Springer-Verlag.

Bagranoff, N.A., Simkin, M.G., Strand, N., & Strand, C.A. (2010). *Core Concepts of Accounting Information Systems* (11 Aufl.). Hoboken, USA: John Wiley & Sons.

Bai, B., Yen, J., & Yang, X. (2008). False Financial Statements: Characteristics of China's Listed Companies and Cart Detecting Approach. *International Journal of Information Technology & Decision Making, 7*(2), 339–359.

Balzert, H. (2009). *Lehrbuch der Softwaretechnik: Basiskonzepte und Requirements Engineering* (3. Aufl.). Heidelberg, Deutschland: Spektrum Akademischer Verlag.

Bandara, W., Miskon, S., & Fielt, E. (2011). A systematic, tool-supported method for conducting literature reviews in information systems. In V. Tuunainen, J. Nandhakumar, M. Rossi, & W. Soliman (Red.), *Proceedings of the 19th European Conference on Information Systems: ICT and Sustainable Service Development*. Helsinki, Finland

Bank, T.W. (2018). GDP (in USD). Abgerufen von http://data.worldbank.org/indicator/NY.GDP.MKTP.CD

Barron, J. (2011). A High-Wire Act: Maintaining Workforce Trust in an Era of High Fraud Losses. *Business Credit, 113*(6), 38–41.

Barse, E.L., Kvarnström, H., & Jonsson, E. (2003). *Synthesizing Test Data for Fraud Detection Systems*. Paper presented at the Proceedings of the 19th Annual Computer Security Applications Conference, Las Vegas, NV, USA.

Baughn, C., Bodie, N.L., Buchanan, M.A., & Bixby, M.B. (2010). Bribery in International Business Transactions. *Journal of Business Ethics, 92*(1), 15–32. doi:10.1007/s10551-009-0136-7

Beasley, M.S. (1996). An Empirical Analysis of the Relation between the Board of Director Composition and Financial Statement Fraud. *The Accounting Review, 71*(4), 443–465.

Beasley, M.S., Carcello, J.V., Hermanson, D.R., & Lapides, P.D. (2000). Fraudulent Financial Reporting: Consideration of Industry Traits and Corporate Governance Mechanisms. *Accounting Horizons, 14*(4), 441–454. doi:10.2308/acch.2000.14.4.441

Beck, L., & Ajzen, I. (1991). Predicting Dishonest Actions Using the Theory of Planned Behavior. *Journal of Research in Personality, 25*(3), 285–301. doi:10.1016/0092-6566(91)90021-h

Belhadji, E.B., Dionne, G., & Tarkhani, F. (2000). A Model for the Detection of Insurance Fraud. *Geneva Papers on Risk & Insurance, 25*(4), 517–538. doi:10.1111/1468-0440.00080

Bell, T.B., & Carcello, J.V. (2000). A Decision Aid for Assessing the Likelihood of Fraudulent Financial Reporting. *Auditing: A Journal of Practice & Theory, 19*(1), 169–184. doi:10.2308/aud.2000.19.1.169

Bell, T.B., Szykowny, S., & Willingham, J.J. (1991). *Assessing the likelihood of fraudulent financial reporting: A cascaded logit approach*. Working Paper, KPMG.

Beneish, M.D. (1997). Detecting GAAP violation: implications for assessing earnings management among firms with extreme financial performance. *Journal of Accounting and Public Policy, 16*(3), 271–309. doi:10.1016/s0278-4254(97)00023-9

Beneish, M.D. (1999). Incentives and Penalties Related to Earnings Overstatements that Violate GAAP. *Accounting Review, 74*(4), 425.

Bentley, P.J. (2000). "Evolutionary, my dear Watson": Investigating Committee-based Evolution of Fuzzy Rules for the Detection of Suspicious Insurance Claims. In L. D. Whitley, D. E. Goldberg, E. Cantú-Paz, L. Spector, I. C. Parmee, & H.-G. Beyer (Red.), *Proceedings of the 2000 Annual Conference on Genetic and Evolutionary Computation* (S. 702-709). Morgan Kaufmann Publishers Inc.

Bentley, P.J., Kim, J., Jung, G.-H., & Choi, J.-U. (2000). Fuzzy Darwinian Detection of Credit Card Fraud. *Proceedings of the 14th Annual Fall Symposium of the Korean Information Processing Society: Vol. 14* (S.1-4).

Bermúdez, L., Pérez, J.M., Ayuso, M., Gómez, E., & Vázquez, F.J. (2008). A Bayesian dichotomous model with asymmetric link for fraud in insurance. *Insurance: Mathematics and Economics, 42*(2), 779–786. doi:10.1016/j.insmatheco.2007.08.002

Bernardi, R.A. (1994). Fraud detection: The effect of client integrity and competence and auditor cognitive style. *Auditing: A Journal of Practice & Theory, 13 (Suppl)*, 68-84.

Best, P.J., Rikhardsson, P., & Toleman, M. (2009). Continuous Fraud Detection in Enterprise Systems through Audit Trial Analysis. *Journal of Digital Forensics, Security and Law, 4*(1), 39-60.

Bezerra, F., & Wainer, J. (2008a). Anomaly detection algorithms in logs of process aware systems. In R. L. Wainwright & H. M. Haddad (Red.), *Proceedings of the 2008 ACM Symposium on Applied Computing* (S. 951–952). New York, NY: USA. doi:10.1145/1363686.1363904

Bezerra, F., & Wainer, J. (2008b). *Fraud Detection in Process Aware Systems*. Paper presented at the Proceedings of the 14th Brazilian Symposium on Multimedia and the Web, New York; USA.

Bezerra, F., & Wainer, J. (2011). Fraud Detection in Process Aware Systems. *International Journal of Business Process Integration and Management, 5*(2), 121-129. doi: https://doi.org/10.1504/IJBPIM.2011.040204

Bezerra, F., & Wainer, J. (2013). Algorithms for anomaly detection of traces in logs of process aware information systems. *Information Systems, 38*(1), 33–44. doi:10.1016/j.is.2012.04.004

Bezerra, F., Wainer, J., & Aalst, W.M.P.v.d. (2009). Anomaly Detection using Process Mining. In T. Halpin, J. Krogstie, S. Nurcan, E. Propoer, R. Schmidt, P. Soffer, R. Ukor (Red.) *Enterprise, Business-Process and Information Systems Modeling: Vol. 29* Lecture Notes in Business Information Processing. (S. 149-161). Berlin/Heidelberg, Deutschland: Springer-Verlag.

Bhargava, B., Zhong, Y., & Lu, Y. (2003). Fraud Formalization and Detection. In G. Goos, J. Hartmanis, J. Leeuwen, Y. Kambayashi, M. Mohania, & W. Wöß (Red.), *Proceedings of the 5th International Conference on Data Warehousing and Knowledge Discovery: Vol.2737 Lecture Notes in Computer Science* (S. 330–339). Berlin/Heidelberg, Deutschland: Springer-Verlag.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J.C. (2011). Data mining for credit card fraud: A comparative study. *Decision support systems, 50*(3), 602–613. doi:10.1016/j.dss.2010.08.008

Bhattacharya, S., & Kumar, K. (2008). Forensic accounting and Benford's law [In the spotlight]. *IEEE Signal Processing Magazine*, *25*(2). 150-152. http://doi.org/10.1109/MSP.2007.914724

Bhattacharya, K., & Suri, T. (2017). The Curious Case of e-Governance. IEEE Internet Computing, 21(1), 62–67.

Biegelman, M. T. (2013). *Faces of Fraud: Cases and Lessons form a Life Fighting Fraudsters* (1.Aufl.). Hoboken, USA: John Wiley & Sons. doi:10.1002/9781118556917

BLS Bureau of Labor Statistics (BLS). (2013, 2018/7/10). Labor Force Statistics from the Current Population Survey. Abgerufen von http://www.bls.gov/cps/cpsaat03.htm

Boczko, T. (2007). *Corporate Accounting Information Systems* (1. Aufl.). Harlow: Prentice-Hall.

Bolton, R.J., & Hand, D.J. (2001). Unsupervised Profiling Methods for Fraud Detection. *Proceedings of the 7th Conference on Credit Scoring and Credit Control, VII, 5–7.*

Bolton, R.J., & Hand, D.J. (2002). Statistical Fraud Detection: A review. *Statistical Science, 17*(3), 235-249. doi:10.1214/ss/1042727940

Bonchi, F., Giannotti, F., Mainetto, G., & Pedreschi, D. (1999). A Classification-based Methodology for Planning Audit Strategies in Fraud Detection. In U. Fayyad, S. Chaudhuri, & D. Madigan (Red.), *Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (S. 175–184). San Diego, California: ACM. doi:10.1145/312129.312224

Bonger, W. A. (1916). *Criminality and Economic Conditions* (10. Aufl). London,UK: Heinemann.

Bönner, A., Riedl, M., & Wenig, S. (2011). *Digitale SAP®-Massendatenanalyse: Risiken erkennen - Prozesse optimieren*. Berlin: Erich Schmidt Verlag.

Bortz, J. & Döring, N. (2006): *Forschungsmethoden und Evaluation*. (4. Aufl.), Springer-Verlag, Heidelberg, Deutschland 2006.

Bose, R.P.J.C., & Aalst, W.M.P.v.d. (2010). *Trace Alignment in Process Mining: Opportunities for Process Diagnostics*. In R. Hull, J. Mendling, S. Tai (Red.), *International Conference on Business Process Management: Vol* 6336 (S. 227-242). Springer, Berlin, Heidelberg

Boukerche, A., & Notare, M.S.M.A. (2000). Neural Fraud Detection in Mobile Phone Operations. In J. Rolim (Red.), *Parallel and Distributed Processing* (S. 636–644). Berlin/Heidelberg, Deutschland: Springer-Verlag.

Boukerche, A., & Notare, M. S. M. A. (2002). Behavior-Based Intrusion Detection in Mobile Phone Systems. *Journal of Parallel and Distributed Computing, 62*(9), 1476–1490. doi:10.1006/jpdc.2002.1857

Bozkaya, M., Gabriels, J., & Werf, J.M.v.d. (2009). Process Diagnostics: A Method Based on Process Mining. In: *International Conference on Information, Process, and Knowledge Management*, eKNOW '09, 22-27.doi: 10.1109/eKNOW.2009.29.

Brandman, B. (2000). Cracking Down on Corporate Crime: Are you being duped? *CMA Magazine, 74*(5), 38–41.

Brause, R., Langsdorf, T., & Hepp, M. (1999). Neural data mining for credit card fraud detection. In D. C. Martin (Red.), *Proceedings of the 11th International Conference on Tools with Artificial Intelligence* (S. 103–106), Chicago, IL, USA: IEEE. doi:10.1109/TAI.1999.809773

Briggs, R. (2006). On theory-driven design and deployment of collaboration systems. *International Journal of Human-Computer Studies, 64*(7), 573–582. doi: 10.1016/j.ijhcs.2006.02.003

Brockett, P.L., Derrig, R.A., Golden, L.L., Levine, A., & Alpert, M. (2002). Fraud Classification Using Principal Component Analysis of RIDITs. *The Journal of Risk and Insurance, 69*(3), 341–371. doi:10.1111/1539-6975.00027

Brockett, P.L., Golden, L.L., Jang, J., & Yang, C. (2006). A Comparison of Neural Network, Statistical Methods, and Variable Choice for Life Insurers' Financial Distress Prediction. *Journal of Risk and Insurance, 73*(3), 397–419. doi:10.1111/j.1539-6975.2006.00181.x

Brockett, P.L., Xia, X., & Derrig, R.A. (1998). Using Kohonen's Self-Organizing Feature Map to Uncover Automobile Bodily Injury Claims Fraud. *Journal of Risk and Insurance, 65*(2), 245–274. doi:10.2307/253535

Brügge, B., & Dutoit, A.H. (2004). *Objektorientierte Softwaretechnik mit UML, Entwurfsmuster und Java* (Vol. 2). München: Pearson Education Deutschland.

Brulenski, F.C., & Zayas, R.J. (2004). Fraud Detection is not Just by the Numbers. *Pennsylvania CPA Journal, 75*(2), 34–37.

Büchner, S., Freytag, A., González, L. G., & Güth, W. (2008). Bribery and public procurement: an experimental study. *Public Choice, 137*(1-2), 103–117. doi:10.1007/s11127-008-9315-9

Buckhoff, T.A. (2002). Preventing Employee Fraud by Minimizing Opportunity. *The CPA Journal, 72*(5), 64–65.

Buckhoff, T.A. (2003). The Benefits of a Fraud Hotline. *The CPA Journal, 73*(7), 62.

Buckhoff, T.A., & Parham, A.G. (2009). Fraud in the NONprofit sector? You bet. *Strategic Finance, 90*(12), 53–56.

Bungartz, O. (2012). *Handbuch Interne Kontrollsysteme (IKS) : Steuerung und Uberwachung von Unternehmen*. Berlin: Schmidt, Erich.

Burge, P., & Shawe-Taylor, J. (1997). Detecting cellular fraud using adaptive prototypes. In B. Kuipers & B. L. Webber (Red.), *AAAI Workshop on AI Approaches to Fraud Detection and Risk Management* (S.9-130). Menlo Park, CA: AAAI Press.

Burge, P., & Shawe-Taylor, J. (2001). An Unsupervised Neural Network Approach to Profiling the Behavior of Mobile Phone Users for Use in Fraud Detection. *Journal of Parallel and Distributed Computing, 61*(7), 915–925. doi:10.1006/jpdc.2000.1720

Burge, P., Shawe-Taylor, J., Cooke, C., Moreau, Y., Preneel, B., & Stoermann, C. (1997). Fraud detection and management in mobile telecommunications networks. *IET Conference Proceedings*, 91-96. doi: 10.1049/cp:19970429IET.

Byington, J. R., & McGee, J. A. (2012). Are Your Cash Transactions Protected? *Journal of Corporate Accounting and Finance, 24*(1), 15–23. doi:10.1002/jcaf.21808

Cahill, M. H., Lambert, D., Pinheiro, J. C., & Sun, D. X. (2002). Detecting Fraud in the Real World. In J. Abello, P. M. Pardalos, & M. G. C. Resende (Red.), *Handbook of Massive Data Sets* (Vol. 4, S. 911–929). Boston (USA): Springer.

Calderon, T. G., & Green, B. P. (1994). Analysts' forecasts as an exogenous risk indicator in analytical auditing. *Advances in Accounting, 12*, 281–300.

Carpenter, T. D., & Reimers, J. L. (2005). Unethical and Fraudulent Financial Reporting: Applying the Theory of Planned Behavior. *Journal of Business Ethics, 60*(2), 115–129. doi:10.1007/s10551-004-7370-9

Caudill, S.B., Ayuso, M., & Guillén, M. (2005). Fraud Detection using a Multinomial Logit Model with Missing Information. *Journal of Risk and Insurance, 72*(4), 539–550. doi: 10.1111/j.1539-6975.2005.00137.x

Cavinato, J. L. (2000). *Supply Chain and Transportation Dictionary* (4 Aufl.). Norwell (USA): Kluwer Academic Publishers.

Cerullo, M.J., & Cerullo, V. (1999a). Using Neural Networks to Predict Financial Reporting Fraud: Part 1. *Computer Fraud & Security, 1999*(5), 14–17. doi:10.1016/s1361-3723(99)80015-3

Cerullo, M. J., & Cerullo, V. (1999b). Using Neural Networks to Predict Financial Reporting Fraud: Part 2. *Computer Fraud & Security, 1999*(6), 14–17. doi:10.1016/s1361-3723(99)80035-9

Chan, P.K., Fan, W., Prodromidis, A.L., & Stolfo, S.J. (1999). Distributed data mining in credit card fraud detection. *Intelligent Systems and their Applications, IEEE, 14*(6), 67-74. doi: 10.1109/5254.809570

Chan, P.K., & Stolfo, S.J. (1998). Towards a scalable learning with non-uniform class and cost distributions: A case study in credit card fraud detection. In R. Agrawal, P. E. Stolorz, & G. Piatetsky-Shapiro (Red.), *Proceedings of the 4th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (Vol.98, S. 164–168). New York, USA: AAAI.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. *ACM Computing Surveys, 41*(3), 1–58. doi:10.1145/1541880.1541882

Chang, W.-H., & Chang, J.-S. (2010). Using Clustering Techniques to Analyze Fraudulent Behavior Changes in Online Auctions. In S. Thatcher & X. Yi (Red.), *International Conference on Networking and Information Technology* (S. 34–38). Manila, Philippines: IEEE. doi:10.1109/ICNIT.2010.5508564.

Chartier, B., & Spillane, T. (2000). Money laundering detection with a neural network. In P. J. G. Lisboa, A. Vellido, & B. Edisbury (Red.), *Business Applications of Neural Networks* (S. 159–172). Singapore: World Scientific.

Chen, G., Lu, Z., & He, F. (2007). An Empirical Research on Detection of Fraudulent Financial Reports Based on Data of Chinese Listed Company. *Auditing Research, 3*.

Chen, H.-J., Huang, S.-Y., & Kuo, C.-L. (2009). Using the artificial neural network to predict fraud litigation: Some empirical evidence from emerging markets. *Expert Systems with Applications, 36*(2), 1478–1484. doi:10.1016/j.eswa.2007.11.030

Chen, R.-C., Chen, T.-S., & Lin, C.-C. (2006). A New Binary Support Vector System for Increasing Detection Rate of Credit Card Fraud. *International Journal of Pattern Recognition and Artificial Intelligence, 20*(02), 227–239. doi:10.1142/s0218001406004624

Chen, R.-C., Chiu, M.-L., Huang, Y.-L., & Chen, L.-T. (2004). Detecting Credit Card Fraud by Using Questionnaire-Responded Transaction Model Based on Support Vector Machines. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, Z. R. Yang, H. Yin, & R. M. Everson

(Red.), *Intelligent Data Engineering and Automated Learning – IDEAL 2004* (S. 800–806). Berlin/Heidelberg, Deutschland: Springer-Verlag.

Chen, R.-C., Luo, S.-T., Liang, X., & Lee, V. C. S. (2005). Personalized Approach Based on SVM and ANN for Detecting Credit Card Fraud. In M. Zhao & Z. Shi (Red.), *Proceedings of the 2005 International Conference on Neural Networks and Brain* (S. 810–815). Peking, China: IEEE. doi: 10.1109/ICNNB.2005.1614747

Chiu, C.-C., & Tsai, C.-Y. (2004). A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection. *Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service*,177–181. doi: 0.1109/EEE.2004.1287306

Choo, F., & Tan, K. (2007). An "American Dream" theory of corporate executive Fraud. *Accounting Forum, 31*(2), 203–215. doi:10.1016/j.accfor.2006.12.004

Christensen, J.A., & Byington, J.R. (2002). Can the CFO Stop White Collar Crime? *Journal of Corporate Accounting and Finance, 14*(1), 39–44. doi:10.1002/jcaf.10118

Christensen, J. A., & Byington, J. R. (2003a). The Computer: An Essential Fraud Detection Tool. *Journal of Corporate Accounting and Finance, 14*(5), 23–27. doi:10.1002/jcaf.10179

Christensen, J.A., & Byington, J.R. (2003b). How secure are your cash transactions? *Journal of Corporate Accounting and Finance, 15*(1), 7-14. doi:10.1002/jcaf.10212

Chuprunov, M. (2011). *Handbuch SAP-Revision* (1 Aufl.). Bonn, Deutschland: Galileo Press.

Clinard, M. B., & Quinney, R. (1967). *Criminal behavior systems: A typology*. New York. USA: Holt, Rinehart, and Winston.

Coderre, D.G. (2009). *Computer Aided Fraud Prevention and Detection: A Step by Step Guide* (1.Aufl.). Hoboken/New Jersey, USA: John Wiley & Sons.

Coenen, T. L. (2008). *Essentials of Corporate Fraud*. Hoboken, USA: John Wiley & Sons.

Cohen, J., Ding, Y., Lesage, C., & Stolowy, H. (2010). Corporate Fraud and Managers' Behavior: Evidence from the Press. *Journal of Business Ethics, 95*(2), 271–315. doi:10.1007/s10551-011-0857-2

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588–608.

Coleman, J.W. (1987). Toward an Integrated Theory of White-Collar Crime. *American Journal of Sociology, 93*(2), 406–439. doi:10.2307/2779590

Conklin, J.E. (1977). *"Illegal but not criminal": Business crime in America*. Englewood Cliffs, USA: Prentice-Hall.

Cook, J.E., & Wolf, A.L. (1998a). Discovering Models of Software Processes from Event-Based Data. *ACM Transactions on Software Engineering and Methodology (TOSEM), 7*(3), 215-249. doi:10.1145/287000.287001

Cook, J.E., & Wolf, A.L. (1998b). Event-based detection of concurrency. *ACM SIGSOFT Software Engineering Notes, 23*(6), 35-45. doi:10.1145/291252.288214

Cortes, C., & Pregibon, D. (2001). Signature-Based Methods for Data Streams. *Data Mining and Knowledge Discovery, 5*(3), 167–182. doi:10.1023/a:1011464915332

Cowan, N. (2005). Counter intelligence. *Supply Management, 10*(6), 32–33.

Cox, E. (1995). A Fuzzy System for Detecting Anomalous Behaviors in Healthcare Provider Claims. In S. Goonatilake & P. C. Treleaven (Red.), *Intelligent Systems for Finance and Business* (S. 111–134). New York, USA: John Wiley & Sons.

Cressey, D.R. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Glencoe, USA: Free Press.

Crocker, K.J., & Tennyson, S. (2002). Insurance Fraud and Optimal Claims Settlement Strategies. *The Journal of Law and Economics, 45(2),* 469–507. doi:10.1086/340394

Dahm, M. (2006). *Grundlagen der Mensch-Computer-Interaktion* (10. Aufl.). München, Deutschland: Pearson Verlag.

Davis, J.H., Schoorman, F.D., & Donaldson, L. (1997). Toward a Stewardship Theory of Management. *Academy of Management Review, 22*(1), 20–47. doi:10.5465/amr.1997.9707180258

De Medeiros, A., & Weijters, A. (2005). Genetic Process Mining. *Applications and Theory of Petri Nets, 3536* 48-69. doi:10.1.1.76.4916

Deling, W. (2005). Dolose Handlungen und Interne Revision - Herausforderung oder Kapitulation?. Abgerufen von http://www.foren-internerevision.de/artikel/eigen/Dolose_Handlungen.pdf

Deng, Q., & Mei, G. (2009). Combining self-organizing map and K-means clustering for detecting fraudulent financial statements. In T. Y. Lin, X. Hu, J. Xia, T.-P. Hong, Z. Shi, J. Han, S. Tsumoto, & X. Shen (Red.), *Proceedings of the 2009 IEEE International Conference on Granular Computing* (S. 126–131). Nanchang, China: IEEE. doi:10.1109/GRC.2009.5255148

Derrig, R.A., & Ostaszewski, K.M. (1995). Fuzzy Techniques of Pattern Recognition in Risk and Claim Classification. *The Journal of Risk and Insurance, 62 (3),* 447-482. doi:10.2307/253819

Deshmukh, A., Romine, J., & Siegel, P.H. (1997). Measurement and combination of red flags to assess the risk of management fraud: A fuzzy set approach. *Managerial Finance, 23*(6), 35–48. doi:10.1108/eb018629

Deshmukh, A., & Talluru, L. (1998). A rule-based fuzzy reasoning system for assessing the risk of management fraud. *International Journal of Intelligent Systems in Accounting, Finance and Management, 7*(4), 223–241. doi:10.1002/(sici)1099-1174(199812)7:4<223::aid-isaf158>3.0.co;2-i

Desrosiers, P. (2010). Take a look around you. *Supply Management, 15*(10), 20–22.

Dharwa, J.N., & Patel, A.R. (2011). A Data mining with Hybrid Approach Based Transaction Risk Score Generation Model (TRSGM) for Fraud Detection of Online Financial Transaction. *International Journal of Computer Applications, 16*(1), 18–25.

Dhurandhar, A., Ravi, R., Graves, B., Maniachari, G., & Ettl, M. (2015). Robust System for Identifying Procurement Fraud. In Proceedings of the Twenty-Seventh Conference on Innovative Applications of Artificial Intelligence (pp. 3896–3903). Association for the Advancement of Artificial Intelligence.

DIIR (2011). Revision der Beschaffung: Prüfungsfragen für die Praxis (Band 11, 4. Aufl.). Berlin, Deutschland: Erich Schmidt Verlag.

DiNapoli, T.P. (2008). *Red Flags for Fraud.* Abgerufen von https://www.osc.state.ny.us/localgov/pubs/red_flags_fraud.pdf

Donaldson, L., & Davis, J.H. (1991). Stewardship Theory or Agency Theory: CEO Governance and Shareholder Returns. *Australian Journal of Management, 16*(1), 49–64. doi:10.1177/031289629101600103

Dongen, B.F.v., Medeiros, A.K.A.d., & Wen, L. (2009). Process Mining: Overview and Outlook of Petri Net Discovery Algorithms. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, K. Jensen, & W. M. P. v. d. Aalst (Red.), *Transactions on Petri Nets and Other Models of Concurrency II* (S. 225–242). Berlin/Heidelberg, Deutschland: Springer-Verlag.

Dongen, B.F.v., Medeiros, A.K.A.d., Verbeek, H.M.W., Weijters, A.J.M.M., & Aalst, W.M.P.v.d. (2005). The ProM framework: A New Era in Process Mining Tool Support. In G. Ciargo, P. Darondeau (Red.) *Applications and Theory of Petri Nets ICAPTN 2005: Vol. 3536* (S. 444-454): Berlin/Heidelberg, Deutschland: Springer-Verlag. doi: /10.1007/11494744_25

Donoho, S. (2004). Early Detection of Insider Trading in Option Markets. In W. Kim, R. Kohavi, J. Gehrke, W. DuMouchel, & S. Donoho (Red.), *Proceedings of the 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (S. 420–429). Seattle, WA, USA: ACM. doi:10.1145/1014052.1014100

Dorminey, J.W., Fleming, A.S., Kranacher, M.-J., & Riley, R.A. (2010). Beyond the Fraud Triangle: Enhancing Deterrence of Economic Crimes. *The CPA Journal, 80*(7), 16–23.

Dorminey, J.W., Fleming, A.S., Kranacher, M.-J., & Riley, R.A. (2012). The Evolution of Fraud Theory. *Issues in Accounting Education, 27*(2), 555–579. doi:10.2308/iace-50131

Dorronsoro, J.R., Ginel, F., Sanchez, C., & Sanat Cruz, C. (1997). Neural fraud detection in credit card operations. *IEEE Transactions on Neural Networks, 8*(4), 827–834. doi:10.1109/72.595879

Duffield, G.M., & Grabosky, P.N. (2001). *The Psychology of Fraud. Trends & Issues in Crime and Criminal Justice: Vol. 199.* Canberra: Australian Institute of Criminology.

Dyck, A., Morse, A., & Zingales, L. (2010). Who Blows the Whistle on Corporate Fraud? *The Journal of Finance, 65*(6), 2213–2253. doi:10.1111/j.1540-6261.2010.01614.x

Dye, K.M. (2007). Corruption and Fraud Detection by Public Sector Auditors. *The EDP Audit, Control and Security Newsletter, 36*(5/6), 6–15. doi:10.1080/07366980701805026

Edelhertz, H. (1970). *The nature, impact and prosecution of white-collar crime*. Washington D.C., USA: National Institute of Law Enforcement and Criminal Justice.

Eining, M.M., Jones, D.R., & Loebbecke, J.K. (1997). Reliance on decision aids: An examination of auditors' assessment of management fraud. *Auditing, 16*(2), 1–19.

Ellinor, R. (2005). Are your systems watertight? *Supply Management, 10*(23), 16.

Ellinor, R. (2009). The Fword. *Supply Management, 14*(8), 22–26.

Ericsson, K.A., & Simon, H.A. (1993). Protocol analysis: Verbal reports as data. *Psychological Review, 87(3),* 215. doi:10.1037/0033-295X.87.3.215

Erven, G.C.G.v., Holanda, M., & Carvalho, R.N. (2017). Detecting Evidence of Fraud in the Brazilian Government Using Graph Databases. Recent Advances in Information Systems and Technologies, 464–473. https://doi.org/10.1007/978-3-319-56538-5

Estévez, P.A., Held, C.M., & Perez, C.A. (2006). Subscription fraud prevention in telecommunications using fuzzy rules and neural networks. *Expert Systems with Applications, 31*(2), 337–344. doi:10.1016/j.eswa.2005.09.028

Fahland, D., & Aalst, W.M.P.v.d. (2015). Model repair—aligning process models to reality. *Information Systems, 47*, 220-243. doi:10.1016/j.is.2013.12.007

Fanning, K.M., & Cogger, K.O. (1998). Neural network detection of management fraud using published financial data. *International Journal of Intelligent Systems in Accounting, Finance and Management, 7*(1), 21–41. doi:10.1002/(SICI)1099-1174(199803)7:1<21::AID-ISAF138>3.0.CO;2-K

Fanning, K.M., Cogger, K.O., & Srivastava, R. (1995). Detection of Management Fraud: A Neural Network Approach *Intelligent Systems in Accounting, Finance and Management, 4(2),* 220–223. doi:10.1002/j.1099-1174.1995.tb00084.x

Fawcett, T., & Provost, F. (1997a). Adaptive Fraud Detection. *Data Mining and Knowledge Discovery, 1*(3), 291–316. doi:10.1023/a:1009700419189

Fawcett, T., & Provost, F. (1997b). Combining data mining and machine learning for effective fraud detection. In B. Kuipers & B. L. Webber (Red.), *Proceedings of the 14th National Conference on Artificial Intelligence* (S. 14–19).

Fawcett, T., & Provost, F. (1999). Activity Monitoring: Noticing interesting changes in behavior. In U. Fayyad, S. Chaudhuri, & D. Madigan (Red.), *Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (S. 53–62). San Diego, California, USA: ACM. doi:10.1145/312129.312195

Fazekas, M., Tóth, I. J., & King, L. P. (2016). An Objective Corruption Risk Index Using Public Procurement Data. *European Journal on Criminal Policy and Research*, 22(3), 369–397. https://doi.org/10.1007/s10610-016-9308-z

Feroz, E.H., Kwon, T.M., Pastena, V.S., & Park, K. (2000). The efficacy of red flags in predicting the SEC's targets: an artificial neural networks approach. *International Journal of Intelligent Systems in Accounting, Finance and Management, 9*(3), 145–157. doi:10.1002/1099-1174(200009)9:3<145::aid-isaf185>3.0.co;2-g

Ferwerda, J., Deleanu, I., & Unger, B. (2016). Corruption in Public Procurement: Finding the Right Indicators. *European Journal on Criminal Policy and Research*, 23(2), 245–267. https://doi.org/10.1007/s10610-016-9312-3

Ferreira, P., Alves, R., Belo, O., & Cortesão, L. (2006). Establishing Fraud Detection Patterns Based on Signatures. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, & P. Perner (Red.), *Advances in Data Mining. Applications in Medicine, Web Mining, Marketing, Image and Signal Mining: Vol. 4065 Lecture Notes in Computer Science* (S. 526–538). Berlin/Heidelberg: Deutschland: Springer- Verlag. doi:10.1007/11790853_41

Fishman, N.H. (2001). Signs of Fraud: A Case by Case Review. *The CPA Journal, 71*(3), 58–59.

Franke, M., Hoser, B., & Schröder, J. (2008). On the Analysis of Irregular Stock Market Trading Behavior. In C. Preisach, H. Burkhardt, L. Schmidt-Thieme, & R. Decker (Red.), *Data Analysis, Machine Learning and Applications. Studies in Classification, Data Analysis, and Knowledge Organization* (S. 355–362). Berlin/ Heidelberg, Deutschland: Springer-Verlag. doi:10.1007/978-3-540-78246-9_42

Frankenfield, G., & Kleiner, B.H. (2000). Effective Employment Screening Practices. *Management Research News, 23*(7/8), 24–29. doi:10.1108/01409170010782118

Fuseini, A., Wotton, S. B., Knowles, T. G., & Hadley, P. J. (2017). Halal Meat Fraud and Safety Issues in the UK: a Review in the Context of the European Union. *Food Ethics*, o. A. https://doi.org/10.1007/s41055-017-0009-1

Gao, Z., & Ye, M. (2007). A framework for data mining-based anti-money laundering research. *Journal of Money Laundering Control, 10*(2), 170–179. doi:10.1108/13685200710746875

Garner, B.A., & Black, H.C. (2004). *Black's law dictionary* (8 Aufl.). St. Paul: Thomson West.

Ghani, R., & Kumar, M. (2011). Interactive Learning for Efficiently Detecting Errors in Insurance Claims. In C. Apte, J. Ghosh, & P. Smyth (Red.), *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (S. 325–333). New York, NY, USA: ACM. doi:10.1145/2020408.2020463

Ghosh, S., & Reilly, D.L. (1994). Credit card fraud detection with a neural-network. In *Proceedings of the 27th Annual Hawaii International Conference on System Sciences* (Vol. 3, S. 621–630). Wailea, HI, USA: IEEE. doi:10.1109/HICSS.1994.323314

Glancy, F.H., & Yadav, S.B. (2011). A computational model for financial reporting fraud detection. *Decision support systems, 50*(3), 595–601. doi:10.1016/j.dss.2010.08.010

Gläser, J. & Laudel, G. (2009): *Experteninterviews und qualitative Inhaltsanalyse: als Instrumente rekonstruierender Untersuchungen*. (3. Aufl.), VS Verlag für Sozialwissenschaften, Wiesbaden, Germany 2009.

Guan, Z., Lee, S., Cuddihy, E., & Ramey, J. (2006). The validity of the stimulated retrospective think-aloud method as measured by eye tracking. *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 1253-1262. New York, USA: ACM. doi:10.1145/1124772.1124961

Goldberg, H.G., Kirkland, D., Lee, D., Shyr, P., & Thakker, D. (2003). The NASD Securities Observation, New Analysis and Regulation System (SONAR). In J. Riedl & R. W. Hill (Red.), *Proceedings of the 15th Conference on Innovative Applications of Artificial Intelligence* (S. 11–18). Acapulco, Mexico: AAAI.

Gong, T., & Zhou, N. (2015). Corruption and marketization: Formal and informal rules in Chinese public procurement. *Regulation & Governance*, 9(1), 63–76. https://doi.org/10.1111/rego.12054

Gottelt, K. (2016). *Combining Process Mining with the "red flag"approach for Fraud Detection*. Interdisziplinäres Projekt: TU-München.

Gradischnig, A. (2015). *Process Mining als Mittel zur Fraud Detection*. Master-Thesis: TU-München.

Graycar, A., & Sidebottom, A. (2012). Corruption and control: a corruption reduction approach. *Journal of Financial Crime, 19*(4), 384–399. doi:10.1108/13590791211266377

Green, B.P., & Choi, J.H. (1997). Assessing the risk of management fraud through neural network technology. *Auditing, 16*(1), 14–28.

Green, P., & Rosemann, M. (2000). Integrated Process Modeling: An Ontological Evaluation. *Information Systems, 25*(2), 73 - 87.

Greenberg, S. (1988). *Using Unix: Collected traces of 168 users*. Research Report, (88/333/45). Calgary, Canada: University of Calgary. doi:10.5072/PRISM/30806

Grieshober, W.E. (2001). Old dogs, new tricks. *Internal Auditor, 58*(4), 77–79.

Griffin, R. (2012). Using Big Data to Combat Enterprise Fraud. *Financial Executive, 28*(10), 44-47.

Grosser, H., Britos, P., & García-Martínez, R. (2005). Detecting Fraud in Mobile Telephony Using Neural Networks. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, M. Ali, & F. Esposito (Red.), *Proceedings of the 18th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems* (Vol. 3533, S. 613–615). Berlin/ Heidelberg, Deutschland: Springer-Verlag. doi:10.1007/11504894_85

Günther, C.W., & Aalst, W.M.P.v.d. (2007). Fuzzy Mining – Adaptive Process Simplification Based on Multi-perspective Metrics. In G. Alonso, P. Dadam, & M. Rosemann (Red.), *Business Process Management* (Vol. 4714, S. 328–343). Berlin/Heidelberg, Deutschland: Springer-Verlag. doi:10.1007/978-3-540-75183-0_24

Günther, C.W., & Rozinat, A. (2012). Disco: Discover Your Processes. *BPM, 940*, 40-44.

Gupta, E. (2014). Process Mining A Comparative Study. *International Journal of Advanced Research in Computer and Communication Engineering, 3*(11), 8594-8598.

Hall, J. A. (2011). *Accounting Information Systems* (7 Aufl.). Mason, USA: Cengage Learning.

Handfield, R.B., & Baumer, D.L. (2006). Managing Conflict of Interest Issues in Purchasing. *Journal of Supply Chain Management, 42*(3), 41–50. doi:10.1111/j.1745-493X.2006.00016.x

Hansen, J.V., McDonald, J.B., Messier, W.F., & Bell, T.B. (1996). A Generalized Qualitative-response Model and the Analysis of Management Fraud. *Management Science, 42*(7), 1022–1032. doi:10.1287/mnsc.42.7.1022

Hassibi, K. (2000). Detecting payment card fraud with neural networks. In P. J. G. Lisboa, A. Vellido, & B. Edisbury (Red.), *Business Applications of Neural Networks* (S. 141–157). Singapore: World Scientific.

Hatchett, S. (2014, Juli 2018). bits of SoftWx: Optimizing the Levenshtein Algorithm in TSQL. Zugegriffen von http://blog.softwx.net/2014/12/optimizing-levenshtein-algorithm-in-tsql.html

Hawkins, S., He, H., Williams, G., & Baxter, R. (2006). Outlier Detection Using Replicator Neural Networks. In Y. Kambayashi, W. Winiwarter, & M. Arikawa (Red.), *Data Warehousing and Knowledge Discovery* (Vol. 2454, S. 170–180). Berlin/Heidelberg, Deutschland: Springer-Verlag. doi:10.1007/3-540-46145-0_17

He, H., Graco, W., & Yao, X. (1999). Application of Genetic Algorithm and k-Nearest Neighbour Method in Medical Fraud Detection. In B. McKay, X. Yao, C. S. Newton, J.-H. Kim, & T. Furuhashi (Red.), *Proceedings of the 2nd Asia-Pacific Conference on Simulated Evolution and Learning* (Vol. 1585, S. 74–81). Berlin/Heidelberg, Deutschland: Springer-Verlag. doi:10.1007/3-540-48873-1_11

He, H., Wang, J., Graco, W., & Hawkins, S. (1997). Application of neural networks to detection of medical fraud. *Expert Systems with Applications, 13*(4), 329–336. doi:10.1016/s0957-4174(97)00045-6

Helmkamp, J., Ball, R. & Townsend, K. (1996). Definitional Dilemma:Can and Should There Be a universal Definition of White Collar Crime? Paper presented at the Acedemic Workshop, Morgantown (USA). Abgerufen von https://www.ncjrs.gov/pdffiles1/Digitization/166244NCJRS.pdf

Henderson, W. T. (2011). Building an Effective and Cost-Efficient Anti-Corruption Program. *Corporate Finance Review, 16*(1), 11–18.

Henselmann, K., & Hofmann, S. (2010). *Accounting Fraud: Case Studies and Practical Implications.* Erich Schmidt Verlag.

Hevner, A.R., March, S.T., Park, J., & Ram, S. (2004b). Design Science in Information Systems Research. *MIS quarterly, 28*(1), 75-105. doi:10.2307/25148625

Hofmann, S. (2008). *Handbuch Anti-Fraud-Management: Bilanzbetrug erkennen - vorbeugen - bekämpfen* (Vol. 1). Berlin: Erich Schmidt Verlag.

Hogan, C. E., Rezaee, Z., Riley, R. A., & Velury, U. K. (2008). Financial Statement Fraud: Insights from the Academic Literature. *Auditing: A Journal of Practice & Theory, 27*(2), 231–252. doi:10.2308/aud.2008.27.2.231

Hollinger, R.C., & Clark, J.P. (1983). Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft. *Social Forces, 62*(2), 398–418. doi:10.1093/sf/62.2.398

Holsbeck, M.v., Canter, R., Johnson, J.Z., & Taylor, P. (2008). The Cure to the Cancer We Know as Fraud. *Internal Auditing, 23*(3), 3–8.

Hopwood, W., Leiner, J., & Young, G. (2007). *Forensic Accounting and Fraud Examination.* (2. Aufl.). New York, USA: McGraw-Hill Companies Inc.

Horne, J., Lochner, H., & Ventner, J. The Red Flag System as the Gatekeeper in Tender Fraud Prevention and Detection of Misrepresentation. *International Journal of African Renaissance Studies,* 13(1), 129-143. doi: 10.1080/18186874.2018.1478655

Hudon, P., & Garzón, C. (2016). Corruption in public procurement: entrepreneurial coali-tion building. *Crime, Law and Social Change*, 66(3), 291–311. https://doi.org/10.1007/s10611-016-9628-

IAASB - The International Auditing and Assurance Standards Board. (2009, 2018/7/10). International Standard on Auditing (ISA) 240: The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements , S. 155–197. Abgerufen von http://www.ifac.org/system/files/downloads/a012-2010-iaasb-handbook-isa-240.pdf

IIA – The Institute of Internat Auditors (2012). International Standards for the Professional Practice of Internal Auditing. Abgerufen von http://www.theiia.org/

IMF, International Monetary Fund. (2016, 2018/7/10). World Economic Outlook-Too Slow for Too Long: Transition and Tension Abgerufen von https://www.imf.org/external/pubs/ft/weo/2016/01/pdf/text.pdf

Imoniana, J.O., Antunes, M.T.P., & Formigoni, H. (2013). The Forensic Accounting and Corporate Fraud. *Journal of Information Systems and Technology Management, 10*(1), 119–144. doi:10.1590/S1807-17752013000100008

Islam, A.K, Corney, M., Mohay, G., Clark, A., Bracher, S., Raub, T., & Flegel, U. (2011). Detecting collusive fraud in enterprise resource planning systems. In K. Rannenberg, J. Sakarovitch, M. Goedicke, A. Tatnall, E. J. Neuhold, A. Pras, F. Tröltzsch, J. Pries-Heje, D. Whitehouse, R. Reis, S. Furnell, U. Furbach, M. Winckler, M. Rauterberg, *IFIP Advances in Information and Communication Technology* (Vol. 361, S. 143-153): Berlin/Heidelber, Deutschland: Springer-Verlag. doi:10.1007/978-3-642-24212-0_11

Islam, A.K., Corney, M.W., Mohay, G.M., Clark, A.J., Bracher, S., Raub, T., & Flegel, U. (2010). Fraud detection in ERP systems using scenario matching. In K. Rannenberg. V. Varadharajan, C. Weber (Red.) *Security and Privacy - Silver Linings in the Cloud* (Vol. 330, S. 112-123). Berlin/Heidelberg: Springer-Verlag. doi:10.1007/978-3-642-15257-3_11

Jaeger, J. (2009). Internal Investigations 101: A Step-by-Step Guide. *Compliance Week, 6*(71), 58–59,73.

Jaeger, J. (2011). Procurement, Compliance Team Up to Fight Fraud. *Compliance Week, 8*(94), 48–49,72.

Jans, M., Alles, M., & Vasarhelyi, M. (2010). Process mining of event logs in auditing: Opportunities and challenges. *International Symposium on Accounting Information Systems*, 1-32. doi:10.2139/ssrn.1578912

Jans, M., Alles, M., & Vasarhelyi, M. (2012a). Process Mining of Event Logs in Auditing: A Field Study of Procurement at a Global Bank. *Proceedings of the 9th International Conference on Enterprise Systems, Accounting and Logistics*, Crete, Griechenland.

Jans, M., Alles, M.G., & Vasarhelyi, M.A. (2012b). Process Mining of Event Logs in Internal Auditing: A Case Study. *European Accounting Association*, 1-26, Ljubljana, Slovenia.

Jans, M., Alles, M.G., & Vasarhelyi, M.A. (2014). A Field Study on the Use of Process Mining of Event Logs as an Analytical Procedure in Auditing. *The Accounting Review, 89*(5), 1751-1773. doi:10.2308/accr-50807

Jans, M., Depaire, B., & Vanhoof, K. (2011). Does Process Mining Add to Internal Auditing? An Experience Report. In T Halpin, S. Nurcan, J. Krogstie, P. Soffer, E. Proper, R. Schmidt, I. Bider (Red.), *Enterprise, Business-Process and Information Systems Modeling* (Vol. 81, S.31-45), Berlin/Heidelberg, Deutschland: Springer-Verlag. doi:10.1007/978-3-642-21759-3_3

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

Jans, M., Lybaert, N., Vanhoof, K., & Werf, J.M.v.d. (2008). Business process mining for internal fraud risk reduction: Results of a case study. *Proceedings of the 2008 International Symposium on Accounting Information Systems* (S.1-27).

Jans, M., Werf, J. M. v. d., Lybaert, N., & Vanhoof, K. (2011). A business process mining application for internal transaction fraud mitigation. *Expert Systems with Applications, 38*(10), 13351–13359. doi:10.1016/j.eswa.2011.04.159

Jensen, M.C., & Meckling, W.H. (1976). Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. *Journal of Financial Economics, 3*(4), 305–360. doi:10.1016/0304-405x(76)90026-x

Johnson, L.R., & Rudolph, H.R. (2009). Cash Buyer Beware! *Journal of Corporate Accounting and Finance, 21*(1), 33–39. doi:10.1002/jcaf.20544

Jonas, J., Pattak, P.B., & Litchko, J.P. (2001). Using Advanced Information Technology to Combat Insider Threats. *Global Business and Organizational Excellence, 20*(4), 19–27. doi:10.1002/npr.1103

Kahneman, D., & Lovallo, D. (1993). Timid Choices and Bold Forecasts: A Cognitive Perspective on Risk Taking. Management Science , 39(1), 17–31.

Kayrak, M. (2008). Evolving challenges for supreme audit institutions in struggling with corruption. *Journal of Financial Crime, 15*(1), 60–70. doi:10.1108/13590790810841707

Kedia, S., & Philippon, T. (2009). The Economics of Fraudulent Accounting. *Review of Financial Studies, 22*(6), 2169–2199. doi:10.1093/rfs/hhm016

Kemper, A., & Eickler, A. (2011). *Datenbanksysteme. Eine Einführung.* (Vol. 8). Oldenbourg: Oldenbourg Verlag.

Khan, R., Corney, M., Clark, A., & Mohay, G. (2010). Transaction Mining for Fraud Detection in ERP Systems. *Industrial Engineering and Management Systems, 9*(2), 141-156. doi: 10.7232/iems.2010.9.2.141

Klein, C. T., & Helweg-Larsen, M. (2002). Perceived Control and the Optimistic Bias: A Meta-Analytic Review. *Psychology & Health*, 17(4), 437–446. doi:10.1080/0887044022000004920

Kohler, J. C., Mitsakakis, N., Saadat, F., Byng, D., & Martinez, M. G. (2015). Does Pharmaceutical Pricing Transparency Matter? Examining Brazil's Public Procurement System. *Globalization and Health*, 11(34), 1–13. https://doi.org/10.1186/s12992-015-0118-8

Kotsiantis, S., Koumanakos, E., Tzelepis, D., & Tampakas, V. (2006). Forecasting Fraudulent Financial Statements using Data Mining. *International Journal of Computational Intelligence (IJCI), 3*(2), 104–110.

Kou, Y., Lu, C.-T., Sirwongwattana, S., & Huang, Y.-P. (2004). Survey of fraud detection techniques. *Networking, Sensing and Control*, 2, 749-754. doi:10.1109/ICNSC.2004.1297040

KPMG. (2011). Who is the typical Fraudster. KPMG analysis of global patterns of fraud. Abgerufen von https://www.ub.unibas.ch/digi/a125/sachdok/2011/BAU_1_5663361.pdf

KPMG. (2013a). Global profile of the fraudster: White-collar crime - present and future. Abgerufen von https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2017/01/global-profiles-of-the-fraudster-v2.pdf

KPMG. (2013b). Integrity Survey 2013. Abgerufen von http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/ https://assets.kpmg.com/content/dam/kpmg/pdf/2013/08/Integrity-Survey-2013-O-201307.pdf

Kranacher, M.-J. (2008). How Many [Fill in the Blank] Does It Take to Change ... ? *The CPA Journal, 78*(2), 80.

Kranacher, M.-J., Riley, R.A., & Wells, J.T. (2011). *Forensic Accounting and Fraud Examination*. Hoboken, USA: John Wiley & Sons.

Kroll. (2011). *Global Fraud Report: Economist Intelligence Unit Survey Results*. Kroll Advisory Solutions. Abgerufen von http://fraud.kroll.com/wp-content/uploads/2013/10/FraudReport_2011-2012.pdf

Kroll. (2012). *Global Fraud Report 2012/13: Economist Intelligence Unit Survey Results*. Kroll Advisory Solutions. Abgerufen von http://www.managementthinking.eiu.com/sites/default/files/downloads/KRL_FraudReport2012-13%20FINALpdf.pdf

Kroll. (2013). *2013/2014 Global Fraud Report: Who's got something to hide?* Kroll Advisory Solutions. Abgerufen von http://fraud.kroll.com/wp-content/uploads/2013/10/Kroll-Global-Fraud-Report-2013-2014-WEB.pdf

Kroll. (2015). *2015/2016 Global Fraud Report: Economist Intelligence Unit Survey Results*. Kroll Advisory Solutions. Abgerufen von http://anticorruzione.eu/wp-content/uploads/2015/09/Kroll_Global_Fraud_Report_2015low-copia.pdf

Kroll. (2017). *2017/2018 Global Fraud Report: Forging New Paths in Times of Uncertainty*. Kroll Advisory Solutions. Abgerufen von https://www.kroll.com/en-us/global-fraud-and-risk-report-2018

Laleh, N., & Azgomi, M.A. (2009). A Taxonomy of Frauds and Fraud Detection Techniques. In S. K. Prasad, S. Routray, R. Khurana, & S. Sahni (Red.), *Information Systems, Technology and Management* (Vol. 31, S. 256–267). Berlin/Heidelberg, Deutschland: Springer-Verlag. doi:10.1007/978-3-642-00405-6_28

Lambert-Mogiliansky, A., & Sonin, K. (2006). Collusive Market Sharing and Corruption in Procurement. *Journal of Economics & Management Strategy, 15*(4), 883–908. doi:10.1111/j.1530-9134.2006.00121.x

Lander, G.H., Kimball, V.J., & Martyn, K.A. (2008). Government Procurement Fraud. *The CPA Journal, 78*(2), 16–22,24.

Langley, A.M. (2003). Phantom Vendors: using a fictitious payment scheme, one employee manages to fluff his nest with company funds. *Internal Auditor, 60*(4), 91-93.

Lanza, B.R.B., & Wells, J.T. (2003). *Proactively Detecting Occupational Fraud Using Computer Audit Reports.* The IIA Research Foundation.

Larsen, M., & Myers, M. (1999). When success turns into failure: a package-driven business process re-engineering project in the financial services industry. *The Journal of Strategic Information Systems, 8*(4), 395-417. doi:10.1016/S0963-8687(00)00025-1

LaSalle, R. E. (2007). Effects of the fraud triangle on students' risk assessments. *Journal of Accounting Education, 25*(1-2), 74–87. doi:10.1016/j.jaccedu.2007.03.002

Lebherz, J. (2014). Leveraging In-Memory Process Mining For Real Time Fraud Detection. (Masterarbeit): TU München.

Lehman, M.W. (2008). Join the Hunt. *Journal of Accountancy, 206*(3), 46–49,12.

Lehman, M.W., & Weidenmier, M.L. (2005). Detecting Occupational Fraud: Billing Schemes. *The CPA Journal, 75*(4), 58–61.

Leinicke, L.M., Ostrosky, J.A., Rexroad, W.M., Baker, J.R., & Beckman, S. (2005). Interviewing as an Auditing Tool. *The CPA Journal, 75*(2), 34–38.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology and Criminal Justice, 8*(4), 389–419. doi:10.1177/1748895808096470

Levi, M. (2010). Hitting the suite spot: sentencing frauds. *Journal of Financial Crime, 17*(1), 116–132. doi:10.1108/13590791011009400

Levi, M., & Burrows, J. (2007). Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey. *British Journal of Criminology, 48*(3), 293–318. doi:10.1093/bjc/azn001

Lewis, C., Rieman J. (1994): Task-Centered User Interface Design: A Practical Introduction. University of Colorado, Boulder. (http://www.hcibib.org/tcuid/).

Lim, T.-S., Loh, W.-Y., & Shih, Y.-S. (2000). A Comparison of Prediction Accuracy, Complexity, and Training Time of Thirty-three Old and New Classification Algorithms. *Machine Learning, 40*(3), 203–228. doi:10.1023/a:1007608224229

Lin, J.W., Hwang, M.I., & Becker, J.D. (2003). A fuzzy neural networks for assessing the risk of fraudulent financial reporting. *Managerial Auditing Journal, 18*(8), 657–665. doi:10.1108/02686900310495151

Liou, F.-M. (2008). Fraudulent financial reporting detection and business failure prediction models: a comparison. *Managerial Auditing Journal, 23*(7), 650–662. doi:10.1108/02686900810890625

Little, A., & Best, P.J. (2003). A framework for separation of duties in an SAP R/3 environment. *Managerial Auditing Journal, 18*(5), 419-430. doi:10.1108/02686900310476882

Lord, A. . (2010). The Prevalence of Fraud: What Should We, as Academics, Be Doing to Address the Problem? *Accounting and Management Information Systems, 9*(1), 4–21.

Lu, F., Boritz, J.E., & Covvey, D. (2006). Adaptive Fraud Detection Using Benford's Law. In L. Lamontagne, M. Marchand (Red.), *Advances in Artificial Intelligence* (Vol:4013, S. 347–358). Berlin/Heidelberg, Deutschland: Springer Verlag. http://doi.org/10.1007/11766247_30

Luell, J. (2010). *Employee fraud detection under real world conditions.* Doctoral dissertation, University of Zurich, Zurich.

Lundin, E., Kvarnström, H., & Jonsson, E. (2002). A Synthetic Fraud Data Generation Methodology. In R. Deng, F. Bao, J. Zhou, & S. Qing (Red.), *Information and Communications Security* (Vol. 2513, S. 265-277). Berlin/Heidelberg, Deutschland: Springer Verlag. doi:10.1007/3-540-36159-6_23

March, S.T., & Smith, G.F. (1995). Design and natural science research on information technology. *Decision support systems, 15*(4), 251-266. doi:10.1016/0167-9236(94)00041-2

Mardani, S., & Shahriari, H.R. (2013). A New Method for Occupational Fraud Detection in Process Aware Information Systems. *Proceedings of the National ISC Conference on Information Security and Cryptology (ISCISC)*, 1-5. doi:10.1109/ISCISC.2013.6767348

Maxion, R.A., & Tan, K.M. (2000). Benchmarking anomaly-based detection systems. In *Proceedings of the Dependable Systems and Networks*, (S. 623-630). *DSN 2000*. New York, USA: IEEE. doi:10.1109/ICDSN.2000.857599

May, C. A. (2005). Go Forth Without Fraud. *Security Management, 49*(6), 117–121.

McNamee, L. (2016). Procurement Fraud. *Economic Crime Forensics Capstones*, 1–31.

McNeal, A. (2012). What's Your Fraud IQ? *Journal of Accountancy, 214*(6), 42–46,48.

Meiners, C. (2005). Detecting and Eliminating the Unintentional Perk. *Risk Management, 52*(4), 50–52,54.

Mercuri, R.T. (2003). On Auditing Audit Trails. *Communications of the ACM, 46*(1), 17-20. doi:10.1145/602421.602436

Merton, R.K. (1938). Social Structure and Anomie. *American Sociological Review, 3*(5), 672. doi:10.2307/2084686

Messner, S. F., & Rosenfeld, R. (1994). *Crime and the American Dream* (1. Aufl.). Belmont, USA: Cengage Learning.

Moeller, R.R. (2011). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes* (2. Aufl.). Hoboken, USA: John Wiley & Sons.

Mooney, J.L., Harrell, H.W., & Ludwig, S.E. (2000). Audit Software that Helps Your Company Stop Fraud. *Journal of Corporate Accounting and Finance, 11*(4), 17–23. doi:10.1002/1097-0053(200005/06)11:4<17::AID-JCAF4>3.0.CO;2-C

Morehead, W.A. (2007). *Internal Control and Governance in Non-Governmental Organizations Designed to Provide Accountability and Deter, Prevent and Detect Fraud and Corruption.* (Dissertation), The University of Southern Mississippi.

Muehlmann, B.W., Burnaby, P.A., & Howe, M.A. (2010). Internal Auditors' Role in Finding Corruption. *Internal Auditing, 25*(5), 8–16.

Muthukrishnan, R.C.A., Chandrasekaran, M., & Upadhyaya, S. (2004). RACOON: rapidly generating user command data for anomaly detection from customizable template. *Paper presented at the Annual Computer Security Applications Conference*, 189-202, Tucson, Arizona. doi:10.1109/CSAC.2004.28

Myka, A., & Güntzer, U. (1996). Fuzzy Full-Text Searches in OCR Databases. In *Digital Libraries Research and Technology Advances* (Bd. 25, S. 131–145). Berlin, Heidelberg: Springer.

Nag, B. (2015). Combating Corruption in Indian Public Procurement – Some Exploratory Case Studies. *The Journal of Institute of Public Enterprise*, 38(1/2), 1–34.

Nanang, H., & Misman, A. F. (2016). Certificate-based strategy to Auction Model for E-Procurement in Indonesia: A review on local ethics and the future challenges. In *2016 6th International Conference on Information and Communication Technology for The Muslim World* (ICT4M) (S. 41–46). IEEE. https://doi.org/10.1109/ICT4M.2016.20

Newell, A., & Simon, H.A. (1972). *Human problem solving* (Vol. 104, No. 9). Englewood Cliffs, NJ, USA: Prentice-Hall.

Ngai, E.W.T., Hu, Y., Wong, Y.H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision support systems, 50*(3), 559–569. doi:10.1016/j.dss.2010.08.006

Nguyen, A. (2005). *Interorganizational Favor Exchange. Definition, Types, and Outcomes.* York University (Canada).

Nilsen, K. (2010). Keeping Fraud in the Cross Hairs. *Journal of Accountancy, 209*(6), 20–24.

Nisbet, R.A., Elder, J.F., & Miner, G. (2009). *Handbook of Statistical Analysis & Data Mining Applications*. Amsterdam, Niederlande; Boston, USA: Elsevier.

Odenthal, R. (2009). *Korruption und Mitarbeiterkriminalität: Wirtschaftskriminalität vorbeugen, erkennen und aufdecken* (2. Aufl.). Wiesbaden, Deutschland: Gabler.

Okrent, M. D., & Vokurka, R. J. (2004). Process mapping in successful ERP implementations. *Industrial Management & Data Systems, 104*(8), 637–643. doi:10.1108/02635570410561618

OMG (2013, July 2018). Business Process Model and Notation. Abgerufen von http://www.omg.org/spec/BPMN/2.0.1/PDF/

Pacini, C., & Brody, R.G. (2005). A Proactive Approach to Combating Fraud. *Internal Auditor, 62*(2), 56–61.

Pang, C., Dharmasthira, Y., Eschinger, C., Motoyoshi, K., & Brant, K.F. (2013, 2013/05/07). Market Share Analysis: ERP Software, Worldwide, 2012. Abgerufen von https://www.gartner.com/doc/2477517

Paper, D.J., Rodger, J.A., & Pendharkar, P.C. (2001). A BPR case study at Honeywell. *Business Process Management Journal, 7 (2)*, 85-99. doi:10.1108/14637150110389416

Pedneault, S. (2009). *Fraud 101: Techniques and Strategies for Understanding Fraud* (3. Aufl.). Hoboken, USA: John Wiley & Sons.

Pejic-Bach, M. (2010). Profiling Intelligent Systems Applications in Fraud Detection and Prevention: Survey of Research Articles. In D. Al-Dabass, A. Pantelous, H. Tawfik, & A. Abraham (Red.), *2010 International Conference on Intelligent Systems, Modelling and Simulation* (S. 80–85). Liverpool, UK: IEEE. doi:10.1109/ISMS.2010.26

Perols, J. (2011). Financial Statement Fraud Detection: An Analysis of Statistical and Machine Learning Algorithms. *Auditing: A Journal of Practice & Theory, 30*(2), 19–50. doi:10.2308/ajpt-50009

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A Comprehensive Survey of Data Mining-based Fraud Detection Research. *Artificial Intelligence Review*, abs/1009.6119, 1-14. doi:10.1016/j.chb.2012.01.002

Plattner, H., & Zeier, A. (2012). *In-Memory Data Management: Technology and Applications* (2 ed.). Heidelberg, Deutschland; New York, USA: Springer.

Porter, M.E. (1998). *Competitive Advantage: Creating and Sustaining Superior Performance*. New York, USA: Free Press.

Prenzler, T. (2009, 2018/07/08). Preventing burglary in commercial and institutioal settings - A Place Management and Partnerships. ASIS Foundation. Washington D.C., VA, USA. Abgerufen von http://www.popcenter.org/library/crisp/commercial-burglary.pdf

Pulliam, S. (2003, 2018/07/08). Ordered to Commit Fraud, A Staffer Balked, Then Caved. Abgerufen von http://online.wsj.com/news/articles/SB105631811322355600

PWC. (2016, 2018/07/08). Global Economic Crime Survey 2016: Adjusting the Lens on Economic Crime: Preparation brings opportunity back into focus. Abgerufen von http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html

Quah, J.T.S., & Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. *Expert Systems with Applications, 35*(4), 1721–1732. doi:10.1016/j.eswa.2007.08.093

Rahmani, T., & Koohshahi, N. M. (2015). Legal Analysis of Procurement Corruption in Iran Economy. *International Journal of Management, Accounting and Economics*, 2(12), 1484–1496.

Ramamoorti, S., & Curtis, S. (2003). Procurement Fraud & Data Analytics. *The Journal of Government Financial Management, 52*(4), 16–24.

Ramberg J. (2010). ICC Guide to Incoterms 2010: Understanding and practical use. Paris (France): ICC Publishing. Abgerufen von http://halleycables.com/img/cms/INCOTERMS%202010%20Guide.pdf

Ravisankar, P., Ravi, V., Raghava Rao, G., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. *Decision support systems, 50*(2), 491–500. doi:10.1016/j.dss.2010.11.006

Rendon, J. M., & Rendon, R. G. (2016). Procurement fraud in the US Department of De-fense: Implications for contracting processes and internal controls. *Managerial Audit-ing Journal*, 31(6/7), 748–767. https://doi.org/10.1108/MAJ-11-2015-1267

Roberts, R.N. (2010). Mandatory Contractor Codes of Ethics and Defense Procurement Integrity. *Journal of Public Procurement, 10*(2), 247–274. doi:10.1108/JOPP-10-02-2010-B004

Romney, M.B., & Steinbart, P.J. (2012). *Accounting Information Systems* (12. Aufl.). Boston, USA: Pearson.

Rozinat, A. (2014, 2018/7/8). Disco User's Guide. Abgerufen von https://fluxicon.com/disco/files/Disco-User-Guide.pdf

Rozinat, A., & Aalst, W.M.P.v.d. (2006). Conformance Testing: Measuring the Fit and Appropriateness of Event Logs and Process Models. In C.J. Bussler, A. Haller (Red.) *Business Process Management Workshops* (Vol. 3812, S. 163-176). Berlin/Heidelberg, Deutschland: Springer-Verlag. doi:10.1007/11678564_15

Rozinat, A., & Aalst, W.M.P.v.d. (2008). Conformance checking of processes based on monitoring real behavior. *Information Systems, 33*(1), 64-95. doi:10.1016/j.is.2007.07.001

Rozinat, A., Jong, I.S.M.d., Guenther, C.W., & Aalst, W.M.P.v.d. (2007). *Process Mining of Test Processes: A Case Study*. BETA Working Paper Series, WP 220, Eindhoven University of Technology, Eindhoven.

Rozinat, A., Medeiros, A.K.A.d., Günther, C.W., Weijters, A.J.M.M., & Aalst, W.M.P.v.d. (2008). The Need for a Process Mining Evaluation Framework in Research and Practice. In A. Hofstede, B. Benatallah, & H.-Y. Paik (Red.), *Business Process Management Workshops* (Vol. 4928, S. 84–89). Berlin/Heidelberg, Deutschland: Springer-Verlag. doi:10.1007/978-3-540-78238-4_10

Sabau, A.S. (2012). Survey of Clustering based Financial Fraud Detection Research. *Informatica Economică, 16*(1), 110–122.

Sammons, P. (2005). Forbidden fruit. *Supply Management, 10*(8), 22–23,25-26.

SAP. (2013a, 2018/7/8). SAP at a Glance: Capital Market Information. Abgerufen von http://global.sap.com/corporate-en/investors/pdf/SAP-Fact-Sheet-EN.pdf

SAP. (2013b, 2018/7/8). Sperren von Rechnungen. Abgerufen von http://help.sap.com/saphelp_erp60_sp/helpdata/de/a8/b99539452b11d189430000e829fbbd/content.htm

SAP. (2014, 2018/7/8). SAP Kundenkontrakt. Abgerufen von http://help.sap.com/saphelp_erp60_sp/helpdata/de/dd/55fd53545a11d1a7020000e829fd11/content.htm24

Saravanan, M. S., & Rama Sree, R.J. (2011). A Role of Heuristics Miner Algorithm in the Business Process System. *International Journal of Computer Technology and Applications, 2*(2), 340-344.

Sarker, S., & Lee, A. (1999). IT-enabled organizational transformation: a case study of BPR failure at TELECO. *The Journal of Strategic Information Systems, 8*(1), 83-103. doi:10.1016/S0963-8687(99)00015-3

Schermann, M., & Boss, S. R. (2014). The White-Collar Hacking Contest: A Novel Approach to Teach Forensic Investigations in a Digital World. In A. Vance, R. Raghav, J. Allen. *Proceedings of 2014 IFIP 8.11/11.13 Dewald Roode Information Security*. Newcastle, England.

Scholl, A. (2009): *Die Befragung*. (2. Aufl.), UVK Verlagsgesellschaft, Konstanz, Deutschland 2009.

Schonlau, M. (1998, 2018/7/10). Masquerading User Data. Abgerufen von http://www.schonlau.net/intrusion.html

Schumann, H., & Müller, W. (2000). *Visualisierung - Grundlagen und allgemeine Methoden*. Berlin/Heidelberg, Deutschland: Springer Verlag.

Seetharaman, A., Senthilvelmurugan, M., & Periyanayagam, R. (2004). Anatomy of computer accounting frauds. *Managerial Auditing Journal, 19*(8), 1055–1072. doi:10.1108/02686900410557953

SFO, (2014, 2018/7/10). Taxonomy of Fraud. Abgerufen von http://www.sfo.gov.uk/taxonomy.swf

Sharma, A., & Panigrahi, P. K. (2012). A Review of Financial Accounting Fraud Detection based on Data Mining Techniques. *International Journal of Computer Applications, 39*(1), 37–47. doi:10.5120/4787-7016

Sheskin, D. J. (2003). *Handbook of Parametric and Nonparametric Statistical Procedures* (5. Aufl.). Boca Raton, USA: Chapman and Hall.

Sikka, P. (2008). Enterprise culture and accountancy firms: new masters of the universe. *Accounting, Auditing and Accountability Journal, 21*(2), 268–295. doi:10.1108/09513570810854437

Silver, B. (2011). *BPMN Method and Style with BPMN Implementer's Guide: A Structured Approach for Business Process Modeling and Implementation Using BPMN 2.0* (2. Aufl.). Aptos, USA: Cody-Cassidy.

Silverstone, H., & Sheetz, M. (2007). *Forensic Accounting and Fraud Investigation for Non-Experts* (2. Aufl). Hoboken, USA: John Wiley & Sons..

Simon, D.R., & Eitzen, D.S. (1982). *Elite deviance*. Boston, USA: Allyn and Bacon.

Singh, K., Best, P., & Mula, J. (2013). Automating Vendor Fraud Detection in Enterprise Systems. *The Journal of Digital Forensics, Security and Law, 8*(2), 7-42. doi:10.15394/jdfsl.2013.1142

Singh, K., Best, P.J., Bojilov, M., & Blunt, C. (2013). Continuous auditing and continuous monitoring in ERP environments: case studies of application implementations. *Journal of Information Systems, 28*(1), 287-310. doi:10.2308/isys-50679

Singh, N. (2012, 2018/7/10). Vendor Account Clearing in SAP T code - F-44 Abgerufen von http://stabnet.blogspot.de/2012/05/vendor-account-clearing-in-sap-t-code-f.html

Song, M., & Aalst, W.M.P.v.d. (2007). Supporting process mining by showing events at a glance. In *Proceedings of the 17th Annual Workshop on Information Technologies and Systems (WITS)* (S. 139-145).

Song, Y. (2008). *Three Essays on Corruption and Competition.* (Dissertation), Indiana University.

Stamler, R.T., Marschdorf, H.J., & Possamai, M. (2014). *Fraud Prevention and Detection: Warning Signs and the Red Flag System*. Boca Raton, USA: Taylor & Francis Inc.

Stierle (2015): Celonis Data Scientist Training, Celonis GmbH.

Strand, C.A., Judd, S.L., & Lancaster, K. (2002). Training: A powerful way to prevent fraud. *Strategic Finance, 84*(4), 28–32.

Strand, C. A., Nowlin, T. S., & Wier, B. (2003). Will you detect fraud if you think you can? *Internal Auditing, 18*(4), 34–38.

Strand, C.A., Welch, S.T., Holmes, S.A., & Strawser, R.H. (2000). Are your vendors stealing from you? *Strategic Finance, 82*(4), 66–71.

Sudjianto, A., Yuan, M., Kern, D., Nair, S., Zhang, A., & Cela-Díaz, F. (2010). Statistical Methods for Fighting Financial Crimes. *Technometrics, 52*(1), 5–19. doi:10.1198/TECH.2010.07032

Sutherland, E.H. (1940). White-Collar Criminality. *American Sociological Review, 5*(1), 1–12. doi:10.2307/2083937

Sutherland, E.H. (1949). *White collar crime*. New York, USA: Dryden Press.

Sutherland, E.H. (1983). *White collar crime: the uncut version*. London, UK: Yale University Press.

Tabuena, J. (2008). Advice for a Successful Conflict-of-Interest Audit. *Compliance Week, 5*(59), 36–37.

Tabuena, J. (2010). Techniques to Stamp Out Procurement Fraud. *Compliance Week, 7*(73), 34–35.

Tackett, J.A. (2010). Bribery and Corruption. *Journal of Corporate Accounting and Finance, 21*(4), 5–9. doi:10.1002/jcaf.20589

Taylor, P. (2004). Inside Threads: System-Based Fraud, Errors, and Misuse. *Internal Auditing, 19*(5), 3–11.

Taylor, P. (2006). Driving Financial Process Improvements. *Strategic Finance, 87*(7), 52–55.

Thai, K.V. (2001). Public Procurement Re-Examined. *Journal of Public Procurement, 1*(1), 9–50. doi:10.1108/JOPP-01-01-2001-B001

Thompson, C. (2000). Whose Mercedes is that? *Internal Auditor, 57*(1), 61–63.

Tran, N.A. (2009). *Corruption, Ranking and Competition.* (Dissertation), Harvard University.

Ulinski, M., Girasa, R.J., & Fanelli, A.L. (2013). Illegal Corporate Activities and Their Effect on Financial Statement Disclosures: How Forensic Accountants Can Help. *The Journal of American Business Review, Cambridge, 2*(1), 72–78.

Vanderfeesten, I. (2004). *Designing workflow systems. An algorithmic approach to process design and a human oriented approach to process automation.* (Masterarbeit), Technische Universiteit Eindhoven, Eindhoven.

Verick, P. (2013). Addressing Dynamic Threats of Fraud. *Financial Executive, 29*(5), 46–49.

Viaene, S., Derrig, R.A., & Dedene, G. (2003). MLP-ARD vs. logistic regression and C4. 5 for PIP claim fraud explication. *Insurance Mathematics & Economics, 32*(1), 154.

Viaene, S., Derrig, R.A., Baesens, B., & Dedene, G. (2002). A comparison of state-of-the-art classification techniques for expert automobile insurance claim fraud detection. *Journal of Risk and Insurance, 69*(3), 373–421. doi:10.1111/1539-6975.00023

Vitell, S.J., Dickerson, E.B., & Festervand, T.A. (2000). Ethical Problems, Conflicts and Beliefs of Small Business Professionals. *Journal of Business Ethics, 28*(1), 15–24. doi:10.1023/a:1006217129077

Viton, P.L. (2003). Creating Fraud Awareness. *SAM Advanced Management Journal, 68*(3), 20–43.

Vona, L.W. (2011). *The Fraud Audit: Responding to the Risk of Fraud in Core Business Systems*. Hoboken, USA: John Wiley & Sons.

Vona, L.W. (2017). *Fraud Data Analytics for Corruption Occurring in the Procurement Process*. In Fraud Data Analytics Methodology: The fraud scenario approach to uncovering fraud in core business systems. Hoboken, USA: John Wiley & Sons, Inc.

Wagner, C. (2014). *Spezifikation und Implementierung eines Big-Data-Generators zur Simulation betrügerischen Verhaltens im SAP-Einkaufsprozess* (Masterarbeit). TU München.

Wang, S. (2010). A Comprehensive Survey of Data Mining-Based Accounting-Fraud Detection Research. In Z. Hou & Y. Wu (Red.), *2010 International Conference on Intelligent Computation Technology and Automation* (S. 50–53). Piscataway, USA: IEEE Press. doi:10.1109/ICICTA.2010.831

Warfel, T. Z. (2009). *Prototyping: A Practitioner's Guide*. New York, NY, USA: Rosenfeld Media.

Webster, J., & Watson, R.T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *Management Information Systems Quarterly, 26*(2), xiii–xxiii.

Weerdt, J.d., Backer, M.d., Vanthienen, J., & Baesens, B. (2012). A multi-dimensional quality assessment of state-of-the-art process discovery algorithms using real-life event logs. *Information Systems, 37*(7), 654–676. doi:10.1016/j.is.2012.02.004

Wegelin, M., & Englbrecht, M. (2009). *SAP-Schnittstellenprogrammierung*. Bonn, Deutschland: Galileo Press.

Weijters, A.J.M.M & Aalst, W.M.v.d. (2001). Process Mining: Discovering Workflow Models from Event-Based Data. In B. Kröse, M. de Rijke, G. Schreiber, & M. van Someren (Red.), *13th Belgium-Netherlands Conf. Artificial Intelligence (BNAIC 2001*) (S. 283-290).

Wells, J.T. (2002a). Billing schemes, Part 1: Shell companies that don't deliver. *Journal of Accountancy, 194*(1), 76–79.

Wells, J.T. (2002b). Billing schemes, Part 2: Pass-throughs. *Journal of Accountancy, 194*(2), 72–74.

Wells, J.T. (2002c). Occupational Fraud: The Audit as Deterrent. *Journal of Accountancy, 193*(4), 24–28.

Wells, J.T. (2003a). Corruption: Causes and Cures. *Journal of Accountancy, 195*(4), 49–52.

Wells, J. T. (2003b). Sherlock Holmes, CPA, Part 1. *Journal of Accountancy, 196*(2), 86.

Wells, J. T. (2003c). Sherlock Holmes, CPA, Part 2. *Journal of Accountancy, 196*(3), 70–75.

Wells, J. T. (2004). Small Business, Big Losses. *Journal of Accountancy, 198*(6), 42–47.

Wells, J.T. (2011). *Corporate Fraud Handbook: Prevention and Detection* (3. Aufl.). Hoboken, USA: John Wiley & Sons..

Wells, J.T., & Gill, J.D. (2007). Assessing Fraud Risk. *Journal of Accountancy, 204*(4), 63–65.

Wiersema, W.H. (2002). Preventing fraud in the procurement department. *Electrical Apparatus, 55*(6), 55–57.

Wilder, B. (2005). Who's Afraid of Fraud: Employee Theft Surprise Small Business Owners. *Catalyst (2002)*, 28–31.

Wilson, R.A. (2004). Employee Dishonesty: National Survey of Risk Managers on Crime. *Journal of Economic Crime Management, 2*(1), 1–25.

Witten, I.H., & Frank, E. (2005). *Data Mining: Practical machine learning tools and techniques.* Burlington, Massachusetts, USA: Morgan Kaufmann.

Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *The CPA Journal, 74*(12), 38–42.

Yang, F. X., Zhang, R. Q., & Zhu, K. (2017). Should purchasing activities be outsourced along with production? *European Journal of Operational Research*, 257(2), 468–482. https://doi.org/10.1016/j.ejor.2016.07.029

Yannikos, Y., Franke, F., Winter, C., & Schneider, M. (2011). 3LSPG: Forensic tool evaluation by three layer stochastic process-based generation of data. In H. F. Sako, K., Saitoh, S. (Red.), *Computational Forensics:* Vol. 6540 (S. 200-211). Berlin/Heidelberg, Deutschland: Springer Verlag.

Yeh, I.-C., & Lien, C.-h. (2009). The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients. *Expert Systems with Applications, 36*(2), 2473–2480. doi:10.1016/j.eswa.2007.12.020

Yin, R. K. (2009). *Case Study Research: Design and Methods* (4. Aufl.). London and Singapore: SAGE Publications, Inc.

Yue, D., Wu, X., Wang, Y., Li, Y., & Chu, C.-H. (2007). A Review of Data Mining-Based Financial Fraud Detection Research. In A. H. Burgmeyer & D. Romeo (Red.), *Proceedings of the 3rd International Conference on Wireless Communications, Networking and Mobile Computing* (S. 5514–5517). Piscataway (USA): IEEE Press.

Zikmund, P.E. (2008). Reducing the Expectation Gap. *The CPA Journal, 78*(6), 20–25.

Anhang A: Fraud Klassifikationsbaum

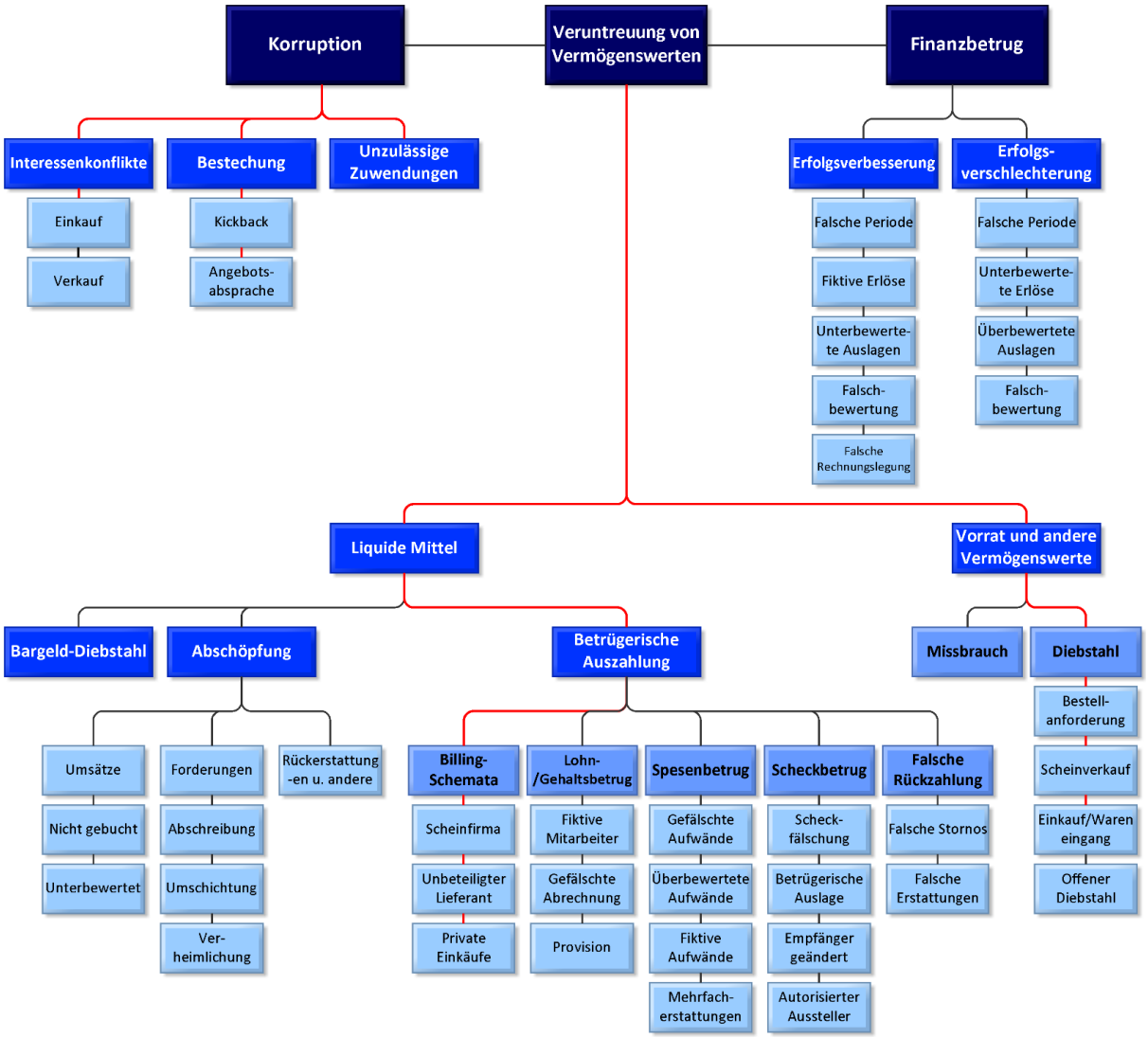


Abbildung 0-1: Fraud Detektionsbaum

Quelle: Eigene Darstellung auf Basis von ACFE (2014)

Anhang B: Algorithmen zur Fraud Detektion

Publikationen	Methode und Fokus		Statistisch		Klassifikation					Clustering		Weitere			
	Verwendete Methode	Fokus[39]	Nicht-Parametrisiert	Parametrisiert	NN	Bayesian Networks	SVM	KNN	Regelbasierend	Partitional	Hierarchisch	Expert Systems	Evolutionär	Fuzzy	Relevant für Stufe B
(Abbott, Park, & Parker, 2000)	Logit Regression			X											
(Abbott, Parker, & Peters, 2001)	Logit Regression	FinBet		X											
(Aleskerov, Freisleben, & Rao, 1997)	Neuronale Netzwerke	KF			X										
(Artís, Ayuso, & Guillén, 1999)	Logit Regression	Vers.		X											
(Artís, Ayuso, & Guillén, 2002)	Logit Regression	Vers.		X											
(Atwood, Robison-Cox, & Shaik, 2006)	Regression und statistische Tests	Vers.		X											
(Bai, Yen, & Yang, 2008)	CART Algorithmus	FinBet		X					X						
(Beasley, 1996)	Logit Regression	FinBet		X											
(Beasley, Carcello, Hermanson, & Lapides, 2000)	T-Tests	FinBet		X											
(Belhadji, Dionne, & Tarkhani, 2000)	Probit Regression	Vers.		X											
Bell, Szykowny, und Willingham (1991)	Cascaded Logit Regression	FinBet		X											
(T. B. Bell, Szykowny, & Willingham, 1991)	Logit Regression	FinBet		X											
(Beneish, 1997)	T-Tests / ChiSquare Tests	FinBet		X											
(Beneish, 1999)	T-Tests / ChiSquare Tests	FinBet		X											
(Bentley, 2000)	Fuzzy logic	Vers.							X					X	
(Bentley, Kim, Jung, & Choi, 2000)	Fuzzy logic Genetische Algorithmen	KF							X				X	X	
(Bermúdez, Pérez, Ayuso, Gómez, & Vázquez, 2008)	Logit Regression Bayesian Belief Netzwerk	Vers.		X		X									
(Bernardi, 1994)	Logit Regression	FinBet		X											
(Bhargava, Zhong, & Lu, 2003)	Profiling mit Association Rules	ECOM							X						
(Bhattacharyya, Jha, Tharakunnel, & Westland, 2011)	Logit Regression SVM Random Forest Entscheidungsbäume	KF		X			X		X						

[39] KF: Kreditkartenfraud; ECOM: E-Commerce Fraud; FinBet: Finanzbetrug; Vers.: Versicherungsfraud; Gedlw.:Geldwäsche; Mitarb.: Mitarbeiterfraud; TELCO: Telekommunikationsfraud; TRAD: Insiderfraud; GEN: Genereller Fraud

(Richard J. Bolton & Hand, 2001)	Peer Group Analysis	KF		X											
(Bonchi, Giannotti, Mainetto, & Pedreschi, 1999)	Statistics und Entscheidungsbaums	FinBet		X					X						
(Boukerche & Notare, 2000)	Radial Basis Function Neuralonale Netzwerke	TELCO			X										
(Boukerche & Notare, 2002)	Neuronlae Netzwerke Kohonen	TELCO			X										
(Brause, Langsdorf, & Hepp, 1999)	Association Rules und NN	KF			X				X						
(Brockett, Derrig, Golden, Levine, & Alpert, 2002)	PRIDIT	Vers.	X												
(Brockett et al., 2006)	ANN (Rückpropagierung und Lernvektor Quanitsierung) multiple discriminant analysis logit regression	Vers.		X	X										X
(Brockett, Xia, & Derrig, 1998)	SOM Neuronale Netzwerke	Vers.			X										
(Burge & Shawe-Taylor, 1997)	SOM Neuronale Netzwerke	TELCO			X										
(Peter Burge & Shawe-Taylor, 2001)	Unsupervised NN	TELCO			X										
(Cahill, Lambert, Pinheiro, & Sun, 2002)	Account Signature Tracking	TELCO	X												
(Calderon & Green, 1994)	Statistische Tests	FinBet		X											
(Caudill, Ayuso, & Guillén, 2005)	Logit Regression	Vers.		X											
(Cerullo & Cerullo, 1999a, 1999b)	Neural Network	FinBet			X										
Chan, Fan, Prodromidis, und Stolfo (1999)	CART Entscheidungsbäume RIPPER Assoziationsregeln Bayesian Belief Network	KF				X			X						
(P. K. Chan & Stolfo, 1998)	C4.5/CART Entscheidungsbäume RIPPER/BAYES Assoziationsregeln	KF							X						
(Chang & Chang, 2010)	X-means C4.5 Entscheidungsbaum	ECOM							X	X					
(Chartier & Spillane, 2000)	ANN	Geldw.			X										
(G. Chen, Lu, & He, 2007)	Logit Regression	FinBet		X											
(H.-J. Chen, Huang, & Kuo, 2009)	Logit Regression ANN	Mitarb. / FinBet		X	X										X
(R.-C. Chen, Chen, & Lin, 2006)	Binary support vector system (SVM und genetic algorithm)	KF					X						X		
(R.-C. Chen, Chiu, Huang, & Chen, 2004)	Fragebogen basierend auf SVM	KF					X								
(R.-C. Chen, Luo, Liang, & Lee, 2005)	SVM ANN	KF			X		X								
(Chiu & Tsai, 2004)	Association Rules	KF							X						

(Cortes & Pregibon, 2001)	Signature Association Rules	TELCO							X						
(Cox, 1995)	Unsupervised NN Neuro-Fuzzy Classification	Vers.			X									X	
(Crocker & Tennyson, 2002)	Logit Regression	Vers.		X											
(Deng & Mei, 2009)	SOM ANN Hybrid K-means	FinBet.			X					X					
(Derrig & Ostaszewski, 1995)	Fuzzy System	Vers.												X	
(Deshmukh, Romine, & Siegel, 1997)	Fuzzy Logic	FinBet.												X	
(Deshmukh & Talluru, 1998)	Rule-based Fuzzy System	FinBet.							X					X	
(Dharwa & Patel, 2011)	Density Based Clustering	KF								X					
(Donoho, 2004)	Logit Regresssion, Entscheidungsbäume, Expert System, Neural Network, K-means	TRAD		X	X				X	X		X			
(Dorronsoro, Ginel, Sanchez, & Sanat Cruz, 1997)	SOM Neural Network Discriminant Analysis Genetic Algorithm	KF		X	X								X		
(Eining, Jones, & Loebbecke, 1997)	Logit Regression Expert System	FinBet.		X								X			
(Estévez, Held, & Perez, 2006)	Fuzzy Rules und ANN	TELCO			X				X					X	
(Fanning & Cogger, 1998)	Generalized Adaptive Neural Network	FinBet.			X										
(Fanning, Cogger, & Srivastava, 1995)	Generalized Adaptive Neural Network, Adaptive Logic Network Neural Network	FinBet.			X										
(Fawcett & Provost, 1997a)	Regelbasierter Ansatz	TELCO							X						
(Fawcett & Provost, 1997b)	Regelbasierter Ansatz	TELCO							X						
(Fawcett & Provost, 1999)	Regelbasierter Ansatz	TELCO							X						
(Feroz et al., 2000)	Logit Regression Artificial Neural Networks	FinBet.		X	X										X
(Ferreira, Alves, Belo, & Cortesão, 2006)	Distanz basierend	TELCO		X											
(Franke, Hoser, & Schröder, 2008)	Spectral Clustering	TRAD								X					
(Gao & Ye, 2007)	Fuzzy Logic	Geldw.												X	
(Ghani & Kumar, 2011)	Repeated Bisection Clustering	Vers.								X					
(Ghosh & Reilly, 1994)	Neuronales Netzwerk	KF			X										
(Glancy & Yadav, 2011)	Expectation Maximization Hierarchical Clustering	FinBet.								X	X				
(Goldberg, Kirkland, Lee, Shyr, & Thakker, 2003)	fuzzy matching, regelbasiert logit regression	TRAD		X					X						
(B. P. Green & Choi, 1997)	Artificial Neural Networks	FinBet.			X										
(Grosser, Britos, & García-Martínez, 2005)	SOM Neural Network	TELCO			X										

(Hansen, McDonald, Messier, & Bell, 1996)	EGB2 Logit und Probit Regression	FinBet.		X											
(Hassibi, 2000)	NN	KF			X										
(Hawkins, He, Williams, & Baxter, 2006)	Replicator Neural Netoworks	GEN			X										
(He, Graco, & Yao, 1999)	KNN und Genetic Algorithm	Vers.						X					X		
(He, Wang, Graco, & Hawkins, 1997)	SOM Neural Network	Vers.			X										
	Profiling mit Feed Forward Neural Networks	TELCO			X										
Hollmen und Tresp (1998)	Hierarchisch mit Bayesian Network	TELCO				X									
Holton (2009)	Naïve Bayes; K-means; Hierarchischesl Clustering	Mitarb.		X						X	X				
Hoogs, Kiehl, LaComb, und Senturk (2007)	Genetische Algorithmen	FinBet.											X		
Huang (2006)	LPM (linear) Regression, Logit Regression	FinBet.		X											
Issa und Vasarhelyi (2011)	K-means	Mitarb.								X					
Jans et al. (2008)	K-means	Mitarb.								X					
Jans et al. (2010)	Multivariate Latent Class Clustering	Mitarb.								X					
Jin, Rejesus, und Little (2005)	Logit Regression, Probit Regression	Vers.		X											
Jurek und Zakrzewska (2008)	Davies-Bouldin Index, Naïve Bayes	Vers.		X						X					
Juszczak, Adams, Hand, Whitrow, und Weston (2008)	NN, SOM Neural Network, SVM	KF			X		X	X							
Kiehl, Hoogs, LaComb, und Senturk (2005)	Genetische Algorithmen	FinBet.											X		
Kim, Ong, und Overill (2003)	Genetische Algorithmen	ECOM											X		
Kim und Kim (2002)	Density Map	KF	X												
Kirkland et al. (1998)	Entscheidungsbaum, Rule Matching	FinBet							X						
Kirkos, Spathis, und Manolopoulos (2007)	ID3 Entscheidungsbaum Backpropagation Neural Network Bayesian Belief Network	FinBet.			X	X			X						
Knorr und Ng (1998)	Distance Based Outlier Detection	KF		X											
Kokkinaki (1997)	Profiling mit Similarity Tree	GEN							X						
Koskivaara (2000)	Multilayered Backpropagation Neural Network	FinBet.			X										
Kotsiantis et al. (2006)	C4.5 Decission Tree, Logit Regression, RBF Neural Network, K2 Bayesian Network, SMO SVM, 3NN KNN, RIPPER Association Rules	FinBet.		X	X	X	X	X	X						X

Krambia-Kapardis, Christodoulou, und Agathocleous (2010)	Multilayer Perceptron Neural Network	GEN			X										
Krenker, Volk, Sedlar, Bešter, und Kos (2009)	Bidirectional Artificial Neural Network	TELCO			X										
Lane und Brodley (1999)	Instance-Based Learning mit custom similarity measure	GEN	X					X							
Lane und Brodley (2003)	Hidden Markov Model Bayesian Network Instance Based Learner	GEN	X			X									
Le Khac und Kechadi	K-means ANN	Geldw.			X					X					
Lenard, Watkins, und Alam (2007)	Logit Regression Fuzzy Logic	FinBet.		X										X	
Leonard (1993)	Expertensystem	KF										X			
Lin, Lin, und Hong (2009)	SOM Neural Network	Vers.			X										
Lin, Lin, Li, und Kuo (2008)	SOM Neural Network Principal component analysis	Vers.	X		X										
Lin et al. (2003)	Fuzzy Neural Network Logit Regression	FinBet.		X	X									X	X
Liou (2008)	Logit Regression, Neuronales Netzwerk, C5.0/ID3 Entscheidungsbäume	FinBet.		X	X				X						X
Little, Johnston, Lovell, Rejesus, und Steed (2002)	Logit Regression	Vers.		X											
Liu, Qian, Mao, und Zhu (2011)	K-means, BIRCH	Geldw.								X	X				
Loebbecke, Eining, und Willingham (1989)	ChiSquared Tests	FinBet.		X											
Macskassy (2005)	Suspicion Scoring	GEN		X											
Macskassy und Provost (2007)	Suspicion Scoring	GEN		X											
Maes, Tuyls, Vanschoenwinkel, und Manderick (2002)	Bayesian Network Neuronale Netzwerke	KF			X	X									
Major und Riedinger (1992)	EFD System	Vers.		X					X			X			
Major und Riedinger (2002)	EFD System	Vers.		X					X			X			
Mercer (1990)	Regression Analysis	Mitarb.		X											
Moreau, Lerouge, Verrelst, Stormann, und Burge (1999)	Rule based ANN	TELCO			X				X						
Moreau et al. (1997)	Rule-based (un)supervised NN	TELCO			X				X						
Moreau, Verrelst, und Vandewalle (1997)	Supervised Neural Networks	TELCO			X										
Murad und Pinkas (1999)	Distance Based Profiling	TELCO		X											
Oliveira, Neto, und Meira (2004)	Multilayered Perceptron NN RBF NN	GEN			X										
Oliveira und Meira (2006)	NN mit robust confidence intervals	Mitarb.			X										

Ormerod, Morley, Ball, Langley, und Spenser (2003)	Bayesian Belief Network	Vers.				X									
Owusu-Ansah, Moyes, Peter Babangida Oyelere, und Hay (2002)	Logit Regression	Mitarb.		X											
Pacheco, Martins, Barcia, und Khator (1996)	Hybrid inductive und deductive system	FinBet.			X							X		X	
Palshikar und Apte (2008)	Graph Based Clustering	TRAD								X					
Panigrahi, Kundu, Sural, und Majumdar (2009)	Density Based Clustering, Rule Based Filter, Bayesian Learner	KF		X					X	X					
Park (2005)	ANN	KF			X										
Pathak, Vidyarthi, und Summers (2005)	Fuzzy Logic Expert System	Vers.											X	X	
Perols (2011)	C4.5 Entscheidungsbaum, Artificial Neural Network, Logit Regression, SVM	FinBet.		X	X		X		X						X
Persons (1995)	Logit Regression	FinBet.		X											
Phua, Alahakoon, und Lee (2004)	C4.5 Entscheidungsbaum, Naïve Bayesian, Backpropagation Neural Networks	GEN		X	X				X						
Pinquet, Ayuso, und Montserrat Guillén (2007)	Probit Regression	Vers.		X											
Quah und Sriganesh (2008)	SOM Neural Network	KF			X										
Ravisankar et al. (2011)	Logit Regression,Multi-layer feedforward/ Probabilistic, Neural Network, SVM, Genetic Algorithm	FinBet.		X	X		X						X		X
Rosset, Murad, Neumann, Idan, und Pinkas (1999)	C4.5 algorithm for rules	TELCO							X						
Sánchez, Vila, Cerda, und Serrano (2009)	Fuzzy Association Rules	KF							X					X	
Sanver und Karahoca (2009)	Entscheidungsbaum RIPPER Association Rules Fuzzy System	TELCO							X					X	
Senator et al. (1995)	Rule based	Geldw.							X						
Shao, Zhao, und Chang (2002)	CHAID Entscheidungsbaum	FinBet.							X						
Spathis (2002)	Logit Regression	FinBet.		X											
Spathis, Doumpos, und Zopounidis (2002)	UTADIS (non-parametric, logit regression based)	FinBet.		X											
Srivastava, Kundu, Sural, und Majumdar (2008)	Hidden Markov Model Bayesian Network	KF				X									
Stefano und Gisella (2001)	Fuzzy System	Vers.												X	
Sternberg und Reynolds (1997)	Cultural Algorithm in Rule Based Expert System	Vers.							X			X	X		
Stolfo, Fan, Lee, Prodromidis, und Chan (1997)	ID3/CART Entscheidungsbaum RIPPER Association Rules Bayes	KF		X					X						

Summers und Sweeney (1998)	Logit Regression	FinBet. / TRAD		X											
Syeda, Yan-Qing Zhang, und Yi Pan (2002)	Fuzzy Neural Network	KF			X									X	
Tang and Yin (2005)	SVM	Geldw.					X								
Taniguchi, Haft, Hollmen, and Tresp (1998)	Feed-forward NN Gaussian mixture model Bayesian Network	TELCO		X	X	X									
Tasoulis, Adams, Weston, and Hand (2008)	Density Based Clustering	KF								X					
Tennyson and Pau Salsas-Forn (2002)	Logit Regression	Vers.		X											
Thiprungsri and Vasarhelyi (2011)	K-means	Vers.								X					
Torgo and Lopes (2011)	Hierarchical agglomerative clustering	FinBet.									X				
Torgo and Soares (2010)	Hierarchical Clustering	FinBet.									X				
Viaene, Derrig, and Dedene (2004)	Naïve Bayes	Vers.		X											
Viaene, Ayuso, Guillén, Gheel, und Dedene (2007)	Logit Regression	Vers.		X											
Viaene, Dedene, und Derrig (2005)	Bayesian Learning Neural Network	Vers.			X	X									
Viaene et al. (2002)	Logit Regression,C4.5 Entscheidungsbaum,Least-Squares SVM, Neural Network, KNN (tree-augmented) Naïve Bayes	Vers.		X	X		X	X	X						X
Viaene et al. (2003)	multilayer perceptron neural networks, Logit Regression, C4.5 Entscheidungsbaum	Vers.		X	X				X						X
Virdhagriswaran und Dakin (2006)	K-means,Entscheidungsbaum Logit Regression	Vers./ TRAD		X					X	X					
Chai, Hoogs, und Verschueren (2006)	Fuzzy Logic, Genetic Algorithm	FinBet.											X	X	
Weisberg und Derrig (1998)	Logit Regression	Vers.		X											
Welch, Reeves, und Welch (1998a)	Neural Network	Mitarb.			X										
Welch, Reeves, und Welch (1998b)	Genetic Algorithm	Mitarb.											X		
Wheeler und Aitken (2000)	Case Based Reasoning (several statistics)	KF	X												
Wu, Xiong, und Chen (2010)	K-means	Vers.								X					
Xiaoyun und Danyue (2010)	Resolution & Density Based Clustering	Vers.								X					
Yamanishi, Takeuchi, Williams, und Milne (2000)	Dicounting Learning Algorithm (param. & non-p.)	Vers.	X	X											
Yang und Hwang (2006)	CBA Association Rules	Vers.							X						
Yeh und Lien (2009)	KNN, Logit Regression, Discriminant Analysis, Naïve Bayesian, Neural	KF		X	X			X	X						X

	Networks, Entscheidungsbaum													
Yen (2007)	ART algorithm in ANN	FinBet.			X									
Yuan, Yuan, und Deng (2008)	Logit Regression	FinBet.		X										
Zaslavsky und Strizhak (2006)	SOM Neural Network	KF			X									
Zhang, Chen, Wu, und Zhang (2006)	CHAMELEON Clustering	Vers.								X				
Zhang, Salerno, und Yu (2003)	Link Discovery based on Correlation Analysis Histogram segmentation based clustering	Geldw.		X						X				
Zhou und Kapoor (2011)	Bayesian Networks Neural Networks	FinBet.			X	X			X					

Tabelle 64: Algorithmen zur Fraud Detektion - Literature Review Matrix
Quelle: Eigene Darstellung basierend auf (Lebherz, 2014)

Anhang C: Fragebogen zur Validierung der Fraud Patterns

Haben wir aus Ihrer Sicht unpassende (irrelevante) Red Flags zu dem jeweiligen Szenario zugeordnet? Falls ja, markieren Sie diese bitte. Markieren Sie bitte zusätzlich noch die aus Ihrer Sicht am besten beschreibenden Red Flags (maximal vier) für das entsprechende Szenario.

Fehlen Ihrer Meinung nach Red Flags im jeweiligen Szenario?

Haben Sie hierzu noch Anmerkungen?

Abschlussfragen:

Ist die Liste der Szenarien aus Ihrer Sicht vollständig? Fallen Ihnen weitere Szenarien ein? Wenn ja, welche? Bitte erläutern Sie das fehlende Szenario kurz.

Können Sie aus Ihrer Berufspraxis Annäherungswerte für die genannten Thresholds liefern?

Haben wir aus Ihrer Sicht etwas Wichtiges zu diesem Thema vergessen?

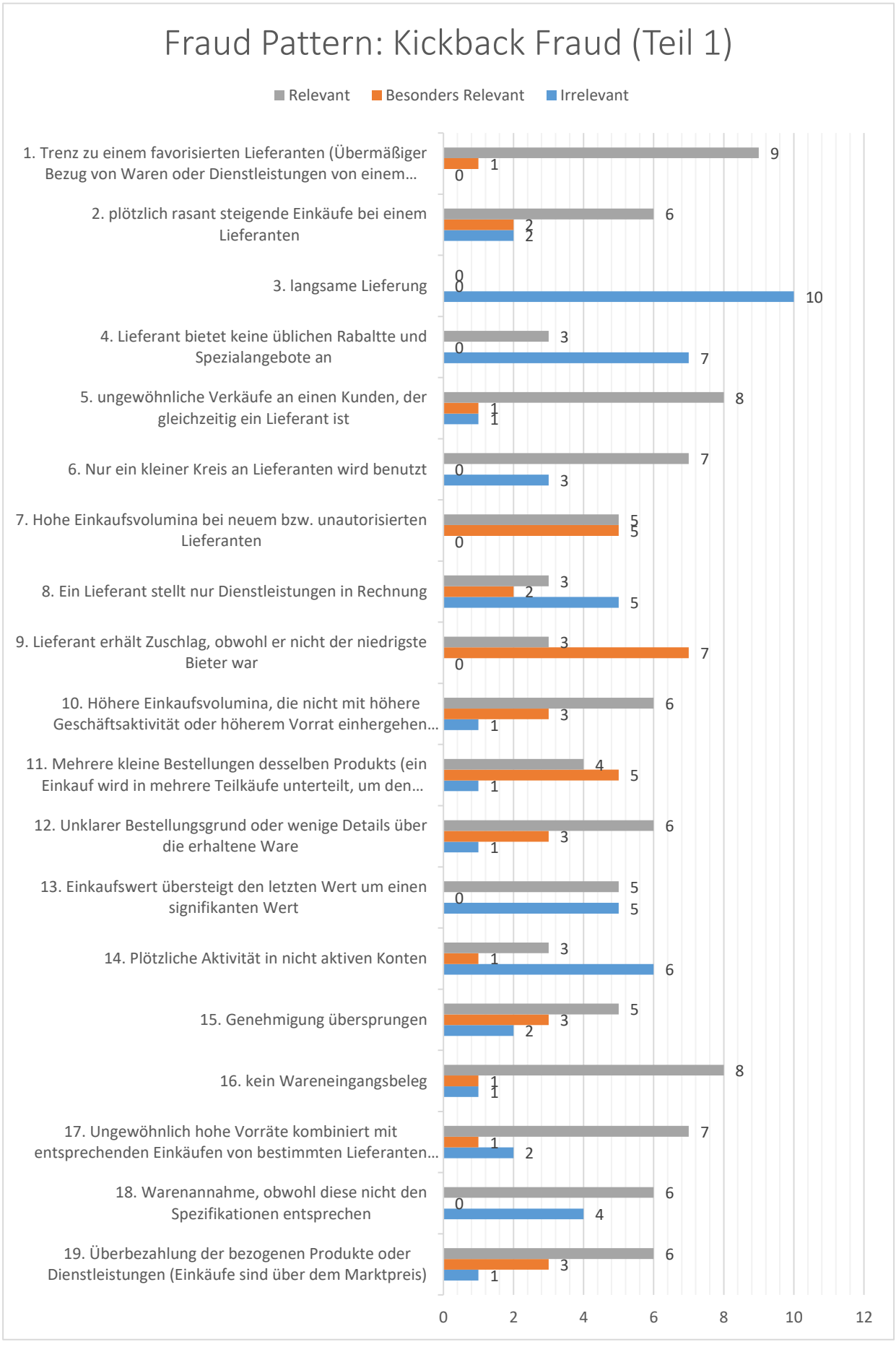
Freiwillige Angaben zu Ihrer Person und zum Unternehmen:

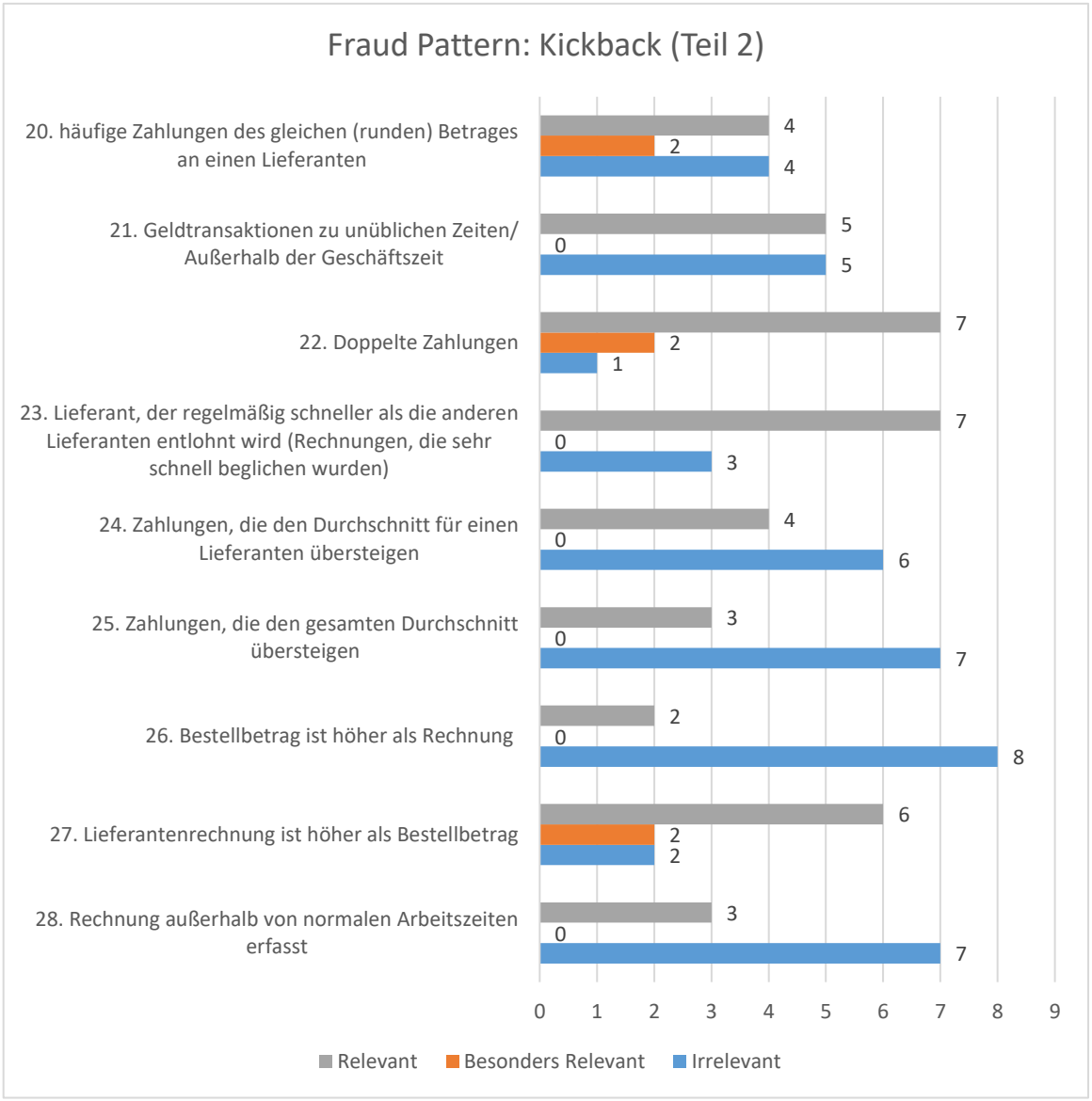
Wie alt sind Sie?

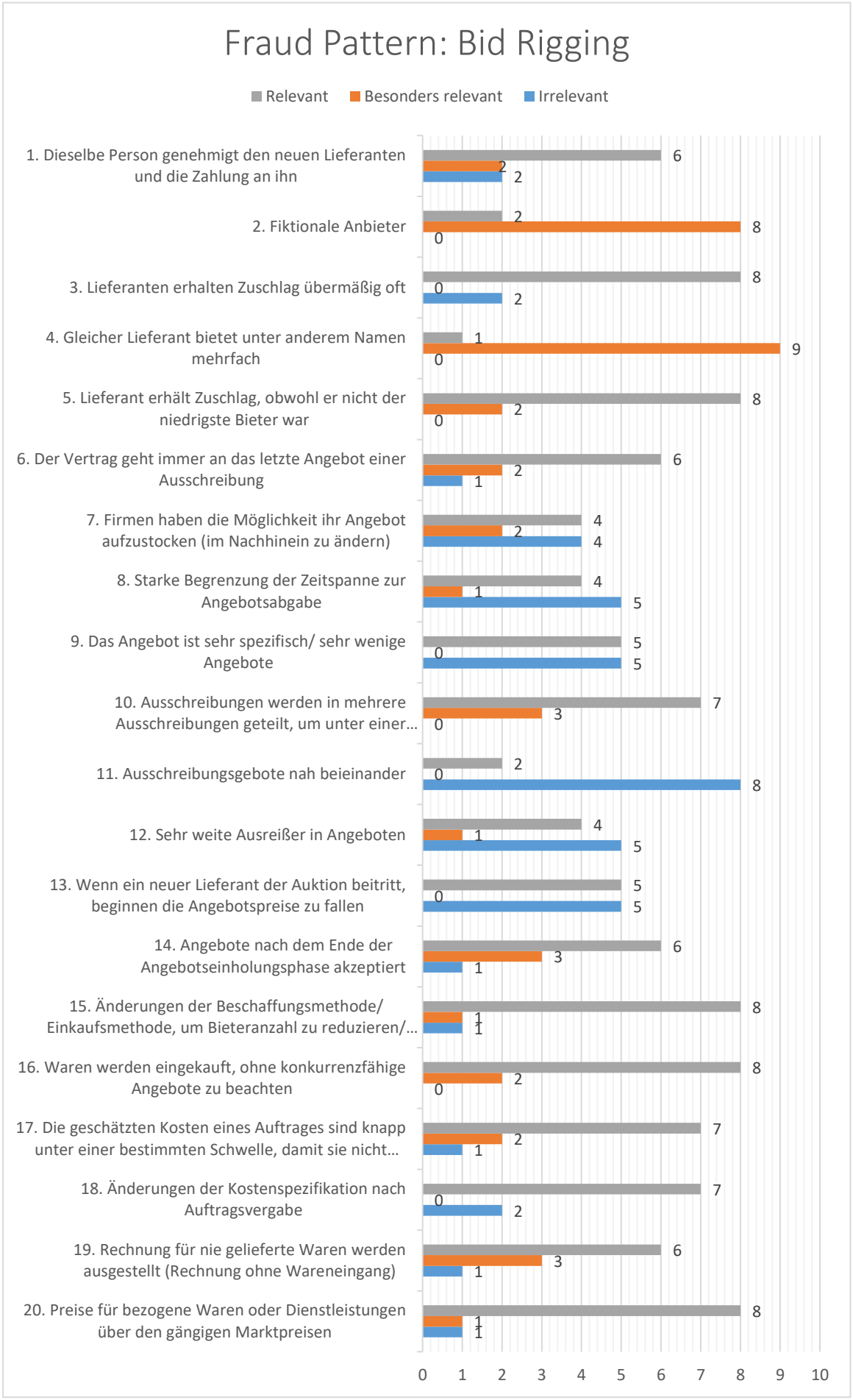
Welchem Geschlecht gehören Sie an?

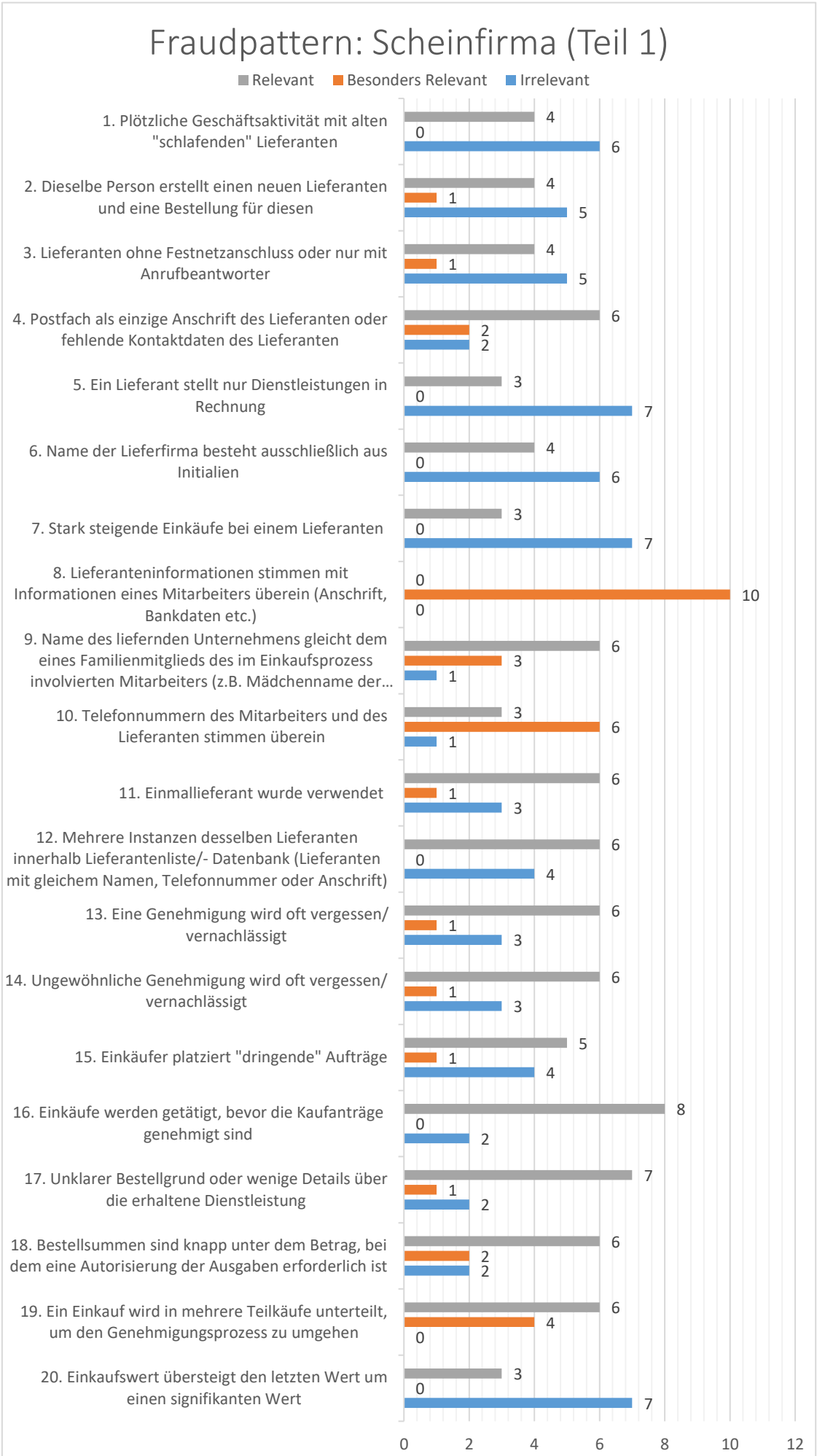
Welche Position haben Sie im Unternehmen und für welche Aufgaben sind Sie zuständig?

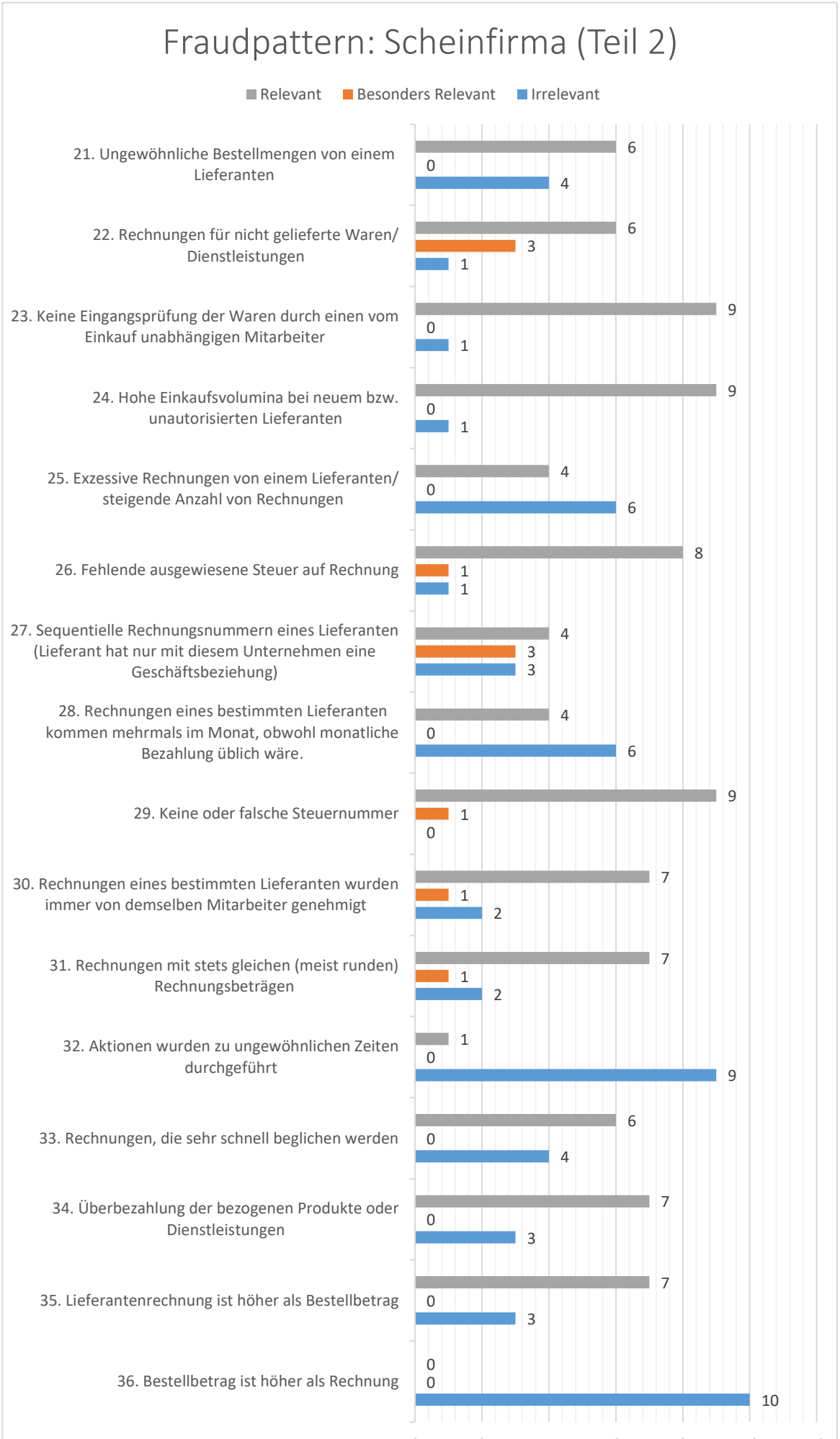
Anhang D: Ergebnisse der Validierung

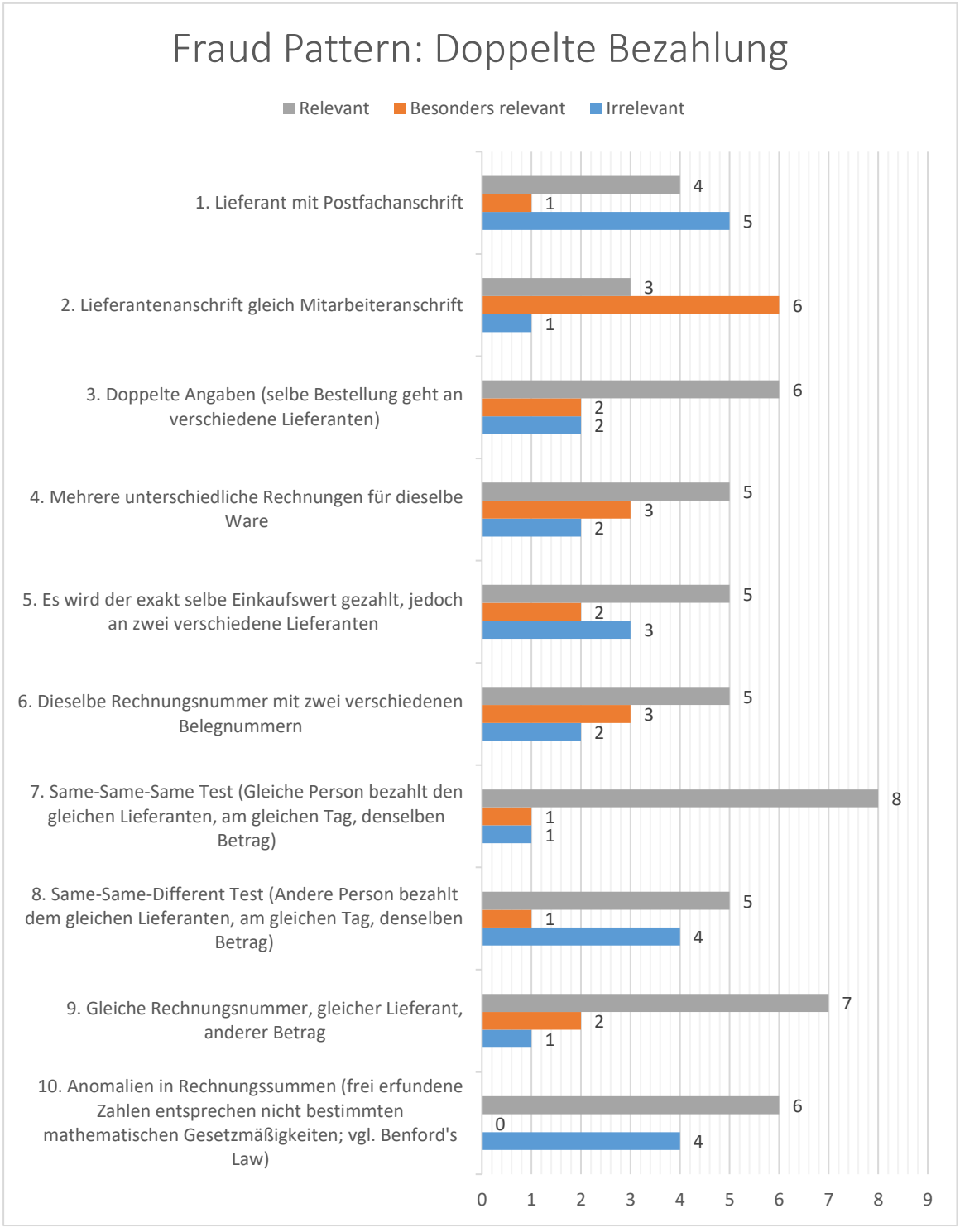


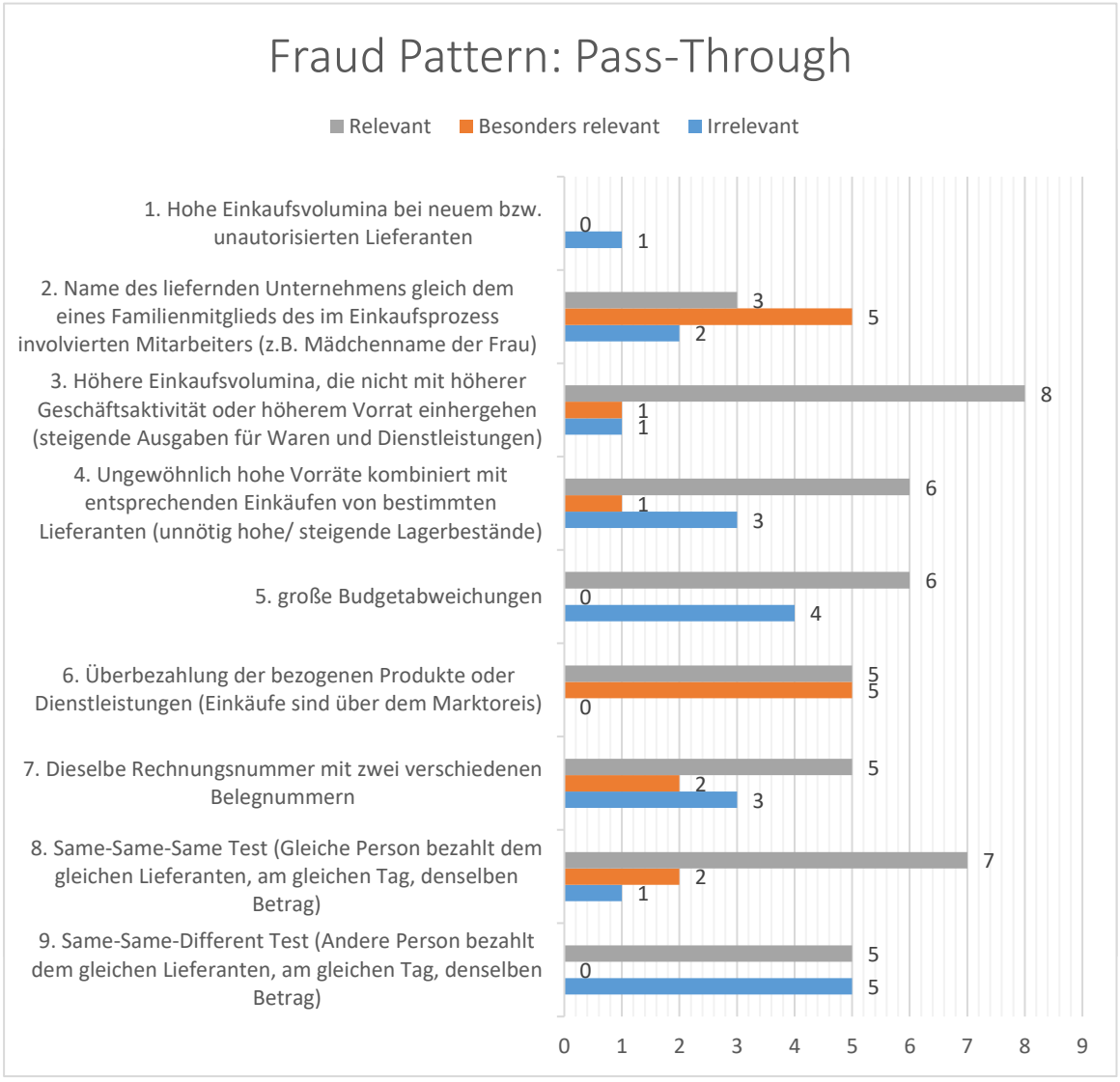

Fraud Pattern: Kickback (Teil 2)
20. häufige Zahlungen des gleichen (runden) Betrages an einen Lieferanten
4
2
4
21. Geldtransaktionen zu unüblichen Zeiten/ Außerhalb der Geschäftszeit
5
0
5
22. Doppelte Zahlungen
7
2
1
23. Lieferant, der regelmäßig schneller als die anderen Lieferanten entlohnt wird (Rechnungen, die sehr schnell beglichen wurden)
7
0
3
24. Zahlungen, die den Durchschnitt für einen Lieferanten übersteigen
4
0
6
25. Zahlungen, die den gesamten Durchschnitt übersteigen
3
0
7
26. Bestellbetrag ist höher als Rechnung
2
0
8
27. Lieferantenrechnung ist höher als Bestellbetrag
6
2
2
28. Rechnung außerhalb von normalen Arbeitszeiten erfasst
3
0
7
0 1 2 3 4 5 6 7 8 9
Relevant
Besonders Relevant
Irrelevant

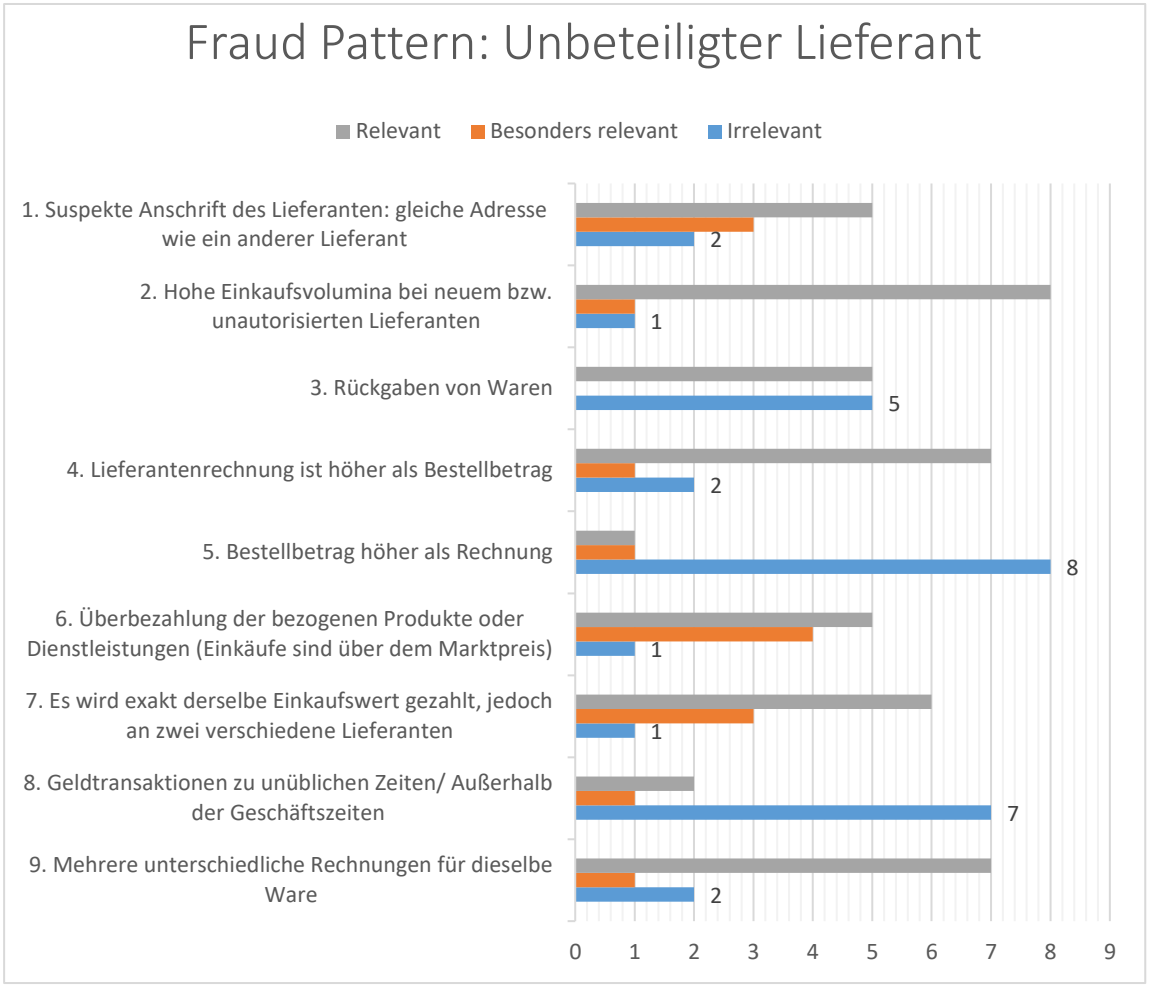

Fraud Pattern: Bid Rigging
Relevant
Besonders relevant
Irrelevant
1. Dieselbe Person genehmigt den neuen Lieferanten und die Zahlung an ihn
6
2
2
2. Fiktionale Anbieter
2
8
0
3. Lieferanten erhalten Zuschlag übermäßig oft
8
0
2
4. Gleicher Lieferant bietet unter anderem Namen mehrfach
1
9
0
5. Lieferant erhält Zuschlag, obwohl er nicht der niedrigste Bieter war
8
2
0
6. Der Vertrag geht immer an das letzte Angebot einer Ausschreibung
6
2
1
7. Firmen haben die Möglichkeit ihr Angebot aufzustocken (im Nachhinein zu ändern)
4
2
4
8. Starke Begrenzung der Zeitspanne zur Angebotsabgabe
4
1
5
9. Das Angebot ist sehr spezifisch/ sehr wenige Angebote
5
0
5
10. Ausschreibungen werden in mehrere Ausschreibungen geteilt, um unter einer...
7
3
0
11. Ausschreibungsgebote nah beieinander
2
0
8
12. Sehr weite Ausreißer in Angeboten
4
1
5
13. Wenn ein neuer Lieferant der Auktion beitritt, beginnen die Angebotspreise zu fallen
5
0
5
14. Angebote nach dem Ende der Angebotseinholungsphase akzeptiert
6
3
1
15. Änderungen der Beschaffungsmethode/ Einkaufsmethode, um Bieteranzahl zu reduzieren/...
8
1
1
16. Waren werden eingekauft, ohne konkurrenzfähige Angebote zu beachten
8
2
0
17. Die geschätzten Kosten eines Auftrages sind knapp unter einer bestimmten Schwelle, damit sie nicht...
7
2
1
18. Änderungen der Kostenspezifikation nach Auftragsvergabe
7
0
2
19. Rechnung für nie gelieferte Waren werden ausgestellt (Rechnung ohne Wareneingang)
6
3
1
20. Preise für bezogene Waren oder Dienstleistungen über den gängigen Marktpreisen
8
1
1
0 1 2 3 4 5 6 7 8 9 10

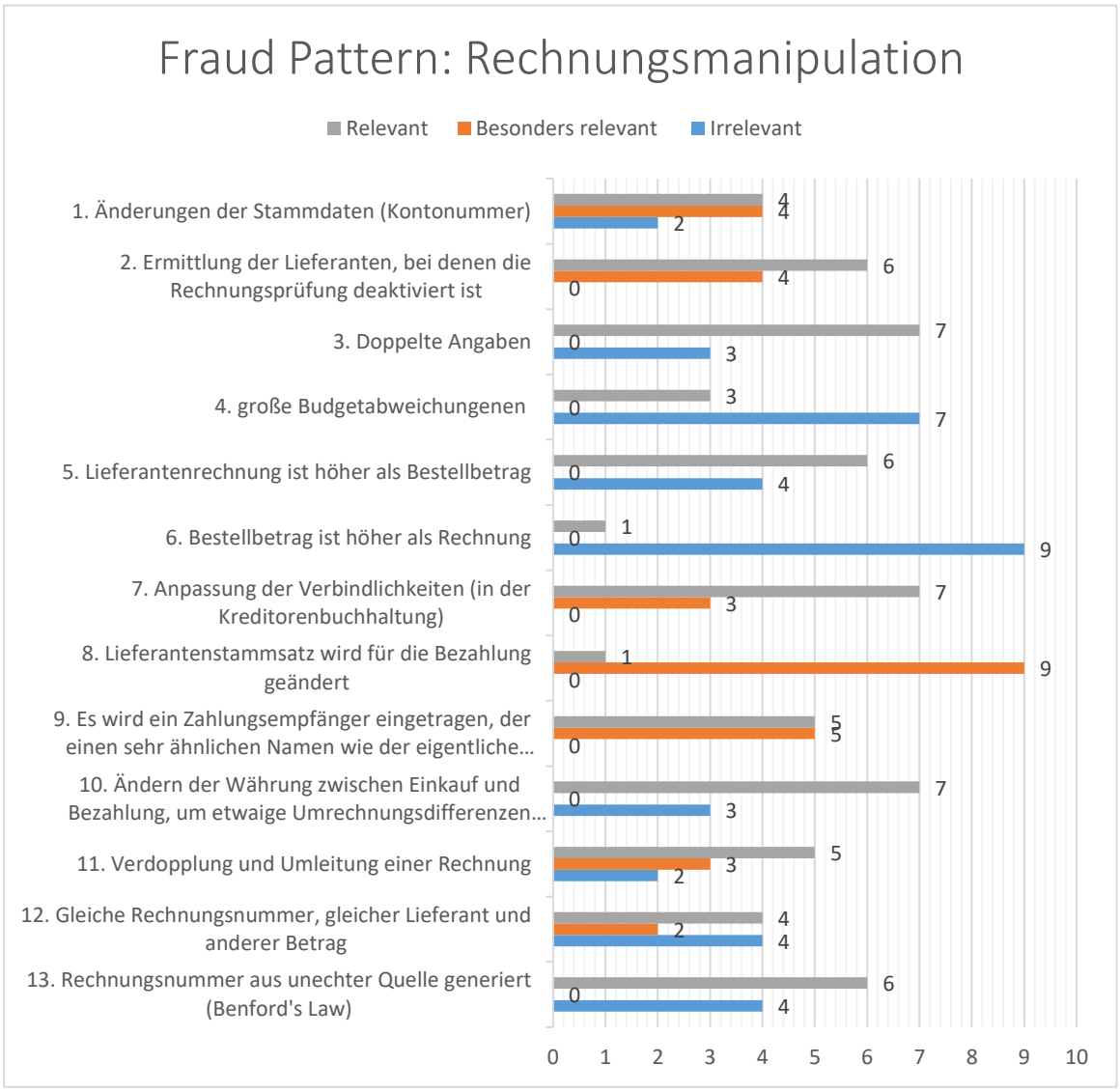

Fraudpattern: Scheinfirma (Teil 1)
Relevant
Besonders Relevant
Irrelevant
1. Plötzliche Geschäftsaktivität mit alten "schlafenden" Lieferanten
4
0
6
2. Dieselbe Person erstellt einen neuen Lieferanten und eine Bestellung für diesen
4
1
5
3. Lieferanten ohne Festnetzanschluss oder nur mit Anrufbeantworter
4
1
5
4. Postfach als einzige Anschrift des Lieferanten oder fehlende Kontaktdaten des Lieferanten
6
2
2
5. Ein Lieferant stellt nur Dienstleistungen in Rechnung
3
0
7
6. Name der Lieferfirma besteht ausschließlich aus Initialien
4
0
6
7. Stark steigende Einkäufe bei einem Lieferanten
3
0
7
8. Lieferanteninformationen stimmen mit Informationen eines Mitarbeiters überein (Anschrift, Bankdaten etc.)
0
10
0
9. Name des liefernden Unternehmens gleicht dem eines Familienmitglieds des im Einkaufsprozess involvierten Mitarbeiters (z.B. Mädchenname der...
6
3
1
10. Telefonnummern des Mitarbeiters und des Lieferanten stimmen überein
3
6
1
11. Einmallieferant wurde verwendet
6
1
3
12. Mehrere Instanzen desselben Lieferanten innerhalb Lieferantenliste/- Datenbank (Lieferanten mit gleichem Namen, Telefonnummer oder Anschrift)
6
0
4
13. Eine Genehmigung wird oft vergessen/ vernachlässigt
6
1
3
14. Ungewöhnliche Genehmigung wird oft vergessen/ vernachlässigt
6
1
3
15. Einkäufer platziert "dringende" Aufträge
5
1
4
16. Einkäufe werden getätigt, bevor die Kaufanträge genehmigt sind
8
0
2
17. Unklarer Bestellgrund oder wenige Details über die erhaltene Dienstleistung
7
1
2
18. Bestellsummen sind knapp unter dem Betrag, bei dem eine Autorisierung der Ausgaben erforderlich ist
6
2
2
19. Ein Einkauf wird in mehrere Teilkäufe unterteilt, um den Genehmigungsprozess zu umgehen
6
4
0
20. Einkaufswert übersteigt den letzten Wert um einen signifikanten Wert
3
0
7
0
2
4
6
8
10
12

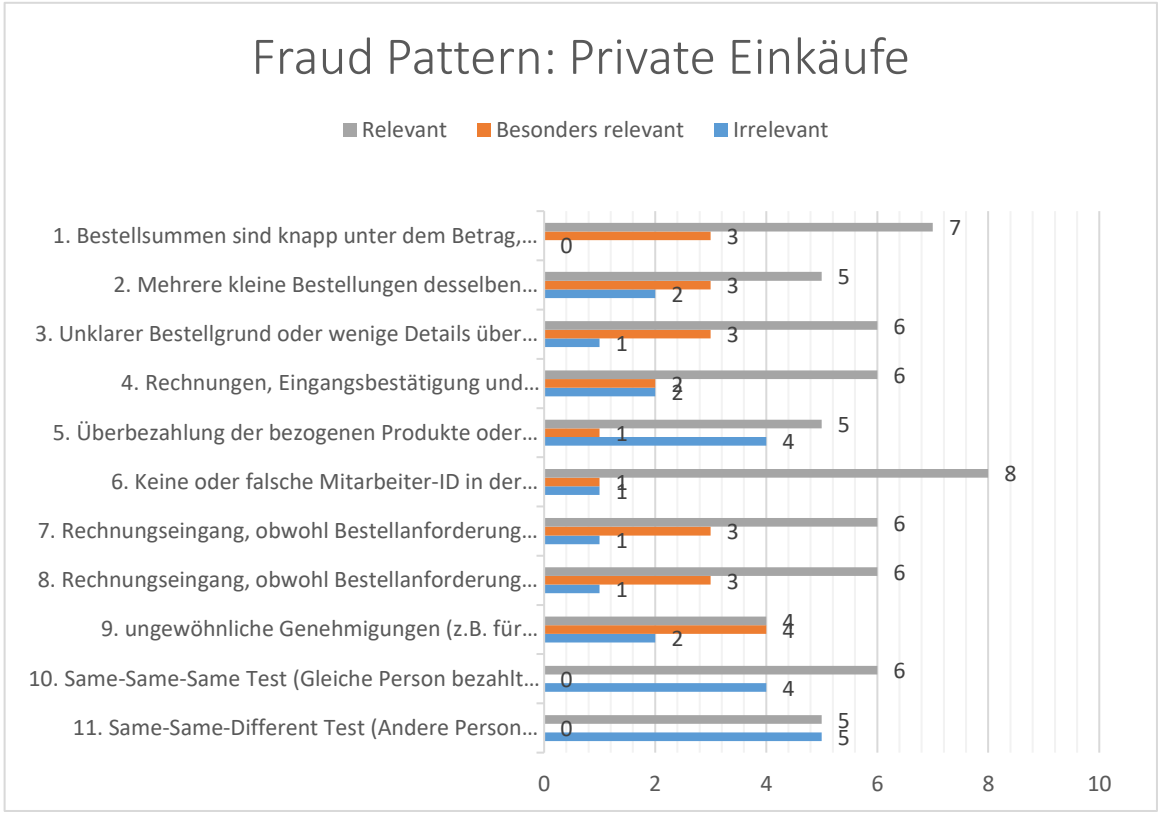

Fraudpattern: Scheinfirma (Teil 2)
Relevant
Besonders Relevant
Irrelevant
21. Ungewöhnliche Bestellmengen von einem Lieferanten
6
0
4
22. Rechnungen für nicht gelieferte Waren/ Dienstleistungen
6
3
1
23. Keine Eingangsprüfung der Waren durch einen vom Einkauf unabhängigen Mitarbeiter
9
0
1
24. Hohe Einkaufsvolumina bei neuem bzw. unautorisierten Lieferanten
9
0
1
25. Exzessive Rechnungen von einem Lieferanten/ steigende Anzahl von Rechnungen
4
0
6
26. Fehlende ausgewiesene Steuer auf Rechnung
8
1
1
27. Sequentielle Rechnungsnummern eines Lieferanten (Lieferant hat nur mit diesem Unternehmen eine Geschäftsbeziehung)
4
3
3
28. Rechnungen eines bestimmten Lieferanten kommen mehrmals im Monat, obwohl monatliche Bezahlung üblich wäre.
4
0
6
29. Keine oder falsche Steuernummer
9
1
0
30. Rechnungen eines bestimmten Lieferanten wurden immer von demselben Mitarbeiter genehmigt
7
1
2
31. Rechnungen mit stets gleichen (meist runden) Rechnungsbeträgen
7
1
2
32. Aktionen wurden zu ungewöhnlichen Zeiten durchgeführt
1
0
9
33. Rechnungen, die sehr schnell beglichen werden
6
0
4
34. Überbezahlung der bezogenen Produkte oder Dienstleistungen
7
0
3
35. Lieferantenrechnung ist höher als Bestellbetrag
7
0
3
36. Bestellbetrag ist höher als Rechnung
0
0
10


Fraud Pattern: Doppelte Bezahlung
Relevant
Besonders relevant
Irrelevant
1. Lieferant mit Postfachanschrift
4
1
5
2. Lieferantenanschrift gleich Mitarbeiteranschrift
3
6
1
3. Doppelte Angaben (selbe Bestellung geht an verschiedene Lieferanten)
6
2
2
4. Mehrere unterschiedliche Rechnungen für dieselbe Ware
5
3
2
5. Es wird der exakt selbe Einkaufswert gezahlt, jedoch an zwei verschiedene Lieferanten
5
2
3
6. Dieselbe Rechnungsnummer mit zwei verschiedenen Belegnummern
5
3
2
7. Same-Same-Same Test (Gleiche Person bezahlt den gleichen Lieferanten, am gleichen Tag, denselben Betrag)
8
1
1
8. Same-Same-Different Test (Andere Person bezahlt dem gleichen Lieferanten, am gleichen Tag, denselben Betrag)
5
1
4
9. Gleiche Rechnungsnummer, gleicher Lieferant, anderer Betrag
7
2
1
10. Anomalien in Rechnungssummen (frei erfundene Zahlen entsprechen nicht bestimmten mathematischen Gesetzmäßigkeiten; vgl. Benford's Law)
6
0
4
0 1 2 3 4 5 6 7 8 9


Fraud Pattern: Pass-Through
Relevant
Besonders relevant
Irrelevant
1. Hohe Einkaufsvolumina bei neuem bzw. unautorisierten Lieferanten
0
1
2. Name des liefernden Unternehmens gleich dem eines Familienmitglieds des im Einkaufsprozess involvierten Mitarbeiters (z.B. Mädchenname der Frau)
3
5
2
3. Höhere Einkaufsvolumina, die nicht mit höherer Geschäftsaktivität oder höherem Vorrat einhergehen (steigende Ausgaben für Waren und Dienstleistungen)
8
1
1
4. Ungewöhnlich hohe Vorräte kombiniert mit entsprechenden Einkäufen von bestimmten Lieferanten (unnötig hohe/ steigende Lagerbestände)
6
1
3
5. große Budgetabweichungen
6
0
4
6. Überbezahlung der bezogenen Produkte oder Dienstleistungen (Einkäufe sind über dem Marktoreis)
5
5
0
7. Dieselbe Rechnungsnummer mit zwei verschiedenen Belegnummern
5
2
3
8. Same-Same-Same Test (Gleiche Person bezahlt dem gleichen Lieferanten, am gleichen Tag, denselben Betrag)
7
2
1
9. Same-Same-Different Test (Andere Person bezahlt dem gleichen Lieferanten, am gleichen Tag, denselben Betrag)
5
0
5
0 1 2 3 4 5 6 7 8 9


Fraud Pattern: Unbeteiligter Lieferant
Relevant
Besonders relevant
Irrelevant
1. Suspekte Anschrift des Lieferanten: gleiche Adresse wie ein anderer Lieferant
2
2. Hohe Einkaufsvolumina bei neuem bzw. unautorisierten Lieferanten
1
3. Rückgaben von Waren
5
4. Lieferantenrechnung ist höher als Bestellbetrag
2
5. Bestellbetrag höher als Rechnung
8
6. Überbezahlung der bezogenen Produkte oder Dienstleistungen (Einkäufe sind über dem Marktpreis)
1
7. Es wird exakt derselbe Einkaufswert gezahlt, jedoch an zwei verschiedene Lieferanten
1
8. Geldtransaktionen zu unüblichen Zeiten/ Außerhalb der Geschäftszeiten
7
9. Mehrere unterschiedliche Rechnungen für dieselbe Ware
2
0 1 2 3 4 5 6 7 8 9


Fraud Pattern: Rechnungsmanipulation
Relevant
Besonders relevant
Irrelevant
1. Änderungen der Stammdaten (Kontonummer)
2. Ermittlung der Lieferanten, bei denen die Rechnungsprüfung deaktiviert ist
3. Doppelte Angaben
4. große Budgetabweichungenen
5. Lieferantenrechnung ist höher als Bestellbetrag
6. Bestellbetrag ist höher als Rechnung
7. Anpassung der Verbindlichkeiten (in der Kreditorenbuchhaltung)
8. Lieferantenstammsatz wird für die Bezahlung geändert
9. Es wird ein Zahlungsempfänger eingetragen, der einen sehr ähnlichen Namen wie der eigentliche...
10. Ändern der Währung zwischen Einkauf und Bezahlung, um etwaige Umrechnungsdifferenzen...
11. Verdopplung und Umleitung einer Rechnung
12. Gleiche Rechnungsnummer, gleicher Lieferant und anderer Betrag
13. Rechnungsnummer aus unechter Quelle generiert (Benford's Law)
0 1 2 3 4 5 6 7 8 9 10


Fraud Pattern: Private Einkäufe
Relevant
Besonders relevant
Irrelevant
1. Bestellsummen sind knapp unter dem Betrag,...
2. Mehrere kleine Bestellungen desselben...
3. Unklarer Bestellgrund oder wenige Details über...
4. Rechnungen, Eingangsbestätigung und...
5. Überbezahlung der bezogenen Produkte oder...
6. Keine oder falsche Mitarbeiter-ID in der...
7. Rechnungseingang, obwohl Bestellanforderung...
8. Rechnungseingang, obwohl Bestellanforderung...
9. ungewöhnliche Genehmigungen (z.B. für...
10. Same-Same-Same Test (Gleiche Person bezahlt...
11. Same-Same-Different Test (Andere Person...
0 2 4 6 8 10

Anhand E: Red Flags im Einkaufsprozess

Red Flags bei Lieferant

	Kickback, corruption	**Kickback; Billing Schemes, Inventory**	**Pass Through**	**Scheinfirma**	**allgemein**	**allgemein**	**Scheinfirma**	**Scheinfirma**	**Kickback**	**allgemein**	**Billing Schemes**	**allgemein**	**Scheinfirma**	**Billing-Schemes (Scheinfirma, Pass-**	**Scheinfirma**	**Scheinfirma,**	**allgemein**	**allgemein**	**Financial Statements, Asset**	**Rationalisierung**	**Scheinfirma**	**Kickback; Scheinfirma,**	**Angebotsmanipulation, Scheinfirma**	**Scheinfirma**	**Scheinfirma**	**Billing-Schemes**	**Kickback; Bid Rigging, Scheinfirma**	**Bid Rigging, Kickback**	**Bid Rigging**	**Bid Rigging**
	Wells (2003)	Wells (2002b)	Wells (2002c)	Wells (2002b)	Taylor, (2006)	Pacini & Brody (2005)	Lehman & Weidenmier (2005)	Lehman (2008)	Cowan (2005)	Christensen & Byington (2003a)	Christensen & Byington (2003b)	Christensen & Byington (2002)	Buckhoff & Morris (2002)	Wells (2013)	Cascarino (2013)	Davies (1995)	KPMG International (2010)	PricewaterhouseCoopers (2009)	Singleton & Singleton (2010)	Anand, Ashforth, & Joshi (2004)	Buckhoff (2002)	Fishman (2001)	Zikmund (2008)	Langley (2003)	Nilsen (2010)	Byington, & McGee (2012)	McNamee (2016)	Rahmani & Koohshahi (2015)	Erven, Holanda & Carvalho(2017)	Vona (2017)
Probleme mit Lieferanten																														
Postfach als Anschrift des Lieferanten		x					x			x			x	x	x	x	x		x		x		x							
Initialen eines Mitarbeiters stimmen mit Namen einer Lieferantenfirma überein		x					x	x											x				x							
Name der Lieferfirma besteht ausschließlich aus Initialen		x		x																										
Fehlende Lieferantendaten							x											x	x		x									
Lieferantenanschrift oder Bankdaten gleichen dem Mitarbeiter		x		x			x	x		x				x	x	x						x		x	x					
Ungültiger Lieferant/nicht autorisierte					x					x																	x	x			
Lieferanten mit gleichem Namen, Telefonnummer oder anschrift						x		x		x						x													x	
Lieferant erfordert									x																					

Barauszahlungen																												
Neue Lieferanten hoch aktiv	x	x	x							x					x					x								
Plötzliche Aktivität in nicht aktiven Konten										x		x																
Lieferant hat mehrere Anschriften											x																	
Lieferant mit fehlender oder ungültigen Umsatzsteuer-Identifikationsnummer													x															
Lieferant stammt nicht von der autorisierten internen Lieferantenliste		x		x							x			x	x	x									x	x	x		
Ungewöhnlicher Standort (z.B. entfernter Lieferant für Routinedienstleistungen)	x															x												
Mehrere Instanzen desselben Lieferanten innerhalb Lieferantenliste/-Datenbank																	x											x

Tabelle 65: Red Flags Lieferant

Quelle: Eigene Darstellung

Red Flags in der Bestellung

	Kickback, corruption	Kickback; Billing Schemes, Inventory	Pass Through	Scheinfirma	allgemein	Asset Misappropriation	allgemein	Billing Schemes	Kickback, Scheinfirma	Billing-Schemes	Scheinfirma	Scheinfirma,	allgemein	allgemein	Financial Statements, Asset	Kickback,Veruntreuung von	allgemein	Kickback; Scheinfirma	Kickback	Kickback	Billing-Schemes	Scheinfirma, allgemein	Bid Rigging, Corruption
	Wells (2003)	Wells (2002b)	Wells (2002c)	Wells (2002a)	Taylor (2006)	Seetharaman et. al. (2004)	Pacini & Brody (2005)	Christensen & Byington (2003b)	Brandman (2000)	Wells (2013)	Cascarino (2013)	Davies (1995)	KPMG International (2010)	PricewaterhouseCoopers (2009)	Singleton & Singleton (2010)	Brulenski, & Zayas (2014)	Strand, Judd, & Lancaster (2002)	Johnson, & Rudolph (2009)	Kranacher (2008)	Morehead (2007)	Byington, & McGee (2012)	Dhurandhar et al., (2015)	Nag (2015)
Unstimmigkeiten mit Bestellungen bei Lieferant																							
Steigende Ausgaben für Waren und Dienstleistungen	x		x	x			x				x				x					x			
Schnell ansteigende Anzahl an Käufen von einem Lieferanten	x	x	x					x	x						x					x	x		
Preise für bezogene Waren oder Dienstleistungen über den gängigen Marktpreisen	x		x			x						x			x		x		x	x			
Doppelte Bestellungen					x			x															
Bestellungen werden aufgegeben vor Zustimmung der Abteilungsleitung																							
Keine autorisierte Lieferantenliste/-Datenbank vorhanden								x					x										
Einkauf von ungewöhnlichen Bestellmengen (z.B großen Mengen)									x	x					x								
keine Rabatte, wo Rabatte üblich sind										x		x			x								
Übermäßiger Bezug von Waren oder Dienstleistungen von einem Lieferanten											x				x								
Mehrere kleine Bestellungen desselben Produkts (suggeriert Umgehung von weiteren Autorisierung des Einkaufs)													x									x	
Nichtnutzung der Skaleneffekte durch mangelnde Informationen von früheren Ausgaben														x									

ungewöhnliche Produkte oder Dienstleistungen werden gekauft													x		x								
Telefonisch übermittelte Aufträge																	x						
dringende Aufträge																	x					x	

Tabelle 66: Red Flags Bestellung

Quelle: Eigene Darstellung

Red Flags im Wareneingang

	Kickback, corruption	**Pass Through**	**Scheinfirma**	**generell**	**Billing Schemes**	**Scheinfirma, Pass-Through, Kickback; Bid-Rigging;**	**Scheinfirma**	**Scheinfirma**	**generell**	**Kickback,Veruntreuung von Vermögenswerte**	**generell**	**generell**	**Kickback**	**Angebotsmanipulation**	**Kickback**	**generell**	**Kickback; Bid Rigging, Scheinfirma**	**Vertragsfraud**	**Bid Rigging, Kickback**	**Bid Rigging**	**Scheinfirma**	**Kickback**
	Wells (2003)	Wells (2002c)	Wells (2002b)	Pacini & Brody (2005)	Christensen & Byington (2003b)	Wells (2013)	Cascarino (2013)	Davies (1995)	KPMG International (2010)	Brulenski, & Zayas (2014)	Strand, Judd, & Lancaster (2002)	Verrick (2013)	Kranacher (2008)	Lander, Kimball, & Martyn (2008)	Morehead (2007)	Roberts (2010)	McNamee (2016)	Yang et al., (2017)	Rahmani & Koohshahi (2015)	Nag (2015)	Rendon & Rendon (2016)	Fuseini et al., (2017)
Probleme Wareneingang																						
Fehlmengen				x							x											
Langsame Lieferungen oder minderwertige Leistung des Lieferanten	x		x												x		x	x	x	x		
Kein Wareneingang			x		x					x	x			x								
Keine Eingangsprüfung der Waren durch einen vom Einkauf unabhängigen Mitarbeiter						x												x				
Ungewöhnliche Vorratserhöhung oder -minderung		x		x			x	x				x	x									
Ungewöhnlich hohe Vorräte kombiniert mit entsprechenden Einkäufen von bestimmten Lieferanten							x	x														
ungewöhnliche Lieferzeiten								x														
Qualitativ Minderwertige Produkte	x								x		x					x	x	x	x	x		x
Kein Lieferbeleg										x												

Tabelle 67: Red Flags Wareneingang
Quelle: Eigene Darstellung

Red Flags im Rechnungseingang

	Kickback; Billing Schemes, Inventory Fraud, Payroll	**Scheinfirma**	**generell**	**generell**	**Scheinfirma**	**Scheinfirma, Angebotsmanipulation**	**Kickback**	**generell**	**Billing Schemes**	**generell**	**Scheinfirma**	**Kickback, Scheinfirma, Angebotsmanipulation**	**Scheinfirma, Pass-Through, Kickback; Bid-Rigging;**	**Scheinfirma**	**generell**	**Scheinfirma,**	**Financial Statements, Asset Misappropriation, Corruption,**	**Kickback,Veruntreuung von Vermögenswerte**	**Scheinfirma**	**Scheinfirma, Angebotsmanipulation, Kickback**	**Angebotsmanipulation, Scheinfirma**	**generell**	**Scheinfirma**	**Kickback**	**Billing-Schemes**	**Kickback; Bid Rigging, Scheinfirma**	**Scheinfirma**	**Bid Rigging**
	Wells (2002)	Wells (2002b)	Taylor (2006)	Pacini & Brody (2005)	Lehman (2008)	Ellinor (2009)	Cowan (2005,)	Christensen & Byington (2003a)	Christensen & Byington (2003b)	Christensen & Byington (2002)	Buckhoff & Morris (2002)	Brandman (2000)	Wells (2013)	Cascarino (2013)	Button & Gee (2013)	Davies (1995)	Singleton & Singleton (2010)	Brulenski, & Zayas (2014)	Buckhoff (2002)	Ellinor (2009)	Zikmund (2008)	Strand, Judd, & Lancaster (2002)	Langley (2003)	Morehead (2007)	Byington, & McGee (2012)	McNamee (2016)	Rendon & Rendon (2016)	Vona (2017)
Unstimmigkeit mit Rechnung bei Lieferant																												
schnelle Zahlung der Rechnung																				x								
Abrechnung der Lieferantenrechnungen mehrmals im Monat	x	x					x		x							x												
Rechnung genau unter Autorisierungsobergrenze	x	x						x								x	x											
Große Rechnungssummen in kleinere gesplittet, um keine Aufmerksamkeit zu erregen	x																							x				
Rechnung für unspezifische Consulting oder andere Dienstleistungen	x				x																				x			
Rechnungsbeleg stimmt nicht mit Bestellung oder Wareneingang überein			x						x				x												x	x	x	
Änderung in der Ausgaben				x								x			x													
Rechnungen ohne Rechnungsempfänger					x																							
Rechnungen autorisiert außerhalb von normalen Arbeitszeiten oder von unbefugten Mitarbeitern oder ohne Autorisierung						x							x							x								

Runde Rechnungssummen						x	x				x					x			x	x		x					
Rechnung ohne Bestellanforderung								x																			x
Sich wiederholende Rechnungssummen							x	x	x	x																	
exzessive Geldtransaktion (hohe Rechnungen)								x		x																x	
Zahlreiche Rechnungen von einem Lieferanten										x																	
Aufeinanderfolgende Rechnungsnummern											x					x		x									
Unzureichende Spezifikation der Rechnung (fehlende Preise, Mengen, Beschreibungen, Bedingungen oder Fristen)													x			x	x	x									
Doppelte Rechnungen													x								x				x		
Rechnungsbearbeitung erst nach Bezahlung der Rechnung													x														
(Lieferantenrechnungen werden nicht elektronisch aufgegeben bzw. dokumentiert)														x													
Beschwerden von Lieferanten über die Abrechnung															x												
Lieferanten/Vertragspartner fordern nur einen bestimmten internen Ansprechpartner (suggeriert Kollusion)															x												
Mit Microsoft Excel erstellten Rechnungen																x		x									
Keine oder falsche Mitarbeiter-ID in der Rechnung vorhanden																x		x									
Keine oder falsche Umsatzsteuer-Identifikationsnummer in der Rechnung vorhanden																x		x									
Handgeschriebene Rechnungen																						x					

Tabelle 68: Red Flags Rechnungseingang

Quelle: Eigene Darstellung

Red Flags bei Zahlung

	generell	**generell**	**Scheinfirma,**	**generell**	**Billing Schemes**	**generell**	**generell**	**generell**	**Financial Statements, Asset**	**Scheinfirma,**	**Kickback; Extortion;**	**Scheinfirma**	**generell**	**Kickback; Bid Rigging,**
	Taylor (2006)	Pacini & Brody (2005)	Ellinor (2009)	Christensen & Byington (2003a)	Christensen & Byington (2003b)	Christensen & Byington (2002)	Petrucelli (2013)	PricewaterhouseCoopers (2009)	Singleton & Singleton (2010)	Ellinor (2009)	Grieshober (2001)	Langley (2003)	Roberts (2010)	McNamee (2016)
Unstimmigkeiten bei Zahlungen														
Doppelte Zahlungen	x	x		x			x	x				x		x
Zahlung stimmt nicht mit Rechnungsbeleg überein					x									
Rechnungen bezahlt innerhalb einer Woche nach Rechnungseingang			x						x					
Übermäßige Fracht-/Versandkosten						x					x			
Sonderbelastungen oder Gebühren									x					
Manuelle Zahlung														
Barzahlungen										x				
steigende Preise													x	

Tabelle 69: Red Flags Zahlung

Quelle: Eigene Darstellung

Red Flags Autorisierung, Rückgabe und Allgemein

		Kickback, corruption	**Pass Through**	**Scheinfirma**	**generell**	**Asset Misappropriation, corruption, verhalten,**	**generell**	**Scheinfirma**	**Kickback**	**Billing Schemes**	**generell**	**Kickback, Scheinfirma, Angebotsmanipulation**	**Kickback**	**Scheinfirma, Pass-Through, Kickback; Bid-Rigging;**	**generell**	**allgemein**	**generell**	**Financial Statements, Asset Misappropriation, Corruption, Billing Schemes,**	**Scheinfirma, rezession**	**Kickback, Money Disbursement**	**Scheinfirma, Angebotsmanipulation, Kickback**	**general**	**generell**	**generell**	**Billing-Schemes (Scheinfirma, Pass-Through, pay-und-return, personal purchase);**	**generell**	**Kickback, Angebotsmanipulation**	**Kickback; Scheinfirma**	**Scheinfirma**	**Kickback**	**Scheinfirma**	**Billing-Schemes**	**Kickback; Bid Rigging, Scheinfirma**	**Scheinfirma, allgemein**	**Bid Rigging, Korruption**
	Wells (2003)																																		
Probleme Autorisierung	Wells (2002c)																																		
Fehlende Funktionstrennung	Wells (2002b)																																		
Einkäufe werden gesplittet, um den Autorisierungsprozess zu umgehen	Taylor (2006)	x			x	x			x	x				x			x																	
Keine Autorisierung	Seetharaman, Senthilvelmurugan, & Perivanavagam (2004)	x				x												x																
Häufige Wechsel der Bankkonten	Pacini & Brody (2005)																																		
immer von selben Person Autorisierung	Lehman (2008)																																		
	Cowan (2005)								x	x																									
	Christensen & Byington (2003b)																																		
	Christensen & Byington,2(002)																																		
	Brandman (2000)																																		
	Allen (2007)																																		
	Wells (2013)													x																					
	Petrucelli (2013)														x																				
	KPMG International (2010)																																		
	PricewaterhouseCoopers (2009)								x	x								x																	
	Singleton & Singleton (2010)								x	x					x																				
	Barron (2011)																																		
	Buckhoff, & Parham (2009)																																		
	Ellinor (2009)																																		
	Wells, & Gill (2007)																																		
	Strand, Judd, & Lancaster (2002)																																		
	Verrick (2013)																																		
	Viton (2003)								x	x																									
	Meiners (2005)								x	x																									
	Graycar, & Sidebottom (2012)								x	x																									
	Johnson, & Rudolph (2009)								x	x																									
	Langley (2003)																																		
	Morehead (2007)								x	x																									
	Nilsen (2010)								x	x																									
	Byington, & McGee (2012)								x	x																									
	McNamee (2016)																																		
	Dhurandhar et al., (2015)																																		
	Hudon & Garzon (2016)																																		

Rückgabe																																	
Rückgaben nicht mit Gutschriften übereinstimmend										x																							
Allgemein																																	
Fehlende Dokumentation oder Belege			x		x	x	x			x	x			x							x								x	x		
Unübliche Zeiten					x							x																					
Strohmann															x																		x

Tabelle 70: Red Flags Autorisierung, Rückgabe und Allgemein

Quelle: Eigene Darstellung

Red Flags Ausschreibung

	Kickback, corruption	**generell**	**generell**	**Kickback**	**Kickback, Scheinfirma, Angebotsmanipulation**	**Scheinfirma, Pass-Through, Kickback; Bid-Rigging**	**Bid Rigging**	**Scheinfirma,**	**allgemein**	**generell**	**Kickback; Scheinfirma, Angebotsmanipulation**	**Bid Rigging, Scheinfirma**	**Bid Rigging**	**Bid Rigging**	**Bid Rigging**	**Kickback**	**Angebotsmanipulation**	**Kickback; Bid Rigging, Scheinfirma**	**Bid Rigging**	**Bid Rigging, Kickback**	**Bid Rigging**	**Bid Rigging, Korruption**	**Bid Rigging, Korruption**	**Bid Rigging, Korruption**	**Bid Rigging, Korruption**	**Bid Rigging**	**Bid Rigging, Kickback**	**Bid Rigging, Korruption**	**Bid Rigging, Korruption**	**Bid Rigging, Korruption**	**Korruption**
	Wells (2003)	Pacini & Brody (2005)	McNeal (2014)	Cowan (2005)	Brandman (2000)	Wells (2013)	Durant (2005)	Davies (1995)	KPMG International (2010)	PricewaterhouseCoopers (2009)	Fishman (2001)	Zikmund (2008)	Lambert-Mogiliansky, & Sonin (2006)	Lander, Kimball, & Martyn (2008)	May (2005)	Morehead (2007)	Sammons (2005)	McNamee (2016)	Vona (2017)	Rahmani & Koohshahi (2015)	Nag (2015)	Gong & Zhou (2015)	Ferwerda et al., (2016)	Fazekas et al., (2016)	Boag (2015)	Nanang & Misman (2016)	Zasada & Fellmann (2016)	Erven, Holanda & Carvalho (2017)	Kohler et al. (2015)	Hudon & Garzon (2016)	Al-ajwad & Carr (2016)	Bhattacharya & Suri (2017)
Ausschreibung																																	
Verträge formuliert, um Wettbewerb auszuschalten (z. B. Rechtfertigung des Bezugs aus einer Quelle)	x	x		x	x	x				x		x	x				x	x	x	x	x	x	x	x								
Derselbe Lieferant erhält häufig den Zuschlag durch ein Angebot, das nur minimal besser ist	x										x					x		x						x								
Fehlende Transparenz														x			x			x	x		x		x	x	x						

Das zuletzt abgegebene Angebot erhält stets den Zuschlag	x														x														
Lieferant, der ohne klaren Wettbewerbsvorteil regelmäßig den Zuschlag erhält	x		x	x																									
Wenn ein neuer Lieferant der Auktion beitritt, beginnen die Angebotspreise zu fallen (suggeriert Kollusion der bis dahin bietenden Lieferanten)			x			x																							
Es beteiligen sich weniger Bieter an der Ausschreibung als üblich (suggeriert absichtliche Begrenzung des Wett-bewerbs)			x																		x								
Qualifizierte Lieferanten geben keine Angebote ab (möglicherweise ist keine Einladung erfolgt, um den Wettbewerb zu begrenzen)			x			x	x	x									x	x											
Alle Lieferanten geben zu hohe Angebote ab			x															x											
Das Gebot, das den Zuschlag erhält, ist zu hoch			x				x			x								x											
Die gleichen Lieferanten bieten für jede Projekt- oder Produktausschreibung (suspekt, wenn es sich um grundverschiedene Produkte handelt)			x														x												
Ein Lieferant gewinnt Großteil der Ausschreibungen (Vertragsumfang unproportional zur Größe des Lieferanten)	x			x		x	x	x																					
Preisänderungen, nachdem Angebote anderer Lieferanten eingesehen werden dürfen						x																							
Annahme von spät eingegangenen Angeboten						x	x	x									x	x			x								
(Fälschung von Qualifikationen, Erfahrung, Kapazität, Ausstattung oder Personal des Lieferanten)						x							x																
(Hinweise einer Beziehung zwischen Bietern)						x											x	x	x		x	x	x				x	x	x
Publizieren von Auftragsausschreibungen in unbedeutenden Publikationen oder während der Urlaubszeiten, um den potenziellen						x											x						x						

Wettbewerb einzuschränken																														
(Preisgabe von Informationen an bevorzugten Lieferanten)						x												x	x										x	x
Starke Begrenzung der Zeitspanne zur Angebotsabgabe (so dass nur Lieferanten mit Informationen im Voraus entsprechend Zeit haben ihr Angebot vorzubereiten)						x												x	x	x			x	x						
Aufteilung eines Auftrags in mehrere Teilaufträge, um Kontrollinstanzen zu umgehen						x								x					x		x	x								
(Lieferant im Ausschreibungsprozess involviert (z. B. in der Auftragsspezifikation)						x													x			x							x	
keine Ausschreibung							x												x			x				x				
(Zahlreiche Anpassungen des Vertrags)								x											x				x						x	
(Änderungen der Kostenspezifikation nach Vertragsvergabe)								x											x				x							
Günstiges Angebot aber viele Änderungsanforderungen (suggeriert Kollusion mit dem Lieferanten)									x																					
ungerechtfertigte Vorauszahlung																x														

Tabelle 71: Red Flags Ausschreibung

Quelle: Eigene Darstellung

Red Flags Verhalten

	Kickback, corruption	**Asset Misappropriation, corruption, verhalten,**	**generell**	**generell**	**Kickback**	**generell**	**generell**	**Kickback, Scheinfirma, Angebotsmanipulation**	**Kickback**	**Scheinfirma, Pass-Through, Kickback; Bid-Rigging;**	**generell**	**Scheinfirma**	**generell**	**generell**	**generell**	**generell**	**generell**	**Conflict of Interest,**	**Kickback; Scheinfirma, Angebotsmanipulation**	**general**	**generell**	**Mitarbeiter**	**generell**	**Billing-Schemes (Scheinfirma, Pass-Through, pay-**	**Kickback, Angebotsmanipulation**	**Kickback; Extortion; Angebotsmanipulation;**	**Kickback; Scheinfirma**	**Scheinfirma**	**Persönliches**	**generell**	**Angebotsmanipulation**	**Kickback; Bid Rigging, Scheinfirma**	**Bid Rigging, Kickback**	**Bid Rigging, Korruption**	**Bid Rigging, Korruption**	**Bid Rigging, Korruption**

	Wells (2003)	(Seetharaman, Senthilvelmurugan, &	(Pacini & Brody, 2005, S. 59)	(McNeal, 2014, S. 40)	(Cowan, 2005, S. 32–33)	(Christensen & Byington, 2003a, S. 25)	(Christensen & Byington, 2002, S. 43)	(Brandman, 2000, S. 40–41)	(Allen, 2007, S. 15)	(Wells, 2013, S. 279–281, 2013, S. 247,	(Petrucelli, 2013, S. 327, 2013, S. 15)	(Cascarino, 2013, S. 192–195)	(Button & Gee, 2013, S. 91–92)	(PricewaterhouseCoopers, 2009, S. 17)	(Association of Certified Fraud Examiners,	(Imoniana, Antunes, & Formigoni, 2013,	(Strand, Welch, Holmes, & Strawser, 2000,	(Handfield & Baumer, 2006, S. 43)	Fishman (2001)	Wells, & Gill (2007)	Strand, Judd, & Lancaster (2002)	Thompson (2000)	Verrick (2013)	Viton (2003)	Graycar, & Sidebottom (2012)	Grieshober (2001)	Johnson, & Rudolph (2009)	Langley (2003)	McNeal (2012)	Roberts (2010)	Sammons (2005)	McName (2016)	Rahmani & Koohshahi (2015)	Al-ajwad & Carr (2016)	Zasada & Fellmann (2016)	Hudon & Garzon (2016)
Verhalten																																		
Plötzliche Veränderungen im Verhalten/ Veränderungen in der (Arbeits-) Moral											x		x	x			x			x	x												
Unfähigkeit den anderen Mitarbeitern in die Augen zu schauen														x																				
Erhöhte Reizbarkeit		x												x	x																			
Ungeregelter/auffälliger Werdegang														x		x																		
Charakterliche Probleme (Labilität)														x											x									
Durchgängige Wut														x	x																			
Tendenz andere zu beschuldigen														x																				
Veränderung(en) im Lebensstil / Leben über eigene Verhältnisse / extravaganter Lebensstil		x					x	x		x	x			x	x	x						x		x		x	x			x			
Unzufriedenheit mit dem Arbeitgeber oder Vorgesetzten														x	x	x																		
Mitarbeiter hat nie Urlaub oder freie Tage (suggeriert Angst vor der Aufdeckung der dolosen Handlungen)			x				x	x			x		x	x	x	x						x											
Finanzielle Sorgen, Schulden							x			x				x	x	x								x				x						
Anzeichen von psychischen Problemen														x		x																		
Ständige Beschwerden über den Vorgesetzten, die Firma, Kollegen oder der Verdienst											x			x	x																		
Kontrollsucht														x															x					
Ablehnung jeglicher Versetzung von der aktuellen Arbeitsstelle (suggeriert Angst vor Aufdeckung); Ablehnung von Beförderung							x		x					x																			

Beziehungen zwischen Beschäftigten und autorisierten Lieferanten	x			x	x	x		x			x		x	x	x			x	x	x					x	x		x	x	x	x	x	x	x	
Widerwille zur Funktions- oder Verantwortlichkeitsteilung; Mitarbeiter hat Kontrolle und macht alles selbst											x				x					x														
Familien- oder Scheidungsprobleme															x													x						
Suchtprobleme (Spiel-, Alkohol oder Drogensucht)								x		x					x							x												
Exzessiver Druck innerhalb des Unternehmens (erhöhte Motivation zur Betrugsbegehung)															x																		x	x
Exzessiver Druck aus der Familie oder dem Lebensumfeld															x																			
Rechtliche Probleme in der Vergangenheit															x																			
Mitarbeiter wickelt Tranaktionen außerhalb gewöhnlicher interner Kanäle ab											x		x																					
Mitarbeiter pflegt feindliche Einstellung gegenüber internen Kontrollmechanismen											x																							
Mitarbeiter überschreitet seinen Verantwortungsbereich							x			x										x														
Unerlaubte Überstunden							x								x							x												
Arbeiten außerhalb der normalen Arbeitszeiten															x							x												
Hinweise von anderen Mitarbeitern		x							x																									
Mitarbeiter unterzeichnet keine Interessenkonflikt-Richtlinien				x																														
Mitarbeiter rechtfertigt Produkt- oder Dienstleistungsfehler eines Lieferanten				x																														
Mitarbeiter akzeptiert regelmäßig unangemessene Geschenke von Lieferanten	x			x														x	x	x					x				x	x	x		x	x	x
Zögern, Informationen dem Auditor preiszugeben												x																						
Personal überlastet ohne hohes Arbeitspensum													x																					

(suggeriert verdeckte Handlungen)																																	
Mitarbeiter hat externe Geschäftsinteressen												x						x															
Autorität und Kontrolle sind auf einen Mitarbeiter konzentriert												x						x		x													
Geringe Gehälter							x																	x									

Tabelle 72: Red Flags Verhalten
Quelle: Eigene Darstellung

Anhang F: Ergebnisse der Thinking Aloud Methode

Fragebogen

Teil 1: Allgemeine Fragen

Persönliche Angaben:

- Alter 25-35, 35-45, 45-55, 55-65

- Geschlecht: m/w

Angaben zum Unternehmen:

- Branche:

- Wie viele Jahre haben Sie Erfahrung in dem Beruf?

- Welche Position haben Sie im Unternehmen? / Für welche Aufgaben sind Sie zuständig?

Teil 2: Beschreibung der aktuellen Situation

Wie gehen Sie typischerweise in Ihrem Unternehmen vor, um Fraud aufzudecken?

Wie verwenden Sie Data Mining, Red Flags oder Process Mining?

Falls ja, welche Erfahrungen haben Sie damit gemacht?

Was ist aus Ihrer Sicht verbesserungswürdig?/Wo sehen sie ihre aktuellen Herausforderungen?

Teil 3: Validierung der Fraud Schemata (Fraud Patterns)

Es werden 8 Fraud Schemata kurz erklärt (siehe Anhang), die typischerweise im Einkaufsprozess eines Unternehmens vorkommen können. Einige Fragen hierzu:

- Ist die Liste der Schemata aus Ihrer Sicht vollständig. Fehlen noch Schemata? Wenn ja, welche?

Neben den reinen Schemata, wurden die dazugehörigen Red Flags (Hinweise auf Fraud) hinzugefügt.

- Fehlen aus Ihrer Sicht noch weitere Red Flags?

- Welche 3-4 der genannten Red Flags erachten Sie als die wichtigsten pro Schema?

- Was sind die größten Herausforderungen mit ihrer aktuellen Kombination von Red Flags?

- Für bestimmte Werte wurden Treshholds angenommen. Beispielsweise sind die Grenzen für Freigaben bei jedem Unternehmen unterschiedlich. Können Sie aus Ihrer Berufspraxis Annäherungswerte für die im Anhang genannten Thresholds liefern?

Teil 4: Testszenario

In diesem kurzen Test wird das Testverfahren Thinking Aloud durchgeführt. Sie sehen eine Anwendung, die auf Basis von Celonis Process Mining und dem Red Flag Ansatz Fraud identifiziert. Sie werden dazu einige kleine Testaufgaben erhalten.

Bitte fühlen Sie sich frei all ihre **Schritte, Gedanken und Kritiken zu kommentieren**! Aus ihren im Test getätigten Aussagen während des Tests werden weitere Verbesserungen für den Prototypen abgeleitet.

Sie sind Fraud Investigator und müssen den Einkaufsprozess eines Fahrradgroßhändlers hinsichtlich Fraud überprüfen.

- Wie viele Fraud Patterns werden identifiziert?
- Suchen Sie nach der Prozessinstanz mit den meisten identifizierten Red Flags und filtern Sie danach.
    - wie viele Red Flags hat diese Prozessinstanz.
    - welche Prozessschritte wurden hier erstellt?

- Filtern Sie nach dem Fraud Schema „Scheinfirma“ Fraud.

    - Wählen Sie eine beliebige Prozessinstanz mit dem entsprechenden Fraudschema.

- Welche Mitarbeiter waren hier beteiligt.
- Wie ist der Prozessinstanz abgelaufen?

Weitere Fragen:

- Welche Informationen zur Identifikation von Fraud vermissen Sie?
- Können Sie sich vorstellen diesen Prototypen auch im täglichen Einsatz für die Frauderkennung einzusetzen?

- Was fehlt Ihnen für die Einsetzung und was würden Sie besser machen?

- Haben wir aus ihrer Sicht etwas Wichtiges in diesem Thema vergessen?

Vielen herzlichen Dank für ihre Teilnahme!

Anforderungen Prozesssicht

Anforderung	Beschreibung	Interviewzitate	Darstellung
Proz_01	Darstellung der Anzahl von Prozessinstanzen	"Da müsst ihr aufpassen, wie viele Prozessinstanzen es gibt ist eine Prozesskennzahl. Die würde ich auch hoch tun zu den Prozesskennzahlen, nicht zu den Fraudkennzahlen" "Generell würde ich die Informationen, die ihr schon drin habt auch drin lassen".	Kennzahl
Proz_02a	Top 10 der Lieferanten	"Eure Top10 der Lieferanten, vielleicht auch der Einkaufssumme pro Produkt könnt ihr drin lassen. Dann kann man sich im Prozess besser orientieren"	Kreisdiagramm
Proz_02b	Top 10 teuerste Produkte		Kreisdiagramm
Proz_03a	Anzahl von aktiven Mitarbeitern	" Als Übersicht finde ich es gut, dass man die aktiven Mitarbeiter, die Rechnungssumme usw. sieht. Praktisch so wie ihr es gemacht habt würde ich es belassen."; "Grundsätzlich finde ich das schon ganz gut mit den Kennzahlen für Fraud und zum Prozess im Allgemeinen. Das kann man schon so lassen"; "Bei Fraud muss man alles immer in Relation sehen. Beispielsweise in Relation von der Gesamtsumme. Deshalb würde ich das mit reinnehmen."; "Zusammenfassung von Informationen, wie beispielsweise die Anzahl der Bestellungen, das Volumen der bestellten Materialien,	Kennzahl
Proz_03b	Anzahl bestellte Materialien		Kennzahl
Proz_03c	Anzahl an Lieferanten		Kennzahl
Proz_03d	Rechnungsbetrag		Kennzahl
Proz_03e	Anzahl eingegangener Rechnungen		Kennzahl

		identifizierte Red Flags sind wichtig."	
Proz_04	Mandant/Buchungskreis	"Da wir ja mit mehreren Mandanten arbeiten wäre es gut, wenn man auswählen kann welcher Mandant jetzt ausgewertet wird. Oder die verschiedene Buchungskreise. GBI ist ja in Deutschland und in Amerika aktiv. Wir haben ja ganz schnell gemerkt, dass es in Deutschland nicht so gut konfiguriert ist das System. Deshalb sollte man Amerika auswählen."	Dropdown-Liste oder Tabelle
Proz_05a	Anzahl von Fraud Patterns	"Übersicht über die Anzahl der identifizierten Fraud wäre gut, aber nicht nur alleine. So fehlt beispielsweise so ne Art Kategorisierung oder so."; "Auch die Anzahl der Fraud patterns finde ich gut. Vielleicht macht es auch Sinn da nochmal zu unterscheiden. Beispielsweise könnte man untersuchen, wie hoch der Verlust pro Fraud Pattern ist. Das kann man ja auch für die Red Flags machen", "Die Übersicht würd ich so lassen, wie ihr sie habt";"Red Flags bezieht sich ja sofort auf die Fraud Patterns. Ok, das passt. Prozessinstanz mit den meisten Red Flags ist gut. Man kann im Vorhinein danach sortieren, damit nicht der Auditor das machen muss. Und man kann es bspw. auf 500 Einträge limitieren. Es kann sein, dass es dir dann nur 500 anzeigt. Ich weiß an dieser Stelle nicht wie das System funktioniert, warum also der Fehler war"	Kennzahl
Proz_05b	Schadenssumme pro Fraud Pattern		Tabelle
Proz_06a	Anzahl von Red Flags		Kennzahl
Proz_07b	Schadenssumme pro Red Flag		Tabelle

Tabelle 73: Anforderungen für die Prozesssicht

Quelle: Eigene Darstellung

Anforderungen Schemaansicht

Anforderung	Beschreibung	Interviewzitate	Darstellung
Schem_01	Identifizierte Red Flags	"In der Patternsicht würde ich dann Details über die Patterns und entsprechend auch dann den Red Flags erwarten."	Tabelle

Schem_02	Filtermöglichkeit nach Fraud Patterns	"Mich würde jetzt interessieren welche Fraud Patterns du identifiziert hast, nicht nur wie viele."; "Ich sehe jetzt 108 Fraud Patterns, was heißt das jetzt konkret. Also welche Verteilung haben diese, wie kann ich diese jetzt genau erklären?"; "Man sollte jetzt beispielsweise nach den Fraud Patterns filtern können. Dann kann man sehen, welche Prozessinstanz dazu gehört."	Tabelle
Schem_03a	Filtermöglichkeit nach Red Flags	"Was ich ganz spannend finden würde, ist, welche Prozessinstanz jetzt wie viele Patterns hat. Das habt ihr ja so schon drin. Aber vielleicht nicht nur die Anzahl der Red Flags. Ich mein, es kann ja sein, dass eine Prozessinstanz wo nur wenig Geld dahinter steckt... das bei so einer Prozessinstanz viele Red Flags auftauchen. Vielleicht braucht man dann die teuersten Prozessinstanzen mit Red Flags"; "Was natürlich auch spannend ist, ist über wie viel Geld wir bei einem Red Flag oder Fraud Pattern sprechen."; "Die Red Flags anhand der Transaktion zu zeigen ist gut. Dann sieht man welche Red Flags jetzt zu welcher Prozessinstanz gehören. Ich stell mir das so vor: Man filtert nach einer Prozessabweichung zum Beispiel und sieht dann welche Red Flags noch zusätzlich vorkommen. So sieht man dann welcher Fraud tatsächlihc vorgekommen ist"; "Ich kann das jetzt nur auf den WCHC beziehen. Da haben wir ja oft das Problem, dass die Leute erstmal rumprobieren. Da würde es schon helfen, wenn man dann ne Übersicht hat von den Red Flags die vorgekommen sind. Beispielsweise kann man meistens ignorieren, wenn jemand keine MwSt. ausgewählt hat. Bei uns ist das aber wichtig.	Tabelle: Möglichkeit nach Top 10 Transaktionen mit den meisten Red Flags oder nach den Top 10 Transaktionen mit der höchsten Verkaufsvolumen zu sortieren) Tabelle Tabelle
Schem_03b	Top Transaktionen (nach Anzahl Red Flags/ nach Transaktionsvolumen)		
Schem_03c	Darstellung von verdächtigen Prozessinstanzen und der Anzahl von Red Flags		
Schem_03d	Anzal Fraud Patterns		Balkendiagramm
Schem_04a	Übersicht über die aufgetretenen Fraud Patterns	"Man könnte beispielsweise darstellen, welche Fraud Patterns wie oft vorgekommen sind"; "Eine Darstellung der Verteilung der Red Flags wäre hilfreich"; "Natürlich würde ich jetzt erstmal erwarten, dass es mir zeigt, welche Red Flags vorkommen, wie diese verteilt sind und dann das gleiche auch für Fraud Patterns";"Man könnte jetzt z.B. zeigen wie sich die Red Flags verteilen."	Balkendiagramm
Schem_04b	Übersicht über die aufgetretenen Red Flags		Kreisdiagramm

Schem_05	Genaue Beschreibung der Red Flags	"Also ich finde es ist sehr wichtig zu verstehen, was euer Red Flag genau macht. Ich finde die Titel nicht immer selbsterklärend. Deshalb braucht es eine präzise Beschreibung, was dieses Red Flag genau tut. Man muss zumindest erklärt bekommen, was fehlt. Eine Erklärung wäre ganz gut möglich..[...] Kann man eine Langbeschreibung reinbekommen?", "Mir ist nicht immer ganz klar, was z.B. jetzt der Same-Same-Different Test macht. Es kann ja sein, dass es total bekannt ist bei professionellen Fraud Auditoren. Aber so ne Definition der Red Flags und der Patterns wäre hilfreich"; "Vielleicht hilft es die Implementierung der Red Flags irgendwie darzustellen. Dann kann man sich leichter darunter was vorstellen"; "Ich würde noch was dazu [zu den Red Flags] machen. So ne Beschreibung z.B."; "Wenn ich mir euren Prototypen so ansehe, finde ich den schon ganz gut. Ich würde jetzt aber nicht davon ausgehen, dass jeder jedes Red Flag kennt. Ihr müsst da etwas präziser sein."	Tabelle
Schem_06	Darstellung der Red Flags und Fraud Patterns in Diagrammen	"Man müsste irgendwie darstellen, welche Red Flags nun zu welchem Fraud Pattern gehören. Das würde helfen die Patterns besser zu verstehen"; "Vielleicht hilft es ja eine Tabelle darzustellen, die zu jedem Pattern Red Flags aufzeigt"; "Was könnte man noch machen? Also in der Schemasicht würde ich jetzt Details zu den Fraud Patterns und Red Flags zeigen, sowas wie welches Red Flag gehört zu welchem Fraud Pattern.";	Tabelle
Schem_07	Zeitlicher Verlauf der Red Flags	"Man kann ja anzeigen, wie sich die Red Flags über die Zeit entwickeln. Vielleicht werden das ja mit der Zeit mehr und dann weiß man, dass es sich dann wahrscheinlich um Fraud handelt."	kann nicht abgebildet werden

Tabelle 74: Anforderungen an Schemaansicht

Quelle: Eigene Darstellugn

Anforderungen Mitarbeitersicht

Anforderung	Beschreibung	Interviewzitate	Darstellung
Mitarb_01	beteiligte Mitarbeiter sollen (pseudonymisiert) dargestellt werden	"Mich würde interessieren, welche Mitarbeiter da beteiligt sind. Manchmal ist das ja nur einer, was ja ein guter Hinweis auf Fraud ist" "Man soll natürlich aufpassen, weil nicht alle Mitarbeiter rausgegeben werden dürfen. Das erlaubt ja schon der Betriebsrat nicht. Dennoch muss es irgendwie anonymisiert werden und anschließend herausgegeben"; "Beteiligte Mitarbeiter, da wäre ich vorsichtig. Da müssen wir das immer pseudonymisierte Mitarbeiter. Aber so, wenn ein neuer Mitarbeiter kommt, dann muss immer der gleich da steht."	Tabelle

Mitarb_02	Art des Users (Dialog vs. Systembenutzer) sollte erkennbar sein	"Es gibt ja einen Unterschied welche Art von Benutzer, also ein Dialog oder ein Systembenutzer, den Schritt durchgeführt hat. Hier in dem Prototypen vermute ich mal, dass CMRemote ein Systemuser ist. Das soll ich aber nicht raten, dass soll da stehen." "Welcher Benutzertyp steht dahinder, IDESESC sollte jetzt ein Systembenutzer. Es wäre aber hilfreich, wenn man weiß ob eine Person oder ein Prozess eine Bestellung oder Bestellanforderung erstellt hat"	nicht möglich
Mitarb_03	Es sollte ersichtlich werden zu welcher Einkäufergruppe der Mitarbeiter gehört	"Was könnte man noch für den Mitarbeiter benötigen. Beispielweise ist die Einkäufergruppe interessant. Dann kann ich sehen von wo der Mitarbeiter kommt."; "Man muss bisschen was über die Struktur der Firma erfahren"	Tabelle
Mitarb_04	Die Anzahl der beteiligten Mitarbeiter ist notwendig	"Bei uns war das ja oft so, dass wir alles mit einem User gemacht haben, um es auszuprobieren. Trotzdem ist es ja nicht in der Praxis so üblich. Deshalb würde ich eine Kennzahl mit der Anzahl der beteiligten User machen" "Du hattest im WCHC ja mal gesagt, dass wir das nicht alles mit einem User machen sollen, sondern realistischer. Trotzdem haben es viele nur mit einem gemacht. Das war für uns ein guter Hinweis auf Fraud". "So ne Übersicht von Transaktionen, die von nur einem Üser gemacht wurden ist hilfreich."	Gesamter Prozessinstanz von einem Mitarbeiter durchgeführt = Red Flag; entsprechende Mitarbeiter pro Prozessinstanz werden in einer Tabelle angezeigt
Mitarb_05	Die Anzahl der Vorgänge, die von einem Mitarbeiter erledigt wurden	"Mich interessiert auch wie viele Vorgänge durch welchen Mitarbeiter geflossen sind"; "Es ist ja immer ein Hinweis für Fraud, was ein Mitarbeiter alles macht, bzw. wie viel einer macht. Deshalb würde ich anzeigen, was ein Mitarbeiter alles macht"	Kreisdiagramm
Mitarb_06	Soziales Netzwerk zwischen den Mitarbeitern darstellen, um kooperation zu erkennen	"Ich würde es spannend finden, welche Mitarbeiter miteinander agieren. Ich könnte mir vorstellen dass so ein soziales Netzwerk entsteht, so wie bei Facebook. Man könnte beispielsweise zeigen, wie eng Mitarbeiter zusammenarbeiten (bspw. über die dicke der Linien)."; "Eine Beziehung zwischen den Mitarbeitern sichtbar zu machen würde helfen."; "Welche Mitarbeiter sich wie wann ausgetauscht haben. Wenn du alle Mitarbeiter im Kreis darstellst und dann zeigst wie sich die Mitarbeiter austauschen. Ich weiß nur nicht, ob sich das mit Celonis darstellen lässt."	nicht möglich

Mitarb_07	Mitarbeiter in Verbindung mit Bestellung/ Bestellanfoderung/ Wareneingang	"Es wäre noch interessant, welcher Mitarbeiter genau was gemacht hat. So könnte man beispielsweise anzeigen, welcher Mitarbeiter für wie viel Geld genau was kauft. Also praktisch sowas wie: Mitarbeiter, Material, und Preiseinheit. Dann sollte man darauf filtern können"; "Ich bin ja so jemand der immer nochmal ins ERP System schaut, weil ich mich auf solche Dashboards nicht so verlasse. Deshalb wäre eine detaillierte Darstellung eines Prozesses interessant (also wer hat was getan). Dann kann es sein, dass ich auch nicht immer ins ERP System schauen muss beim WCHC"	Tabelle für jeden Prozesschritt (Banf, Wareneingang, Änderungen durchgeführt, Bezahlung)

Tabelle 75: Anforderungen Mitarbeitersicht
Quelle: Eigene Darstellung

Anforderungen Lieferantensicht

Anforderung	Beschreibung	Interviewzitate	Darstellung
Lief_01	Darstellung des Banklandes und des Landes aus dem der Lieferant seinen Sitz hat (Markierung wenn diese beiden Werte voneinander abweichen)	"Ich finde es sehr verdächtig, wenn der Lieferant in einem bestimmten Land sitzt, indem er keine Bankdaten hat. Also sollte mir das Tool das Land zeigen, indem er sitzt und wo er sein Konto hat. Sollte es zu Abweichungen kommen, so sollen bitte eine rote Markierung oder so kommen"; "Mich interssieren die Ländern. Ein Red Flag was mich interessieren würde, wäre wenn das Lieferantenland von dem Bankland abweicht. Du kannst bei der IBAN vorne DE dran erkennen, dass das Konto in Deutschland hat. Wenn du ein deutscher Lieferant bist und deine Bank in den Cayman Islands liegt, dann ist das ein bisschen ungünstig."	Tabelle: Lieferantenland vs. Bankland (leider keine farbliche Markierung bei Unterschied möglich)
Lief_02	Volumen des „Fraud“-Einkaufs vs. Einkaufsvolumen insgesamt sollte dargestellt werden	"Wichtig ist die Fraud Summe. Für 2,50 € rechnen sich die Kosten für die Identifikation des Frauds gar nicht. Also würde mich interessieren, wie hoch die geschätzte Summe ist. Und wie viel dieser Lieferant sonst liefert. Also so ne Art Abhängigkeit von der Gesamtsumme. Dann kann ich bewerten, wie hoch der Schaden ist"; "Cool wäre es, wenn man gleich sehen würde wie hoch der Schadensfall ist"; "Was mir noch fehlt ist, wie groß der Fraud ist. So ein Kugelschreiber zu klauen ist jetzt nicht so schlimm, wie bspw. einen Laptop mitzunehmen."	Kreisdiagramm
Lief_03	Darstellung des Volumens des Einkaufs	"So n Bubble Chart macht durchaus sinn.Praktisch pro Einkauf wie viel der Betellpreis war. So kann man z.B. Ausreisser gut erkennen"	Bubble Chart (Lieferant vs. Bestellpreis)

Lief_04	Volumen und Anzahl der Einkäufe pro Lieferant sollen dargestellt werden	"Volumen und Anzahl pro Lieferant und pro Pattern wäre interessant. Also du kannst Sachen einstellen, die nicht gefiltert werden können. Weil ich kann dann sehen wie viel Prozent davon Fraud ist. Soviel Prozent von meinem Einkaufsvolumen betrifft es denn jetzt?"	
Lief_4a	Darstellung der Anzahl der Einkäufe bei diesem Lieferanten	"Auch kann in diesem Zug gezeigt werden, wie viele Einkäufe pro Lieferant (also jetzt rein auf die Anzahl, oder das Volumen) getätigt werden."; "Auch hier würde ich erstmal ein Übersicht machen über welche Lieferanten gibt es, wie viel wird bei ihnen gekauft usw"	Kreisdiagramm
Lief_4b	Darstellung der Einkaufsvolumina pro Lieferant		Kreisdiagramm
Lief_05	Distanz zum Warenempfänger soll dargestellt werden	"Ich weiß nicht ob man das Darstellen kann, aber so ne Distanz. Man sollte den Lieferweg sehen. Es macht beispielsweise keinen Sinn kleine Ersatzteile vom anderen Ende der Welt einzukaufen"	Nicht mit Celonis realisierbar
Lief_06	Darstellung der Anzahl von Lieferanten pro Land	"Eine Übersicht über die Lieferanten pro Land wäre wichtig. So kann man beispielsweise erkennen, wenn es zu Kooperationen mit eher korrupten Ländern kommt.";"Man sollte sehen können, aus welchem Land die Lieferanten kommen."	Kreisdiagramm
Lief_07	Schlafende und wieder aktive Lieferanten	"Es ist wichtig zu sehen wenn beispielsweise ein Lieferant für 12 Monate geschlafen hat und plötzlich wieder aktiv ist und neue Rechnungen verschickt."	Red Flag
Lief_08	Anzahl der Red Flags pro Lieferant	"Wenn man rausfinden will, welcher Lieferant wahrscheinlich kriminell ist, so macht es vielleicht Sinn, wenn man eine Aufstellung von Red Flags pro Lieferant macht"; "Ganz nach dem Motto viel hilft viel: Die Top Lieferanten mit den meisten Red Flags darstellen und dann nach diesen Lieferanten filtern lassen."; "Ich weiß nicht ob das geht, aber vielleicht so die Red Flags die sich jetzt speziell auf den Lieferanten beziehen genau anzeigen. Oder eben einfach die Red Flags pro Lieferant (also Anzahl der Red Flags pro Lieferant)."	Kreisdiagramm
Lief_09	Bestellvolumen/ bestellte Ware pro Lieferant	"Ich würde den Lieferanten noch mit Ware verknüpfen. Also praktisch eine Tabelle bei der dann aggregiert festgehalten wird welche Ware bei welchem Lieferant für welchen Preis gekauft wird."	Tabelle

Tabelle 76: Anforderungen Lieferantensicht

Quelle: Eigene Darstellung

Anforderungen Materialsicht

Anforderung	Beschreibung	Interviewzitate	Darstellung

Mat_01	Darstellung welches Material gekauft wurde; Darstellung der Mengen und der Einheit (Stück, Palette usw.)	"Ein Kollege hat neulich ein Netzteil auf der Dienstreise gekauft. Wir waren beim Kunden und ohne Netzteil konnte er nichts machen. Also musste er in den Saturn nebenan und sich ein Netzteil kaufen. Ob das jetzt ein Netzteil für seinen Laptop ist kann dir später keiner mehr nachweisen. Das ist so ein privater Einkauf, den man super über die Dienstreiseabrechnung abrechnen kann."; "Da hilft ja zunächst mal eine Übersicht welches Material, in welcher Stückzahl und zu welchem Preis eingekauft wurde"; "Worüber reden wir denn hier eigentlich? Mich würde interessieren was genau gekauft wurde"; "Wenn man auf ein bestimmtes Fraud Pattern filtert, dann würde mich interessieren welche Materialien betrifft das alles, wie viel und in welchre Einheit"	Tabelle
Mat_02 a	Darstellung wie häufig ein Material gekauft wird	"Wie häufig das Material (vielleicht noch irgendwie geclustert) gekauft wurde würde mich noch interessieren"; "Ein bisschen noch die Materialgruppe, bzw. Materialklassen würde mich noch interessieren"	Kreisdiagramm
Mat_02 b	Darstellung wie häufig eine Materialgruppe gekauft wurde		Kreisdiagramm
Mat_03 a	Preis aller Bestellungen Pro Material	"Es gibt ja ein internes Kontrollsystem. Bis zu einem gewissen Grad darf ich ja selbst einkaufen. Ich geh ja davon aus, dass es ab irgendwann problematisch wird, weil ich mindestens einen brauche der noch Mitspielt. Und wenn einer dann mitmacht, dann kann ich jedes System umgehen. Aber so einen dreistelligen Bereich, ist scheiße, tut aber dem Unternehmen nicht weh. Wenn das auffliegt, dann kommt ist der Mitarbeiter raus, mehr aber auch nicht."	Kreisdiagramm
Mat_03 b	Preis aller Bestellungen Pro Materialgruppe		Kreisdiagramm
Mat_04	Falls Möglich: Darstellung ob es sich um ein verderbliches Material handelt	"Ich weiß nicht in wieweit das in SAP implementiert ist, aber ich könnte mir noch vorstellen, dass man einzieht ob es sich um verderbliche Materialien handelt. Sowas kann man noch mit reinziehen"	leider passendes Feld in SAP Tabellen nicht gefunden
Mat_05	Handelt es sich um ein Commodity oder Spezialmaterial	"Unterschiede wirst du sehen zwischen Commodity und Spezialthemen, also Spezialkäufe und Logistikkäufe."	Keine Aufteilung zwischen Commodity und Spezialmaterial in SAP Tabellen; Deshalb Aufteilung Material

			oder Dienstleistung
Mat_06	Darstellung, wenn es sich um eine Dienstleistung handelt	"Beispielsweise habe ich einen Maler. Dem würde ich einen Auftrag gaben f´ür 900Euro. Ich würde ihm nur nicht die Firmenadresse, sondern meine Adresse zu Hause geben. Ich würde aber den normalen Wareneingang machen. Dann siehst du es gar nicht. Du kannst eigentlich nur über den Text gehen. Also die Beschreibung rein."	Karstellungdiagramm
Mat_07	Logistikeinkäufe	Wenn ich Logistikeinkäufe kaufe, wirst du Unterschiede sehen.	keine Möglichkeit gefunden
Mat_08	Zeitl. Verlauf Einkaufsvolumen pro Produkt	"Es wäre spannend zu erfahren, wie der zeitliche Verlauf eines Produktes aussieht, also gibt es spitzen wann dieser besonders oft gekauft wird und wann dieser kaum eingekauft wird"	Zeitreihe

Tabelle 77: Anfoderungen Materialsicht

Quelle: Eigene Darstellung

Zusätzliche Allgemeine Anforderungen

Anforderung	**Zitat**
Trennzeichen in Zahlen sind notwendig	"Zuerst einmal: Die Punkte müssen rein. Man braucht Trennzeichen, sonst kann das kein Mensch lesen."
Anschauliche Graphen (Kreisdiagramm Bar Chart)	„Visualisierungen helfen.“; Ich würde noch ein paar Diagramme rein. Man könnte noch mehr Balken-, Kreis- usw.. Diagramme reinnehmen.
Filterung nach Fraud Patterns und Red Flags	„Was ja bei Celonis echt gut ist, vor allem jetzt mit der neuen Version. Man kann ja jetzt Filtern und das wird dann auf alle möglichen Fraud Diagrammen und Tabellen ausgeführt.“
Kleinere Schriftart verwenden	"Für mich müssen die Zahlen nicht so groß sein, ich bin noch relativ gut im Lesen. Für mich muss auch Prozessübersicht allgemein nicht so groß sein."
Sichten reinlassen	"Ich finde es schon ganz gut wie ihr es gemacht habt mit den Sichten. Da fehlen mir nur paar Informationen"; "Wenn man alles auf ein Tab bekommt, dann kannst du auch alles auf einen Tab legen. Ich befürchte allerdings, dass es einen erschlägt. Deshalb brauchst du eine sinnvolle Aufteilung. Ich glaube das eine sinnvolle Aufteilung in Mitarbeiter, nein Einkäufergruppen, Material und Lieferant gut ist.
Prozessdiagramm gleich lassen	"Der Linke Bereich soll immer gleich bleiben. Das kommt aus der klassischen Sicht von Celonis vor. Man kann entweder die Prozessinstanz nur auf die erste Seite machen oder immer gleich links. Aber ich finde es immer spannend die Prozessinstanz sehen. Ich würde weitergehen und da auch noch Risiko reinnehmen (also auch Prozessineffizienz noch mit reinnehmen"

Anhang G: Skripte zur Erstellung von Activity, Case und Process Tabelle

Erstellung Aktivitätstabelle

```
--Activity Script
--Dieses Skript fügt die einzelnen Aktivitäten der Aktivitätentabelle hinzu

/*
	Alle Aktivitäten sind im gleichen Muster aufgebaut
	Im Selectteil müssen folgende Angaben gemacht werden
		*Eindeutige CaseId aufgebaut aus Mandant, Einkaufsbelegsnummer
und Einkaufsbelegposition
		*Einer textuellen Angabe der Aktivität
		*Dem Zeitstempel, wann die Aktivität durchgeführt wurde
		*Eine interne Sortieung
		*Der Nutzer, der die Aktivität ausgeführt hat
	Der Fromteil kann unterschiedlich gestalltet werden, solange die
nötigen Felder
	für den Select vorhanden sind.
*/

--Erstellt die Activitätentabelle
CREATE COLUMN TABLE _CEL_P2P_ACTIVITIES
(
	CaseId NVARCHAR(30),
	Activity NVARCHAR(50),
	EventTime DATETIME,
	Sorting INTEGER,
	EventUser NVARCHAR(20)
)
;


--New Activity: Lege Bestellanforderung an
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
	EBAN.MANDT || EBAN.EBELN || EBAN.EBELP AS CaseID,
	'Lege Bestellanforderung an' AS Activity,
	--EBAN.ERDAT AS EventTime,
	TO_TIMESTAMP(TO_TIMESTAMP(CONCAT (EBAN.BADAT, EBAN.UZEIT),
'YYYYMMDDHH24MISS')) AS EventTime,
	10 AS Sorting,
	EBAN.ERNAM AS EventUser
FROM X0_STUDENT_001.EBAN
JOIN X0_STUDENT_001.EKPO
	ON EKPO.EBELN = EBAN.EBELN
	AND EKPO.EBELP = EBAN.EBELP
	AND EKPO.MANDT = EBAN.MANDT
;


--New Activity: Ändere BANF
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
	EBAN.MANDT || EBAN.EBELN || EBAN.EBELP AS CaseID,
	(CASE
```

```
            WHEN CDPOS.FNAME IN ('PREIS','MENGE') THEN CONCAT('Änderung von
BANF ', CDPOS.FNAME)
            WHEN CDPOS.FNAME = 'LIFNR' THEN 'Änderung von BANF
Wunschlieferant'
      END) AS Activity,
      TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
      11 AS Sorting,
      CDHDR.USERNAME AS EventUser
FROM X0_STUDENT_001.EBAN
JOIN X0_STUDENT_001.CDPOS ON
            CDPOS.TABKEY= CONCAT(EBAN.MANDT, CONCAT(EBAN.BANFN,
EBAN.BNFPO))
            AND CDPOS.TABNAME = 'EBAN'
            AND CDPOS.FNAME IN ('PREIS','MENGE','LIFNR')
            AND CDPOS.MANDANT = EBAN.MANDT
JOIN X0_STUDENT_001.CDHDR ON
      CDPOS.CHANGENR = CDHDR.CHANGENR
      AND CDPOS.MANDANT = CDHDR.MANDANT
;



--New Activty: Anlegen Anfrage (noch keine Bestellung durchgeführt)
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseID,
      'Lege Anfrage an' AS Activity,
            CASE
            WHEN CDHDR.UTIME IS NOT NULL
            AND CDHDR.UDATE IS NOT NULL THEN
                  TO_TIMESTAMP(CONCAT (CDHDR.UDATE, CDHDR.UTIME),
'YYYYMMDDHH24MISS')
            ELSE
            EKPO.AEDAT
      END AS EventTime,
      20 AS Sorting,
      EKKO.ERNAM
FROM X0_STUDENT_001.EKPO
JOIN X0_STUDENT_001.EKKO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
LEFT JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.MANDANT = EKKO.MANDT
      AND CDPOS.TABKEY = CONCAT(EKKO.MANDT,EKKO.EBELN)
      AND CDPOS.TABNAME = 'EKKO'
      AND CDPOS.CHNGIND = 'I'
LEFT JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.MANDANT = CDPOS.MANDANT
      AND CDHDR.CHANGENR = CDPOS.CHANGENR
WHERE EKKO.BSTYP = 'A'
AND NOT EXISTS
      (SELECT ep2.EBELN
      FROM X0_STUDENT_001.EKPO ep2
      WHERE EKPO.EBELN = ep2.ANFNR)
;


-- New Activity: Anfrage Anlegen (Bestellung bereits druchgeführt)
INSERT INTO _CEL_P2P_ACTIVITIES
```

```
SELECT
      EKPO.MANDT || ep2.EBELN || ep2.EBELP AS CaseID,
      'Lege Anfrage an' AS Activity,
            CASE
            WHEN CDHDR.UTIME IS NOT NULL
            AND CDHDR.UDATE IS NOT NULL THEN
                  TO_TIMESTAMP(CONCAT (CDHDR.UDATE, CDHDR.UTIME),
'YYYYMMDDHH24MISS')
            ELSE
            EKPO.AEDAT
      END AS EventTime,
      21 AS Sorting,
      EKKO.ERNAM
FROM X0_STUDENT_001.EKPO
JOIN X0_STUDENT_001.EKKO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.EKPO ep2 on
      EKPO.EBELN = ep2.ANFNR
      AND EKPO.MANDT = ep2.MANDT
LEFT JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.MANDANT = EKKO.MANDT
      AND CDPOS.TABKEY = CONCAT(EKKO.MANDT,EKKO.EBELN)
      AND CDPOS.TABNAME = 'EKKO'
      AND CDPOS.CHNGIND = 'I'
LEFT JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.MANDANT = CDPOS.MANDANT
      AND CDHDR.CHANGENR = CDPOS.CHANGENR
WHERE EKKO.BSTYP = 'A'
;

--New Activity: Absagekennzeichen geändert
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseID,
      (CASE
            WHEN CDPOS.VALUE_NEW = 'X' THEN 'Angebot abgelehnt'
            WHEN CDPOS.VALUE_NEW = '' THEN  'Absagekennzeichen
zurückgenommen'
      END
      ) AS Activity,
      TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
      22 AS Sorting,
      CDHDR.USERNAME
FROM X0_STUDENT_001.EKPO
JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      AND CDPOS.MANDANT = EKPO.MANDT
JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.CHANGENR = CDPOS.CHANGENR
      AND CDHDR.MANDANT = CDPOS.MANDANT
WHERE CDPOS.TABNAME = 'EKPO'
AND CDPOS.FNAME = 'ABSKZ'
;

--New Activity: Angebot eintragen/verändern
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseID,
```

```
      (CASE
            WHEN LTRIM(CDPOS.VALUE_OLD) in ('0','0.00') THEN 'Angebot
eingetragen'
            ELSE 'Angebot verändert'
      END) AS Activity,
      TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
      23 AS Sorting,
      CDHDR.USERNAME
FROM X0_STUDENT_001.EKPO
JOIN X0_STUDENT_001.EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      AND CDPOS.MANDANT = EKPO.MANDT
JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.CHANGENR = CDPOS.CHANGENR
      AND CDHDR.MANDANT = CDPOS.MANDANT
WHERE EKKO.BSTYP = 'A'
AND CDPOS.TABNAME = 'EKPO'
AND CDPOS.FNAME = 'NETPR'
;


-- New Activity: Anlage Bestellposition
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseID,
      (CASE
            WHEN LENGTH(LTRIM(EKPO.ANFNR)) = 0 AND EKPO.MEINS <> 'LE' THEN
'Lege Bestellposition an'
            WHEN LENGTH(LTRIM(EKPO.ANFNR)) = 0 AND EKPO.MEINS = 'LE' THEN
'Bestelle Dienstleistung'
            WHEN LENGTH(LTRIM(EKPO.ANFNR)) <> 0 THEN 'Lege Bestellpostion
aus Anfrage an'
      END) AS Activity,
      CASE
            WHEN CDHDR.UTIME IS NOT NULL
            AND CDHDR.UDATE IS NOT NULL THEN
                  TO_TIMESTAMP(CONCAT (CDHDR.UDATE, CDHDR.UTIME),
'YYYYMMDDHH24MISS')
            ELSE
            EKPO.AEDAT
      END AS EventTime,
      30 AS Sorting,
      EKKO.ERNAM
FROM
      X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
LEFT JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.MANDANT = EKKO.MANDT
      AND CDPOS.TABKEY = CONCAT(EKKO.MANDT,EKKO.EBELN)
      AND CDPOS.TABNAME = 'EKKO'
      AND CDPOS.CHNGIND = 'I'
LEFT JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.MANDANT = CDPOS.MANDANT
      AND CDHDR.CHANGENR = CDPOS.CHANGENR
```

```
WHERE
	EKKO.BSTYP = 'F'
	AND EKPO.RETPO <> 'X'
;


--New Activity: Bestellung Freigeben
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
	EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
	'Freigabe für Bestellung erteilt' AS Activity,
	TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
	31 AS Sorting,
	CDHDR.USERNAME
FROM X0_STUDENT_001.EKKO
JOIN X0_STUDENT_001.EKPO ON
	EKPO.EBELN = EKKO.EBELN
	AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.CDPOS ON
	CDPOS.TABKEY = EKKO.MANDT || EKKO.EBELN
	AND CDPOS.MANDANT = EKKO.MANDT
JOIN X0_STUDENT_001.CDHDR ON
	CDHDR.CHANGENR = CDPOS.CHANGENR
	AND CDHDR.MANDANT = CDPOS.MANDANT
WHERE
	CDPOS.TABNAME = 'EKKO'
	AND CDPOS.FNAME = 'FRGZU'
	AND CDPOS.VALUE_NEW = 'X'
;


-- New Activity: Änderung von Preis oder Menge in Einkaufsbelegposition

INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
	EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseID,
	concat ('Geändet ', CDPOS.FNAME) AS Activity,
	TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
	32 AS Sorting,
	CDHDR.USERNAME AS EventUser
FROM X0_STUDENT_001.EKPO
INNER JOIN X0_STUDENT_001.CDPOS ON
	CDPOS.TABKEY= concat (EKPO.MANDT, concat (EKPO.EBELN, EKPO.EBELP))
	AND CDPOS.TABNAME = 'EKPO'
	AND CDPOS.FNAME IN ('NETPR','MENGE')
	AND CDPOS.MANDANT = EKPO.MANDT
INNER JOIN X0_STUDENT_001.CDHDR ON
	CDPOS.MANDANT = CDHDR.MANDANT
	AND CDPOS.CHANGENR = CDHDR.CHANGENR
;


--New Activity: Änder Skonto
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
	EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseID,
	(CASE
		WHEN CDPOS.FNAME = 'ZBD1P' THEN 'Ändere Skontoprozent Stufe 1'
```

```
            WHEN CDPOS.FNAME = 'ZBD1T' THEN 'Ändere Skontotage Stufe 1'
            WHEN CDPOS.FNAME = 'ZBD2P' THEN 'Ändere Skontoprozent Stufe 2'
            WHEN CDPOS.FNAME = 'ZBD2T' THEN 'Ändere Skontotage Stufe 2'
            WHEN CDPOS.FNAME = 'ZBD3T' THEN 'Ändere Skontotage Stufe 2'
      END) AS Activity,
      TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
      33 AS Sorting,
      CDHDR.USERNAME AS EventUser
FROM X0_STUDENT_001.EKKO
RIGHT JOIN X0_STUDENT_001.EKPO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.TABKEY = concat (EKKO.MANDT, EKKO.EBELN)
      AND CDPOS.TABNAME = 'EKKO'
      AND CDPOS.FNAME IN ('ZBD1P', 'ZBD1T', 'ZBD2P', 'ZBD2T', 'ZBD3T')
      AND CDPOS.MANDANT = EKKO.MANDT
JOIN X0_STUDENT_001.CDHDR ON
      CDPOS.CHANGENR = CDHDR.CHANGENR
      AND CDPOS.MANDANT = CDHDR.MANDANT
;

-- New Activity: Einkäufergruppe geändert
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseID,
      'Einkaufergruppe geändert' AS Activity,
      TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
      34 AS Sorting,
      CDHDR.USERNAME AS EventUser
FROM X0_STUDENT_001.EKPO
JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      AND CDPOS.MANDANT = EKPO.MANDT
JOIN X0_STUDENT_001.CDHDR ON
      CDPOS.MANDANT = CDHDR.MANDANT
      AND CDPOS.CHANGENR = CDHDR.CHANGENR
WHERE
      CDPOS.TABNAME = 'EKKO'
      AND CDPOS.FNAME = 'EKGRP'
;


--New Activity: Wechselkurs manuell angepasst
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Wechselkurs manuell angepasst' AS Activity,
      TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
      35 AS Sorting,
      CDHDR.USERNAME
FROM X0_STUDENT_001.EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN
```

```
      AND CDPOS.MANDANT = EKPO.MANDT
JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.CHANGENR = CDPOS.CHANGENR
      AND CDHDR.MANDANT = CDPOS.MANDANT
WHERE
      CDPOS.TABNAME = 'EKKO'
      AND CDPOS.CHNGIND ='U'
      AND CDPOS.FNAME = 'WKURS'
;


--New Activity: Retourenposition anlegen
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Lege Retourenposition an' AS Activity,
      EKKO.AEDAT AS EventTime,
      37 AS Sorting,
      EKKO.ERNAM
FROM X0_STUDENT_001.EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKPO.RETPO = 'X'
;


--New Activtiy: Allgemeine Änderung in Einkaufsbelegkopf
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      CONCAT('Änderung in Einkaufsbelegkopf: ', CDPOS.FNAME) AS Activity,
      TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
      38 AS Sorting,
      CDHDR.USERNAME
FROM X0_STUDENT_001.EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN
      AND CDPOS.MANDANT = EKPO.MANDT
JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.CHANGENR = CDPOS.CHANGENR
      AND CDHDR.MANDANT = CDPOS.MANDANT
WHERE
      CDPOS.TABNAME = 'EKKO'
      AND CDPOS.CHNGIND ='U'
      AND CDPOS.FNAME NOT IN
            ('LOEKZ', 'ZBD1P', 'ZBD1T', 'ZBD2P', 'ZBD2T', 'ZBD3T',
'PROCSTAT', 'EKGRP', 'STATU')
;


--New Activity: Allgmeine Änderungen in Einkaufsbelegposition
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
```

```
      CONCAT('Änderung in Einkaufsbelegposition: ', CDPOS.FNAME) AS
Activity,
      TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
      39 AS Sorting,
      CDHDR.USERNAME
FROM X0_STUDENT_001.EKPO
JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      AND CDPOS.MANDANT = EKPO.MANDT
JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.CHANGENR = CDPOS.CHANGENR
      AND CDHDR.MANDANT = CDPOS.MANDANT
WHERE
      CDPOS.TABNAME = 'EKPO'
      AND CDPOS.CHNGIND ='U'
      AND CDPOS.FNAME NOT IN ('LOEKZ', 'AEDAT', 'NETWR', 'BRTWR', 'EFFWR')
;


--New Activity: Warenausgang&eingang
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKBE.MANDT || EKBE.EBELN || EKBE.EBELP AS CaseID,
      CASE WHEN EKBE.SHKZG = 'S' THEN 'Wareneingang'
            WHEN EKBE.SHKZG = 'H' THEN 'Warenausgang'
            ELSE 'Error'
      END   AS Activity,
      TO_TIMESTAMP(CONCAT (EKBE.CPUDT, EKBE.CPUTM), 'YYYYMMDDHH24MISS') AS
EventTime,
      40 AS Sorting,
      EKBE.ERNAM AS EventUser
FROM X0_STUDENT_001.EKBE
WHERE EKBE.VGABE = '1'
;


--New Activity: Verschrottung von Inventar
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseID,
      'Verschrottung von Inventar' AS Activity,
      TO_TIMESTAMP(CONCAT (MKPF.CPUDT, MKPF.CPUTM), 'YYYYMMDDHH24MISS') AS
EventTime,
      41 AS Sorting,
      MKPF.USNAM AS EventUser
FROM X0_STUDENT_001.MKPF
JOIN X0_STUDENT_001.MSEG ON
      MKPF.MBLNR = MSEG.MBLNR
      AND MKPF.MANDT = MSEG.MANDT
      AND MKPF.MJAHR = MSEG.MJAHR
JOIN X0_STUDENT_001.EKPO ON
      EKPO.MANDT = MSEG.MANDT
      AND EKPO.EBELN = MSEG.EBELN
      AND EKPO.EBELP = MSEG.EBELP
WHERE MSEG.MATNR = EKPO.MATNR
AND MSEG.BWART = 551
;
```

```
--New Activity: Verschrottung von Inventar
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseID,
      'Weiterverkauf von Inventar' AS Activity,
      TO_TIMESTAMP(CONCAT (MKPF.CPUDT, MKPF.CPUTM), 'YYYYMMDDHH24MISS') AS
EventTime,
      42 AS Sorting,
      MKPF.USNAM AS EventUser
FROM X0_STUDENT_001.MKPF
JOIN X0_STUDENT_001.MSEG ON
      MKPF.MBLNR = MSEG.MBLNR
      AND MKPF.MANDT = MSEG.MANDT
      AND MKPF.MJAHR = MSEG.MJAHR
JOIN X0_STUDENT_001.EKPO ON
      EKPO.MANDT = MSEG.MANDT
      AND EKPO.EBELN = MSEG.EBELN
      AND EKPO.EBELP = MSEG.EBELP
WHERE MSEG.MATNR = EKPO.MATNR
AND MSEG.BWART = 251
;


--New Activity: Leistungserfassung
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      ESSR_MANDT + ESSR_EBELN + ESSR_EBELP AS CaseId,
      'Erfassung Dienstleistung' AS Activity,
      ESSR_ERDAT AS EventTime,
      43 AS Sorting,
      ESSR_ERNAM as EventUser
FROM ESSR
JOIN EKKO ON
      EKKO_EBELN = ESSR_EBELN
      AND EKKO_MANDT = ESSR_MANDT
WHERE
      ESSR_FRGRL = 'X'


--New Activity: Dienstleistung abnehmen
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      ESSR.MANDT + ESSR_EBELN + ESSR_EBELP AS CaseId,
      'Abnahme Dienstleistung' AS Activity,
      dbo.GetTimeStamp(CDHDR_UDATE, CDHDR_UTIME) AS EventTime,
      44 AS Sorting,
      ESSR_ERNAM AS EventUser
FROM CDPOS
JOIN CDHDR ON
      CDHDR_CHANGENR = CDPOS_CHANGENR
      AND CDHDR_MANDANT = CDPOS_MANDANT
JOIN ESSR ON
      CDPOS_TABKEY = ESSR_MANDT + ESSR_LBLNI
      AND CDPOS_MANDANT = ESSR_MANDT
JOIN EKKO ON
      EKKO_EBELN = ESSR_EBELN
      AND EKKO_MANDT = ESSR_MANDT
WHERE
      CDPOS_FNAME = 'FRGRL'
      AND CDPOS_VALUE_NEW = ''
```

```
      AND CDPOS_VALUE_OLD = 'X'

*/
--New Activity: Rechnungseingang&ausgang
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKBE.MANDT || EKBE.EBELN || EKBE.EBELP AS CaseID,
      CASE WHEN EKBE.SHKZG = 'S' THEN 'Rechnungseingang'
            WHEN EKBE.SHKZG = 'H' THEN 'Rechnungsausgang'
            ELSE 'Error'
      END AS Activity,
      TO_TIMESTAMP(CONCAT (EKBE.CPUDT, EKBE.CPUTM), 'YYYYMMDDHH24MISS') AS
EventTime,
      50 AS Sorting,
      EKBE.ERNAM AS EventUser
FROM X0_STUDENT_001.EKBE
WHERE EKBE.VGABE = '2'
;

--New Activity: Ändere Rechnungseingang
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseID,
      (CASE WHEN CDPOS.FNAME = 'MENGE' THEN 'Rechnungsbetrag angepasst'
            WHEN CDPOS.FNAME = 'WRBTR' THEN 'Warenpreis in Rechnung
angepasst' END) AS Activity,
      TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
      51 AS Sorting,
      CDHDR.USERNAME AS EventUser
FROM X0_STUDENT_001.RSEG
JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.TABKEY = concat(RSEG.MANDT, concat(RSEG.BELNR,
concat(RSEG.GJAHR, RSEG.BUZEI)))
      AND CDPOS.TABNAME = 'RSEG'
      AND CDPOS.FNAME IN ('MENGE', 'WRBTR')
JOIN X0_STUDENT_001.CDHDR ON
      CDPOS.CHANGENR = CDHDR.CHANGENR
      AND CDPOS.MANDANT = CDHDR.MANDANT
;


--New Activity: Löschen in PO
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaeID,
      CASE WHEN CDPOS.VALUE_OLD = '' AND CDPOS.VALUE_NEW = 'L' THEN
'Position gelöscht'
            WHEN CDPOS.VALUE_OLD = '' AND CDPOS.VALUE_NEW = 'S' THEN
'Position gesperrt'
            WHEN CDPOS.VALUE_OLD = 'S' AND CDPOS.VALUE_NEW = 'L' THEN
'gesperrtes Löschen'
            WHEN CDPOS.VALUE_OLD = 'L' AND CDPOS.VALUE_NEW = '' THEN
'Löschung aufgehoben'
            WHEN CDPOS.VALUE_OLD = 'S' AND CDPOS.VALUE_NEW = '' THEN
'Sperrung aufgehoben'
            ELSE  'Ändere Kennezeichen'
      END AS Activity,
      TO_TIMESTAMP (CONCAT (CDHDR.UDATE, CDHDR.UTIME), 'YYYYMMDDHH24MISS')
AS EventTime,
```

```
      60 AS Sorting,
      CDHDR.USERNAME AS EventUser
FROM X0_STUDENT_001.CDPOS
JOIN X0_STUDENT_001.EKPO ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.CHANGENR = CDPOS.CHANGENR
      AND CDHDR.MANDANT = CDPOS.MANDANT
WHERE
      CDPOS.TABNAME = 'EKPO'
      AND CDPOS.FNAME = 'LOEKZ'
;


--New Activity: Rechnung beglichen'
INSERT INTO _CEL_P2P_ACTIVITIES
SELECT
      RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseID,
      'Rechnung beglichen' AS Activity,
      BSAK.AUGDT AS EventTime,
      80 AS Sorting,
      BKPF.USNAM AS EventUser
FROM X0_STUDENT_001.RSEG
JOIN X0_STUDENT_001.BKPF ON
      BKPF.AWKEY = concat(RSEG.BELNR, RSEG.GJAHR)
      AND BKPF.MANDT = RSEG.MANDT
JOIN X0_STUDENT_001.BSAK ON
      BKPF.MANDT = BSAK.MANDT
      AND BKPF.BELNR = BSAK.BELNR
      AND BKPF.BUKRS = BSAK.BUKRS
      AND BKPF.GJAHR = BSAK.GJAHR
;
```

Prozess- und Falltabelle erstellen

```
-- Script creates case and process table for Celonis

 -- Input:
--       _CEL_Z_ACTIVITIES = Activity Table with Columns "CASE_ID",
 --"ACTIVITY",     "EventTime",      "Sorting"
-- Output:
--       _CEL_ACTIVITIES = Activity Table with Columns "CASE_ID",
 /*"ACTIVITY",
       "EventTime",
       "Sorting",
       "_LIFECYCLE",
       "_PRIMARY_KEY",
       "CASE_NUM_ID" --       _CEL_ACTIVITIES_PROCESS_TABLE = Process Table
--       _CEL_CASES = Case Table (joined with Master Table, e.g. VBAP, EKPO,
AFPO, etc.) with columns "CASE_ID","CASE_NUM_ID","_PATH",
 "_PATH_ID" -- Also checks for paths longer than 5000 characters -> this
results in a HANA error, since max NVARCHAR length is 5000. Alerts only,
does not delete.
 --%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%*/
-- Lifecycle Calculation
--%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

```
DROP table _CEL_ACTIVITIES;
CREATE COLUMN TABLE _CEL_ACTIVITIES AS ( SELECT
       X0_STUDENT_001._CEL_P2P_ACTIVITIES.* ,
       ROW_NUMBER() OVER (PARTITION BY "CASEID" ORDER BY "EVENTTIME",
       "SORTING") AS "_LIFECYCLE" ,
       ROW_NUMBER() OVER (
            ORDER BY "CASEID") AS "_PRIMARY_KEY" ,
       DENSE_RANK() OVER (
            ORDER BY "CASEID") AS "CASE_NUM_ID"
      FROM X0_STUDENT_001._CEL_P2P_ACTIVITIES )
;
-- Check
SELECT
       COUNT(1)
FROM _CEL_ACTIVITIES;

 --%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
-- Create Process Table
--%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

DROP table _CEL_ACTIVITIES_PROCESS_TABLE;
CREATE COLUMN TABLE _CEL_ACTIVITIES_PROCESS_TABLE AS ( SELECT
       ROW_NUMBER() OVER (
            ORDER BY ACTIVITY) AS ACTIVITY_ID ,
      ACTIVITY
      FROM ( SELECT
       DISTINCT ACTIVITY
            FROM _CEL_ACTIVITIES ) )
;
 --%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
-- Create Case Table (1/3): Create _PATH
--%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

DROP table _CEL_Z_TMP_CASES;
create column table _CEL_Z_TMP_CASES ( "CASE_ID" NVARCHAR(50) ,
      "_PATH" NVARCHAR(5000) -- NVARCHAR(5000), sonst CLOB
,
      "CASE_NUM_ID" BIGINT )
;
INSERT
INTO _CEL_Z_TMP_CASES SELECT
       "CASEID" ,
      CASE WHEN LENGTH(STRING_AGG(';' || "ACTIVITY_ID" || ';',
       '') ) >5000
THEN 'path_too_long'
ELSE STRING_AGG(';' || "ACTIVITY_ID" || ';',
       '')
END AS "_PATH" ,
      "CASE_NUM_ID"
FROM ( SELECT
       _CEL_ACTIVITIES_PROCESS_TABLE."ACTIVITY_ID" ,
      _CEL_ACTIVITIES."CASEID" ,
      _CEL_ACTIVITIES."CASE_NUM_ID"
      FROM _CEL_ACTIVITIES
      LEFT JOIN _CEL_ACTIVITIES_PROCESS_TABLE ON _CEL_ACTIVITIES."ACTIVITY"
= _CEL_ACTIVITIES_PROCESS_TABLE."ACTIVITY"
      ORDER BY "_LIFECYCLE" ) AS A
GROUP BY "CASEID",
       "CASE_NUM_ID"
```

```
;
 --%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
-- Create Case Table (2/3): Find too long paths
--%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

DROP table _TMP_PATH_TOO_LONG;
create column table "_TMP_PATH_TOO_LONG" as( select
       "CASE_ID"
      from "_CEL_Z_TMP_CASES"
      where "_PATH" = 'path_too_long' )
;
select
       *
from "_TMP_PATH_TOO_LONG"
;

 --%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
-- Create Case Table (3/3): Create _PATH_ID
--%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

DROP table _CEL_Z_TMP2_CASES;
CREATE COLUMN TABLE "_CEL_Z_TMP2_CASES" AS ( SELECT
       _CEL_Z_TMP_CASES."CASE_ID" ,
      _CEL_Z_TMP_CASES."CASE_NUM_ID" ,
      _CEL_Z_TMP_CASES."_PATH" ,
       "pathid_tmp"."_PATH_ID"
      FROM _CEL_Z_TMP_CASES
      LEFT JOIN ( SELECT
       ROW_NUMBER() OVER(
                  ORDER BY "_PATH" ) AS "_PATH_ID",
       "_PATH" --2.) give them IDs

            FROM ( SELECT
       DISTINCT "_PATH"
                  FROM _CEL_Z_TMP_CASES --1.) reduce to distinct pathes
) ) "pathid_tmp" ON "pathid_tmp"."_PATH" = _CEL_Z_TMP_CASES."_PATH" --3.)
join the ID to every path in the _CEL_Z_TMP_CASES table
)
;

 --%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
-- Join to Master Case Table
--%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

DROP table _CEL_CASES;
CREATE COLUMN TABLE _CEL_CASES AS( SELECT
EKPO."TXZ01",
      _CEL_Z_TMP2_CASES."CASE_ID" ,
      _CEL_Z_TMP2_CASES."CASE_NUM_ID" ,
      _CEL_Z_TMP2_CASES."_PATH" ,
      _CEL_Z_TMP2_CASES."_PATH_ID"
      FROM _CEL_Z_TMP2_CASES
      JOIN EKPO ON
            CASE_ID = (EKPO.MANDT || EKPO.EBELN || EKPO.EBELP)
      );
/*DELETE FROM _CEL_CASES
      WHERE _PATH = 'path_too_long';*/

-- Check
SELECT
```

```
       COUNT(1)
FROM _CEL_CASES
;
-- create process table
DROP Table X0_STUDENT_001.CELONIS_P2P_PROCESSES;

CREATE TABLE X0_STUDENT_001.CELONIS_P2P_PROCESSES( ActivityName
varchar(100) ,
       IntegerValue INTEGER )
;
 INSERT
INTO X0_STUDENT_001.CELONIS_P2P_PROCESSES( SELECT
       DISTINCT CELONIS_P2P_ACTIVITIES.Activity AS ActivityName ,
      CELONIS_P2P_ACTIVITIES.Sorting AS IntegerValue
      FROM CELONIS_P2P_ACTIVITIES)
;
```

Anhang H: Implementierung Fraud Patterns

Generierung Red Flag Tabellen

```
--Red Flag Preprocessing
/*Dieses Skript übernimmt die Vorarbeiten für die Red Flag
Suche. Es muss nur einmalig ausgeführt werden.
*/

--Create table for Flag occurences
CREATE COLUMN TABLE _CEL_FLAGED_CASES
(
      ID INT NOT NULL PRIMARY KEY generated by default as IDENTITY,
      CaseId NVARCHAR(30) NOT NULL,
      FlagId NVARCHAR(30) NOT NULL,
      SchemeId NVARCHAR(30)
)
;

--Create Table for Red Flags
CREATE COLUMN TABLE _CEL_RED_FLAG_CATALOGUE
(
      FLAG_FlagId NVARCHAR(30) NOT NULL PRIMARY KEY,
      FlagDescription NVARCHAR(200) NOT NULL,
      FlagDescriptionLong NVARCHAR(500) NOT NULL,
      CategorieId NVARCHAR(30) NOT NULL,
      SchemeId NVARCHAR(30)
)
;


--BISHER NICHT UNTERSTÜTZT VON HANA
--csv export liegt bei
--Insert Flags
-- INSERT INTO _CEL_RED_FLAG_CATALOGUE
-- VALUES
```

```
--Create Table for Fraudschemes
CREATE COLUMN TABLE _CEL_SCHEME_CATALOGUE
(
	SCHEME_SchemeId NVARCHAR(30) NOT NULL PRIMARY KEY,
	Name NVARCHAR(50)
)
;


--Create Table for Fraud Categories
CREATE COLUMN TABLE _CEL_FLAG_CATEGORIES
(
	CATEGORIE_CategorieId NVARCHAR(30) NOT NULL PRIMARY KEY,
	Description NVARCHAR(50)
)
;
```

Rechnungsmanipulation

```
--Red Flag Processing
--Collection of Red Flag Scripts for Scheme Check tempering

--Flag_A1 - Budgetabweichung
--Generiert Liste aller Nettobestellungen eines Mitarbeiters pro Monat
CREATE LOCAL TEMPORARY TABLE #SPENDING_PER_MOTH_A1
(MANDT VARCHAR(20), ERNAM VARCHAR(30), SPENDING_YEAR INT, SPENDING_MONTH
INT, SPENDING DOUBLE)
;

INSERT INTO #SPENDING_PER_MOTH_A1
SELECT
	EKKO.MANDT,
	EKKO.ERNAM,
	YEAR(EKKO.AEDAT),
	MONTH(EKKO.AEDAT),
	SUM(EKPO.NETWR)
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
	EKPO.EBELN = EKKO.EBELN
	AND EKPO.MANDT = EKKO.MANDT
WHERE LENGTH(LTRIM(EKKO.ERNAM)) > 0
GROUP BY EKKO.MANDT, EKKO.ERNAM, YEAR(EKKO.AEDAT), MONTH(EKKO.AEDAT)
HAVING SUM(EKPO.NETWR) > 0
ORDER BY EKKO.MANDT
;

--Sucht auffällige Transaktionen
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDERS_A1
(MANDT VARCHAR(20), ERNAM VARCHAR(30), SPENDING_YEAR INT, SPENDING_MONTH
INT)
;

INSERT INTO #SUSPICIOUS_ORDERS_A1
SELECT
	MANDT,
	ERNAM,
	SPENDING_YEAR,
```

```
      SPENDING_MONTH
FROM #SPENDING_PER_MOTH_A1 s1
WHERE EXISTS
      (SELECT
            ERNAM
      FROM #SPENDING_PER_MOTH_A1 s2
      WHERE
            s2.ERNAM = s1.ERNAM
            AND s2.MANDT = s1.MANDT
            --Versucht den Vormonat in der Liste zu finden
            --Dazu wird sowohl über das Jahr als auch den Monat gejoined
            AND s2.SPENDING_YEAR = YEAR(ADD_MONTHS(TO_DATE(s1.SPENDING_YEAR
|| '-' || s1.SPENDING_MONTH || '-01', 'YYYY-MM-DD'),-1))
            AND s2.SPENDING_MONTH =
MONTH(ADD_MONTHS(TO_DATE(s1.SPENDING_YEAR || '-' || s1.SPENDING_MONTH || '-
01', 'YYYY-MM-DD'),-1))
            --Eintrag wird in Liste aufgenommen wenn Nettobetrag größer als
der Vormonat * Prozent ist
            AND s1.SPENDING > 4 * s2.SPENDING
      )
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_A01' AS FlagId
FROM #SUSPICIOUS_ORDERS_A1, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.ERNAM = #SUSPICIOUS_ORDERS_A1.ERNAM
      AND YEAR(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_A1.SPENDING_YEAR
      AND MONTH(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_A1.SPENDING_MONTH
      AND EKKO.MANDT = #SUSPICIOUS_ORDERS_A1.MANDT
;


--Flag_A02 - Rechnungsdiskrepanz
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,

      CASE
            WHEN RSEG.WRBTR < EKPO.BRTWR THEN 'Flag_A02a'
            WHEN RSEG.WRBTR > EKPO.BRTWR THEN 'Flag_A02b'
      END

FROM X0_STUDENT_001.EKPO
JOIN X0_STUDENT_001.RSEG ON
      RSEG.EBELN = EKPO.EBELN
      AND  RSEG.EBELP = EKPO.EBELP
      AND RSEG.MANDT = EKPO.MANDT
--Rechnungsbetrag und Bestellbetrag stimmen nicht überein
WHERE LTRIM(RSEG.WRBTR) <> LTRIM(EKPO.BRTWR)
;

--Flag_A03 - Anpassung Verbindlichkeiten
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
```

```
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP As CaseId,
      'Flag_A03' AS FlagId
FROM X0_STUDENT_001.CDPOS
JOIN X0_STUDENT_001.CDHDR ON
      CDPOS.CHANGENR = CDHDR.CHANGENR
      AND CDPOS.MANDANT = CDHDR.MANDANT
JOIN X0_STUDENT_001.EKPO ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP

--Suche Änderungen des Rechnungsbetrags
WHERE
      CDPOS.TABNAME = 'RBKP'
      AND CDPOS.FNAME = 'RMWWR'
      AND CDPOS.CHNGIND = 'U'
;



--Flag_A04b - Änderung Lieferantenstammsatz Version 2 - Änderung
--Lieferantenstammsatz

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_A04' AS FlagId
FROM X0_STUDENT_001.RBKP
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = RBKP.BELNR
      AND RSEG.GJAHR = RBKP.GJAHR
      AND RSEG.MANDT = RBKP.MANDT
JOIN X0_STUDENT_001.BKPF ON
      BKPF.AWKEY = concat(RSEG.BELNR, RSEG.GJAHR)
      AND BKPF.MANDT = RSEG.MANDT
JOIN X0_STUDENT_001.BSAK ON
      BKPF.BELNR = BSAK.BELNR
      AND BKPF.MANDT = BSAK.MANDT
      AND BKPF.GJAHR = BSAK.GJAHR
      AND BKPF.BUKRS = BSAK.BUKRS
JOIN X0_STUDENT_001.CDPOS ON
      RBKP.LIFNR = CDPOS.OBJECTID
JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.CHANGENR = CDPOS.CHANGENR
      AND CDHDR.MANDANT = CDPOS.MANDANT
      -- Vergleicht letzten Nutzer
      AND RBKP.USNAM = CDHDR.USERNAME
      -- Vergleicht Rechnungserfasser
      -- AND RBKP.ERFNAM = CDHDR.USERNAME
      AND CDHDR.UDATE BETWEEN RBKP.BLDAT AND BSAK.AUGDT
WHERE
      --Suche Einträge bei denen in der Tabelle der Lieferantenbankdaten
      --die Kontonummer oder Bankleitzahl verändert wurde
      CDPOS.TABNAME = 'LFBK'
      AND (
            CDPOS.FNAME = 'BANKN'
            OR CDPOS.FNAME = 'BANKL')
      --Diese änderung sollte am Tag des Rechnugseingangs oder kurz danach
geschehen sein
      AND RBKP.BLDAT between CDHDR.UDATE and
ADD_DAYS(CDHDR.UDATE,RBKP.ZBD1T)
```

```
      --Suche nach einem weiteren Eintrag welcher  wieder eine Änderung der
Bankverbindung für den
      --gleichen Lieferanten vom gleichen Benutzer druchgeführt wurde
      AND EXISTS

            FROM X0_STUDENT_001.CDPOS c2
            JOIN X0_STUDENT_001.CDHDR h2 ON
                  h2.CHANGENR = c2.CHANGENR
                  AND h2.MANDANT = c2.MANDANT
            WHERE
                  c2.TABNAME = 'LFBK'
            AND (
                  c2.FNAME = 'BANKN'
                  OR c2.FNAME = 'BANKL')
            AND c2.CHANGENR <> CDPOS.CHANGENR
            AND c2.OBJECTID = CDPOS.OBJECTID
            AND h2.USERNAME = CDHDR.USERNAME
            AND h2.UDATE between CDHDR.UDATE and ADD_DAYS(BSAK.AUGDT,3)
            )
;



--Flag_A04
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_A04a' AS FlagId
FROM X0_STUDENT_001.CDPOS
JOIN X0_STUDENT_001.EKPO ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
JOIN X0_STUDENT_001.CDHDR ON
      CDPOS.CHANGENR = CDHDR.CHANGENR
      AND CDPOS.MANDANT = CDHDR.MANDANT

WHERE
      --Suche Einträge bei denen in der Tabelle der Lieferantenbankdaten
      --die Kontonummer oder Bankleitzahl verändert wurde
      CDPOS.TABNAME = 'LFBK'
      AND (
            CDPOS.FNAME = 'BANKN'
            OR CDPOS.FNAME = 'BANKL')
      AND EXISTS
            (SELECT c2.CHANGENR
            FROM X0_STUDENT_001.CDPOS c2
            JOIN X0_STUDENT_001.CDHDR h2 ON
                  h2.CHANGENR = c2.CHANGENR
                  AND h2.MANDANT = c2.MANDANT
            WHERE
                  c2.TABNAME = 'LFBK'
            AND (
                  c2.FNAME = 'BANKN'
                  OR c2.FNAME = 'BANKL')
            AND c2.CHANGENR <> CDPOS.CHANGENR
            AND c2.OBJECTID = CDPOS.OBJECTID
            AND h2.USERNAME = CDHDR.USERNAME
            )
;

-- Flag_A04c
```

```
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
select      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseID ,
      'Flag_A04' AS FlagId
FROM GBI_001.CDHDR
JOIN GBI_001.CDPOS ON
CDPOS.CHANGENR = CDHDR.CHANGENR
JOIN GBI_001.LFA1 ON
CDHDR.OBJECTID = LFA1.LIFNR
JOIN GBI_001.EKKO ON
LFA1.LIFNR = EKKO.LIFNR AND
LFA1.MANDT = EKKO.MANDT
JOIN GBI_001.EKPO on
EKKO.EBELN = EKPO.EBELN AND
EKKO.MANDT = EKPO.MANDT
JOIN GBI_001.RBKP on
RBKP.LIFNR = CDPOS.OBJECTID

where
            CDPOS.TABNAME = 'LFBK'
      AND (
            CDPOS.FNAME = 'BANKN'
            OR CDPOS.FNAME = 'BANKL'
            OR CDPOS.FNAME = 'LIFNR'
            OR CDPOS.FNAME = 'KOINH'
            OR CDPOS.OBJECTCLAS = 'KRED'
)
      AND (
            RBKP.BLDAT between CDHDR.UDATE and
ADD_DAYS(CDHDR.UDATE,RBKP.ZBD1T)

);

--Flag_A05
--Inkompatibel mit HANA da kein geeigneter Matching Algorithmus vorhanden
ist

--Flag_A06 - Änderung Währung
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_A06' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.RSEG ON
      RSEG.EBELN = EKKO.EBELN
      AND RSEG.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.RBKP ON
      RBKP.BELNR = RSEG.BELNR
      AND RBKP.GJAHR = RSEG.GJAHR
      AND RBKP.MANDT = RSEG.MANDT
--Suche Rechnungen die eine andere Waehrung benutzen
--als die Bestellung
WHERE EKKO.WAERS <> RBKP.WAERS
;


--Flag_A07 - Doppelte Lieferanten
--Erstellt Liste mit Lieferanten der Lifnr und Name ungleich sind
--alle anderen Adressdaten jedoch identisch
CREATE LOCAL TEMPORARY TABLE #DOUBLE_VENDORS_A7
(LIFNR VARCHAR(30), MANDT VARCHAR(20))
```

```
;

INSERT INTO #DOUBLE_VENDORS_A7
SELECT
      DISTINCT l1.LIFNR,
      l1.MANDT
FROM X0_STUDENT_001.LFA1 l1
WHERE
      LENGTH(LTRIM(l1.LIFNR)) > 0
AND EXISTS
      (SELECT
            l2.LIFNR
      FROM X0_STUDENT_001.LFA1 l2
      WHERE
            LENGTH(LTRIM(l2.LIFNR)) > 0
            AND l2.LIFNR <> l1.LIFNR
            AND l2.NAME1 <> l1.NAME1
            AND l2.MANDT = l1.MANDT
            AND l2.STRAS = l1.STRAS
            AND l2.PSTLZ = l1.PSTLZ
            AND l2.ORT01 = l1.ORT01
            AND l2.LAND1 = l1.LAND1
      )

;

--Suche alle Bestellungen an auffällige Lieferanten
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_A07' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN #DOUBLE_VENDORS_A7 ON
      #DOUBLE_VENDORS_A7.MANDT = EKKO.MANDT
      AND #DOUBLE_VENDORS_A7.LIFNR = EKKO.LIFNR
WHERE
      EKKO.BSTYP = 'F'
;

--Flag_A08 - Unterschiedliche Rechnungsempfaenger
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_A08' AS FlagId
FROM X0_STUDENT_001.RBKP r1
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.MANDT = r1.MANDT
      AND RSEG.GJAHR = r1.GJAHR
WHERE
      LENGTH(LTRIM(r1.XBLNR)) > 0
--Suche nach einer zweiten Rechnung welche,
AND EXISTS
      (SELECT
            r2.BELNR
      FROM X0_STUDENT_002.RBKP r2
      WHERE
```

```
            --die gleiche Referenzrechnungsnummer hat
            r2.XBLNR = r1.XBLNR
            AND r2.MANDT = r1.MANDT
            --den gleichen Rechnungsbetrag
            AND r2.RMWWR = r1.RMWWR
            --einen anderen Lieferanten
            AND r2.LIFNR <> r1.LIFNR
            --Ausschluss, dass die gleiche Rechnung miteinander verbunden
wird
            AND r2.BELNR <> r1.BELNR
            AND LENGTH(LTRIM(r2.XBLNR)) > 0
      )
;

--Flag_A09 - Rechnungsnummer mit anderem Betrag
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_A09' AS FlagId
FROM X0_STUDENT_001.RBKP r1
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.MANDT = r1.MANDT
      AND RSEG.GJAHR = r1.GJAHR
WHERE
      LENGTH(LTRIM(r1.XBLNR)) > 0
      AND LENGTH(LTRIM(r1.LIFNR)) > 0
--Suche eine zweite Rechnung welche,
AND EXISTS
      (SELECT
            r2.BELNR
      FROM X0_STUDENT_001.RBKP r2
      WHERE
            --die gleiche Referenzrechnungsnummer hat
            r2.XBLNR = r1.XBLNR
            AND r2.MANDT = r1.MANDT
            AND r2.GJAHR = r1.GJAHR
            --denselben Lieferanten
            AND r2.LIFNR = r1.LIFNR
            --einen anderen Rechnungsbetrag
            AND r2.RMWWR <> r1.RMWWR
            --Ausschluss, dass die gleiche Rechnung miteinander verbunden
wird
            AND r2.BELNR <> r1.BELNR
            AND LENGTH(LTRIM(r2.XBLNR)) > 0
      )
;

--Flag_A10 - Änderung der Bestellung
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP As CaseId,
      'Flag_A03' AS FlagId
FROM X0_STUDENT_001.CDPOS
JOIN X0_STUDENT_001.CDHDR ON
      CDPOS.CHANGENR = CDHDR.CHANGENR
      AND CDPOS.MANDANT = CDHDR.MANDANT
JOIN X0_STUDENT_001.EKPO ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
```

```
--Suche Änderungen des Bestellbetrags
WHERE
      CDPOS.TABNAME = 'EKPO'
      AND CDPOS.FNAME = 'RMWWR'
      AND CDPOS.CHNGIND = 'U'
;
--Flag_A11 – Lieferant ohne Bankkonto

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_A11' AS FlagId
FROM X0_STUDENT_001.CDPOS
JOIN X0_STUDENT_001.EKPO ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
JOIN X0_STUDENT_001.CDHDR ON
      CDPOS.CHANGENR = CDHDR.CHANGENR
      AND CDPOS.MANDANT = CDHDR.MANDANT
WHERE
      AND LENGTH(LTRIM(LFBK.BANKS)) = 0
;



--Scheme Konfigration
--Beispiel
--Um ein eigenes Schema zu Konfigurieren müssen die FlagId
--der gewünschten Flags eingetragen werden
--Wird statt dem Intersect ein Union benutzt, werde alle Transaktionen
--markiert die mindestens einen der aufgeführten Flags besitzen
--im Fall von Intersect müssen alle Flags vorhanden sein

UPDATE _CEL_FLAGED_CASES
SET SCHEMEID = 'A1-Checktempering'
WHERE CASEID IN
(
SELECT
      FC1.CASEID
FROM _CEL_FLAGED_CASES FC1
WHERE FLAGID = 'Flag_A01'

INTERSECT


SELECT
FC2.CASEID
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_A06'
)
AND FLAGID IN ('Flag_A01','Flag_A06');
```

Scheinfirma

```
--https://www.consolut.com/s/sap-ides-zugriff/d/e/doc/T-RBKP
--http://www.sapdatasheet.org/abap/doma/VGABE.html#


--Red Flag Processing
```

```
--Collection of Red Flag Scripts for Scheme Dhell Company

--
--Red Flag Suche
--
--Flag_B01 - Plötzliche Geschäftsaktivitäten
--TIME_THRESHOLD (hier jetzt 1)
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT e1.MANDT || e1.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B01' AS FlagId
FROM EKKO e1
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = e1.EBELN
      AND EKPO.MANDT = e1.MANDT
JOIN X0_STUDENT_001.LFA1 ON
      LFA1.LIFNR = e1.LIFNR
      AND LFA1.MANDT = e1.MANDT
WHERE
      LENGTH(LTRIM(e1.LIFNR)) > 0
--Suche Bestellungen bei denen keine weitere Bestellung exisitert die
AND NOT EXISTS
      (SELECT
            e2.EBELN
      FROM EKKO e2
      WHERE
            --an den gleichen Lieferanten geht
            e1.LIFNR = e2.LIFNR
            AND e1.EBELN <> e2.EBELN
            AND e1.MANDT = e2.MANDT
            --die Bestellung nicht innerhalb der gewählten Zeit aufgegebn
wurde
            AND e2.AEDAT between ADD_YEARS(e1.AEDAT,-1) and e1.AEDAT)
--Lieferant wurde bereits vor dem gewählten Zeitraum erstellt
AND LFA1.ERDAT < ADD_YEARS(e1.AEDAT,-1)
;


--Flag_B02 - Lieferantenersteller ist Genehmiger
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B02' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.LFA1 ON
      LFA1.LIFNR = EKKO.LIFNR
      AND LFA1.MANDT = EKKO.MANDT
--Verwendeter Lieferant wurde vom Besteller erstellt
WHERE
      EKKO.ERNAM = LFA1.ERNAM
;

--Flag_B03 - Keine Genehmigungsstufe
--ORDER_THRESHOLD_STAGE1 (jetzt 50000.00)
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
```

```
      'Flag_B03' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
--Die Bestellung hat keine Freigabestrategie
WHERE LENGTH(LTRIM(EKKO.FRGSX)) = 0

GROUP BY
      EKKO.EBELN,
      EKKO.MANDT,
      EKPO.EBELP
--Aber ihr Bestellwert ist größer als der Grenzwert
--ab der eine erweiterte Freigabe nötig ist
HAVING
      SUM(EKPO.NETWR) > 50000.00
;
--Check the field FRGZU, this field contains the level of approval.
--If FRGZU contains Value 'XX' then that means, the PO in context is in 3rd
level of approver.
--select EKKO.FRGZU from EKKO;


--Flag_B04 - Ungewöhliche Genehmigung
--Erstelle Liste von Mitarbeitern die an einem Tag
--besonders viele Bestellungen durchgeführt haben
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDERS_B4b
(MANDT VARCHAR(30), ERNAM VARCHAR(30), AEDAT DATE)
;

INSERT INTO #SUSPICIOUS_ORDERS_B4b
SELECT
      e1.MANDT,
      e1.ERNAM,
      e1.AEDAT

FROM EKKO e1
WHERE LENGTH(LTRIM(e1.ERNAM)) > 0
GROUP BY
      e1.MANDT,
      e1.ERNAM,
      e1.AEDAT
HAVING
      --Bestellungen des Tages übersteigen Durchschnittswert des letzten
Jahres
      --5+ ist ein Sockel. Ohne diesen geht der Durchschnitt bei wenigen
Bestellungen
      --gegen Null
      COUNT(e1.EBELN) > 25+4*
            (SELECT
                  --Komplettes Jahr
                  --COUNT(e2.EKKO_EBELN)/365
                  --Arbeitstage 2016 Bayern
                  COUNT(e2.EBELN)/250
            FROM EKKO e2
            WHERE
                  e2.AEDAT >= ADD_YEARS(e1.AEDAT,-1)
                  AND e2.AEDAT <= e1.AEDAT
                  --Durchschnitt aller Mitarbeiter oder nur des aktuellen
                  AND e2.ERNAM = e1.ERNAM
```

```
                AND e2.MANDT = e1.MANDT
            )
;

--Markiere Bestellungen an auffälligen Tagen
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP  AS CaseId,
      'Flag_B04' AS FlagId
FROM #SUSPICIOUS_ORDERS_B4b, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.ERNAM = #SUSPICIOUS_ORDERS_B4b.ERNAM
      AND EKKO.AEDAT = #SUSPICIOUS_ORDERS_B4b.AEDAT
      AND EKKO.MANDT = #SUSPICIOUS_ORDERS_B4b.MANDT
      AND EKKO.BSTYP = 'F'
;

--Flag_B05 - Schnelle Bestellung
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EBAN.MANDT || EBAN.EBELN || EBAN.EBELP AS CaseId,
      'Flag_B05' AS FlagId

FROM X0_STUDENT_001.EBAN
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELP = EBAN.EBELP
      AND EKPO.EBELN = EBAN.EBELN
      AND EKPO.MANDT = EBAN.MANDT
JOIN X0_STUDENT_001.EKBE ON
      EKBE.EBELP = EKPO.EBELP
      AND EKBE.EBELN = EKPO.EBELN
      AND EKBE.MANDT = EKPO.MANDT
WHERE
       EKBE.VGABE = '1'
      AND EKBE.SHKZG = 'S'
      AND DAYS_BETWEEN(EBAN.BADAT, EKBE.CPUDT) < 1
;

--Flag_B06 - Genehmigung Übersprungen
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B06' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      --Freigabe wurde noch nicht erteillt
      EKKO.FRGRL = 'X'
      AND LENGTH(LTRIM(EKKO.FRGSX)) > 0
      --Es existiert aber schon ein Waren- oder Rechnungseingang
      AND EXISTS
            (SELECT EKBE.EBELN
            FROM X0_STUDENT_001.EKBE
            WHERE
                  EKBE.VGABE IN ('1','2')
```

```
                AND EKBE.SHKZG = 'S'
                AND EKBE.MANDT = EKPO.MANDT
                AND EKBE.EBELN = EKPO.EBELN
                AND EKBE.EBELP = EKPO.EBELP
            )
;

--Flag_B07 - Steigende Rechnugsanzahl
--Erstellt Liste von Bestellungen mit Rechnungseingang pro Monat
CREATE LOCAL TEMPORARY TABLE #INVOICES_PER_MONTH_B7
(MANDT VARCHAR (20), LIFNR VARCHAR(30), INVOICE_YEAR INT, INVOICE_MONTH
INT, INVOICES INT)
;

INSERT INTO #INVOICES_PER_MONTH_B7
SELECT
      EKKO.MANDT AS MANDT,
      EKKO.LIFNR AS LIFNR,
      YEAR(EKKO.AEDAT) AS INVOICE_YEAR,
      MONTH(EKKO.AEDAT) AS INOIVCE_MONTH,
      COUNT(EKBE.EBELN) AS INVOICES
FROM X0_STUDENT_001.EKBE
JOIN EKKO ON
      EKKO.EBELN = EKBE.EBELN
      AND EKKO.MANDT = EKBE.MANDT
WHERE
      EKBE.VGABE = '2'
      AND EKBE.SHKZG = 'S'
      AND EKKO.AEDAT between TO_DATE(YEAR(EKKO.AEDAT)|| '-' ||
MONTH(EKKO.AEDAT) || '-01', 'YYYY-MM-DD') and LAST_DAY(EKKO.AEDAT)
GROUP BY EKKO.MANDT, EKKO.LIFNR, YEAR(EKKO.AEDAT), MONTH(EKKO.AEDAT)
HAVING COUNT(EKBE.EBELN) > 1
;

--Vergleicht Liste miteinander und sucht nach plötzlich steigenden
Rechnungseingängen
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_VENDOR_DATA_B7
(MANDT VARCHAR (20), LIFNR VARCHAR(30), LIF_YEAR INT, LIF_MONTH INT)
;

INSERT INTO #SUSPICOUS_VENDOR_DATA_B7
SELECT
      i1.MANDT,
      i1.LIFNR AS LIFNR,
      i1.INVOICE_YEAR AS LIF_YEAR,
      i1.INVOICE_MONTH AS LIF_MONTH
FROM #INVOICES_PER_MONTH_B7 i1
WHERE EXISTS (SELECT i2.INVOICES
                        FROM #INVOICES_PER_MONTH_B7 i2
                        WHERE i2.LIFNR = i1.LIFNR
                        AND i2.MANDT = i1.MANDT
                        AND i2.INVOICE_MONTH =
MONTH(ADD_MONTHS(TO_DATE(i1.INVOICE_YEAR|| '-' || i1.INVOICE_MONTH || '-
01','YYYY-MM-DD'),-1))
                        AND i2.INVOICE_YEAR =
YEAR(ADD_MONTHS(TO_DATE(i1.INVOICE_YEAR|| '-' || i1.INVOICE_MONTH || '-
01','YYYY-MM-DD'),-1))
                        --Rechnungseinggänge des Vormonats sind [X]-fach
weniger als der aktuelle Monat
                        AND i1.INVOICES > 3*i2.INVOICES
```

```
                        AND i2.INVOICES > 0
                        )
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B07' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN #SUSPICOUS_VENDOR_DATA_B7 ON
      EKKO.LIFNR = #SUSPICOUS_VENDOR_DATA_B7.LIFNR
      AND EKKO.MANDT = #SUSPICOUS_VENDOR_DATA_B7.MANDT
      AND MONTH(EKKO.AEDAT) = #SUSPICOUS_VENDOR_DATA_B7.LIF_MONTH
      AND YEAR(EKKO.AEDAT) = #SUSPICOUS_VENDOR_DATA_B7.LIF_YEAR
;

--Flag_B8 - Rechnung ohne Wahrenlieferung
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_B08' AS FlagId
FROM X0_STUDENT_001.RSEG
JOIN X0_STUDENT_001.BKPF ON
      BKPF.AWKEY = concat(RSEG.BELNR, RSEG.GJAHR)
      AND BKPF.MANDT = RSEG.MANDT
--Rechnung muss bereits im Lieferantenausgleich vorhanden sein
JOIN X0_STUDENT_001.BSAK ON
      BKPF.BELNR = BSAK.BELNR
      AND BKPF.MANDT = BSAK.MANDT
      AND BKPF.GJAHR = BSAK.GJAHR
      AND BKPF.BUKRS = BSAK.BUKRS
WHERE
      --Schließe Dienstleistungen aus, da hier nicht zwingend ein
Wareneingang
      --verzeichnet wird.
      RSEG.MEINS <> 'LE'
AND NOT EXISTS
      --Es exisitert kein Wareneingang in der Bestellhistorie
      (SELECT EKBE.EBELN
      FROM X0_STUDENT_001.EKBE
      WHERE
            EKBE.VGABE = '1'
            AND EKBE.SHKZG = 'S'
            AND EKBE.EBELN = RSEG.EBELN
            AND EKBE.EBELP = RSEG.EBELP
            AND EKBE.MANDT = RSEG.MANDT)
;

--Flag_B09 - Fehlende Telefonnummer
--Erstelle Liste mit Lieferanten die keine Telefonnummer haben
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B09' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
```

```
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.LFA1 ON
      LFA1.LIFNR = EKKO.LIFNR
      AND LFA1.MANDT = EKKO.MANDT
WHERE
      LENGTH(LTRIM(LFA1.TELF1)) = 0
      AND LENGTH(LTRIM(LFA1.TELF2)) = 0
;


--Flag_B10 - Fehlende Anschrift

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B10' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN x0_STUDENT_001.LFA1 ON
      LFA1.MANDT = EKKO.MANDT
      AND LFA1.LIFNR = EKKO.LIFNR
WHERE
      LENGTH(LTRIM(LFA1.ORT01)) = 0
      AND LENGTH(LTRIM(LFA1.PSTLZ)) = 0
      AND LENGTH(LTRIM(LFA1.STRAS)) = 0
;

--Flag_B11 - Materialbeschreibung
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B11' AS FlagId
FROM X0_STUDENT_001.EKPO
WHERE
      --Kein Materialstammssatz gewählt
      LENGTH(LTRIM(EKPO.MATNR)) = 0
      --Materialtext kleiner als gewählte Grenze
      AND LENGTH(LTRIM(EKPO.TXZ01)) < 6
;

--Flag_B12 - Grenzwerte
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT e1.MANDT || e1.EBELN || p1.EBELP AS CaseId,
      'Flag_B12' AS FlagId
FROM EKKO e1
JOIN X0_STUDENT_001.EKPO p1 ON
      e1.EBELN =  p1.EBELN
      AND e1.MANDT = p1.MANDT
WHERE
      --Summe der Nettowerte ist nahe an Grenzwert 1
      (SELECT
            SUM(p2.NETWR)
      FROM X0_STUDENT_001.EKPO p2
      WHERE
            p2.EBELN = e1.EBELN
            AND p2.MANDT = e1.MANDT) between (5000.00-10) and (5000.00-
0.01)
```

```
OR
      --Summe der Nettowerte ist nahe an Grenzwert 2
      (SELECT
            SUM(p2.NETWR)
      FROM X0_STUDENT_001.EKPO p2
      WHERE p2.EBELN = e1.EBELN
      AND p2.MANDT = e1.MANDT) between (50000.00-10) and (50000.00-0.01)
GROUP BY
      e1.MANDT,
      e1.EBELN,
      p1.EBELP
;

--Flag_B13 - Teure Beratung
--Erstelle Liste von Lieferanten die nur Dienstleistungen anbieten
CREATE LOCAL TEMPORARY TABLE #SERVICE_ONLY_VENDORS_B13
(MANDT VARCHAR(20), LIFNR VARCHAR(30))
;

INSERT INTO #SERVICE_ONLY_VENDORS_B13
SELECT
      ek1.MANDT,
      ek1.LIFNR
FROM X0_STUDENT_001.EKPO e1
JOIN EKKO ek1 ON
      ek1.EBELN = e1.EBELN
      AND ek1.MANDT = e1.MANDT
WHERE
-- Nimm Lieferant nur in Liste auf wenn es keine Bestellung
-- gibt die keine Dienstleistung ist
NOT EXISTS
      (SELECT e2.EBELN
      FROM X0_STUDENT_001.EKPO e2
      JOIN EKKO ek2 ON
            ek2.EBELN = e2.EBELN
            AND ek2.MANDT = e2.MANDT
      WHERE ek2.LIFNR = ek1.LIFNR
      AND ek2.MANDT = ek1.MANDT
      AND LENGTH(LTRIM(e2.MEINS)) > 0
      AND e2.MEINS <> 'LE')
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B13' AS FlagId
FROM X0_STUDENT_001.EKBE
JOIN EKKO ON
      EKKO.EBELN = EKBE.EBELN
      AND EKKO.MANDT = EKBE.MANDT
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN #SERVICE_ONLY_VENDORS_B13 ON
      #SERVICE_ONLY_VENDORS_B13.MANDT = EKKO.MANDT
      AND #SERVICE_ONLY_VENDORS_B13.LIFNR = EKKO.LIFNR
WHERE EKBE.VGABE = '2'
GROUP BY EKKO.MANDT, EKKO.EBELN, EKPO.EBELP
--Dienstleistung ist entweder sehr klein und benötigt keine zusätzliche
Freigabe
```

```
--oder sehr groß
HAVING
      SUM(EKPO.NETWR) NOT BETWEEN 5000.00 AND 50000.00
;

--Flag_B14 - Neuer Lieferant
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B14' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.LFA1 ON
      LFA1.LIFNR = EKKO.LIFNR
      AND LFA1.MANDT = EKKO.MANDT
WHERE
      --Lieferant wurde erst vor einer Woche erstellt
      LENGTH(LTRIM(EKKO.LIFNR)) > 0
      AND LFA1.ERDAT between ADD_DAYS(EKKO.AEDAT,-7) and EKKO.AEDAT
--Bestellvolumen ist größer als das Limit
AND
      (SELECT
            SUM(p2.NETWR)
      FROM X0_STUDENT_001.EKPO p2
      WHERE
            p2.EBELN = EKKO.EBELN
            AND p2.MANDT = EKKO.MANDT) > 5000.00
;

--Flag_B15 - Keine Steuern
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_B15' AS FlagId
FROM X0_STUDENT_001.RBKP
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = RBKP.BELNR
      AND RSEG.GJAHR = RBKP.GJAHR
      AND RSEG.MANDT = RBKP.MANDT
JOIN EKKO ON
      EKKO.EBELN = RSEG.EBELN
      AND EKKO.MANDT = RSEG.MANDT
--Steuern in Rechnung sind 0
WHERE RBKP.WMWST1 = 0
;

--Flag_B16 - Aufteigende Rechnungsnummer
--Erstelle Liste mit Referenzrechnungsnummern
--und der logisch nächsten Nummer
DROP TABLE #NEXT_XBLNR;
CREATE LOCAL TEMPORARY TABLE #NEXT_XBLNR
(MANDT VARCHAR(30), XBLNR VARCHAR(30), NEXT_XBLNR VARCHAR(30))
;

INSERT INTO #NEXT_XBLNR
SELECT
      RBKP.MANDT,
      RBKP.XBLNR,
```

```
      (CASE
            WHEN
            LENGTH(ltrim(RBKP.XBLNR,'0123456789')) = 0
            THEN CAST((CAST(RBKP.XBLNR AS bigint) + 1) AS varchar)
            ELSE NULL
      END) AS NEXT_XBLNR
FROM X0_STUDENT_001.RBKP
WHERE LENGTH(LTRIM(RBKP.XBLNR)) > 0
;


INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_B16' AS FlagId
FROM X0_STUDENT_001.RBKP r1
--Verbinde die aktuelle Rechnungsnummer
JOIN #NEXT_XBLNR ON
      #NEXT_XBLNR.XBLNR = r1.XBLNR
      AND #NEXT_XBLNR.MANDT = r1.MANDT
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.GJAHR = r1.GJAHR
      AND RSEG.MANDT = r1.MANDT
WHERE
      LENGTH(LTRIM(r1.XBLNR)) > 0
      AND r1.BELNR <> r1.XBLNR
      AND #NEXT_XBLNR.NEXT_XBLNR IS NOT NULL
--Für diesen Eintrag exisitiert eine weitere Rechnung
--welche als Referenzrechnungsnummern die logisch nächste hat
AND EXISTS
      (SELECT r2.XBLNR
      FROM X0_STUDENT_001.RBKP r2
      WHERE
            r2.LIFNR = r1.LIFNR
            AND r2.XBLNR = #NEXT_XBLNR.NEXT_XBLNR
            AND r2.MANDT = r1.MANDT)
;


--Flag_B17 - Initialien als Lieferantennm
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B17' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE EKKO.LIFNR IN
      (SELECT
            LFA1.LIFNR
      FROM X0_STUDENT_001.LFA1
      WHERE
            --Name ist besonders kurz
            (LENGTH(LTRIM(LFA1.NAME1)) between 1 and 3
            --Der Unterschied zwischen dem Originalnamen und einem von
Punkten
            --befreiten Namen ist größer als 3
            --Mindestens drei Punkte
```

```
            OR (LENGTH(LFA1.NAME1) - LENGTH(REPLACE(LFA1.NAME1, '.', '')))
> 3)

      )
;


--Flag_B18 - Steigende Einkäufe
--Erstelle Liste für jeden Lieferanten und Mitarbeiter über die
Bestellungen pro Monat
CREATE LOCAL TEMPORARY TABLE #ORDERS_PER_MONTH_B18
(MANDT VARCHAR(20), LIFNR VARCHAR(30), ERNAM VARCHAR(30), ORDER_YEAR INT,
ORDER_MONTH INT, ORDERS DOUBLE)
;

INSERT INTO #ORDERS_PER_MONTH_B18
SELECT
      EKKO.MANDT AS MANDT,
      EKKO.LIFNR AS LIFNR,
      EKKO.ERNAM AS ERNAM,
      YEAR(EKKO.AEDAT) AS ORDER_YEAR,
      MONTH(EKKO.AEDAT) AS ORDER_MONTH,
      COUNT(EKKO.EBELN) AS ORDERS
FROM EKKO
WHERE
      LENGTH(LTRIM(EKKO.LIFNR)) > 0
--    AND s2.BLDAT between TO_DATE(YEAR(s1.BLDAT) || '-' || MONTH(s1.BLDAT)
|| '-01','YYYY-MM-DD') and LAST_DAY(s1.BLDAT)
      AND EKKO.AEDAT between TO_DATE(YEAR(EKKO.AEDAT)|| '-' ||
MONTH(EKKO.AEDAT) || '-01','YYYY-MM-DD') and LAST_DAY(EKKO.AEDAT)
GROUP BY
      EKKO.MANDT,
      EKKO.LIFNR,
      EKKO.ERNAM,
      YEAR(EKKO.AEDAT),
      MONTH(EKKO.AEDAT)
--HAVING COUNT(EKKO.EBELN) > 10
;

--Suche ob die Bestellungen bei einem Liferanten von einem Mitarbeiter
--signifikant größer sind als die des Vormonats
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDERS_B18
(MANDT VARCHAR(20), LIFNR VARCHAR(30), ERNAM VARCHAR(30), ORDER_YEAR INT,
ORDER_MONTH INT)
;

INSERT INTO #SUSPICIOUS_ORDERS_B18
SELECT
      MANDT,
      LIFNR,
      ERNAM,
      ORDER_YEAR,
      ORDER_MONTH
FROM #ORDERS_PER_MONTH_B18 o1
WHERE EXISTS
      (SELECT o2.ORDERS
            FROM #ORDERS_PER_MONTH_B18 o2
            WHERE
                  o2.LIFNR = o1.LIFNR
                  AND o2.MANDT = o1.MANDT
```

```
                    AND o2.ERNAM = o1.ERNAM
                    AND o2.ORDER_MONTH =
MONTH(ADD_MONTHS(TO_DATE(o1.ORDER_YEAR|| '-' || o1.ORDER_MONTH || '-
01','YYYY-MM-DD'),-1))
                    AND o2.ORDER_YEAR =
YEAR(ADD_MONTHS(TO_DATE(o1.ORDER_YEAR|| '-' || o1.ORDER_MONTH || '-
01','YYYY-MM-DD'),-1))
                    AND o1.ORDERS > 2*o2.ORDERS
                    AND o2.ORDERS > 0
             )
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B18' AS FlagId
FROM #SUSPICIOUS_ORDERS_B18, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.LIFNR = #SUSPICIOUS_ORDERS_B18.LIFNR
      AND EKKO.MANDT = #SUSPICIOUS_ORDERS_B18.MANDT
      AND EKKO.ERNAM = #SUSPICIOUS_ORDERS_B18.ERNAM
      AND YEAR(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_B18.ORDER_YEAR
      AND MONTH(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_B18.ORDER_MONTH
;

--Flag_B19 - Mehrmaliger Rechnungseingang
--Erstelle Liste aller Dienstleistungsbestellungen
CREATE LOCAL TEMPORARY TABLE #SERVICE_INVOCES_B19
(MANDT VARCHAR(30), EBELN  VARCHAR(30), EBELP VARCHAR(30), LIFNR
VARCHAR(30), MTRTXT VARCHAR(50), BLDAT DATE)
;

INSERT INTO #SERVICE_INVOCES_B19
SELECT
      EKPO.MANDT,
      EKPO.EBELN,
      EKPO.EBELP,
      EKKO.LIFNR,
      EKPO.TXZ01,
      RBKP.BLDAT
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.RSEG ON
      RSEG.EBELN = EKPO.EBELN
      AND RSEG.MANDT = EKPO.MANDT
JOIN X0_STUDENT_001.RBKP ON
      RBKP.BELNR = RSEG.BELNR
      AND RBKP.GJAHR = RSEG.GJAHR
      AND RBKP.MANDT = RSEG.MANDT
WHERE
      LENGTH(LTRIM(EKPO.MEINS)) > 0
      AND EKPO.MEINS = 'LE'
;

--Erstelle Liste mit allen auffälligen Bestellungen
```

```
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDER_B19
(MANDT VARCHAR(30), EBELN VARCHAR(30), EBELP VARCHAR(30), LIFNR
VARCHAR(30), BLDAT DATE)
;

INSERT INTO #SUSPICIOUS_ORDER_B19
SELECT
      MANDT,
      EBELN,
      EBELP,
      LIFNR,
      BLDAT
FROM #SERVICE_INVOCES_B19 s1
--Bei denen existiert
WHERE EXISTS
      (SELECT LIFNR
      FROM #SERVICE_INVOCES_B19 s2
      WHERE
            --gleicher Lieferant
            s2.LIFNR = s1.LIFNR
            --gleiche Dienstleistung
            AND s2.MTRTXT = s1.MTRTXT
            AND s2.EBELN <> s1.EBELN
            AND s2.MANDT = s1.MANDT
            --Rechnungseingang im gleichen Monat
            AND s2.BLDAT between TO_DATE(YEAR(s1.BLDAT) || '-' ||
MONTH(s1.BLDAT) || '-01','YYYY-MM-DD') and LAST_DAY(s1.BLDAT)
      )
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B19' AS FlagId
FROM X0_STUDENT_001.EKPO
JOIN #SUSPICIOUS_ORDER_B19 ON
      #SUSPICIOUS_ORDER_B19.EBELN = EKPO.EBELN
      AND #SUSPICIOUS_ORDER_B19.EBELP = EKPO.EBELP
      AND #SUSPICIOUS_ORDER_B19.MANDT = EKPO.MANDT
;

--Flag_B20 - Miterabeiteradresse als Lieferantenadresse
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
       DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
       'Flag_B20' AS FlagId
 FROM EKKO
 JOIN X0_STUDENT_001.EKPO ON
       EKPO.EBELN = EKKO.EBELN
       AND EKPO.MANDT = EKKO.MANDT
 WHERE
       --Der benutzte Lieferant ist in einer Liste von
       --Lieferanten die sowohl Straße als auch PLZ
       --Mit einem Mitarbeiter teilen
       EKKO.LIFNR in
             (
             SELECT LFA1.LIFNR
             FROM X0_STUDENT_001.LFA1
             INNER JOIN X0_STUDENT_001.USR03 on
                   LFA1.STRAS = USR03.STRAS
```

```
                AND LFA1.PSTLZ = USR03.PSTLZ
                AND LFA1.MANDT = USR03.MANDT
            WHERE LFA1.MANDT = EKKO.MANDT
            )
 ;

--Flag_B21 - Telefonnummern stimmen überein
-- PRINT 'Flag_B21:';

-- INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
-- SELECT
--     DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.MANDT AS CaseId,
--     'Flag_B21' AS FlagId
-- FROM EKKO
-- JOIN X0_STUDENT_001.EKPO ON
--     EKPO.EBELN = EKKO.EBELN
--     AND EKPO.MANDT = EKKO.MANDT
-- WHERE
--     EKKO.LIFNR in
--           (
--           SELECT
--                 LFA1.LIFNR
--           FROM X0_STUDENT_001.LFA1
--          --Die Telefonnummer eines Mitarbeiters stimmt mit de
--          --eines Lieferanten überein
--           INNER JOIN X0_STUDENT_001.USR03 ON
--                 LFA1.MANDT = USR03.MANDT and
--                (LFA1.TELF1 = USR03.TEL01 or
--                 LFA1.TELF1 = USR03.TEL02 or
--                 LFA1.TELF1 = USR03.TELNR or
--                 LFA1.TELF1 = USR03.TELPR or
--                 LFA1.TELF2 = USR03.TEL01 or
--                 LFA1.TELF2 = USR03.TEL02 or
--                 LFA1.TELF2 = USR03.TELNR or
--                 LFA1.TELF2 = USR03.TELPR)
--               WHERE LFA1.MANDT = EKKO.MANDT
--           )
-- ;

--Flag_B22 - Keine Steuernummer
CREATE LOCAL TEMPORARY TABLE #VENDOR_WITHOUT_TAXNUMBER
(MANDT VARCHAR(20), LIFNR VARCHAR(130), NAME VARCHAR(130))
;

INSERT INTO #VENDOR_WITHOUT_TAXNUMBER
SELECT
      LFA1.MANDT,
      LFA1.LIFNR,
      LFA1.NAME1
FROM X0_STUDENT_001.LFA1
WHERE
      --Keine der Steueridentifikationsnummern ist gefüllt
      LENGTH(LTRIM(LFA1.STCD1)) = 0
      AND LENGTH(LTRIM(LFA1.STCD2)) = 0
      AND LENGTH(LTRIM(LFA1.STCD3)) = 0
      AND LENGTH(LTRIM(LFA1.STCD4)) = 0
      AND LENGTH(LTRIM(LFA1.STCEG)) = 0
      AND LENGTH(LTRIM(LFA1.STENR)) = 0
;
```

```
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B22' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN #VENDOR_WITHOUT_TAXNUMBER ON
      #VENDOR_WITHOUT_TAXNUMBER.MANDT = EKKO.MANDT
      AND #VENDOR_WITHOUT_TAXNUMBER.LIFNR = EKKO.LIFNR
;


--Flag_B23 - Rechnungsgenehmiger
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_B23' AS FlagId
FROM X0_STUDENT_001.RBKP
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = RBKP.BELNR
      AND RSEG.GJAHR = RBKP.GJAHR
      AND RSEG.MANDT = RBKP.MANDT
JOIN EKKO ON
      EKKO.EBELN = RSEG.EBELN
      AND EKKO.MANDT = RSEG.MANDT
WHERE
      --Die Rechnung dieses Lieferanten wurden nie
      --von einem anderen geprüft
      LENGTH(LTRIM(RBKP.LIFNR)) > 0
AND
NOT EXISTS
      (SELECT r2.BELNR
      FROM X0_STUDENT_001.RBKP r2
      WHERE
            r2.LIFNR = RBKP.LIFNR
            AND r2.MANDT = RBKP.MANDT
            -- Vergleicht mit dem letzte Nutzer
            AND r2.USNAM <> RBKP.USNAM
            -- Vergleicht mit dem Erfasser
            -- AND r2.ERFNAM <> RBKP.ERFNAM
            AND NOT r2.BELNR = RBKP.BELNR)
;

--Flag_B24 - Teilkäufe
--Erstelle Liste mit käufen von Materialen bei Lieferanten
--diese werden pro Tag gruppiert und die Tagessumme berechnet
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_ORDERS_B24
(MANDT VARCHAR(30), ERNAM VARCHAR(30), AEDAT DATE, MATNR VARCHAR(30), LIFNR
VARCHAR(30), ORDER_VOLUME DOUBLE, ORDER_COUNT DOUBLE)
;

INSERT INTO #SUSPICOUS_ORDERS_B24
SELECT
      EKKO.MANDT,
      EKKO.ERNAM,
      EKKO.AEDAT,
      EKPO.MATNR,
      EKKO.LIFNR,
```

```
      SUM(EKPO.NETWR) AS "Order Volume",
      COUNT(EKKO.EBELN) AS "Count"
FROM X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE
      LENGTH(LTRIM(EKKO.LIFNR)) > 0
      AND LENGTH(LTRIM(EKKO.FRGSX)) = 0
      AND LENGTH(LTRIM(EKPO.MATNR)) > 0
      AND LENGTH(LTRIM(EKKO.ERNAM)) > 0
GROUP BY
      EKKO.MANDT, EKKO.ERNAM, EKKO.AEDAT, EKPO.MATNR, EKKO.LIFNR
HAVING
      --Beachte nur Einträge die mehr als zwei Bestellungen pro Tag haben
      COUNT(EKKO.EBELN) > 2
      --Die Summe der einzelnen Bestellungen übersteigt die Freigebegrenze
      AND SUM(EKPO.NETWR) > 50000.00
--ORDER BY
      --EKKO_ERNAM, EKKO_AEDAT, EKKO_LIFNR
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B24' AS FlagId
FROM #SUSPICOUS_ORDERS_B24, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.MANDT = #SUSPICOUS_ORDERS_B24.MANDT
      AND EKKO.ERNAM = #SUSPICOUS_ORDERS_B24.ERNAM
      AND EKKO.AEDAT = #SUSPICOUS_ORDERS_B24.AEDAT
      AND EKPO.MATNR = #SUSPICOUS_ORDERS_B24.MATNR
      AND EKKO.LIFNR = #SUSPICOUS_ORDERS_B24.LIFNR
;

--Flag_B25 - Runde gleiche Beträge
--Erstelle Liste mit Lieferanten, Mitarbeiter, Material Kombination
--die runde Beträge haben und oft den gleichen Betrag
CREATE LOCAL TEMPORARY TABLE #SAME_AVG_VOLUME_B25
(MANDT VARCHAR(20), LIFNR VARCHAR(30), MATNR VARCHAR(30), ERNAM
VARCHAR(40))
;

INSERT INTO #SAME_AVG_VOLUME_B25
SELECT
      EKKO.MANDT,
      EKKO.LIFNR,
      EKPO.MATNR,
      EKKO.ERNAM
FROM X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE
      EKPO.NETWR > 0
      AND LENGTH(EKKO.LIFNR) > 0
      AND LENGTH(EKPO.MATNR) > 0
```

```
	AND
		--Zähle Anzahl wie oft ein runder Betrag bestellt wurde
		(SELECT
			COUNT(p2.EBELN)
		FROM X0_STUDENT_001.EKPO p2
		JOIN EKKO e2 ON
			e2.EBELN = p2.EBELN
			AND e2.MANDT = p2.MANDT
		WHERE
			EKKO.LIFNR = e2.LIFNR
			AND EKKO.ERNAM = e2.ERNAM
			AND EKKO.MANDT = e2.MANDT
			--Erweiterung auf Material
			AND EKPO.MATNR = p2.MATNR
			--Betrag ist rund wenn gleich ob ab- oder aufgerundet
			and FLOOR(p2.NETWR) <> CEILING(p2.NETWR)) < 10
GROUP BY EKKO.MANDT, EKKO.LIFNR, EKPO.MATNR, EKKO.ERNAM
HAVING
	STDDEV(EKPO.NETWR) < 5
	and COUNT(EKKO.EBELN) > 1
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
	DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
	'Flag_B25' AS FlagId
FROM #SAME_AVG_VOLUME_B25, EKKO
JOIN X0_STUDENT_001.EKPO ON
	EKPO.EBELN = EKKO.EBELN
	AND EKPO.MANDT = EKKO.MANDT
WHERE
	EKKO.LIFNR = #SAME_AVG_VOLUME_B25.LIFNR
	AND EKPO.MATNR = #SAME_AVG_VOLUME_B25.MATNR
	AND EKPO.MANDT = #SAME_AVG_VOLUME_B25.MANDT
	AND EKKO.ERNAM = #SAME_AVG_VOLUME_B25.ERNAM
;

--Flag_B26 - ungewoehnliche Zeit
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
	DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
	'Flag_B26' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
	EKPO.EBELN = EKKO.EBELN
	AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.CDPOS ON
	CDPOS.TABKEY = EKKO.MANDT || EKKO.EBELN
JOIN X0_STUDENT_001.CDHDR ON
	CDHDR.CHANGENR = CDPOS.CHANGENR
	AND CDHDR.MANDANT = CDPOS.MANDANT
WHERE
	--Eintrag wurde erstellt
	CDPOS.CHNGIND = 'I'
	--Es sich um einen Eintrag im Einkaufsprozess handelt
	AND (CDPOS.TABNAME = 'EKKO'
	OR CDPOS.TABNAME = 'EKPO'
	OR CDPOS.TABNAME = 'RSEG'
	OR CDPOS.TABNAME = 'RBKP'
	OR CDPOS.TABNAME = 'EKBE'
```

```
      OR CDPOS.TABNAME = 'EBAN')
      --Wurde nach 21 Uhr angelegt
      AND (CDHDR.UTIME > '21:00:00.0000000'
      --Wurde vor 5:30 angelegt
      OR CDHDR.UTIME < '05:30:00.0000000')
;


--Flag_B27 - Schnelle Zahlung
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_B27' AS FlagId
FROM X0_STUDENT_001.RSEG
JOIN X0_STUDENT_001.RBKP ON
      RBKP.BELNR = RSEG.BELNR
      AND RBKP.GJAHR = RSEG.GJAHR
      AND RBKP.MANDT = RSEG.MANDT
JOIN X0_STUDENT_001.BKPF ON
      BKPF.AWKEY = concat(RSEG.BELNR, RSEG.GJAHR)
      AND BKPF.MANDT = RSEG.MANDT
JOIN X0_STUDENT_001.BSAK ON
      BSAK.BELNR = BKPF.BELNR
      AND BSAK.GJAHR = BKPF.GJAHR
      AND BSAK.MANDT = BKPF.MANDT
      AND BSAK.BUKRS = BKPF.BUKRS
WHERE
      --Zahlungsziel für ersten Skonto angegeben
      RBKP.ZBD1T > 0
      --Ausgleich der Rechnung zwischen erfassung der Rechnung und der
hälfte
      --der Skontozeit
      AND BSAK.AUGDT between RBKP.BLDAT and
ADD_DAYS(RBKP.BLDAT,(RBKP.ZBD1T/2))
;

--Flag_B28 - Teuerer Einkauf
--Kurzliste der Bestellungen mit Gesamtsumme jeder Bestellung
CREATE LOCAL TEMPORARY TABLE #LIST
(MANDT VARCHAR(30), LIFNR VARCHAR(30), AEDAT DATE, EBELN VARCHAR(30),
NETSUM DOUBLE)
;

INSERT INTO #LIST
SELECT
      EKKO.MANDT,
      EKKO.LIFNR,
      EKKO.AEDAT,
      EKKO.EBELN,
      SUM(EKPO.NETWR)
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE LENGTH(LTRIM(EKKO.LIFNR)) > 0
GROUP BY EKKO.MANDT, EKKO.LIFNR, EKKO.AEDAT, EKKO.EBELN
HAVING SUM(EKPO.NETWR) > 0
ORDER BY EKKO.LIFNR, EKKO.AEDAT
;
```

```
--Suche eine Bestellung
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_ORDERS_B29
(MANDT VARCHAR(30), EBELN VARCHAR(30))
;

select * from EKPO;

INSERT INTO #SUSPICOUS_ORDERS_B29
SELECT
      MANDT,
      EBELN
FROM #LIST l1
WHERE EXISTS
      --Bei der es eine vorhergehende Bestellung gibt
      --deren Wert signifikant kleiner ist
      (SELECT l2.EBELN
      FROM #LIST l2
      WHERE
            l2.EBELN < l1.EBELN
            AND l2.LIFNR = l1.LIFNR
            AND l2.MANDT = l1.MANDT
            AND l2.NETSUM*3.00 < l1.NETSUM
            --Und es keine Bestellung dazwischen gibt
            AND NOT EXISTS
                  (SELECT l3.EBELN
                  FROM #LIST l3
                  WHERE
                        l2.LIFNR = l3.LIFNR
                        AND l2.MANDT = l3.MANDT
                        AND l3.EBELN < l1.EBELN
                        AND l3.EBELN > l2.EBELN)
      )
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B28' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN #SUSPICOUS_ORDERS_B29 ON
      #SUSPICOUS_ORDERS_B29.MANDT = EKKO.MANDT
      AND #SUSPICOUS_ORDERS_B29.EBELN = EKKO.EBELN
;

--Flag_B29 - Ausreiser Bestellung
--Erstelle Liste mit den Durschnittlichen Bestellsummen pro Lieferant
CREATE LOCAL TEMPORARY TABLE #VENDOR_AVERGAE_B30
(MANDT VARCHAR(20), LIFNR VARCHAR(30), AVERAGE_VOLUME DOUBLE, STD_VARIANCE
DOUBLE)
;

INSERT INTO #VENDOR_AVERGAE_B30
SELECT
      EKKO.MANDT,
      EKKO.LIFNR,
      ROUND(AVG(EKPO.NETWR),2),
      ROUND(STDDEV(EKPO.NETWR),2)
```

```
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE LENGTH(LTRIM(EKKO.LIFNR)) > 0
GROUP BY EKKO.MANDT, EKKO.LIFNR
HAVING ROUND(STDDEV(EKPO.NETWR),2) > 0.00
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B29' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN #VENDOR_AVERGAE_B30 ON
      #VENDOR_AVERGAE_B30.LIFNR = EKKO.LIFNR
      AND #VENDOR_AVERGAE_B30.MANDT = EKKO.MANDT
GROUP BY
      EKKO.MANDT,
      EKPO.EBELN,
      EKPO.EBELP,
      EKKO.LIFNR,
      EKPO.NETWR,
      EKPO.NETWR,
      #VENDOR_AVERGAE_B30.AVERAGE_VOLUME,
      #VENDOR_AVERGAE_B30.STD_VARIANCE
HAVING
      --Sehr einfache Variante
      --EKPO_NETWR > (VENDOR_AVERGAE_B30.AVERAGE_VOLUME +
VENDOR_AVERGAE_B30.STD_VARIANCE)
      --Z-Wert
      ((EKPO.NETWR-
#VENDOR_AVERGAE_B30.AVERAGE_VOLUME)/#VENDOR_AVERGAE_B30.STD_VARIANCE) > 3
;

--Flag_B30 - Einmallieferant
--Erstelle Liste von Bestellungen die keinen bekannten Lieferant
--nutzen und über einem gesetzten Limit sind
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDERS_B31
(MANDT VARCHAR(30), EBELN VARCHAR(30))
;

INSERT INTO #SUSPICIOUS_ORDERS_B31
SELECT
      EKKO.MANDT,
      EKKO.EBELN
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
GROUP BY EKKO.MANDT, EKKO.EBELN
HAVING SUM(EKPO.NETWR) > 5000.00
EXCEPT
SELECT
      EKKO.MANDT,
      EKKO.EBELN
FROM EKKO
```

```
JOIN X0_STUDENT_001.LFA1 ON
      LFA1.LIFNR = EKKO.LIFNR
      AND LFA1.MANDT = EKKO.MANDT
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B30' AS FlagId
FROM EKKO
JOIN #SUSPICIOUS_ORDERS_B31 ON
      #SUSPICIOUS_ORDERS_B31.EBELN = EKKO.EBELN
      AND #SUSPICIOUS_ORDERS_B31.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
;

-- Schema 31 Mehrere Instanzen desselben Lieferanten innerhalb
Lieferantenliste/-Datenbank
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B31' AS FlagId
 FROM X0_STUDENT_001.EKKO

 JOIN X0_STUDENT_001.EKPO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
 JOIN LFA1 l1 ON
      l1.LIFNR = EKKO.LIFNR
      AND l1.MANDT = EKKO.MANDT
WHERE
      -- Ein Lieferanteneintrag vorhanden ist
      LENGTH(LTRIM(l1.LIFNR)) > 0
      -- und ein Eintrag existiert, bei dem der Name, der Lieferant, der
Ort und die Postleitzahl gleich sind,
      -- jedoch nicht die eindeutige Lieferantennummer
AND    EXISTS
      (SELECT l2.NAME1
      FROM X0_STUDENT_001.LFA1 l2
      WHERE
            l1.MANDT = l2.MANDT
            -- Vergleicht das Name, Land, Ort und Postleitzahl gleich sind
            AND l1.NAME1 = l2.NAME1
            AND l1.LAND1 = l2.LAND1
            AND l1.ORT01 = l2.ORT01
            AND l1.PSTLZ = l2.PSTLZ
            -- Es aber unterschiedliche Lieferantennummern sind
            AND l1.LIFNR <> l2.LIFNR
      )
;

--Flag_B33 - Steuerlich begünstigtes Land

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_B33' AS FlagId
FROM X0_STUDENT_001.CDPOS
```

```
JOIN X0_STUDENT_001.EKPO ON
      CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
JOIN X0_STUDENT_001.CDHDR ON
      CDPOS.CHANGENR = CDHDR.CHANGENR
      AND CDPOS.MANDANT = CDHDR.MANDANT
WHERE
      --Suche Bankland in Tax Haven (Bahamas, Andorra, Monaco, Bulgarien,
Panama, Mauritius, Dubai, Guernsey, Cayman Islands und Schweiz)
      LFBK.BANKS = 'BS'
      OR
      LFBK.BANKS = 'AD'
      OR
      LFBK.BANKS = 'MC'
      OR
      LFBK.BANKS = 'BG'
      OR
      LFBK.BANKS = 'PA'
      OR
      LFBK.BANKS = 'MU'
      OR
      LFBK.BANKS = 'AE'
      OR
      LFBK.BANKS = 'GG'
      OR
      LFBK.BANKS = 'KY'
      OR
      LFBK.BANKS = 'CH'
;


--Scheme Konfigration
--Beispiel
--Um ein eigenes Schema zu Konfigurieren müssen die FlagId
--der gewünschten Flags eingetragen werden
--Wird statt dem Intersect ein Union benutzt, werde alle Transaktionen
--markiert die mindestens einen der aufgeführten Flags besitzen
--im Fall von Intersect müssen alle Flags vorhanden sein

UPDATE _CEL_FLAGED_CASES
SET SCHEMEID = 'B1-Shell Company'
WHERE CASEID IN
(


SELECT
      FC2.CASEID
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_B18'

INTERSECT

SELECT
      FC2.CASEID
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_B24'


)
AND FLAGID IN ('Flag_B18','Flag_B24');
```

Doppelte Bezahlung

```
--Red Flag Processing
--Collection of Red Flag Scripts for Scheme Double Payment

--Flag_C01 - Mehrere Rechnungen
--Sucht Rechnungen für das selbe Produkt vom selben
--Lieferanten in sehr kurzem Abstand
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT p1.MANDT || p1.EBELN || p1.EBELP AS CaseId,
      'Flag_C01' AS FlagId
FROM X0_STUDENT_001.RSEG p1
JOIN X0_STUDENT_001.RBKP e1 ON
      p1.BELNR = e1.BELNR
      AND p1.GJAHR = e1.GJAHR
      AND p1.MANDT = e1.MANDT
WHERE
      LENGTH(LTRIM(p1.MATNR)) > 0
      AND LENGTH(LTRIM(e1.LIFNR)) > 0
      AND LENGTH(LTRIM(e1.USNAM)) > 0
      AND EXISTS
      (SELECT p2.EBELN
      FROM X0_STUDENT_001.RSEG p2
      JOIN X0_STUDENT_001.RBKP e2 ON
            p2.BELNR = e2.BELNR
            AND p2.GJAHR = e2.GJAHR
            AND p2.MANDT = e2.MANDT
      WHERE
            --Es exisitert eine Rechnung
            --mit dem selben Produkt
            p2.MATNR = p1.MATNR
            --dem selben Lieferanten
            AND e2.LIFNR = e1.LIFNR
            AND e2.BELNR <> e1.BELNR
            --vom gleichen Genehmiger
            AND e2.USNAM = e1.USNAM
            --innerhalb von zwei Tagen
            AND e2.BLDAT BETWEEN e1.BLDAT AND ADD_DAYS(e1.BLDAT,2)
            AND p2.MANDT = p1.MANDT
            AND LENGTH(LTRIM(p2.MATNR)) > 0
            AND LENGTH(LTRIM(e2.LIFNR)) > 0
            AND LENGTH(LTRIM(e2.USNAM)) > 0)
;

--Flag_C02 - Anschriften wiederverwendet
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_C02' AS FlagId
FROM X0_STUDENT_001.EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      --Bestellung benutzt einen Lieferanten dessen Adresse wiederverwendet
```

```
      --wird
      EKKO.LIFNR IN
            (SELECT
                  l1.LIFNR
            FROM X0_STUDENT_001.LFA1 l1
            WHERE
                  LENGTH(LTRIM(l1.PSTLZ)) > 0
                  AND LENGTH(LTRIM(l1.STRAS)) > 0
                  AND LENGTH(LTRIM(l1.ORT01)) > 0
                  AND LENGTH(LTRIM(l1.ORT02)) > 0
                  AND l1.MANDT = EKKO.MANDT
            AND EXISTS
                  (SELECT l2.LIFNR
                  FROM X0_STUDENT_001.LFA1 l2
                  WHERE l2.LIFNR <> l1.LIFNR
                  AND l2.MANDT = l1.MANDT
                  AND LENGTH(LTRIM(l2.PSTLZ)) > 0
                  AND LENGTH(LTRIM(l2.STRAS)) > 0
                  AND LENGTH(LTRIM(l2.ORT01)) > 0
                  AND LENGTH(LTRIM(l2.ORT02)) > 0
                  AND l2.STRAS = l1.STRAS
                  AND
                        (l2.ORT01 in (l1.ORT01, l1.ORT02)
                        OR l2.ORT02 in (l1.ORT01, l1.ORT02))
                  AND l2.PSTLZ = l2.PSTLZ)
            )
;


--Flag_C03 - Einkaufswert doppelt gezahlt
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES"(CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_C03' AS FlagId
FROM X0_STUDENT_001.RBKP r1
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.GJAHR =  r1.GJAHR
      AND RSEG.MANDT = r1.MANDT
WHERE
      LENGTH(LTRIM(r1.RMWWR)) > 0
      AND r1.RMWWR > 0
      AND LENGTH(LTRIM(r1.LIFNR)) > 0
AND EXISTS
      (SELECT r2.BELNR
      FROM X0_STUDENT_001.RBKP r2
      WHERE
            --Es exisitert eine zweite Rechnungn
            r2.BELNR <> r1.BELNR
            AND r2.MANDT = r1.MANDT
            --Mit gleichem Rechnungsbetrag
            AND r2.RMWWR = r1.RMWWR
            --gleichem Lieferanten
            AND r2.LIFNR <> r1.LIFNR
            --Und wurde innerhalb von 14 Tagen eingegeben
            AND r2.CPUDT between r1.CPUDT and ADD_DAYS(r1.CPUDT,14)
            AND LENGTH(LTRIM(r1.RMWWR)) > 0
            AND LENGTH(LTRIM(r1.LIFNR)) > 0)
;
```

```
--Flag_C04 - Referenzrechnungsnummer doppelt
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES"(CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_C04' AS FlagId
FROM X0_STUDENT_001.RBKP r1
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.GJAHR = r1.GJAHR
      AND RSEG.MANDT = r1.MANDT
WHERE
      LENGTH(LTRIM(r1.XBLNR)) > 0
      AND LENGTH(LTRIM(r1.LIFNR)) > 0
      AND EXISTS
      (SELECT r2.BELNR
      FROM X0_STUDENT_001.RBKP r2
      WHERE
            --Suche nach einer zweiten Rechnungn mit selber
            --Referenzrechnungsnummer im selben Geschaeftsjahr
            --vom selben Lieferanten
            r2.BELNR <> r1.BELNR
            AND r2.MANDT = r1.MANDT
            AND r2.GJAHR = r1.GJAHR
            AND r2.XBLNR = r1.XBLNR
            AND r2.LIFNR =  r1.LIFNR
            AND LENGTH(LTRIM(r2.XBLNR)) > 0
            AND LENGTH(LTRIM(r2.LIFNR)) > 0)
;

--Flag_C05 - Selber Betrag mehrmahls bezahlt
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_C05' AS FlagId
FROM X0_STUDENT_001.RBKP r1
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.MANDT = r1.MANDT
      AND RSEG.GJAHR = r1.GJAHR
WHERE
      LENGTH(LTRIM(r1.RMWWR)) > 0
      AND r1.RMWWR > 0
      AND LENGTH(LTRIM(r1.LIFNR)) > 0
AND EXISTS
      (SELECT
            r2.BELNR
      FROM X0_STUDENT_001.RBKP r2
      WHERE
            --Es exisiert eine Rechnung vom selben Nutzer
            -- Mit gleichem Betrag an den gleichen Lieferanten
            -- und dem gleichen Mitarbeiter
            r2.USNAM = r1.USNAM
            AND r2.MANDT = r1.MANDT
            AND r2.RMWWR = r1.RMWWR
            AND r2.CPUDT = r1.CPUDT
            AND r2.LIFNR = r1.LIFNR
            AND r2.BELNR <> r1.BELNR
      )
;
```

```
--Flag_C06 - Selbe Rechnung doppelt mehrfach bezahlt
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_C06' AS FlagId
FROM X0_STUDENT_001.RBKP r1
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.MANDT = r1.MANDT
      AND RSEG.GJAHR = r1.GjAHR
WHERE
      LENGTH(LTRIM(r1.LIFNR)) > 0
AND EXISTS
      (SELECT
            r2.BELNR
      FROM X0_STUDENT_001.RBKP r2
      WHERE
            --Es exisiert eine Rechnung mit dem selben Betrag
            --an den gleichen Lieferanten aber einem anderen
            --Mitarbeiter
            r2.RMWWR = r1.RMWWR
            AND r2.CPUDT = r1.CPUDT
            AND r2.LIFNR = r1.LIFNR
            AND r2.BELNR <> r1.BELNR
            AND r2.USNAM <> r1.USNAM
            AND r2.MANDT = r1.MANDT
      )
;

--Flag_C07 - Rechnungsnummer mit anderem Betrag
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_C07' AS FlagId
FROM X0_STUDENT_001.RBKP r1
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.MANDT = r1.MANDT
      AND RSEG.GJAHR = r1.GJAHR
WHERE
      LENGTH(LTRIM(r1.XBLNR)) > 0
      AND LENGTH(LTRIM(r1.LIFNR)) > 0
AND EXISTS
      (SELECT
            r2.BELNR
      FROM X0_STUDENT_001.RBKP r2
      WHERE
            -- Es exisiert eine Rechnung mit gleicher
            -- Referenzrechnungsnummer an den gleichen Lieferanten
            -- aber anderem Betrag
            r2.XBLNR = r1.XBLNR
            AND r2.MANDT = r1.MANDT
            AND r2.LIFNR = r1.LIFNR
            AND r2.RMWWR <> r1.RMWWR
            AND LENGTH(LTRIM(r2.XBLNR)) > 0
      )
;


--Scheme Konfigration
```

```
--Beispiel
--Um ein eigenes Schema zu Konfigurieren müssen die FlagId
--der gewünschten Flags eingetragen werden
--Wird statt dem Intersect ein Union benutzt, werde alle Transaktionen
--markiert die mindestens einen der aufgeführten Flags besitzen
--im Fall von Intersect müssen alle Flags vorhanden sein

UPDATE _CEL_FLAGED_CASES
SET SCHEMEID = 'C1-Double Payment'
WHERE CASEID IN
(

SELECT
      FC2.CASEID
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_C02'

INTERSECT

SELECT
      FC2.CASEID
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_C04'

INTERSECT

SELECT
      FC2.CASEID
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_C07'

)
AND FLAGID IN ('Flag_C02','Flag_C04','Flag_C07');
```

Kickback

```
--Red Flag Processing
--Collection of Red Flag Scripts for Scheme Overpay


--Flag_D01 - Favorisierter Lieferant
--Suche Mitarbeiter die den großteil der Bestellungen
--bei einenm Lieferanten generiert

drop table #RESULT_D1;
CREATE LOCAL TEMPORARY TABLE #RESULT_D1
(MANDT INT, ERNAM VARCHAR(40), LIFNR VARCHAR(40), ORDER_YEAR INT,
ORDER_MONTH INT);


INSERT INTO #RESULT_D1
SELECT
      e1.MANDT,
      e1.ERNAM,
      e1.LIFNR,
      YEAR(e1.AEDAT),
      MONTH(e1.AEDAT)
FROM EKKO e1
```

```
WHERE LENGTH(LTRIM(e1.LIFNR))> 0
GROUP BY e1.MANDT, e1.ERNAM, e1.LIFNR, YEAR(e1.AEDAT), MONTH(e1.AEDAT)
HAVING
      --Mindestanzahl an Bestellungen an den Lieferant
      --Kleine Zahlen führen zu mehr Markierungen
      --da es leichter ist den Großteil der Bestellungen
      --durchzuführen
      COUNT(e1.EBELN) > 25
      AND COUNT(e1.EBELN)
                        --Es werden mehr als 80 Prozent der Bestellungen
                        --bei diesen Lieferanten von einem
                        --Mitarbeiter durchgeführt
                        > (0.80 *
                                    (SELECT
                                          COUNT(e3.EBELN)
                                    FROM EKKO e3
                                    WHERE
                                          e3.LIFNR = e1.LIFNR
                                          AND e3.MANDT = e1.MANDT
                                          AND YEAR(e3.AEDAT) =
YEAR(e1.AEDAT)
                                          AND MONTH(e3.AEDAT) =
MONTH(e1.AEDAT))
                                          )
;

INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES"(CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D01' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN #RESULT_D1 ON
      #RESULT_D1.ERNAM = EKKO.ERNAM
      AND #RESULT_D1.MANDT = EKKO.MANDT
      AND #RESULT_D1.LIFNR = EKKO.LIFNR
      AND #RESULT_D1.ORDER_YEAR = YEAR(EKKO.AEDAT)
      AND #RESULT_D1.ORDER_MONTH = MONTH(EKKO.AEDAT)
;

--Flag_D02 - Durschnittspreis überstiegen
--Erstelle Liste mit Durschnittspreis der Materialien
drop table #MATERIAL_AVERAGE_D2;
CREATE LOCAL TEMPORARY TABLE #MATERIAL_AVERAGE_D2
(MANDT VARCHAR(20), MATNR VARCHAR(40), AVG_PRICE DOUBLE, PRICE_STDEV
DOUBLE)
;

INSERT INTO #MATERIAL_AVERAGE_D2
SELECT
      EKPO.MANDT AS MANDT,
      EKPO.MATNR AS MATNR,
      ROUND(AVG(EKPO.NETPR),2) AS AVG_PRICE,
      ROUND(STDDEV(EKPO.NETPR),2) AS PRICE_STDEV
FROM X0_STUDENT_001.EKPO
WHERE LENGTH(LTRIM(EKPO.MATNR)) > 0
GROUP BY EKPO.MANDT, EKPO.MATNR
HAVING ROUND(STDDEV(EKPO.NETPR),2) > 0.00
```

```
;

--Suche Bestellungen bei denen der Materialpreis weit vom
--Durchschnitt abweicht
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D02' AS FlagId
FROM X0_STUDENT_001.EKPO
JOIN #MATERIAL_AVERAGE_D2 ON
      #MATERIAL_AVERAGE_D2.MATNR = EKPO.MATNR
      AND #MATERIAL_AVERAGE_D2.MANDT = EKPO.MANDT
WHERE
      --Sehr einfach Variante
      --EKPO_NETPR > (MATERIAL_AVERAGE_D2.AVG_PRICE +
MATERIAL_AVERAGE_D2.PRICE_STDEV)
      --Z-Wert
      ((EKPO.NETPR-
#MATERIAL_AVERAGE_D2.AVG_PRICE)/#MATERIAL_AVERAGE_D2.PRICE_STDEV) > 4
;

--Flag_D03 - steigende Ausgaben
--Erstelle Liste der Monatlichen Bestellsummen
drop table #YEARLY_ORDERS_D3;
CREATE LOCAL TEMPORARY TABLE #YEARLY_ORDERS_D3
(MANDT VARCHAR(20), ORDER_YEAR INT, ORDER_MONTH INT, SUM_NETWR DOUBLE)
;

INSERT INTO #YEARLY_ORDERS_D3
SELECT
      EKKO.MANDT,
      YEAR(EKKO.AEDAT),
      MONTH(EKKO.AEDAT),
      ROUND(SUM(EKPO.NETWR),2)
FROM EKKO
JOIN X0_STUDENT_001.EKPO  on
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE
      EKPO.NETWR > 0
GROUP BY EKKO.MANDT, YEAR(EKKO.AEDAT),MONTH(EKKO.AEDAT)
--ORDER BY YEAR(EKKO_AEDAT)
;

--Erstelle Liste mit der Monatlichen Bestellsummen bei einem Lieferant
drop table #ORDER_VALUE_VENDORS_D3;
CREATE LOCAL TEMPORARY TABLE #ORDER_VALUE_VENDORS_D3
(MANDT VARCHAR(20), LIFNR VARCHAR(30), ORDER_YEAR INT, ORDER_MONTH INT,
SUM_NETWR DOUBLE)
;

INSERT INTO #ORDER_VALUE_VENDORS_D3
SELECT
      EKKO.MANDT,
      EKKO.LIFNR,
      YEAR(EKKO.AEDAT),
      MONTH(EKKO.AEDAT),
      SUM(EKPO.NETWR)
FROM EKKO
JOIN X0_STUDENT_001.EKPO on
```

```
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE LENGTH(LTRIM(EKKO.LIFNR)) > 0
GROUP BY EKKO.MANDT, EKKO.LIFNR, YEAR(EKKO.AEDAT), MONTH(EKKO.AEDAT)
HAVING SUM(EKPO.NETWR) > 0
--ORDER BY EKKO_LIFNR, YEAR(EKKO_AEDAT)
;

--Vergleiche die beiden Bestellsummen
drop table #SUSPICOUS_ORDERS_D3;
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_ORDERS_D3
(MANDT VARCHAR(20), LIFNR VARCHAR(30), ORDER_YEAR INT, ORDER_MONTH INT)
;

INSERT INTO #SUSPICOUS_ORDERS_D3
SELECT
      o1.MANDT,
      o1.LIFNR,
      o1.ORDER_YEAR,
      o1.ORDER_MONTH
FROM #YEARLY_ORDERS_D3 y1
JOIN #ORDER_VALUE_VENDORS_D3 o1 ON
      o1.ORDER_YEAR = y1.ORDER_YEAR
      AND o1.ORDER_MONTH = y1.ORDER_MONTH
      AND o1.MANDT = y1.MANDT
WHERE EXISTS
      (SELECT LIFNR
      FROM #YEARLY_ORDERS_D3 y2
      JOIN #ORDER_VALUE_VENDORS_D3 o2 ON
            o2.ORDER_YEAR = y2.ORDER_YEAR
            AND o2.ORDER_MONTH = y2.ORDER_MONTH
            AND o2.MANDT = y2.MANDT
      WHERE
            y2.ORDER_YEAR = YEAR(ADD_MONTHS(TO_DATE(y1.ORDER_YEAR || '-' ||
y1.ORDER_MONTH || '-01', 'YYYY-MM-DD'),-1))
            AND y2.ORDER_MONTH = MONTH(ADD_MONTHS(TO_DATE(y1.ORDER_YEAR ||
'-' || y1.ORDER_MONTH || '-01', 'YYYY-MM-DD'),-1))
            AND o2.LIFNR = o1.LIFNR
            AND o2.MANDT = o1.MANDT
            AND
                  --Steigt der Anteil eines Lieferanten an den
Bestellsummen rasant an
                  (o1.SUM_NETWR/y1.SUM_NETWR) >
15*(o2.SUM_NETWR/y2.SUM_NETWR)
      )
;

INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D03' AS FlagId
FROM #SUSPICOUS_ORDERS_D3, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.LIFNR = #SUSPICOUS_ORDERS_D3.LIFNR
      AND YEAR(EKKO.AEDAT) = #SUSPICOUS_ORDERS_D3.ORDER_YEAR
      AND MONTH(EKKO.AEDAT) = #SUSPICOUS_ORDERS_D3.ORDER_MONTH
      AND EKKO.MANDT = #SUSPICOUS_ORDERS_D3.MANDT
```

```
;

--FLAG_D04 - rasant steigende Einkäufe bei Lieferant
--Erstelle Liste der Bestellsummen bei einem Lieferant
drop table #ORDER_VALUE_VENDORS_D4 ;
CREATE LOCAL TEMPORARY TABLE #ORDER_VALUE_VENDORS_D4
(MANDT VARCHAR(20), LIFNR VARCHAR(30), ORDER_YEAR INT, ORDER_MONTH INT,
SUM_NETWR DOUBLE)
;

INSERT INTO #ORDER_VALUE_VENDORS_D4
SELECT
      EKKO.MANDT,
      EKKO.LIFNR,
      YEAR(EKKO.AEDAT) AS ORDER_YEAR,
      MONTH(EKKO.AEDAT) AS ORDSER_MONTH,
      SUM(EKPO.NETWR) AS SUM_NETWR
FROM EKKO
JOIN X0_STUDENT_001.EKPO on
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE LENGTH(LTRIM(EKKO.LIFNR)) > 0
GROUP BY EKKO.MANDT, EKKO.LIFNR, YEAR(EKKO.AEDAT), MONTH(EKKO.AEDAT)
HAVING SUM(EKPO.NETWR) > 0
;

--Suche nach plötzlich signifikant Ansteigenden Bestellsummen
drop table #SUSPICIOUS_ORDERS_D4 ;
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDERS_D4
(MANDT VARCHAR(20), LIFNR VARCHAR(30), ORDER_YEAR INT, ORDER_MONTH INT)
;

INSERT INTO #SUSPICIOUS_ORDERS_D4
SELECT
      MANDT,
      LIFNR,
      ORDER_YEAR,
      ORDER_MONTH
FROM
      #ORDER_VALUE_VENDORS_D4 o1
WHERE EXISTS
      (SELECT o2.LIFNR
      FROM #ORDER_VALUE_VENDORS_D4 o2
      WHERE
            o2.LIFNR = o1.LIFNR
            AND o2.MANDT = o1.MANDT
            AND o2.ORDER_YEAR = YEAR(ADD_MONTHS(TO_DATE(o1.ORDER_YEAR || '-
' ||o1.ORDER_MONTH || '-01', 'YYYY-MM-DD'),-1))
            AND o2.ORDER_MONTH = MONTH(ADD_MONTHS(TO_DATE(o1.ORDER_YEAR ||
'-' ||o1.ORDER_MONTH || '-01', 'YYYY-MM-DD'),-1))
            AND o1.SUM_NETWR > 4*o2.SUM_NETWR
      )
;

INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D04' AS FlagId
FROM #SUSPICIOUS_ORDERS_D4, EKKO
JOIN X0_STUDENT_001.EKPO ON
```

```
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.LIFNR = #SUSPICIOUS_ORDERS_D4.LIFNR
      AND EKKO.MANDT = #SUSPICIOUS_ORDERS_D4.MANDT
      AND YEAR(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_D4.ORDER_YEAR
      AND MONTH(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_D4.ORDER_MONTH
;

--FLAG_D05 - Langsame Lieferung
--Erstellt Liste der Durchschnittlichen Lieferzeit pro Produkt
Drop TABLE #AVG_DELIVERY_TIME_D5 ;
CREATE LOCAL TEMPORARY TABLE #AVG_DELIVERY_TIME_D5
(MANDT VARCHAR(20), MATNR VARCHAR(30), AVG_DELIVERY_TIME DOUBLE,
STDEV_DELIVERY_TIME DOUBLE)
;

INSERT INTO #AVG_DELIVERY_TIME_D5
SELECT EKKO.MANDT, EKPO.MATNR, AVG(DAYS_BETWEEN(EKKO.AEDAT,EKBE.CPUDT)),
ROUND(STDDEV(DAYS_BETWEEN(EKKO.AEDAT,EKBE.CPUDT)),0)
      FROM X0_STUDENT_001.EKPO
      JOIN X0_STUDENT_001.EKBE ON
            EKBE.EBELN = EKPO.EBELN
            AND EKBE.EBELP = EKPO.EBELP
            AND EKBE.MANDT = EKPO.MANDT
      JOIN EKKO ON
            EKKO.EBELN = EKPO.EBELN
            AND EKKO.MANDT = EKPO.MANDT
      WHERE EKBE.VGABE = '1' AND EKBE.SHKZG = 'S'
      AND LENGTH(LTRIM(EKPO.MATNR)) > 0
      GROUP BY EKKO.MANDT, EKPO.MATNR
      HAVING ROUND(STDDEV(DAYS_BETWEEN(EKKO.AEDAT,EKBE.CPUDT)),0) > 0
;

--Suche Bestellung bei der die Lieferzeit weit über dem
--Durchschnitt liegen
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D05' AS FlagId
FROM X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
JOIN X0_STUDENT_001.EKBE ON
      EKBE.EBELN = EKPO.EBELN
      AND EKBE.EBELP = EKPO.EBELP
      AND EKBE.MANDT = EKPO.MANDT
JOIN #AVG_DELIVERY_TIME_D5 ON
      #AVG_DELIVERY_TIME_D5.MATNR = EKPO.MATNR
      AND #AVG_DELIVERY_TIME_D5.MANDT = EKPO.MANDT
WHERE
      EKBE.VGABE = '1'
      AND EKBE.SHKZG = 'S'
      --Sehr einfach Variante
      --AND DATEDIFF(day,EKKO_AEDAT,EKBE_CPUDT) > AVG_DELIVERY_TIME +
STDEV_DELIVERY_TIME
      AND ((DAYS_BETWEEN(EKKO.AEDAT,EKBE.CPUDT)-
#AVG_DELIVERY_TIME_D5.AVG_DELIVERY_TIME
)/#AVG_DELIVERY_TIME_D5.STDEV_DELIVERY_TIME) > 4
```

```
;

--FLAG_D06 - Teilkäufe
--Suche Bestellungen von einem Tag, dem gleichen Mitarbeiter
--dem gleichen Material und Lieferanten
--werden diese Aufsummiert übersteigt die Gesamtsummt
--eine Freigabegrenze
drop table #SUSPICOUS_ORDERS_D6;
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_ORDERS_D6
(MANDT VARCHAR(20), ERNAM VARCHAR(30), AEDAT DATE, MATNR VARCHAR(30), LIFNR
VARCHAR(30), ORDER_VOLUME DOUBLE, ORDER_COUNT INT)
;

INSERT INTO #SUSPICOUS_ORDERS_D6
SELECT
      EKKO.MANDT,
      EKKO.ERNAM,
      EKKO.AEDAT,
      EKPO.MATNR,
      EKKO.LIFNR,
      SUM(EKPO.NETWR) AS "Order Volume",
      COUNT(EKKO.EBELN) AS "Count"
FROM X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE
      LENGTH(EKKO.LIFNR) > 0
      AND LENGTH(EKKO.FRGSX) = 0
      AND LENGTH(EKPO.MATNR) > 0
GROUP BY
      EKKO.MANDT, EKKO.ERNAM, EKPO.MATNR, EKKO.AEDAT, EKKO.LIFNR
HAVING
      COUNT(EKKO.EBELN) > 2
      AND SUM(EKPO.NETWR) > 50000.00
--ORDER BY
      --EKKO_ERNAM, EKKO_AEDAT, EKKO_LIFNR
;

INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D06' AS FlagId
FROM #SUSPICOUS_ORDERS_D6, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.ERNAM = #SUSPICOUS_ORDERS_D6.ERNAM
      AND EKKO.AEDAT = #SUSPICOUS_ORDERS_D6.AEDAT
      AND EKPO.MATNR = #SUSPICOUS_ORDERS_D6.MATNR
      AND EKKO.LIFNR = #SUSPICOUS_ORDERS_D6.LIFNR
      AND EKKO.MANDT = #SUSPICOUS_ORDERS_D6.MANDT
;

--FLAG_D07 - Runde gleiche Beträge
--Erstelle Liste mit Lieferanten, Mitarbeiter, Material Kombination
--die runde Beträge haben und oft den gleichen Betrag
drop table  #SAME_AVG_VOLUME_D7;
CREATE LOCAL TEMPORARY TABLE #SAME_AVG_VOLUME_D7
```

```
(MANDT VARCHAR(20), LIFNR VARCHAR(30), MATNR VARCHAR(30), ERNAM
VARCHAR(40))
;

INSERT INTO #SAME_AVG_VOLUME_D7
SELECT
      EKKO.MANDT,
      EKKO.LIFNR,
      EKPO.MATNR,
      EKKO.ERNAM
FROM X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE
      EKPO.NETWR > 0
      AND LENGTH(EKKO.LIFNR) > 0
      AND LENGTH(EKPO.MATNR) > 0
      AND
            --Zähle Anzahl wie oft ein runder Betrag bestellt wurde
            (SELECT
                  COUNT(p2.EBELN)
            FROM X0_STUDENT_001.EKPO p2
            JOIN EKKO e2 ON
                  e2.EBELN = p2.EBELN
                  AND e2.MANDT = p2.MANDT
            WHERE
                  EKKO.LIFNR = e2.LIFNR
                  AND EKKO.ERNAM = e2.ERNAM
                  --Erweiterung auf Material
                  AND EKPO.MATNR = p2.MATNR
                  AND EKPO.MANDT = p2.MANDT
                  --Betrag ist rund wenn gleich ob ab- oder aufgerundet
                  and FLOOR(p2.NETWR) <> CEILING(p2.NETWR)) < 10
GROUP BY EKKO.MANDT, EKKO.LIFNR, EKPO.MATNR, EKKO.ERNAM
HAVING
      STDDEV(EKPO.NETWR) < 5
      and COUNT(EKKO.EBELN) > 1
;

INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D07' AS FlagId
FROM #SAME_AVG_VOLUME_D7, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.LIFNR = #SAME_AVG_VOLUME_D7.LIFNR
      AND EKPO.MATNR = #SAME_AVG_VOLUME_D7.MATNR
      AND EKPO.MANDT = #SAME_AVG_VOLUME_D7.MANDT
      AND EKKO.ERNAM = #SAME_AVG_VOLUME_D7.ERNAM
;


--FLAG_D08 - steigende Lagerbestände
--Erstelle Liste mit Einkaufsmengen für Produkte pro Monat
drop table #MATERIAL_ORDER_VOLUME_D8;
CREATE LOCAL TEMPORARY TABLE #MATERIAL_ORDER_VOLUME_D8
```

```
(MANDT VARCHAR(20), MATNR VARCHAR(30), ERNAM VARCHAR(40), ORDER_YEAR INT,
ORDER_MONTH INT, VOLUME DOUBLE)
;
INSERT INTO #MATERIAL_ORDER_VOLUME_D8
SELECT
      EKKO.MANDT AS MANDT,
      EKPO.MATNR AS MATNR,
      EKKO.ERNAM AS ERNAM,
      YEAR(EKKO.AEDAT) AS ORDER_YEAR,
      MONTH(EKKO.AEDAT) AS ORDER_MONTH,
      SUM(EKPO.MENGE) AS VOLUME
FROM X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE
      EKPO.MEINS = 'ST'
      AND LENGTH(LTRIM(EKPO.MATNR)) > 0
      AND LENGTH(LTRIM(EKKO.ERNAM)) > 0
GROUP BY
      EKKO.MANDT,
      EKPO.MATNR,
      EKKO.ERNAM,
      YEAR(EKKO.AEDAT),
      MONTH(EKKO.AEDAT)
HAVING SUM(EKPO.MENGE) > 0
--ORDER BY EKPO_MATNR
;

--Suche Bestellungen bei denen plötzlich einen sehr große
--Menge an Teilen gekauft wurde
drop table #SUSPICIOUS_ORDERS_D8;
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDERS_D8
(MANDT VARCHAR(20), MATNR VARCHAR(30), ERNAM VARCHAR(20), ORDER_YEAR INT,
ORDER_MONTH INT)
;

INSERT INTO #SUSPICIOUS_ORDERS_D8
SELECT
      MANDT,
      MATNR,
      ERNAM,
      ORDER_YEAR,
      ORDER_MONTH
FROM #MATERIAL_ORDER_VOLUME_D8 m1
WHERE EXISTS
            (SELECT m2.VOLUME
            FROM #MATERIAL_ORDER_VOLUME_D8 m2
            WHERE
                  m2.MATNR = m1.MATNR
                  AND m2.MANDT = m1.MANDT
                  AND m2.ERNAM = m1.ERNAM
                  AND m2.ORDER_MONTH =
MONTH(ADD_MONTHS(TO_DATE(m1.ORDER_YEAR || '-' || m1.ORDER_MONTH || '-01',
'YYYY-MM-DD'),-1))
                  AND m2.ORDER_YEAR = YEAR(ADD_MONTHS(TO_DATE(m1.ORDER_YEAR
|| '-' || m1.ORDER_MONTH || '-01', 'YYYY-MM-DD'),-1))
                  AND m1.VOLUME > 3*m2.VOLUME
            )
;
```

```
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D08' AS FlagId
FROM #SUSPICIOUS_ORDERS_D8, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKPO.MATNR = #SUSPICIOUS_ORDERS_D8.MATNR
      AND EKPO.MANDT = #SUSPICIOUS_ORDERS_D8.MANDT
      AND YEAR(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_D8.ORDER_YEAR
      AND MONTH(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_D8.ORDER_MONTH
;


--Flag_D10 - Ungewoehnliche Zeit
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D10' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.TABKEY = EKKO.MANDT || EKKO.EBELN
JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.CHANGENR = CDPOS.CHANGENR
      AND CDHDR.MANDANT = CDPOS.MANDANT
WHERE
      --Eintrag wurde erstellt
      CDPOS.CHNGIND = 'I'
      --Wurde nach 21 Uhr angelegt
      AND (CDHDR.UTIME > '21:00:00.0000000'
      --Wurde vor 5:30 angelegt
      OR CDHDR.UTIME < '05:30:00.0000000')
;

--Flag_D11 - Kein Wareneingangsbeleg
--Suche bezahlte Rechnungen für die kein Wareneingang
--verzeichnet wurde
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_D11' AS FlagId
FROM X0_STUDENT_001.RSEG
JOIN X0_STUDENT_001.BKPF ON
      BKPF.AWKEY = concat(RSEG.BELNR, RSEG.GJAHR)
      AND BKPF.MANDT = RSEG.MANDT
JOIN X0_STUDENT_001.BSAK ON
      BKPF.BELNR = BSAK.BELNR
      AND BKPF.MANDT = BSAK.MANDT
      AND BKPF.GJAHR = BSAK.GJAHR
      AND BKPF.BUKRS = BSAK.BUKRS
WHERE       --Schließe Dienstleistungen aus, da hier nicht zwingend ein
Wareneingang
      --verzeichnet wird.
      RSEG.MEINS <> 'LE'
```

```
AND NOT EXISTS
      (SELECT EKBE.EBELN
      FROM X0_STUDENT_001.EKBE
      WHERE
            EKBE.VGABE = '1'
            AND EKBE.SHKZG = 'S'
            AND EKBE.EBELN = RSEG.EBELN
            AND EKBE.EBELP = RSEG.EBELP
            AND EKBE.MANDT = RSEG.MANDT)
;

--Flag_D12 - Lieferant als Käufer
--Suche Lieferanten die auch als Käufer aufgetreten sind
 --CREATE LOCAL TEMPORARY TABLE #VENDOR_CUSTOMER_D12
 --(MANDT VARCHAR(20), LIFNR VARCHAR(30))
 --;

 --INSERT INTO #VENDOR_CUSTOMER_D12
 --SELECT
--     LFA1.MANDT,
--     LFA1.LIFNR
-- FROM LFA1
-- WHERE
--     LENGTH(LTRIM(LFA1.ORT01)) > 0
--     AND LENGTH(LTRIM(LFA1.PSTLZ)) > 0
--     AND LENGTH(LTRIM(LFA1.STRAS)) > 0
-- AND EXISTS
--     (SELECT
--           KNA1.KUNNR
--     FROM KNA1
--     WHERE
--           KNA1.ORT01 = LFA1.ORT01
--           AND KNA1.PSTLZ = LFA1.PSTLZ
--           AND KNA1.STRAS = LFA1.STRAS
--           AND LENGTH(LTRIM(KNA1.ORT1)) > 0
--           AND LENGTH(LTRIM(KNA1.PSTLZ)) > 0
--           AND LENGTH(LTRIM(KNA1.STRAS)) > 0
--           AND KNA1.MANDT = LFA1.MANDT
--     )
 --;

-- INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
-- SELECT
      -- DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      -- 'Flag_D12' AS FlagId
-- FROM #VENDOR_CUSTOMER_D12, EKPO
-- JOIN EKKO ON
      -- EKKO.EBELN = EKPO.EBELN
      -- AND EKKO.MANDT = EKPO.MANDT
-- JOIN #VENDOR_CUSTOMER_D12 ON
      -- #VENDOR_CUSTOMER_D12.MANDT = EKKO.MANDT
      -- AND #VENDOR_CUSTOMER_D12.LIFNR = EKKO.LIFNR
-- GROUP BY
      -- EKKO.EBELN,
      -- EKPO.MANDT,
      -- EKPO.EBELN,
      -- EKPO.EBELP
-- --Optional: Bestellung ist unter einem gewissen Schwellenwert
-- HAVING
      -- SUM(EKPO.NETWR) < 5000.00
```

```
-- ;

--Fag_D13 - schnelle Zahlung
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_D13' AS FlagId
FROM X0_STUDENT_001.RSEG
JOIN X0_STUDENT_001.RBKP ON
      RBKP.BELNR = RSEG.BELNR
      AND RBKP.MANDT = RSEG.MANDT
      AND RBKP.GJAHR = RSEG.GJAHR
JOIN X0_STUDENT_001.BKPF ON
      BKPF.AWKEY = concat(RSEG.BELNR, RSEG.GJAHR)
      AND BKPF.MANDT = RSEG.MANDT
JOIN X0_STUDENT_001.BSAK ON
      BSAK.BELNR = BKPF.BELNR
      AND BSAK.BUKRS = BKPF.BUKRS
      AND BSAK.MANDT =  BKPF.MANDT
      AND BSAK.GJAHR = BKPF.GJAHR
WHERE
      --Zahlungsziel für ersten Skonto angegeben
      RBKP.ZBD1T > 0
      --Ausgleich der Rechnung zwischen erfassung der Rechnung und der
hälfte
      --der Skontozeit
      AND BSAK.AUGDT between RBKP.BLDAT and
ADD_DAYS(RBKP.BLDAT,(RBKP.ZBD1T/2))
;

--Flag_D14 - Signifikant hoher Einkauf
--Kurzliste der Bestellungen mit Gesamtsumme jeder Bestellung
drop table #LIST14;
CREATE LOCAL TEMPORARY TABLE #LIST14
(MANDT VARCHAR(30), LIFNR VARCHAR(30), AEDAT DATE, EBELN VARCHAR(30),
NETSUM DOUBLE)
;

INSERT INTO #LIST14
SELECT
      EKKO.MANDT,
      EKKO.LIFNR,
      EKKO.AEDAT,
      EKKO.EBELN,
      SUM(EKPO.NETWR)
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE LENGTH(LTRIM(EKKO.LIFNR)) > 0
GROUP BY EKKO.MANDT, EKKO.LIFNR, EKKO.AEDAT, EKKO.EBELN
HAVING SUM(EKPO.NETWR) > 0
--ORDER BY EKKO_LIFNR, EKKO_AEDAT
;

Drop TABLE #SUSPICOUS_ORDERS_D14 ;
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_ORDERS_D14
(MANDT VARCHAR(30), EBELN VARCHAR(30))
;
```

```
INSERT INTO #SUSPICOUS_ORDERS_D14
SELECT
      MANDT,
      EBELN
FROM #LIST14 l1
WHERE EXISTS
      --Bei der es eine vorhergehende Bestellung gibt
      --deren Wert signifikant kleiner ist
      (SELECT l2.EBELN
      FROM #LIST14 l2
      WHERE
            l2.EBELN < l1.EBELN
            AND l2.LIFNR = l1.LIFNR
            AND l2.MANDT = l1.MANDT
            AND l2.NETSUM*3 < l1.NETSUM
            --Und es keine Bestellung dazwischen gibt
            AND NOT EXISTS
                  (SELECT l3.EBELN
                  FROM #LIST14 l3
                  WHERE
                        l2.LIFNR = l3.LIFNR
                        AND l2.MANDT = l3.MANDT
                        AND l3.EBELN < l1.EBELN
                        AND l3.EBELN > l2.EBELN)
      )
;


INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D14' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN #SUSPICOUS_ORDERS_D14 ON
      #SUSPICOUS_ORDERS_D14.MANDT = EKKO.MANDT
      AND #SUSPICOUS_ORDERS_D14.EBELN = EKKO.EBELN
;

--Flag_D15 - Übersteigt Durschnitt
--Erstelle Liste mit den Durschnittlichen Bestellsummen pro Lieferant
DROP TABLE #VENDOR_AVERGAE_D15 ;
CREATE LOCAL TEMPORARY TABLE #VENDOR_AVERGAE_D15
(MANDT VARCHAR(20), LIFNR VARCHAR(30), AVERAGE_VOLUME DOUBLE, STD_VARIANCE
DOUBLE)
;

INSERT INTO #VENDOR_AVERGAE_D15
SELECT
      EKKO.MANDT,
      EKKO.LIFNR,
      ROUND(AVG(EKPO.NETWR),2),
      ROUND(STDDEV(EKPO.NETWR),2)
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE LENGTH(EKKO.LIFNR) > 0
```

```
GROUP BY EKKO.MANDT, EKKO.LIFNR
HAVING ROUND(STDDEV(EKPO.NETWR),2) > 0
;

INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D15' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN #VENDOR_AVERGAE_D15 ON
      #VENDOR_AVERGAE_D15.LIFNR = EKKO.LIFNR
      AND #VENDOR_AVERGAE_D15.MANDT = EKKO.MANDT
GROUP BY
      EKPO.MANDT,
      EKPO.EBELN,
      EKPO.EBELP,
      EKKO.LIFNR,
      EKPO.NETWR,
      #VENDOR_AVERGAE_D15.AVERAGE_VOLUME,
      #VENDOR_AVERGAE_D15.STD_VARIANCE
HAVING
      --Sehr einfache Variante
      --EKPO_NETWR > (VENDOR_AVERGAE_B30.AVERAGE_VOLUME +
VENDOR_AVERGAE_B30.STD_VARIANCE)
      --Z-Wert
      ((EKPO.NETWR-
#VENDOR_AVERGAE_D15.AVERAGE_VOLUME)/#VENDOR_AVERGAE_D15.STD_VARIANCE) > 4
;

--Flag_D16 - Wenige Lieferanten
--Erstelle Liste wei viele Lieferanten jeder Mitarbeiter für
--ein Material benutzt
DROP TABLE #SUSPICOUS_MATERIALS ;
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_MATERIALS
(MANDT VARCHAR(20), ERNAM VARCHAR(30), MATNR VARCHAR(30), LIF_COUNT INT)
;

INSERT INTO #SUSPICOUS_MATERIALS
SELECT
      EKKO.MANDT,
      EKKO.ERNAM,
      EKPO.MATNR,
      COUNT(DISTINCT EKKO.LIFNR)
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      LENGTH(LTRIM(EKKO.ERNAM)) > 0
      AND LENGTH(LTRIM(EKPO.MATNR)) > 0
GROUP BY
      EKKO.MANDT,
      EKKO.ERNAM,
      EKPO.MATNR
HAVING
      COUNT(DISTINCT EKKO.LIFNR) < 2
;
```

```
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D16' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN #SUSPICOUS_MATERIALS ON
      #SUSPICOUS_MATERIALS.MATNR = EKPO.MATNR
      AND #SUSPICOUS_MATERIALS.ERNAM = EKKO.ERNAM
      AND #SUSPICOUS_MATERIALS.MANDT = EKKO.MANDT
;

--Flag_D17 - Übersteit Gesamtdurchschnitt
--Generiere Liste mit Bestellsummen für alle Bestellungen
DROP TABLE #ORDER_SUMS_D17 ;
CREATE LOCAL TEMPORARY TABLE #ORDER_SUMS_D17
(MANDT VARCHAR(20), EBELN VARCHAR(30), NETWR DOUBLE)
;

INSERT INTO #ORDER_SUMS_D17
SELECT
      EKPO.MANDT AS MANDT,
      EKPO.EBELN AS EBELN,
      SUM(EKPO.NETWR) AS NETWR
FROM X0_STUDENT_001.EKPO
GROUP BY EKPO.MANDT, EKPO.EBELN
HAVING SUM(EKPO.NETWR) > 0
;

--Berechne den Durchschnitt alle Bestellungen
DROP TABLE #AVG_PURCHASE_D17 ;
CREATE LOCAL TEMPORARY TABLE #AVG_PURCHASE_D17
(MANDT VARCHAR(20), VOLUME DOUBLE, STD_VARIANCE DOUBLE)
;

INSERT INTO #AVG_PURCHASE_D17
SELECT
      MANDT,
      ROUND(AVG(NETWR),2),
      ROUND(STDDEV(NETWR),2)
FROM #ORDER_SUMS_D17
GROUP BY MANDT
HAVING ROUND(STDDEV(NETWR),2) > 0
;

INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D17' AS FlagId
FROM X0_STUDENT_001.EKPO
JOIN #AVG_PURCHASE_D17 ON
      #AVG_PURCHASE_D17.MANDT = EKPO.MANDT
GROUP BY
      EKPO.MANDT, EKPO.EBELN,EKPO.EBELP, #AVG_PURCHASE_D17.VOLUME,
#AVG_PURCHASE_D17.STD_VARIANCE
HAVING
      --Sehr einfache Variante
```

```
      --SUM(EKPO_NETWR) > AVG_PRUCHASE_D17.VOLUME +
AVG_PRUCHASE_D17.STD_VARIANCE
      --Z-Verteiling
      ((SUM(EKPO.NETWR)-
#AVG_PURCHASE_D17.VOLUME)/#AVG_PURCHASE_D17.STD_VARIANCE) > 3
;

--Flag_D18 - Rechnung außerhalb von normalen Arbeitszeiten erfasst
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES"(CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_D18' AS FlagId
FROM X0_STUDENT_001.RBKP r1
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.GJAHR =  r1.GJAHR
      AND RSEG.MANDT = r1.MANDT
WHERE
      (r1.CPUTM > '20:00:00.0000000')
;


--Flag_D19 - Manuelle Zahlungen
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES"(CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_D19' AS FlagId
FROM X0_STUDENT_001.RBKP r1
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.GJAHR =  r1.GJAHR
      AND RSEG.MANDT = r1.MANDT
WHERE
      (r1.CPUTM > '20:00:00.0000000')
;


--Flag_D20 - Lieferantenwechsel

      INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT e1.MANDT || e1.EBELN || EKPO.EBELP AS CaseId,
      'Flag_D20' AS FlagId
FROM EKKO e1
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = e1.EBELN
      AND EKPO.MANDT = e1.MANDT
JOIN X0_STUDENT_001.LFA1 ON
      LFA1.LIFNR = e1.LIFNR
      AND LFA1.MANDT = e1.MANDT
WHERE
      LENGTH(LTRIM(e1.LIFNR)) > 0
--Suche Bestellungen bei denen keine weitere Bestellung exisitert die
AND NOT EXISTS
      (SELECT
            e2.EBELN
      FROM EKKO e2
      WHERE
            --an den gleichen Lieferanten geht
            e1.LIFNR = e2.LIFNR
```

```
            AND e1.EBELN <> e2.EBELN
            AND e1.MANDT = e2.MANDT
            --die Bestellung nicht innerhalb der gewählten Zeit aufgegebn
wurde
            AND e2.AEDAT between ADD_YEARS(e1.AEDAT,-1) and e1.AEDAT)
--Lieferant wurde bereits vor dem gewählten Zeitraum erstellt
AND LFA1.ERDAT < ADD_YEARS(e1.AEDAT,-1)
;


--Flag_D21 - Username ist nicht in der Einkaufsabteilung
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
       DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
       'Flag_D21' AS FlagId
 FROM EKKO
 JOIN GBI_003.EKPO ON
       EKPO.EBELN = EKKO.EBELN
       AND EKPO.MANDT = EKKO.MANDT
 WHERE
       --Der benutzte Username ist nicht in der Einkaufsabteilung
       EKKO.ERNAM in
             (
             SELECT LFA1.LIFNR
             FROM GBI_003.LFA1
             INNER JOIN GBI_003.USR03 on
                   LFA1.STRAS = USR03.STRAS
                   AND LFA1.PSTLZ = USR03.PSTLZ
                   AND LFA1.MANDT = USR03.MANDT
             WHERE USR03.ABTLG <> 'Einkf'
             )
 ;

--Scheme Konfigration
--Beispiel
--Um ein eigenes Schema zu Konfigurieren müssen die FlagId
--der gewünschten Flags eingetragen werden
--Wird statt dem Intersect ein Union benutzt, werde alle Transaktionen
--markiert die mindestens einen der aufgeführten Flags besitzen
--im Fall von Intersect müssen alle Flags vorhanden sein


UPDATE _CEL_FLAGED_CASES
SET SCHEMEID = 'D1-Overpay'
WHERE CASEID IN
(


SELECT
      FC2.CASEID
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_D18'

INTERSECT

SELECT
      FC2.CASEID
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_D19'
```

```
)
AND FLAGID IN ('Flag_D18','Flag_D19');
```

Angebotsmanipulation

```
--Red Flag Processing
--Collection of Red Flag Scripts for Bid Rigging


--Flag_E01 - Letztes Angebot
--Der Flag wird in der aktuellen Form nicht von der HANA unterstüzt,
--da eine gezielte Abfrage des letzten Gebots mit der aktuell
--gewählten Strategie nicht möglich ist.

--Flag_E02 - Lieferantenersteller ist Genehmiger
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      END) AS CaseId,
      'Flag_E02' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.LFA1 ON
      LFA1.LIFNR = EKKO.LIFNR
      AND LFA1.MANDT = EKKO.MANDT
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = EKPO.MANDT
      AND e2.ANFNR = EKPO.EBELN
WHERE
      --Lieferant wurd von Anfrageersteller angelegt
      EKKO.ERNAM = LFA1.ERNAM
      AND EKKO.BSTYP = 'A'
;

--Flag_E03 - Angebotsänderung

--Suche nach Anfragen bei denen der Preis mehr als einmal
--geändert wird und der Preis danach niedriger ist
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      END) AS CaseId,
      'Flag_E03' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKKO.EBELN =  EKPO.EBELN
```

```
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = EKPO.MANDT
      AND e2.ANFNR = EKPO.EBELN
WHERE
      EKKO.BSTYP = 'A'
      AND EXISTS
            (SELECT CDPOS.CHANGENR
            FROM X0_STUDENT_001.CDPOS
            WHERE
                  CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
                  AND CDPOS.FNAME = 'NETPR'
                  AND CDPOS.VALUE_NEW < CDPOS.VALUE_OLD
            )
;

--Flag_E04 - Kurze Angebotsphase
--Suche alle Anfragen bei denen die Angebotsphase
--kürzer ist als die gewählte Grenze
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      END) AS CaseId,
      'Flag_E04' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = EKPO.MANDT
      AND e2.ANFNR = EKPO.EBELN
WHERE
      EKKO.BSTYP = 'A'
      AND EKKO.ANGDT between EKKO.AEDAT and ADD_DAYS(EKKO.AEDAT,3)
;

--Flag_E05 - Wenige Angebote
--Suche nach Anfragen bei denen nur sehr wenige Teilnehmer
--ausgewählt wurden
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      END) AS CaseId,
      'Flag_E05' AS FlagId
FROM EKKO e1
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = e1.EBELN
      AND EKPO.MANDT = e1.MANDT
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = EKPO.MANDT
      AND e2.ANFNR = EKPO.EBELN
WHERE
      LENGTH(LTRIM(e1.SUBMI)) > 0
```

```
      AND (SELECT COUNT(e2.EBELN)
            FROM EKKO e2
            WHERE
                  LENGTH(LTRIM(e2.SUBMI)) > 0
                  AND e1.SUBMI = e2.SUBMI
                  GROUP BY e2.SUBMI) < 3
;

--Flag_E06 - Geteilte Ausschreibung
--Erstelle List von Mitarbeiter
--die für ihre Anfragen die gleichen Lieferanten auf
--verschiedene Anfragen aufteilt
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_BIDS_E6
(MANDT VARCHAR(20), ERNAM VARCHAR(30), SUB_YEAR INT, SUB_MONTH INT)
;

INSERT INTO #SUSPICOUS_BIDS_E6
SELECT
      EKKO.MANDT,
      EKKO.ERNAM,
      YEAR(EKKO.AEDAT) AS "Year",
      MONTH(EKKO.AEDAT) AS "Month"
FROM EKKO
WHERE
      LENGTH(LTRIM(EKKO.SUBMI)) > 0
GROUP BY
      EKKO.MANDT,
      EKKO.ERNAM,
      YEAR(EKKO.AEDAT),
      MONTH(EKKO.AEDAT)
HAVING
      COUNT(DISTINCT EKKO.LIFNR) <= COUNT(EKKO.EBELN)
;

--Suche alsauffällig markierte Anfragen
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      END) AS CaseId,
      'Flag_E06' AS FlagId
FROM #SUSPICOUS_BIDS_E6, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = EKPO.MANDT
      AND e2.ANFNR = EKPO.EBELN
WHERE
      EKKO.ERNAM = #SUSPICOUS_BIDS_E6.ERNAM
      AND EKKO.MANDT = #SUSPICOUS_BIDS_E6.MANDT
      AND YEAR(EKKO.AEDAT) = #SUSPICOUS_BIDS_E6.SUB_YEAR
      AND MONTH(EKKO.AEDAT) = #SUSPICOUS_BIDS_E6.SUB_MONTH
      AND EKKO.BSTYP = 'A'
;
```

```
--Flag_E08 - Fktionale Anbieter
--Suche Lieferanten die keine Anschrift haben
CREATE LOCAL TEMPORARY TABLE #susp_vendors_E8
(LIFNR VARCHAR(130), NAME1 VARCHAR(140))
;

INSERT INTO #susp_vendors_E8
      SELECT
            LFA1.LIFNR,
            LFA1.NAME1
      FROM X0_STUDENT_001.LFA1
      WHERE
            LENGTH(LTRIM(LFA1.TELF1)) = 0
            or LENGTH(LTRIM(LFA1.ORT01)) = 0
            or LENGTH(LTRIM(LFA1.PSTLZ)) = 0
            or LENGTH(LTRIM(LFA1.STRAS)) = 0
            or LENGTH(LTRIM(LFA1.STCD1)) = 0
;

--Suche Anfragen die mit einem fiktiven Lieferanten
--erstellt wurden
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      END) AS CaseId,
      'Flag_E08' AS FlagId
FROM EKKO e1
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = e1.EBELN
      AND EKPO.MANDT = e1.MANDT
JOIN X0_STUDENT_001.LFA1 ON
      LFA1.LIFNR = e1.LIFNR
      AND LFA1.MANDT = e1.MANDT
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = EKPO.MANDT
      AND e2.ANFNR = EKPO.EBELN
WHERE
      ((LENGTH(LTRIM(e1.SUBMI)) > 0
      AND e1.BSTYP = 'A')
      OR LENGTH(LTRIM(EKPO.ANFNR)) > 0
      )
      and ( EXISTS
                        (SELECT sp.LIFNR
                        FROM #susp_vendors_E8 sp
                        WHERE sp.LIFNR = e1.LIFNR)
            OR EXISTS
                        (SELECT LFA1.LIFNR
                        FROM X0_STUDENT_001.LFA1
                        WHERE
                              LFA1.ERNAM = e1.ERNAM)
                        )
;

--Flag_E09 - Ausreißer
--Erstelle Liste mit allen Durchschnittspreisen
--der Anfragen
```

```
CREATE LOCAL TEMPORARY TABLE #SUBMI_PRICES_E9
(MANDT VARCHAR(10), SUBMI VARCHAR(30), AVG_PRICE DOUBLE, PRICE_STDEV
DOUBLE)
;

INSERT INTO #SUBMI_PRICES_E9
SELECT
      EKKO.MANDT,
      EKKO.SUBMI AS SUBMI,
      ROUND(AVG(EKPO.NETPR), 2) AS AVG_PRICE,
      ROUND(STDDEV(EKPO.NETPR),2) AS PRICE_STDV
FROM X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE EKPO.BSTYP = 'A'
AND
      (EKPO.NETPR > '0'
      OR EKPO.NETPR > '0.00')
GROUP BY EKKO.MANDT, EKKO.SUBMI
HAVING ROUND(STDDEV(EKPO.NETPR),2) > 0
;

INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      END) AS CaseId,
      'Flag_E09' AS FlagId
FROM X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
JOIN #SUBMI_PRICES_E9 ON
      #SUBMI_PRICES_E9.SUBMI = EKKO.SUBMI
      AND #SUBMI_PRICES_E9.MANDT = EKKO.MANDT
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = EKPO.MANDT
      AND e2.ANFNR = EKPO.EBELN
WHERE EKPO.BSTYP = 'A'
AND
      (EKPO.NETPR > '0'
      OR EKPO.NETPR > '0.00')
AND
      --Sehr einfache Variante
      --(EKPO_NETPR > AVG_PRICE + PRICE_STDEV
      --OR EKPO_NETPR < AVG_PRICE - PRICE_STDEV)
      --Z-Wert
      --Suche Ausreise sowohl nach oben als auch unten
      (

            ((EKPO.NETPR-AVG_PRICE)/PRICE_STDEV) > 3
            OR
            ((EKPO.NETPR-AVG_PRICE)/PRICE_STDEV) < -3

      )
;
```

```
-- Flag_E07 Angebote liegen nah beieinander
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      END) AS CaseId,
      'Flag_E07' AS FlagId
FROM X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
JOIN #SUBMI_PRICES_E9 ON
      #SUBMI_PRICES_E9.SUBMI = EKKO.SUBMI
      AND #SUBMI_PRICES_E9.MANDT = EKKO.MANDT
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = EKPO.MANDT
      AND e2.ANFNR = EKPO.EBELN
WHERE EKPO.BSTYP = 'A'
AND
      (EKPO.NETPR > '0'
      OR EKPO.NETPR > '0.00')
AND
      --Suche nach Werten, die sehr nah beieinander liegen
      (
            ((EKPO.NETPR-AVG_PRICE)/PRICE_STDEV) < 1
            AND
            ((EKPO.NETPR-AVG_PRICE)/PRICE_STDEV) > -1
      )
;


--Flag_E10 - Kein Angebotsprozess
--Für eine Bestellung über einem bestimmten Grenzwert
--ab dem eigentlich eine Anfrage gestellt werden müsste
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_BIDS_E10
(MANDT VARCHAR(20), EBELN VARCHAR(30), EBELP VARCHAR(20))
;

INSERT INTO #SUSPICOUS_BIDS_E10
SELECT
      e1.MANDT,
      e1.EBELN,
      p1.EBELP
FROM EKKO e1
JOIN X0_STUDENT_001.EKPO p1 ON
      p1.EBELN = e1.EBELN
      AND p1.MANDT = e1.MANDT
WHERE
      LENGTH(LTRIM(p1.ANFNR)) = 0
      --exisitert keine Anfrage
      --für das gleiche Material
      --bei dem gewählten Lieferant
      --innerhalb des leten Monats
      AND NOT EXISTS
            (SELECT
```

```
                e2.EBELN
            FROM EKKO e2
            JOIN X0_STUDENT_001.EKPO p2 ON
                p2.MANDT = e2.MANDT
                AND p2.EBELN = e2.EBELN
            WHERE
                e2.MANDT = e1.MANDT
                AND e2.LIFNR = e1.LIFNR
                AND p2.MATNR = p1.MATNR
                AND e2.BSTYP = 'A'
                AND e2.AEDAT BETWEEN ADD_MONTHS(e1.AEDAT,-1) AND e1.AEDAT
            )
GROUP BY e1.MANDT, e1.EBELN, p1.EBELP
HAVING SUM(p1.NETWR) > 25000
;


INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  E10.MANDT || E10.EBELN || E10.EBELP
      END) AS CaseId,
      'Flag_E10' AS FlagId
FROM #SUSPICOUS_BIDS_E10 E10
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = E10.MANDT
      AND e2.ANFNR = E10.EBELN
;

--Flag_E11 - Limits
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_BIDS_E11
(MANDT VARCHAR(20), EBELN VARCHAR(30), EBELP VARCHAR(20))
;

INSERT INTO #SUSPICOUS_BIDS_E11
SELECT
      EKKO.MANDT,
      EKKO.EBELN,
      EKPO.EBELP
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.BSTYP = 'A'
GROUP BY
      EKKO.MANDT, EKKO.EBELN, EKPO.EBELP
--Geschätzter Bestellwert unterschreitet kanpp eine Grenze
--an der eine weitere Freigabe nötig wäre
HAVING
      SUM(EKPO.NETWR) between (5000.00-10) and (5000.00-0.01)
      OR SUM(EKPO.NETWR) between (50000.00-10) and (50000.00-0.01)
;

INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
```

```
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  E11.MANDT || E11.EBELN || E11.EBELP
      END) AS CaseId,
      'Flag_E11' AS FlagId
FROM #SUSPICOUS_BIDS_E11 E11
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = E11.MANDT
      AND e2.ANFNR = E11.EBELN
;

--Flag_E12 - Favorisierter Lieferant
--Erstelle Liste der gewonnenen Anfragen pro Lieferant
CREATE LOCAL TEMPORARY TABLE #ORDER_NUMBERS_E12
(MANDT VARCHAR(20), LIFNR VARCHAR(30), ORDERS DOUBLE)
;

INSERT INTO #ORDER_NUMBERS_E12
SELECT
      EKKO.MANDT,
      EKKO.LIFNR,
      COUNT(EKKO.EBELN)
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE LENGTH(LTRIM(EKPO.ANFNR)) > 0
GROUP BY EKKO.MANDT, EKKO.LIFNR
;

CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_BIDS_E12
(MANDT VARCHAR(20), EBELN VARCHAR(30), EBELP VARCHAR(20))
;

--Suche nach Bestellungen bei einem Lieferant
--der die meisten Anfragen gewinnt
INSERT INTO #SUSPICOUS_BIDS_E12
SELECT
      EKKO.MANDT,
      EKKO.EBELN,
      EKPO.EBELP
FROM X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
JOIN #ORDER_NUMBERS_E12 ON
      #ORDER_NUMBERS_E12.LIFNR = EKKO.LIFNR
      AND #ORDER_NUMBERS_E12.MANDT = EKKO.MANDT
WHERE
      LENGTH(LTRIM(EKPO.ANFNR)) > 0
GROUP BY
      EKKO.MANDT,
      EKKO.EBELN,
      EKPO.EBELP,
      #ORDER_NUMBERS_E12.ORDERS
HAVING
      #ORDER_NUMBERS_E12.ORDERS > 2*(SELECT
                                          AVG(o2.ORDERS)
```

```
                                                        FROM
#ORDER_NUMBERS_E12 o2)
;

INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  E12.MANDT || E12.EBELN || E12.EBELP
      END) AS CaseId,
      'Flag_E12' AS FlagId
FROM #SUSPICOUS_BIDS_E12 E12
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = E12.MANDT
      AND e2.ANFNR = E12.EBELN
;

--Flag_E13 - Mehrfach Angebote
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      END) AS CaseId,
      'Flag_E13' AS FlagId
FROM EKKO e1
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = e1.EBELN
      AND EKPO.MANDT = e1.MANDT
JOIN X0_STUDENT_001.LFA1 l1 ON
      l1.LIFNR = e1.LIFNR
      AND l1.MANDT = e1.MANDT
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = EKPO.MANDT
      AND e2.ANFNR = EKPO.EBELN
WHERE
      e1.BSTYP = 'A'
      --Es Existiert eine weiter Anfrage
      --die einen anderen Lieferant benutzt
      --der jedoch die gleichen Daten eines bereits benutzten
      --Lieferanten hat
      AND EXISTS
            (SELECT
                  e2.EBELN
            FROM EKKO e2
            JOIN X0_STUDENT_001.LFA1 l2 ON
                  l2.LIFNR = e2.LIFNR
                  AND l2.MANDT = e2.MANDT
            WHERE
                  e2.SUBMI = e1.SUBMI
                  AND e2.LIFNR <> e1.LIFNR
                  AND
                        (
                              (l2.STRAS = l1.STRAS
                              AND l2.PSTLZ = l1.PSTLZ)
                        OR
```

```
                                l2.NAME1 = l1.NAME1)
            )
;
-- Flag_E15
--Suche nach Anfragen bei denen der Preis geändert wird, obwohl eine
Bestellung bereits existiert
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT DISTINCT
      (CASE
            WHEN e2.EBELN IS NOT NULL THEN
                  e2.MANDT || e2.EBELN || e2.EBELP
            ELSE
                  EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
      END) AS CaseId,
      'Flag_E14' AS FlagId
FROM EKKO e1
JOIN X0_STUDENT_001.EKPO ON
      e1.EBELN =  EKPO.EBELN
LEFT JOIN X0_STUDENT_001.EKPO e2 ON
      e2.MANDT = EKPO.MANDT
      AND e2.ANFNR = EKPO.EBELN
WHERE
      e1.BSTYP = 'A' and
      LENGTH(LTRIM(e1.ERNAM)) > 0
      AND EXISTS
            (SELECT CDPOS.CHANGENR
            FROM X0_STUDENT_001.CDPOS
            JOIN X0_STUDENT_001.CDHDR ON
            CDPOS.CHANGENR = CDHDR.CHANGENR
            AND CDPOS.MANDANT = CDHDR.MANDANT
            WHERE
                  CDPOS.TABKEY = EKPO.MANDT || EKPO.EBELN || EKPO.EBELP
                  AND CDPOS.FNAME = 'NETPR'
                  AND CDHDR.UDATE > e1.AEDAT
            )
;


--Scheme Konfigration
--Beispiel
--Um ein eigenes Schema zu Konfigurieren müssen die FlagId
--der gewünschten Flags eingetragen werden
--Wird statt dem Intersect ein Union benutzt, werde alle Transaktionen
--markiert die mindestens einen der aufgeführten Flags besitzen
--im Fall von Intersect müssen alle Flags vorhanden sein

UPDATE _CEL_FLAGED_CASES
SET SCHEMEID = 'E1-Bid Rigging'
WHERE CASEID IN
(

SELECT
      FC2.CASEID
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_E02'

INTERSECT

SELECT
      FC2.CASEID
```

```
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_E08'

)
AND FLAGID IN ('Flag_E02','Flag_E08');
```

Pass Through

```
--FLAG_F01 - steigende Lagerbestände
--Erstelle Liste mit Einkaufsmengen für Produkte pro Monat
drop table #MATERIAL_ORDER_VOLUME_D8;
CREATE LOCAL TEMPORARY TABLE #MATERIAL_ORDER_VOLUME_D8
(MANDT VARCHAR(20), MATNR VARCHAR(30), ERNAM VARCHAR(40), ORDER_YEAR INT,
ORDER_MONTH INT, VOLUME DOUBLE)
;
INSERT INTO #MATERIAL_ORDER_VOLUME_D8
SELECT
      EKKO.MANDT AS MANDT,
      EKPO.MATNR AS MATNR,
      EKKO.ERNAM AS ERNAM,
      YEAR(EKKO.AEDAT) AS ORDER_YEAR,
      MONTH(EKKO.AEDAT) AS ORDER_MONTH,
      SUM(EKPO.MENGE) AS VOLUME
FROM X0_STUDENT_001.EKPO
JOIN EKKO ON
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE
      EKPO.MEINS = 'ST'
      AND LENGTH(LTRIM(EKPO.MATNR)) > 0
      AND LENGTH(LTRIM(EKKO.ERNAM)) > 0
GROUP BY
      EKKO.MANDT,
      EKPO.MATNR,
      EKKO.ERNAM,
      YEAR(EKKO.AEDAT),
      MONTH(EKKO.AEDAT)
HAVING SUM(EKPO.MENGE) > 0
--ORDER BY EKPO_MATNR
;


--Suche Bestellungen bei denen plötzlich einen sehr große
--Menge an Teilen gekauft wurde
drop table #SUSPICIOUS_ORDERS_D8;
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDERS_D8
(MANDT VARCHAR(20), MATNR VARCHAR(30), ERNAM VARCHAR(20), ORDER_YEAR INT,
ORDER_MONTH INT)
;

INSERT INTO #SUSPICIOUS_ORDERS_D8
SELECT
      MANDT,
      MATNR,
      ERNAM,
      ORDER_YEAR,
```

```
      ORDER_MONTH
FROM #MATERIAL_ORDER_VOLUME_D8 m1
WHERE EXISTS
            (SELECT m2.VOLUME
            FROM #MATERIAL_ORDER_VOLUME_D8 m2
            WHERE
                  m2.MATNR = m1.MATNR
                  AND m2.MANDT = m1.MANDT
                  AND m2.ERNAM = m1.ERNAM
                  AND m2.ORDER_MONTH =
MONTH(ADD_MONTHS(TO_DATE(m1.ORDER_YEAR || '-' || m1.ORDER_MONTH || '-01',
'YYYY-MM-DD'),-1))
                  AND m2.ORDER_YEAR = YEAR(ADD_MONTHS(TO_DATE(m1.ORDER_YEAR
|| '-' || m1.ORDER_MONTH || '-01', 'YYYY-MM-DD'),-1))
                  AND m1.VOLUME > 3*m2.VOLUME
            )
;

INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_F01' AS FlagId
FROM #SUSPICIOUS_ORDERS_D8, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKPO.MATNR = #SUSPICIOUS_ORDERS_D8.MATNR
      AND EKPO.MANDT = #SUSPICIOUS_ORDERS_D8.MANDT
      AND YEAR(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_D8.ORDER_YEAR
      AND MONTH(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_D8.ORDER_MONTH
;


--FLAG_F02 - steigende Ausgaben
--Erstelle Liste der Monatlichen Bestellsummen
drop table #YEARLY_ORDERS_D3;
CREATE LOCAL TEMPORARY TABLE #YEARLY_ORDERS_D3
(MANDT VARCHAR(20), ORDER_YEAR INT, ORDER_MONTH INT, SUM_NETWR DOUBLE)
;

INSERT INTO #YEARLY_ORDERS_D3
SELECT
      EKKO.MANDT,
      YEAR(EKKO.AEDAT),
      MONTH(EKKO.AEDAT),
      ROUND(SUM(EKPO.NETWR),2)
FROM EKKO
JOIN X0_STUDENT_001.EKPO  on
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE
      EKPO.NETWR > 0
GROUP BY EKKO.MANDT, YEAR(EKKO.AEDAT),MONTH(EKKO.AEDAT)
--ORDER BY YEAR(EKKO_AEDAT)
;

--Erstelle Liste mit der Monatlichen Bestellsummen bei einem Lieferant
drop table #ORDER_VALUE_VENDORS_D3;
CREATE LOCAL TEMPORARY TABLE #ORDER_VALUE_VENDORS_D3
```

```
(MANDT VARCHAR(20), LIFNR VARCHAR(30), ORDER_YEAR INT, ORDER_MONTH INT,
SUM_NETWR DOUBLE)
;

INSERT INTO #ORDER_VALUE_VENDORS_D3
SELECT
      EKKO.MANDT,
      EKKO.LIFNR,
      YEAR(EKKO.AEDAT),
      MONTH(EKKO.AEDAT),
      SUM(EKPO.NETWR)
FROM EKKO
JOIN X0_STUDENT_001.EKPO on
      EKKO.EBELN = EKPO.EBELN
      AND EKKO.MANDT = EKPO.MANDT
WHERE LENGTH(LTRIM(EKKO.LIFNR)) > 0
GROUP BY EKKO.MANDT, EKKO.LIFNR, YEAR(EKKO.AEDAT), MONTH(EKKO.AEDAT)
HAVING SUM(EKPO.NETWR) > 0
--ORDER BY EKKO_LIFNR, YEAR(EKKO_AEDAT)
;

--Vergleiche die beiden Bestellsummen
drop table #SUSPICOUS_ORDERS_D3;
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_ORDERS_D3
(MANDT VARCHAR(20), LIFNR VARCHAR(30), ORDER_YEAR INT, ORDER_MONTH INT)
;

INSERT INTO #SUSPICOUS_ORDERS_D3
SELECT
      o1.MANDT,
      o1.LIFNR,
      o1.ORDER_YEAR,
      o1.ORDER_MONTH
FROM #YEARLY_ORDERS_D3 y1
JOIN #ORDER_VALUE_VENDORS_D3 o1 ON
      o1.ORDER_YEAR = y1.ORDER_YEAR
      AND o1.ORDER_MONTH = y1.ORDER_MONTH
      AND o1.MANDT = y1.MANDT
WHERE EXISTS
      (SELECT LIFNR
      FROM #YEARLY_ORDERS_D3 y2
      JOIN #ORDER_VALUE_VENDORS_D3 o2 ON
            o2.ORDER_YEAR = y2.ORDER_YEAR
            AND o2.ORDER_MONTH = y2.ORDER_MONTH
            AND o2.MANDT = y2.MANDT
      WHERE
            y2.ORDER_YEAR = YEAR(ADD_MONTHS(TO_DATE(y1.ORDER_YEAR || '-' ||
y1.ORDER_MONTH || '-01', 'YYYY-MM-DD'),-1))
            AND y2.ORDER_MONTH = MONTH(ADD_MONTHS(TO_DATE(y1.ORDER_YEAR ||
'-' || y1.ORDER_MONTH || '-01', 'YYYY-MM-DD'),-1))
            AND o2.LIFNR = o1.LIFNR
            AND o2.MANDT = o1.MANDT
            AND
                  --Steigt der Anteil eines Lieferanten an den
Bestellsummen rasant an
                  (o1.SUM_NETWR/y1.SUM_NETWR) >
15*(o2.SUM_NETWR/y2.SUM_NETWR)
      )
;
```

```
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_F02' AS FlagId
FROM #SUSPICOUS_ORDERS_D3, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.LIFNR = #SUSPICOUS_ORDERS_D3.LIFNR
      AND YEAR(EKKO.AEDAT) = #SUSPICOUS_ORDERS_D3.ORDER_YEAR
      AND MONTH(EKKO.AEDAT) = #SUSPICOUS_ORDERS_D3.ORDER_MONTH
      AND EKKO.MANDT = #SUSPICOUS_ORDERS_D3.MANDT
;



--Flag_F03 - Budgetabweichung
--Generiert Liste aller Nettobestellungen eines Mitarbeiters pro Monat
CREATE LOCAL TEMPORARY TABLE #SPENDING_PER_MOTH_F3
(MANDT VARCHAR(20), ERNAM VARCHAR(30), SPENDING_YEAR INT, SPENDING_MONTH
INT, SPENDING DOUBLE)
;

INSERT INTO #SPENDING_PER_MOTH_F3
SELECT
      EKKO.MANDT,
      EKKO.ERNAM,
      YEAR(EKKO.AEDAT),
      MONTH(EKKO.AEDAT),
      SUM(EKPO.NETWR)
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE LENGTH(LTRIM(EKKO.ERNAM)) > 0
GROUP BY EKKO.MANDT, EKKO.ERNAM, YEAR(EKKO.AEDAT), MONTH(EKKO.AEDAT)
HAVING SUM(EKPO.NETWR) > 0
ORDER BY EKKO.MANDT
;


--Sucht auffällige Transaktionen
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDERS_F3
(MANDT VARCHAR(20), ERNAM VARCHAR(30), SPENDING_YEAR INT, SPENDING_MONTH
INT)
;

INSERT INTO #SUSPICIOUS_ORDERS_F3
SELECT
      MANDT,
      ERNAM,
      SPENDING_YEAR,
      SPENDING_MONTH
FROM #SPENDING_PER_MOTH_F3 s1
WHERE EXISTS
      (SELECT
            ERNAM
      FROM #SPENDING_PER_MOTH_F3 s2
      WHERE
```

```
            s2.ERNAM = s1.ERNAM
            AND s2.MANDT = s1.MANDT
            --Versucht den Vormonat in der Liste zu finden
            --Dazu wird sowohl über das Jahr als auch den Monat gejoined
            AND s2.SPENDING_YEAR = YEAR(ADD_MONTHS(TO_DATE(s1.SPENDING_YEAR
|| '-' || s1.SPENDING_MONTH || '-01', 'YYYY-MM-DD'),-1))
            AND s2.SPENDING_MONTH =
MONTH(ADD_MONTHS(TO_DATE(s1.SPENDING_YEAR || '-' || s1.SPENDING_MONTH || '-
01', 'YYYY-MM-DD'),-1))
            --Eintrag wird in Liste aufgenommen wenn Nettobetrag größer als
der Vormonat * Prozent ist
            AND s1.SPENDING > 4 * s2.SPENDING
      )
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_F02' AS FlagId
FROM #SUSPICIOUS_ORDERS_F3, EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.ERNAM = #SUSPICIOUS_ORDERS_F3.ERNAM
      AND YEAR(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_F3.SPENDING_YEAR
      AND MONTH(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_F3.SPENDING_MONTH
      AND EKKO.MANDT = #SUSPICIOUS_ORDERS_F3.MANDT
;


--Flag_F04 - Neuer Lieferant
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_F04' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.LFA1 ON
      LFA1.LIFNR = EKKO.LIFNR
      AND LFA1.MANDT = EKKO.MANDT
WHERE
      --Lieferant wurde erst vor einer Woche erstellt
      LENGTH(LTRIM(EKKO.LIFNR)) > 0
      AND LFA1.ERDAT between ADD_DAYS(EKKO.AEDAT,-7) and EKKO.AEDAT
--Bestellvolumen ist größer als das Limit
AND
      (SELECT
            SUM(p2.NETWR)
      FROM X0_STUDENT_001.EKPO p2
      WHERE
            p2.EBELN = EKKO.EBELN
            AND p2.MANDT = EKKO.MANDT) > 5000.00
;


--Flag_F05 - Durschnittspreis überstiegen
```

```
--Erstelle Liste mit Durschnittspreis der Materialien
drop table #MATERIAL_AVERAGE_D2;
CREATE LOCAL TEMPORARY TABLE #MATERIAL_AVERAGE_D2
(MANDT VARCHAR(20), MATNR VARCHAR(40), AVG_PRICE DOUBLE, PRICE_STDEV
DOUBLE)
;

INSERT INTO #MATERIAL_AVERAGE_D2
SELECT
      EKPO.MANDT AS MANDT,
      EKPO.MATNR AS MATNR,
      ROUND(AVG(EKPO.NETPR),2) AS AVG_PRICE,
      ROUND(STDDEV(EKPO.NETPR),2) AS PRICE_STDEV
FROM X0_STUDENT_001.EKPO
WHERE LENGTH(LTRIM(EKPO.MATNR)) > 0
GROUP BY EKPO.MANDT, EKPO.MATNR
HAVING ROUND(STDDEV(EKPO.NETPR),2) > 0.00
;

--Suche Bestellungen bei denen der Materialpreis weit vom
--Durchschnitt abweicht
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_F05' AS FlagId
FROM X0_STUDENT_001.EKPO
JOIN #MATERIAL_AVERAGE_D2 ON
      #MATERIAL_AVERAGE_D2.MATNR = EKPO.MATNR
      AND #MATERIAL_AVERAGE_D2.MANDT = EKPO.MANDT
WHERE
      --Sehr einfach Variante
      --EKPO_NETPR > (MATERIAL_AVERAGE_D2.AVG_PRICE +
MATERIAL_AVERAGE_D2.PRICE_STDEV)
      --Z-Wert
      ((EKPO.NETPR-
#MATERIAL_AVERAGE_D2.AVG_PRICE)/#MATERIAL_AVERAGE_D2.PRICE_STDEV) > 4
;

--Flag_F06 - Bestellung bei neuem Lieferant
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_F06' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.LFA1 ON
      LFA1.LIFNR = EKKO.LIFNR
      AND LFA1.MANDT = EKKO.MANDT
WHERE
      --Lieferant wurde erst vor einer Woche erstellt
      LENGTH(LTRIM(EKKO.LIFNR)) > 0
      AND LFA1.ERDAT between ADD_DAYS(EKKO.AEDAT,-7) and EKKO.AEDAT
--Bei dem eine Bestellung existiert
AND EXISTS
      (SELECT
      FROM X0_STUDENT_001.EKPO p2
      WHERE
            p2.EBELN = EKKO.EBELN
```

```
            AND p2.MANDT = EKKO.MANDT)
;
--Flag_B12 - Grenzwerte
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT e1.MANDT || e1.EBELN || p1.EBELP AS CaseId,
      'Flag_B12' AS FlagId
FROM EKKO e1
JOIN GBI_003.EKPO p1 ON
      e1.EBELN =  p1.EBELN
      AND e1.MANDT = p1.MANDT
WHERE
      --Summe der Nettowerte ist nahe an Grenzwert 1
      (SELECT
            SUM(p2.NETWR)
      FROM GBI_003.EKPO p2
      WHERE
            p2.EBELN = e1.EBELN
            AND p2.MANDT = e1.MANDT) between (5000.00-10) and (5000.00-
0.01)
OR
      --Summe der Nettowerte ist nahe an Grenzwert 2
      (SELECT
            SUM(p2.NETWR)
      FROM GBI_003.EKPO p2
      WHERE p2.EBELN = e1.EBELN
      AND p2.MANDT = e1.MANDT) between (50000.00-10) and (50000.00-0.01)
GROUP BY
      e1.MANDT,
      e1.EBELN,
      p1.EBELP
;

--Scheme Konfigration
--Beispiel
--Um ein eigenes Schema zu Konfigurieren müssen die FlagId
--der gewünschten Flags eingetragen werden
--Wird statt dem Intersect ein Union benutzt, werde alle Transaktionen
--markiert die mindestens einen der aufgeführten Flags besitzen
--im Fall von Intersect müssen alle Flags vorhanden sein

UPDATE _CEL_FLAGED_CASES
SET SCHEMEID = 'F1-Pass_Through'
WHERE CASEID IN
(

SELECT
      FC2.CASEID
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_F02'

INTERSECT

SELECT
      FC2.CASEID
FROM _CEL_FLAGED_CASES FC2
WHERE FLAGID = 'Flag_F04'

)
```

```
AND FLAGID IN ('Flag_F02','Flag_F04');
```

Unbeteiligter Lieferant

```
--Flag_G01 - Gutschrift
--INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EBAN.MANDT || EBAN.EBELN || EBAN.EBELP AS CaseId,
      'Flag_G01' AS FlagId,
      EKBE.GJAHR, EKBE.DMBTR, EKBE.SHKZG
FROM X0_STUDENT_001.EBAN
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELP = EBAN.EBELP
      AND EKPO.EBELN = EBAN.EBELN
      AND EKPO.MANDT = EBAN.MANDT
JOIN X0_STUDENT_001.EKBE ON
      EKBE.EBELP = EKPO.EBELP
      AND EKBE.EBELN = EKPO.EBELN
      AND EKBE.MANDT = EKPO.MANDT
WHERE
       EKBE.VGABE = '1'
      AND EKBE.SHKZG = 'H'
      AND DAYS_BETWEEN(EBAN.BADAT, EKBE.CPUDT) < 1
;



--Flag_G02 - Doppelte Lieferanten
--Erstellt Liste mit Lieferanten der Lifnr und Name ungleich sind
--alle anderen Adressdaten jedoch identisch
CREATE LOCAL TEMPORARY TABLE #DOUBLE_VENDORS_A7
(LIFNR VARCHAR(30), MANDT VARCHAR(20))
;

INSERT INTO #DOUBLE_VENDORS_A7
SELECT
      DISTINCT l1.LIFNR,
      l1.MANDT
FROM X0_STUDENT_001.LFA1 l1
WHERE
      LENGTH(LTRIM(l1.LIFNR)) > 0
AND EXISTS
      (SELECT
            l2.LIFNR
      FROM X0_STUDENT_001.LFA1 l2
      WHERE
            LENGTH(LTRIM(l2.LIFNR)) > 0
            AND l2.LIFNR <> l1.LIFNR
            AND l2.NAME1 <> l1.NAME1
            AND l2.MANDT = l1.MANDT
            AND l2.STRAS = l1.STRAS
            AND l2.PSTLZ = l1.PSTLZ
            AND l2.ORT01 = l1.ORT01
            AND l2.LAND1 = l1.LAND1
      )

;
```

```
--Suche alle Bestellungen an auffällige Lieferanten
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_G02' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN #DOUBLE_VENDORS_A7 ON
      #DOUBLE_VENDORS_A7.MANDT = EKKO.MANDT
      AND #DOUBLE_VENDORS_A7.LIFNR = EKKO.LIFNR
WHERE
      EKKO.BSTYP = 'F'
;


--Flag_G03 - Rechnungsdiskrepanz
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,

      CASE
            WHEN RSEG.WRBTR < EKPO.BRTWR THEN 'Flag_G03'
            WHEN RSEG.WRBTR > EKPO.BRTWR THEN 'Flag_G04'
      END

FROM X0_STUDENT_001.EKPO
JOIN X0_STUDENT_001.RSEG ON
      RSEG.EBELN = EKPO.EBELN
      AND  RSEG.EBELP = EKPO.EBELP
      AND RSEG.MANDT = EKPO.MANDT
--Rechnungsbetrag und Bestellbetrag stimmen nicht überein
WHERE LTRIM(RSEG.WRBTR) <> LTRIM(EKPO.BRTWR)
;


--Flag_G05 - Durschnittspreis überstiegen
--Erstelle Liste mit Durschnittspreis der Materialien
drop table #MATERIAL_AVERAGE_D2;
CREATE LOCAL TEMPORARY TABLE #MATERIAL_AVERAGE_D2
(MANDT VARCHAR(20), MATNR VARCHAR(40), AVG_PRICE DOUBLE, PRICE_STDEV
DOUBLE)
;

INSERT INTO #MATERIAL_AVERAGE_D2
SELECT
      EKPO.MANDT AS MANDT,
      EKPO.MATNR AS MATNR,
      ROUND(AVG(EKPO.NETPR),2) AS AVG_PRICE,
      ROUND(STDDEV(EKPO.NETPR),2) AS PRICE_STDEV
FROM X0_STUDENT_001.EKPO
WHERE LENGTH(LTRIM(EKPO.MATNR)) > 0
GROUP BY EKPO.MANDT, EKPO.MATNR
HAVING ROUND(STDDEV(EKPO.NETPR),2) > 0.00
;

--Suche Bestellungen bei denen der Materialpreis weit vom
--Durchschnitt abweicht
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
```

```
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_G05' AS FlagId
FROM X0_STUDENT_001.EKPO
JOIN #MATERIAL_AVERAGE_D2 ON
      #MATERIAL_AVERAGE_D2.MATNR = EKPO.MATNR
      AND #MATERIAL_AVERAGE_D2.MANDT = EKPO.MANDT
WHERE
      --Sehr einfach Variante
      --EKPO_NETPR > (MATERIAL_AVERAGE_D2.AVG_PRICE +
MATERIAL_AVERAGE_D2.PRICE_STDEV)
      --Z-Wert
      ((EKPO.NETPR-
#MATERIAL_AVERAGE_D2.AVG_PRICE)/#MATERIAL_AVERAGE_D2.PRICE_STDEV) > 4
;

--Flag_G06 - Ungewoehnliche Zeit
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_G06' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.CDPOS ON
      CDPOS.TABKEY = EKKO.MANDT || EKKO.EBELN
JOIN X0_STUDENT_001.CDHDR ON
      CDHDR.CHANGENR = CDPOS.CHANGENR
      AND CDHDR.MANDANT = CDPOS.MANDANT
WHERE
      --Eintrag wurde erstellt
      CDPOS.CHNGIND = 'I'
      --Wurde nach 21 Uhr angelegt
      AND (CDHDR.UTIME > '21:00:00.0000000'
      --Wurde vor 5:30 angelegt
      OR CDHDR.UTIME < '05:30:00.0000000')
;
--Flag_G07 - Mehrere Rechnungen
--Sucht Rechnungen für das selbe Pridukt vom selben
--Lieferanten in sehr kurzem Abstand
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT p1.MANDT || p1.EBELN || p1.EBELP AS CaseId,
      'Flag_G07' AS FlagId
FROM X0_STUDENT_001.RSEG p1
JOIN X0_STUDENT_001.RBKP e1 ON
      p1.BELNR = e1.BELNR
      AND p1.GJAHR = e1.GJAHR
      AND p1.MANDT = e1.MANDT
WHERE
      LENGTH(LTRIM(p1.MATNR)) > 0
      AND LENGTH(LTRIM(e1.LIFNR)) > 0
      AND LENGTH(LTRIM(e1.USNAM)) > 0
      AND EXISTS
      (SELECT p2.EBELN
      FROM X0_STUDENT_001.RSEG p2
      JOIN X0_STUDENT_001.RBKP e2 ON
            p2.BELNR = e2.BELNR
            AND p2.GJAHR = e2.GJAHR
```

```
            AND p2.MANDT = e2.MANDT
      WHERE
            --Es exisitert eine Rechnung
            --mit dem selben Produkt
            p2.MATNR = p1.MATNR
            --dem selben Lieferanten
            AND e2.LIFNR = e1.LIFNR
            AND e2.BELNR <> e1.BELNR
            --vom gleichen Genehmiger
            AND e2.USNAM = e1.USNAM
            --innerhalb von zwei Tagen
            AND e2.BLDAT BETWEEN e1.BLDAT AND ADD_DAYS(e1.BLDAT,2)
            AND p2.MANDT = p1.MANDT
            AND LENGTH(LTRIM(p2.MATNR)) > 0
            AND LENGTH(LTRIM(e2.LIFNR)) > 0
            AND LENGTH(LTRIM(e2.USNAM)) > 0)
;

--Flag_G08 - Neuer Lieferant
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_G08' AS FlagId
FROM EKKO
JOIN X0_STUDENT_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
JOIN X0_STUDENT_001.LFA1 ON
      LFA1.LIFNR = EKKO.LIFNR
      AND LFA1.MANDT = EKKO.MANDT
WHERE
      --Lieferant wurde erst vor einer Woche erstellt
      LENGTH(LTRIM(EKKO.LIFNR)) > 0
      AND LFA1.ERDAT between ADD_DAYS(EKKO.AEDAT,-7) and EKKO.AEDAT
--Bestellvolumen ist größer als das Limit
AND
      (SELECT
            SUM(p2.NETWR)
      FROM X0_STUDENT_001.EKPO p2
      WHERE
            p2.EBELN = EKKO.EBELN
            AND p2.MANDT = EKKO.MANDT) > 5000.00
;


--Flag_G09 - Einkaufswert doppelt gezahlt
INSERT INTO "X0_STUDENT_001"."_CEL_FLAGED_CASES"(CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_G09' AS FlagId
FROM X0_STUDENT_001.RBKP r1
JOIN X0_STUDENT_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.GJAHR =  r1.GJAHR
      AND RSEG.MANDT = r1.MANDT
WHERE
      LENGTH(LTRIM(r1.RMWWR)) > 0
      AND r1.RMWWR > 0
      AND LENGTH(LTRIM(r1.LIFNR)) > 0
AND EXISTS
```

```
      (SELECT r2.BELNR
      FROM X0_STUDENT_001.RBKP r2
      WHERE
            --Es exisitert eine zweite Rechnungn
            r2.BELNR <> r1.BELNR
            AND r2.MANDT = r1.MANDT
            --Mit gleichem Rechnungsbetrag
            AND r2.RMWWR = r1.RMWWR
            --gleichem Lieferanten
            AND r2.LIFNR <> r1.LIFNR
            --Und wurde innerhalb von 14 Tagen eingegeben
            AND r2.CPUDT between r1.CPUDT and ADD_DAYS(r1.CPUDT,14)
            AND LENGTH(LTRIM(r1.RMWWR)) > 0
            AND LENGTH(LTRIM(r1.LIFNR)) > 0)
;

--Flag_A04 - Änderung Lieferantenstammsatz
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_A04' AS FlagId
FROM GBI_003.RBKP
JOIN GBI_003.RSEG ON
      RSEG.BELNR = RBKP.BELNR
      AND RSEG.GJAHR = RBKP.GJAHR
      AND RSEG.MANDT = RBKP.MANDT
JOIN GBI_003.BKPF ON
      BKPF.AWKEY = concat(RSEG.BELNR, RSEG.GJAHR)
      AND BKPF.MANDT = RSEG.MANDT
JOIN GBI_003.BSAK ON
      BKPF.BELNR = BSAK.BELNR
      AND BKPF.MANDT = BSAK.MANDT
      AND BKPF.GJAHR = BSAK.GJAHR
      AND BKPF.BUKRS = BSAK.BUKRS
JOIN GBI_003.CDPOS ON
      RBKP.LIFNR = CDPOS.OBJECTID
JOIN GBI_003.CDHDR ON
      CDHDR.CHANGENR = CDPOS.CHANGENR
      AND CDHDR.MANDANT = CDPOS.MANDANT
      -- Vergleicht letzten Nutzer
      AND RBKP.USNAM = CDHDR.USERNAME
      -- Vergleicht Rechnungserfasser
      -- AND RBKP.ERFNAM = CDHDR.USERNAME
      AND CDHDR.UDATE BETWEEN RBKP.BLDAT AND BSAK.AUGDT
WHERE
      --Suche Einträge bei denen in der Tabelle der Lieferantenbankdaten
      --die Kontonummer oder Bankleitzahl verändert wurde
      CDPOS.TABNAME = 'LFBK'
      AND (
            CDPOS.FNAME = 'BANKN'
            OR CDPOS.FNAME = 'BANKL')
      --Diese änderung sollte am Tag des Rechnugseingangs oder kurz danach
geschehen sein
      AND RBKP.BLDAT between CDHDR.UDATE and
ADD_DAYS(CDHDR.UDATE,RBKP.ZBD1T)
      --Suche nach einem weiteren Eintrag welcher  wieder eine Änderung der
Bankverbindung für den
      --gleichen Lieferanten vom gleichen Benutzer druchgeführt wurde
      AND EXISTS
```

```
            (SELECT c2.CHANGENR
            FROM GBI_003.CDPOS c2
            JOIN GBI_003.CDHDR h2 ON
                  h2.CHANGENR = c2.CHANGENR
                  AND h2.MANDANT = c2.MANDANT
            WHERE
                  c2.TABNAME = 'LFBK'
            AND (
                  c2.FNAME = 'BANKN'
                  OR c2.FNAME = 'BANKL')
            AND c2.CHANGENR <> CDPOS.CHANGENR
            AND c2.OBJECTID = CDPOS.OBJECTID
            AND h2.USERNAME = CDHDR.USERNAME
            AND h2.UDATE between CDHDR.UDATE and ADD_DAYS(BSAK.AUGDT,3)
            )
;
```

Private Einkäufe

```
-- Flag_H01
-- Rechnungseingang, obwohl die Bestellanforderung geblockt wurde

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EBAN.MANDT || EBAN.EBELN || EBAN.EBELP AS CaseId,
      'Flag_H01' AS FlagId

FROM GBI_001.EBAN
JOIN GBI_001.EKPO ON
      EKPO.EBELP = EBAN.EBELP
      AND EKPO.EBELN = EBAN.EBELN
      AND EKPO.MANDT = EBAN.MANDT
JOIN GBI_001.EKBE ON
      EKBE.EBELP = EKPO.EBELP
      AND EKBE.EBELN = EKPO.EBELN
      AND EKBE.MANDT = EKPO.MANDT
WHERE
       EKBE.VGABE = '2'
      -- Ein Wert in BLCKD zeigt an, dass die Bestellanforderung blockiert
wurde
      AND LENGTH(LTRIM(EBAN.BLCKD)) > 0
;

-- Flag_H02
-- Rechnungseingang, obwohl die Bestellanforderung nicht genehmigt wurde

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EBAN.MANDT || EBAN.EBELN || EBAN.EBELP AS CaseId,
      'Flag_H02' AS FlagId

FROM GBI_001.EBAN
JOIN GBI_001.EKPO ON
      EKPO.EBELP = EBAN.EBELP
      AND EKPO.EBELN = EBAN.EBELN
      AND EKPO.MANDT = EBAN.MANDT
JOIN GBI_001.EKBE ON
      EKBE.EBELP = EKPO.EBELP
```

```
      AND EKBE.EBELN = EKPO.EBELN
      AND EKBE.MANDT = EKPO.MANDT
WHERE
       EKBE.VGABE = '2'
      -- Ein Wert in BLCKD zeigt an, dass die Bestellanforderung blockiert
wurde
      AND EBAN.FRGDT IS NULL
      OR EBAN.FRGDT=' '
;

--Flag_H03 - Grenzwerte
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT e1.MANDT || e1.EBELN || p1.EBELP AS CaseId,
      'Flag_H03' AS FlagId
FROM EKKO e1
JOIN GBI_001.EKPO p1 ON
      e1.EBELN =  p1.EBELN
      AND e1.MANDT = p1.MANDT
WHERE
      --Summe der Nettowerte ist nahe an Grenzwert 1
      (SELECT
            SUM(p2.NETWR)
      FROM GBI_001.EKPO p2
      WHERE
            p2.EBELN = e1.EBELN
            AND p2.MANDT = e1.MANDT) between (5000.00-10) and (5000.00-
0.01)
OR
      --Summe der Nettowerte ist nahe an Grenzwert 2
      (SELECT
            SUM(p2.NETWR)
      FROM GBI_001.EKPO p2
      WHERE p2.EBELN = e1.EBELN
      AND p2.MANDT = e1.MANDT) between (50000.00-10) and (50000.00-0.01)
GROUP BY
      e1.MANDT,
      e1.EBELN,
      p1.EBELP
;



--Flag_H04 - Durschnittspreis überstiegen
--Erstelle Liste mit Durschnittspreis der Materialien
drop table #MATERIAL_AVERAGE_D2;
CREATE LOCAL TEMPORARY TABLE #MATERIAL_AVERAGE_D2
(MANDT VARCHAR(20), MATNR VARCHAR(40), AVG_PRICE DOUBLE, PRICE_STDEV
DOUBLE)
;

INSERT INTO #MATERIAL_AVERAGE_D2
SELECT
      EKPO.MANDT AS MANDT,
      EKPO.MATNR AS MATNR,
      ROUND(AVG(EKPO.NETPR),2) AS AVG_PRICE,
      ROUND(STDDEV(EKPO.NETPR),2) AS PRICE_STDEV
FROM GBI_001.EKPO
WHERE LENGTH(LTRIM(EKPO.MATNR)) > 0
GROUP BY EKPO.MANDT, EKPO.MATNR
```

```
HAVING ROUND(STDDEV(EKPO.NETPR),2) > 0.00
;

--Suche Bestellungen bei denen der Materialpreis weit vom
--Durchschnitt abweicht
INSERT INTO "GBI_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
      'Flag_H04' AS FlagId
FROM GBI_001.EKPO
JOIN #MATERIAL_AVERAGE_D2 ON
      #MATERIAL_AVERAGE_D2.MATNR = EKPO.MATNR
      AND #MATERIAL_AVERAGE_D2.MANDT = EKPO.MANDT
WHERE
      --Sehr einfach Variante
      --EKPO_NETPR > (MATERIAL_AVERAGE_D2.AVG_PRICE +
MATERIAL_AVERAGE_D2.PRICE_STDEV)
      --Z-Wert
      ((EKPO.NETPR-
#MATERIAL_AVERAGE_D2.AVG_PRICE)/#MATERIAL_AVERAGE_D2.PRICE_STDEV) > 4
;



--Flag_H05 - Ungewöhliche Genehmigung
--Erstelle Liste von Mitarbeitern die an einem Tag
--besonders viele Bestellungen durchgeführt haben
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDERS_B4b
(MANDT VARCHAR(30), ERNAM VARCHAR(30), AEDAT DATE)
;

INSERT INTO #SUSPICIOUS_ORDERS_B4b
SELECT
      e1.MANDT,
      e1.ERNAM,
      e1.AEDAT

FROM EKKO e1
WHERE LENGTH(LTRIM(e1.ERNAM)) > 0
GROUP BY
      e1.MANDT,
      e1.ERNAM,
      e1.AEDAT
HAVING
      --Bestellungen des Tages übersteigen Durchschnittswert des letzten
Jahres
      --5+ ist ein Sockel. Ohne diesen geht der Durchschnitt bei wenigen
Bestellungen
      --gegen Null
      COUNT(e1.EBELN) > 25+4*
            (SELECT
                  --Komplettes Jahr
                  --COUNT(e2.EKKO_EBELN)/365
                  --Arbeitstage 2016 Bayern
                  COUNT(e2.EBELN)/250
            FROM EKKO e2
            WHERE
                  e2.AEDAT >= ADD_YEARS(e1.AEDAT,-1)
                  AND e2.AEDAT <= e1.AEDAT
                  --Durchschnitt aller Mitarbeiter oder nur des aktuellen
```

```
                AND e2.ERNAM = e1.ERNAM
                AND e2.MANDT = e1.MANDT
            )
;

--Markiere Bestellungen an auffälligen Tagen
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
      DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP  AS CaseId,
      'Flag_H05' AS FlagId
FROM #SUSPICIOUS_ORDERS_B4b, EKKO
JOIN GBI_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.ERNAM = #SUSPICIOUS_ORDERS_B4b.ERNAM
      AND EKKO.AEDAT = #SUSPICIOUS_ORDERS_B4b.AEDAT
      AND EKKO.MANDT = #SUSPICIOUS_ORDERS_B4b.MANDT
      AND EKKO.BSTYP = 'F'
;

--Flag_H06 - Selber Betrag mehrmahls bezahlt
INSERT INTO "GBI_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_H06' AS FlagId
FROM GBI_001.RBKP r1
JOIN GBI_001.RSEG ON
      RSEG.BELNR = r1.BELNR
      AND RSEG.MANDT = r1.MANDT
      AND RSEG.GJAHR = r1.GJAHR
WHERE
      LENGTH(LTRIM(r1.RMWWR)) > 0
      AND r1.RMWWR > 0
      AND LENGTH(LTRIM(r1.LIFNR)) > 0
AND EXISTS
      (SELECT
            r2.BELNR
      FROM GBI_001.RBKP r2
      WHERE
            --Es exisiert eine Rechnung vom selben Nutzer
            -- Mit gleichem Betrag an den gleichen Lieferanten
            -- und dem gleichen Mitarbeiter
            r2.USNAM = r1.USNAM
            AND r2.MANDT = r1.MANDT
            AND r2.RMWWR = r1.RMWWR
            AND r2.CPUDT = r1.CPUDT
            AND r2.LIFNR = r1.LIFNR
            AND r2.BELNR <> r1.BELNR
      )
;

--Flag_H07 - Selbe Rechnung doppelt mehrfach bezahlt
INSERT INTO "GBI_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
      DISTINCT RSEG.MANDT || RSEG.EBELN || RSEG.EBELP AS CaseId,
      'Flag_H07' AS FlagId
FROM GBI_001.RBKP r1
JOIN GBI_001.RSEG ON
      RSEG.BELNR = r1.BELNR
```

```
      AND RSEG.MANDT = r1.MANDT
      AND RSEG.GJAHR = r1.GjAHR
WHERE
      LENGTH(LTRIM(r1.LIFNR)) > 0
AND EXISTS
      (SELECT
            r2.BELNR
      FROM GBI_001.RBKP r2
      WHERE
            --Es exisiert eine Rechnung mit dem selben Betrag
            --an den gleichen Lieferanten aber einem anderen
            --Mitarbeiter
            r2.RMWWR = r1.RMWWR
            AND r2.CPUDT = r1.CPUDT
            AND r2.LIFNR = r1.LIFNR
            AND r2.BELNR <> r1.BELNR
            AND r2.USNAM <> r1.USNAM
            AND r2.MANDT = r1.MANDT
      )
;

--Flag_H08 - Budgetabweichung
--Generiert Liste aller Nettobestellungen eines Mitarbeiters pro Monat
CREATE LOCAL TEMPORARY TABLE #SPENDING_PER_MOTH_A1
(MANDT VARCHAR(20), ERNAM VARCHAR(30), SPENDING_YEAR INT, SPENDING_MONTH
INT, SPENDING DOUBLE)
;

INSERT INTO #SPENDING_PER_MOTH_A1
SELECT
      EKKO.MANDT,
      EKKO.ERNAM,
      YEAR(EKKO.AEDAT),
      MONTH(EKKO.AEDAT),
      SUM(EKPO.NETWR)
FROM EKKO
JOIN GBI_001.EKPO ON
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE LENGTH(LTRIM(EKKO.ERNAM)) > 0
GROUP BY EKKO.MANDT, EKKO.ERNAM, YEAR(EKKO.AEDAT), MONTH(EKKO.AEDAT)
HAVING SUM(EKPO.NETWR) > 0
ORDER BY EKKO.MANDT
;


--Sucht auffällige Transaktionen
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDERS_A1
(MANDT VARCHAR(20), ERNAM VARCHAR(30), SPENDING_YEAR INT, SPENDING_MONTH
INT)
;

INSERT INTO #SUSPICIOUS_ORDERS_A1
SELECT
      MANDT,
      ERNAM,
      SPENDING_YEAR,
      SPENDING_MONTH
FROM #SPENDING_PER_MOTH_A1 s1
WHERE EXISTS
```

```
	(SELECT
		ERNAM
	FROM #SPENDING_PER_MOTH_A1 s2
	WHERE
		s2.ERNAM = s1.ERNAM
		AND s2.MANDT = s1.MANDT
		--Versucht den Vormonat in der Liste zu finden
		--Dazu wird sowohl über das Jahr als auch den Monat gejoined
		AND s2.SPENDING_YEAR = YEAR(ADD_MONTHS(TO_DATE(s1.SPENDING_YEAR
|| '-' || s1.SPENDING_MONTH || '-01', 'YYYY-MM-DD'),-1))
		AND s2.SPENDING_MONTH =
MONTH(ADD_MONTHS(TO_DATE(s1.SPENDING_YEAR || '-' || s1.SPENDING_MONTH || '-
01', 'YYYY-MM-DD'),-1))
		--Eintrag wird in Liste aufgenommen wenn Nettobetrag größer als
der Vormonat * Prozent ist
		AND s1.SPENDING > 4 * s2.SPENDING
	)
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
	DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
	'Flag_H08' AS FlagId
FROM #SUSPICIOUS_ORDERS_A1, EKKO
JOIN GBI_001.EKPO ON
	EKPO.EBELN = EKKO.EBELN
	AND EKPO.MANDT = EKKO.MANDT
WHERE
	EKKO.ERNAM = #SUSPICIOUS_ORDERS_A1.ERNAM
	AND YEAR(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_A1.SPENDING_YEAR
	AND MONTH(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_A1.SPENDING_MONTH
	AND EKKO.MANDT = #SUSPICIOUS_ORDERS_A1.MANDT
;


-Flag_H09 - Steigende Einkäufe
--Erstelle Liste für jeden Lieferanten und Mitarbeiter über die
Bestellungen pro Monat
CREATE LOCAL TEMPORARY TABLE #ORDERS_PER_MONTH_B18
(MANDT VARCHAR(20), LIFNR VARCHAR(30), ERNAM VARCHAR(30), ORDER_YEAR INT,
ORDER_MONTH INT, ORDERS DOUBLE)
;

INSERT INTO #ORDERS_PER_MONTH_B18
SELECT
	EKKO.MANDT AS MANDT,
	EKKO.LIFNR AS LIFNR,
	EKKO.ERNAM AS ERNAM,
	YEAR(EKKO.AEDAT) AS ORDER_YEAR,
	MONTH(EKKO.AEDAT) AS ORDER_MONTH,
	COUNT(EKKO.EBELN) AS ORDERS
FROM EKKO
WHERE
	LENGTH(LTRIM(EKKO.LIFNR)) > 0
--	AND s2.BLDAT between TO_DATE(YEAR(s1.BLDAT) || '-' || MONTH(s1.BLDAT)
|| '-01','YYYY-MM-DD') and LAST_DAY(s1.BLDAT)
	AND EKKO.AEDAT between TO_DATE(YEAR(EKKO.AEDAT)|| '-' ||
MONTH(EKKO.AEDAT) || '-01','YYYY-MM-DD') and LAST_DAY(EKKO.AEDAT)
GROUP BY
	EKKO.MANDT,
```

```
	EKKO.LIFNR,
	EKKO.ERNAM,
	YEAR(EKKO.AEDAT),
	MONTH(EKKO.AEDAT)
--HAVING COUNT(EKKO.EBELN) > 10
;

--Suche ob die Bestellungen bei einem Liferanten von einem Mitarbeiter
--signifikant größer sind als die des Vormonats
CREATE LOCAL TEMPORARY TABLE #SUSPICIOUS_ORDERS_B18
(MANDT VARCHAR(20), LIFNR VARCHAR(30), ERNAM VARCHAR(30), ORDER_YEAR INT,
ORDER_MONTH INT)
;

INSERT INTO #SUSPICIOUS_ORDERS_B18
SELECT
	MANDT,
	LIFNR,
	ERNAM,
	ORDER_YEAR,
	ORDER_MONTH
FROM #ORDERS_PER_MONTH_B18 o1
WHERE EXISTS
	(SELECT o2.ORDERS
		FROM #ORDERS_PER_MONTH_B18 o2
		WHERE
			o2.LIFNR = o1.LIFNR
			AND o2.MANDT = o1.MANDT
			AND o2.ERNAM = o1.ERNAM
			AND o2.ORDER_MONTH =
MONTH(ADD_MONTHS(TO_DATE(o1.ORDER_YEAR|| '-' || o1.ORDER_MONTH || '-
01','YYYY-MM-DD'),-1))
			AND o2.ORDER_YEAR =
YEAR(ADD_MONTHS(TO_DATE(o1.ORDER_YEAR|| '-' || o1.ORDER_MONTH || '-
01','YYYY-MM-DD'),-1))
			AND o1.ORDERS > 2*o2.ORDERS
			AND o2.ORDERS > 0
		)
;

INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
	DISTINCT EKKO.MANDT || EKKO.EBELN || EKPO.EBELP AS CaseId,
	'Flag_H09' AS FlagId
FROM #SUSPICIOUS_ORDERS_B18, EKKO
JOIN GBI_001.EKPO ON
	EKPO.EBELN = EKKO.EBELN
	AND EKPO.MANDT = EKKO.MANDT
WHERE
	EKKO.LIFNR = #SUSPICIOUS_ORDERS_B18.LIFNR
	AND EKKO.MANDT = #SUSPICIOUS_ORDERS_B18.MANDT
	AND EKKO.ERNAM = #SUSPICIOUS_ORDERS_B18.ERNAM
	AND YEAR(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_B18.ORDER_YEAR
	AND MONTH(EKKO.AEDAT) = #SUSPICIOUS_ORDERS_B18.ORDER_MONTH
;


--Flag_H10 - Rechnungsdiskrepanz
INSERT INTO _CEL_FLAGED_CASES (CaseId, FlagId)
SELECT
```

```
	DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,

	CASE
		WHEN RSEG.WRBTR < EKPO.BRTWR THEN 'Flag_H10a'
		WHEN RSEG.WRBTR > EKPO.BRTWR THEN 'Flag_H10b'
	END

FROM GBI_001.EKPO
JOIN GBI_001.RSEG ON
	RSEG.EBELN = EKPO.EBELN
	AND  RSEG.EBELP = EKPO.EBELP
	AND RSEG.MANDT = EKPO.MANDT
--Rechnungsbetrag und Bestellbetrag stimmen nicht überein
WHERE LTRIM(RSEG.WRBTR) <> LTRIM(EKPO.BRTWR)
;


--FLAG_H11 - Teilkäufe
--Suche Bestellungen von einem Tag, dem gleichen Mitarbeiter
--dem gleichen Material und Lieferanten
--werden diese Aufsummiert übersteigt die Gesamtsummt
--eine Freigabegrenze
drop table #SUSPICOUS_ORDERS_D6;
CREATE LOCAL TEMPORARY TABLE #SUSPICOUS_ORDERS_D6
(MANDT VARCHAR(20), ERNAM VARCHAR(30), AEDAT DATE, MATNR VARCHAR(30), LIFNR
VARCHAR(30), ORDER_VOLUME DOUBLE, ORDER_COUNT INT)
;

INSERT INTO #SUSPICOUS_ORDERS_D6
SELECT
	EKKO.MANDT,
	EKKO.ERNAM,
	EKKO.AEDAT,
	EKPO.MATNR,
	EKKO.LIFNR,
	SUM(EKPO.NETWR) AS "Order Volume",
	COUNT(EKKO.EBELN) AS "Count"
FROM GBI_001.EKPO
JOIN EKKO ON
	EKKO.EBELN = EKPO.EBELN
	AND EKKO.MANDT = EKPO.MANDT
WHERE
	LENGTH(EKKO.LIFNR) > 0
	AND LENGTH(EKKO.FRGSX) = 0
	AND LENGTH(EKPO.MATNR) > 0
GROUP BY
	EKKO.MANDT, EKKO.ERNAM, EKPO.MATNR, EKKO.AEDAT, EKKO.LIFNR
HAVING
	COUNT(EKKO.EBELN) > 2
	AND SUM(EKPO.NETWR) > 50000.00
--ORDER BY
	--EKKO_ERNAM, EKKO_AEDAT, EKKO_LIFNR
;

INSERT INTO "GBI_001"."_CEL_FLAGED_CASES" (CaseId, FlagId)
SELECT
	DISTINCT EKPO.MANDT || EKPO.EBELN || EKPO.EBELP AS CaseId,
	'FLAG_H11' AS FlagId
FROM #SUSPICOUS_ORDERS_D6, EKKO
JOIN GBI_001.EKPO ON
```

```
      EKPO.EBELN = EKKO.EBELN
      AND EKPO.MANDT = EKKO.MANDT
WHERE
      EKKO.ERNAM = #SUSPICOUS_ORDERS_D6.ERNAM
      AND EKKO.AEDAT = #SUSPICOUS_ORDERS_D6.AEDAT
      AND EKPO.MATNR = #SUSPICOUS_ORDERS_D6.MATNR
      AND EKKO.LIFNR = #SUSPICOUS_ORDERS_D6.LIFNR
      AND EKKO.MANDT = #SUSPICOUS_ORDERS_D6.MANDT
;
```