Datenanalysen im Anti Fraud-Management

Nutzen und Ansätze der Internen Revision

Aus der Serie der Fachbeiträge des DIIR Nr. 5

Version 1.0 Dezember 2023

Verfasser:
Arbeitsgruppe „Datenanalysen“ im DIIR-Arbeitskreis „Anti-Fraud-Management, Compliance und Interne Revision“

DIIR
Deutsches Institut für Interne Revision e.V.

Hinweis der Verfasser

Dieser Fachbeitrag beinhaltet Empfehlungen zum praktischen Umgang mit datenanalytischen Verfahren im Zuge des Anti-Fraud-Managements. Er wurde in der Arbeitsgruppe „Datenanalysen“ des DIIR-Arbeitskreises „Anti-Fraud-Management, Compliance und Interne Revision“ erstellt. Das Dokument soll Grundlage für eine fortlaufende Erweiterung sein. Dies betrifft insbesondere die im Anhang wiedergegebenen Verfahren zur Durchführung von Analysen aus unterschiedlichen Anlässen und mit unterschiedlichen Zielsetzungen. Hinweise zu Ergänzungen oder Korrekturen nimmt der Arbeitskreis gerne entgegen.

Durch den aktiven Beitrag der Anti-Fraud-Management-Community kann der Fachbeitrag mit möglichst umfassendem Inhalt fortgeschrieben werden. Die Verfasser streben eine möglichst weitreichende Sammlung von Verfahrenshinweisen mit hoher praktischer Relevanz für alle an, die an Datenanalysen interessiert sind.

Inhalt

Hinweis der Verfasser 2

1 Zielsetzung 4

2 Einleitung 6

3 Vorbereitung der Datenanalysen 8

4 Anwendung von Data Analytics-Verfahren zur Identifikation von Auffälligkeiten 11

4.1 Einsatzgebiete von Data Analytics 11

4.2 Prüferische Ziele beim Einsatz von Data Analytics 12

4.2.1 Prevention 12

4.2.2 Detection 13

4.2.3 Investigation 13

4.3 Data Analytics: Methoden, Verfahren, Tools 14

5 Vorgehensweise bei der Datenanalyse 19

5.1 Wichtige Rahmenbedingungen für die Analytik 19

5.2 Generische Prozesselemente der Datenanalyse 20

6 Herausforderungen/Kritische Parameter bei Datenanalysen 25

7 Datenanalysen und Datenschutz 28

8 Beispiele für praktische Fallkonstellationen: Zu verwendende Datenbestände .. 29

9 Literaturverzeichnis 44

1 Zielsetzung

Data Analytics beschreibt Verfahren, die zur Exploration, Transformation und Analyse großer Datenmengen angewendet werden können, um Trends und Muster zu identifizieren, die den Entscheidungsfindungsprozess unterstützen. Die Analyse großer Datenmengen kann zum Verständnis der vorliegenden Grundmenge von Daten und damit der Geschäftsfälle wesentlich beitragen.[1] Auch für prüfende Berufe sind Data Analytics Tools relevant. So bieten beispielsweise unter anderem Wirtschaftsprüfungsgesellschaften eine breite Palette an Dienstleistungen rund um Data Analytics an.[2] Dies resultiert u. a. daraus, dass Physische Stichprobenverfahren hinsichtlich ihrer Aussagefähigkeit regelmäßig begrenzt sind. Die Verwendung datenanalytischer Verfahren führt zu einer höheren Prüfungseffizienz und -effektivität sowie verlässlicheren Prüfungsergebnissen. Auch ermöglichen sie die Verwendung einer umfangreicheren Menge betrachteter Geschäftsvorfälle, als sie bei herkömmlichen stichprobenbasierten Prüfungen zum Einsatz kommt.[3]

Mit der Anwendung von Data Analytics werden vielfältige Vorteile verbunden, die gerade für den praktischen Nutzen im Kontext der Internen Revision von wesentlicher Bedeutung sind:

I. Mit der Untersuchung einer vollständigen Grundgesamtheit von Transaktionen können Anomalien und Fraud systematisch identifiziert und relevante Prüfungsnachweise gesammelt werden.[4]

II. Datenanalysen können eine intensive Überprüfung von Sachverhalten bzw. weiterführenden Konkretisierungsbedarf unterstützen.[5]

III. Für datenanalytische Verfahren sprechen Effizienzgewinne bei der Sammlung von Prüfungsnachweisen, der Identifikation möglicher Risiken und der Bestimmung von Kontrollschwächen in Prozessen.[6] Daher können auch Fraud-Risiken frühzeitig identifiziert und damit unter Umständen einer zielgerichteten Aufklärung zugeführt werden.[7]

---

[1] Vgl. Earley, 2015.
[2] Vgl. Deloitte, 2023; EY, 2023; KPMG, 2023; PwC, 2023.
[3] Vgl. Eulerich et al., 2020; Christ et al., 2020.
[4] Vgl. Cao et al., 2015.
[5] Vgl. Brown-Liburd/Issa/Lombardi, 2015.
[6] Vgl. Eulerich et al., 2020; Kalinichenko, 2016.
[7] Vgl. Dai und Vasarhelyi, 2020.

IV. Die Verwendung von Datenanalysen erlaubt es den Prüfern, mehr Zeit auf die Interpretation der gewonnenen Ergebnisse oder die Analyse komplexere Vorgänge zu verwenden.[8]

V. Auch ermöglicht kontinuierliches Monitoring der Geschäftsaktivitäten auf datenanalytischer Basis eine effiziente Erkennung potenzieller Risiken.[9]

In der jüngeren Vergangenheit rückt die Notwendigkeit für die Interne Revision, sich mit Digitalisierungsthemen zu befassen, immer stärker in den Fokus.[10] So beschreibt eine US-amerikanische Studie eine höhere Skepsis von Geschworenen in Verfahren, wenn Prüfer statt datenanalytischer Verfahren traditionelle statistische Stichprobenverfahren anwenden.[11]

Die Anwendung von Data Analytics in der Revisionspraxis ist dennoch begrenzt. Dies ist u. a. darauf zurückzuführen, dass adäquate Ressourcen derzeit überwiegend lediglich bei größeren Unternehmen vorliegen.[12]

---

[8] Vgl. Eulerich/Kalinichenko, 2018.
[9] Vgl. Eulerich, Georgi und Schmidt, 2020.
[10] Vgl. exemplarisch Bünis/Gossens, 2022; Haas/Schreckenberger/Stottrop2022; Odenthal/Odenthal, 2023.
[11] Vgl. Bar-Pulliam et al., 2023.
[12] Vgl. Wagner, 2017.

2 Einleitung

Die Ursachen für eine derzeit nur begrenzte Nutzung von Data Analytics in der Internen Revision sind bisher nicht umfassend untersucht worden. Da die Umstellung der Prüfungstätigkeit auf datenanalytische Ansätze gegebenenfalls einen komplexeren Transformationsprozess erfordert, könnte eine Zurückhaltung bei den Verantwortlichen wegen eines zu erwartenden hohen Aufwands von Relevanz sein. Ebenso könnten Zweifel an der Tragfähigkeit neuer analytischer Verfahren und deren zielgerichteter Einsatzmöglichkeiten bestehen. Schließlich verbindet sich mit den notwendigen, IT-basierten Neuerungen bei Analyseverfahren eine grundsätzlich zunehmende Abhängigkeit von den verfügbaren Daten und Verarbeitungsprozeduren innerhalb des Unternehmens. Zusätzlich erfordert eine zielgerichtete Datennutzung für Prüfungstätigkeiten eine nähere Kenntnis der verfügbaren Datenstrukturen insbesondere bei der Zusammenführung oder Verbindung originär separater Datenbestände. Als besonders wichtig muss hervorgehoben werden, dass die Anwendung datenanalytischer Verfahren geeignete Fertigkeiten bzw. Kenntnisse erfordert. Hier kann sogar von der Notwendigkeit eines Up-Skillings für Interne Revisorinnen und Revisoren gesprochen werden.[13] In der Konsequenz kann dies eine Hemmschwelle für die Transformation zu datenanalytischen Prüfungsverfahren bedeuten. Insgesamt gilt: Entscheidungen zur Adaption datenanalytischer Verfahren müssen vor dem Hintergrund des notwendigen Aufwands und eventuell erforderlicher Prozessanpassungen immer im Kontext der unternehmensspezifischen Konstellationen und Anforderungen gesehen werden. Die Komplexität erfordert eine angemessene Auseinandersetzung mit den angestrebten Zielen der Prüfung und die Berücksichtigung möglicher Risiken bei der Zielerreichung. Aus Sicht der Autoren dieses Fachbeitrags überwiegen jedoch die Vorteile.

Gleichzeitig wird der Bedarf einer Unterstützung bei der Umsetzung solcher Transformationsvorhaben ersichtlich. Dieser Fachbeitrag soll diese Unterstützung bieten. Es werden Handlungsoptionen für die Nutzung von Data Analytics aufgezeigt und praktische Bezüge hergestellt. Dies resultiert in praxisorientierten Hinweisen zur Realisierung der Vorteile. Insbesondere werden jene Prüferinnen und Prüfer unterstützt, die bisher aufgrund begrenzter Ressourcen die Transformation der Prüfungsmethodik nicht in die Praxis umsetzen konnten oder innerhalb ihres Unternehmens nach Umsetzungsgrundlagen suchen.

Es werden Handlungsempfehlungen für interessierte Anwender angeboten. Dazu werden klassische Schritte beschrieben, die für die erfolgreiche Anwendung der Verfahren

[13] Vgl. Haas/Schreckenberger/Stottrop, 2022.

notwendig sind. Es erfolgt dabei die Unterscheidung nach den Zielen Prevention, Detection und Investigation. Die anzuwendenden Verfahren unterscheiden sich dabei im Wesentlichen durch die Art der Vorbereitung sowie das angestrebte Ergebnis und die Ergebnisverwendung bzw. -interpretation.

Weiterhin werden die wesentlichen Herausforderungen bei der Anwendung von Data Analytics thematisiert. Hier soll dem künftigen Anwender Unterstützung geboten werden, um klassische Fehler zu vermeiden bzw. potenzielle Risiken frühzeitig zu berücksichtigen. Ergänzt wird der Fachbeitrag durch eine Reihe praktischer Anwendungshinweise anhand ausgewählter Fraud-Konstellationen. Orientiert an einer etablierten Kategorisierung der Association of Certified Fraud Examiners (ACFE)[14] werden Vorschläge hinsichtlich zu verwendender Datenbestände für unterschiedliche Analysezwecke vorgestellt.

[14] Vgl. ACFE, 2022.

3 Vorbereitung der Datenanalysen

Die Breite an erwähnten Vorteilen führt bisher nur bedingt dazu, dass die Interne Revision tatsächlich auch auf Data Analytics zurückgreift.[15] Eine Kategorisierung nach Reifegraden ergibt: Die Unterstützung der Revisionstätigkeit durch IT-Tools befindet sich noch in der Reifungsphase, auch hinsichtlich der Ersetzung stichprobenbasierter Prüfungen durch datenanalytisch gestützte Vollprüfungen.[16] In einer Untersuchung des DIIR zeigen sich beim praktischen Nutzungsgrad von Data Analytics noch wesentliche Verbesserungspotenziale.[17]

Eine Möglichkeit ist, dass die erforderlichen technischen Fertigkeiten für Datenanalysen bei Revisorinnen und Revisoren bisher noch unzureichend ausgeprägt sind.[18] Dies lässt eine angemessene strategische Planung für die Transformation zu datenanalytischen Verfahren sinnvoll erscheinen: Neben der Einführung solcher Verfahren ist gleichzeitig zu klären, wie die technischen Fertigkeiten der Prüferinnen und Prüfer weiterentwickelt werden können. Ebenso sollte klargestellt werden, inwiefern einzelne Personen innerhalb des Revisionsteams zu Datenanalyseexperten weiterentwickelt werden können oder sollen. Auch ist die flexible Einbeziehung externer Spezialisten sinnvoll, da sie umfangreiche praktische Erfahrungen in der Analytik mitbringen können.

Eventuell sind auch inhaltliche Vorbehalte ein Hemmnis für datenanalytische Ansätze. Beispielsweise kann eine unzureichende analytische Eingrenzung eine übergroße Anzahl von „Treffern“ liefern und auch ohne Anomalien zu falschen Rückschlüssen (false positives) führen. Eine Vielzahl vermeintlich erkannter „Treffer“ erschwert die Identifikation der gesuchten tatsächlichen „Treffer“ ggf. erheblich.

Primäre Anforderung bei der Nutzung datenanalytischer Verfahren ist insbesondere die Verfügbarkeit einer geeigneten Datengrundlage. In aller Regel werden die benötigten Daten erst für die Prüfung zur Verfügung gestellt. Das bedeutet im Einzelnen:

- Die benötigten Daten müssen eindeutig identifiziert werden. Es sind detaillierte Kenntnisse zu den für die Analytik erforderlichen Datenfeldern erforderlich.

---

[15] Vgl. DIIR, 2023; Eilifsen, Kinserdal, Messier und McKee, 2020; Gepp et al., 2018.
[16] Vgl. Wagner, 2017; Gutzmer, 2021.
[17] Vgl. Bünis/Gossens, 2022; DIIR, 2023.
[18] Vgl. Haas/Schreckenberger/Stottrop, 2023; Bar-Pulliem et al., 2020; Gutzmer, 2021.

- Der Zugriff auf die Daten muss mit der IT-Abteilung abgestimmt werden. Sowohl der eigenstände Zugriff als auch die Bereitstellung der benötigten Daten ist möglich.
- Da häufig erst die Kombination von Daten aus unterschiedlichen Datenquellen sinnvolle Zusammenhänge erschließen lässt, müssen ggf. Kenntnisse über die Datenstrukturen vorhanden sein. (Beispiel: Es kann sinnvoll sein, für analytische Zwecke parallel Daten aus der Finanzbuchhaltung und dem Warenwirtschaftssystem zu ziehen.)
- Die Daten müssen für die Analytik aufbereitet werden. Dies erfordert eindeutig definierte Datenstrukturen und Verarbeitungsverfahren. Erst wenn diese Voraussetzungen vorliegen, sollte ein Einsatz in der Praxis initiiert werden.
- Während der Vorbereitung der Datenanalyse sollte bereits geklärt werden, wie mit den erwarteten Analyseergebnissen und mit den möglichen „false positives“ umgegangen werden soll. Dies hilft, einen unklaren Status nach Durchführung einer Analyse zu vermeiden.

Data Analytics bietet grundsätzlich kosteneffiziente Lösungen, um Hinweise oder Indikatoren insbesondere in Bezug auf Fraud-Risiken wirksam und effizient zu erfassen.[19] In der Praxis ist es besonders wichtig, die erforderliche Datengrundlage exakt zu benennen, um die angestrebten Analysen durchführen zu können. Dies betrifft sowohl die zur Analyse benötigten Datenfelder und die Kenntnis ihrer jeweiligen inhaltlichen Bedeutung wie auch die zu einer Verknüpfung separater Datenbestände verwendeten Identifizierungsmerkmale. Häufig müssen benötigte Datenbestände auch zunächst noch aufbereitet (z. B. formatiert) werden, um die angestrebten Analysen durchführen zu können.

Neben technischen Grundlagen sind die Analytik-Kenntnisse der Prüferinnen und Prüfer von wesentlicher Bedeutung. Die Schulung der Anwendung von Data Analytics in Bezug auf Fraud-Konstellationen kann allerdings eingeschränkt sein. So bieten öffentlich zugängliche Datenbanken (bspw. SEC Enforcement Database, Lexis Nexis) zu bekannten Fraud-Fällen wenig für Schulungszwecke verwertbares Material. Dies ist auf mehrere Faktoren zurückzuführen:[20] Unternehmen, die Fraud-Fälle aufdecken, wollen diese regelmäßig nicht öffentlich machen, da Reputation oder finanzieller Erfolg gefährdet sein könnten. Weiterhin ändern Betrüger nach der Entdeckung meist ihre Methode. Typische Muster sind daher lediglich begrenzt für Vorhersagemodelle anwendbar.

Das darf aber nicht darüber hinwegtäuschen, dass der große Nutzen der Datenanalyse gerade im Erkennen möglicher Muster im Datenbestand liegt. Diese Muster können Hinweise auf betrügerische Handlungen liefern. Frühzeitige Überlegungen zum Ziel der

---

[19] Vgl. Kim und Vasarhelyi, 2012.
[20] Vgl. Kim und Vasarhelyi, 2012.

angestrebten Datenanalyse und zu den zu erwartenden Merkmalen (bzw. Mustern), mit denen die Zielsetzung gestützt werden kann, sind deshalb sehr wichtig. Andernfalls werden die technischen Methoden für prüferische Zwecke ggf. nur unzureichend genutzt.

4 Anwendung von Data Analytics-Verfahren zur Identifikation von Auffälligkeiten

Zur Identifikation von Auffälligkeiten und Hinweisen auf wirtschaftskriminelle Handlungen in Prozessen können datenanalytische Verfahren anhand verschiedener Ansätze herangezogen werden. Hierzu sollen die drei Ziele Prevention, Detection und Investigation unterschieden werden, deren Grenzen oft fließend verlaufen. In allen Ansätzen werden ähnliche datenanalytische Ansätze eingesetzt, jedoch mit unterschiedlicher Zielsetzung.

- Zum Beispiel dienen Datenanalysen in der Prevention der Vorbeugung von Fraud. Bereits die Etablierung und Bekanntmachung von routinemäßigen Kontrollen und Auswertungen kann eine abschreckende Wirkung entfalten.
- Bei der Detection können automatisierte Kontrollen (bspw. anhand von Listen mit ungewöhnlichen oder fragwürdigen Transaktionen, Kreditoren o. Ä.) Ansatzpunkte für vertiefte Untersuchungen liefern.
- Bei der Untersuchung konkreter Verdachtsfälle (Investigation) werden Analyse-Tools verwendet, um die Vorwürfe zu konkretisieren bzw. nachzuweisen oder auch hinsichtlich des (Schadens-)Ausmaßes zu beschreiben.

Es ist von entscheidender Bedeutung, dass die Klärung der relevanten Datenanalysemethoden – das heißt, welche Ziele auf welche Weise erreicht werden sollen – Vorrang hat, bevor eine Entscheidung über die einzusetzenden Tools getroffen wird. Die Verwendung eines Tools kann keineswegs einen gezielten Datenstrukturierungsprozess ersetzen.

4.1 Einsatzgebiete von Data Analytics

Die potenziellen Einsatzgebiete von Data Analytics im Bereich von Interner Revision, Compliance und Anti-Fraud-Management sind vielfältig. Sie variieren je nach angestrebtem Untersuchungszweck, den verfügbaren Daten und den einsetzbaren Methoden. Um ihre Verwendung effektiv und effizient zu gestalten, muss im Vorfeld der Durchführung das Ziel der Analysen klar und eindeutig festgelegt werden. Dies gilt insbesondere für Data Analytics im Bereich des Anti-Fraud Managements, da das geplante Einsatzfeld einen besonders hohen Einfluss auf die Festlegung der zu analysierenden Datenbestände, Methoden und Dokumentationsanforderungen hat. Darüber hinaus ergeben sich Fragen hinsichtlich des

adäquaten Datenschutzes und der eventuell erforderlichen, rechtzeitigen Einbeziehung von Arbeitnehmervertretern. Auch die präventive Ausarbeitung einer passenden Betriebsvereinbarung ist ein wesentlicher Aspekt, der bei der Durchführung der Analysen berücksichtigt werden sollte.

4.2 Prüferische Ziele beim Einsatz von Data Analytics

4.2.1 Prevention

Das Ziel von Data Analytics im Bereich der Prevention ist eine verbesserte Überwachung der Unternehmensprozesse und die Stärkung des Anti-Fraud-Management-Systems. Dabei werden potenzielle Schwachstellen im Internen Kontrollsystem (IKS), wie z. B. fehlende Funktionstrennungen, identifiziert. Ein weiterer Aspekt zur Stärkung des Anti Fraud-Management-Systems ist die Identifizierung sogenannter red flags, welche Hinweise auf mögliche Fraud-Handlungen geben. Beispielhaft sei hier die Umgehung von definierten Bestellprozessen oder die fehlende Nachverfolgung von überfälligen Forderungen genannt. Eine Gemeinsamkeit aller Analysen im Bereich der Prevention ist, dass diese verdachtsunabhängig und vorbeugend durchgeführt werden.

Nutzen von datenanalytischen Verfahren im Rahmen der Prevention:

- Schwachstellen in Prozessen bspw. im IKS werden erkannt. Dies ist die Grundlage für anschließende Maßnahmen zur Verbesserung der Prozesse bzw. des IKS.
- Bei Bekanntmachung des Einsatzes von Data Analytics zur Vorbeugung und zum Erkennen von Fraud können potenzielle Täter abgeschreckt werden, was die Wirksamkeit der Prävention erhöht.

Voraussetzung für die Qualität der Datenanalyse in der Prevention ist eine gute Datengrundlage. Die zu analysierenden Daten dienen als Grundlage, um herauszufinden, ob bestehende Prozesse eingehalten werden.

4.2.2 Detection

Das primäre Ziel bei der Detection ist die Entdeckung von betrügerischen Aktivitäten, die bereits stattgefunden haben. Es ist denkbar, Kontrollen oder Maßnahmen zur frühzeitigen Aufdeckung bisher unentdeckter betrügerischer Ereignisse auch ohne speziellen Anlass, beispielsweise routinemäßig oder als integraler Bestandteil des IKS, zu implementieren. Detektive Maßnahmen zielen darauf ab, betrügerische Handlungen möglichst früh zu erkennen, um eine Ausweitung des Schadens zu verhindern.[21] Grundlage für die Data Analytics im Bereich Detection können die im Rahmen der Prevention identifizierten und definierten red flags – also Warnhinweise zu potenziellen Fraud-Aktivitäten – sein.

Ziel ist das Erkennen von Anomalien oder Abweichungen in Standardprozessen, also die Identifikation von Warnhinweisen oder Verstößen bei einzelnen Vorgängen. Qualifizierendes Merkmal ist deshalb, über die Identifikation von Risiken hinaus (wie bspw. in der Prevention), die Ermittlung von Soll-Ist-Abweichungen auf Grundlage eines bekannten Soll-Zustandes. Sollten im Rahmen von Data Analytics Sachverhalte entdeckt werden, welche auf potenzielle red flags hindeuten, so sind diese im Nachgang zu untersuchen.

Weiterhin können im Rahmen der Detection identifizierte Verstöße zum Anlass genommen werden, auch in bisher nicht näher beleuchteten Unternehmensbereichen tätig zu werden.

4.2.3 Investigation

Die Investigation bezieht sich auf die anlass-, also einzelfallbezogene Untersuchung und Konkretisierung von Verdachtsfällen. Oftmals zielt sie auf die Aufklärung von Vorgängen ab, um als Grundlage für Entscheidungen zu dienen. Dies gilt insbesondere im Zusammenhang mit Schädigungen des Unternehmens und gegebenenfalls mit dem Ziel, Schadensersatz zu erlangen. Sie dient aber auch zur Schaffung einer Sachverhaltsgrundlage für Entscheidungen zu weiterführenden Maßnahmen, um z. B. Schwachstellen oder Prozessmängel zu beheben.

Ist eine Beweissicherung erforderlich, sollte diese auch zu einer gerichtsfesten Dokumentation führen. Ggf. setzt die Investigation auf zuvor gewonnenen Erkenntnissen aus der Detection auf, oder sie befasst sich mit der Evaluierung von erkannten Vorgängen aus der Detection. Da es sich um anlassbezogene Prozesse handelt, ist der Umfang der

[21] Vgl. Kümpel und Kohlhoff, 2007.

Investigation durch Orientierung an spezifischen Parametern oder Kriterien präziser abgegrenzt als bei der Detection.

Sie unterscheidet sich somit von den beiden vorangegangenen Einsatzbereichen darin, dass nicht auf potenziell kritische Fraud-Risiken abgestellt wird, sondern sich die Analyse auf einen konkreten Verdachtsfall beschränkt. Denkbar ist auch, dass Prüfungserkenntnisse zu weiterführenden (ggf. auch nicht zum ursprünglichen Untersuchungszweck gehörenden) Untersuchungen führen können.

4.3 Data Analytics: Methoden, Verfahren, Tools

Im Folgenden werden Methoden der Datenanalyse, mögliche Verfahren und Tools exemplarisch dargestellt. Es werden auch Tools genannt, die in der Praxis häufig (noch) nicht eingesetzt werden. Die Verfahren können hinsichtlich eines zunehmenden Komplexitätsgrades von a) bis d) charakterisiert werden. Damit kann auch die Aussagekraft – in Abhängigkeit von der angestrebten Nutzung – variieren.

a) *Descriptive Analytics*: Ermittlung von Tendenzen anhand von Rohdaten

   Descriptive Analytics beschäftigt sich mit der Zusammenfassung, Visualisierung und Analyse von Rohdaten, um Muster, Trends und Zusammenhänge zu identifizieren. Somit wird darauf abgezielt, das Verständnis von dem zu verbessern, was passiert ist, indem quantitative (bspw. Finanzdaten) und qualitative Daten (bspw. Merkmale operativer Prozesse) analysiert werden. Beispiele für Descriptive Analytics sind Verfahren zur Beschreibung der Charakteristika von Daten anhand tabellarischer oder graphischer Ansätze – wie z. B. Berichte und Grafiken, die Zusammenfassungen von Daten darstellen. Exemplarische Tools: Microsoft Excel, Tableau, Power BI.

b) *Diagnostic Analytics*: Ursachenanalyse durch Aufdeckung von Korrelationen zwischen Variablen und die Ermittlung kausaler Beziehungen

   Diagnostic Analytics geht einen Schritt weiter als Descriptive Analytics, indem es Ursachen und Wirkungen untersucht und sich mit der Frage beschäftigt, warum etwas passiert ist. Diese Art von Analyse erfordert in der Regel tiefere Datenanalysen und statistische Methoden, um die Zusammenhänge zwischen verschiedenen Variablen und Ereignissen zu identifizieren. Beispiele für Diagnostic Analytics sind Korrelations-, Regressions- und Ursache-Wirkungs-Analysen. Exemplarisches Verfahren: Process Mining.

c) *Predictive Analytics:* Analyse historischer Daten in Verbindung mit Branchentrends zur Vorausschau perspektivischer Entwicklungen

Verfahren zur Methode der Predictive Analytics nutzen historische Daten in Verbindung mit Branchentrends, um Vorhersagen über zukünftige Ereignisse oder Entwicklungen zu treffen. Somit wird darauf abgezielt, Vorhersagen darüber zu treffen, was in der Zukunft möglicherweise passieren wird. Bei dieser Analyseform spielen komplexe Algorithmen und Maschinenlernen sowie KI im Allgemeinen eine wichtige Rolle. Die Genauigkeit der Prognosen hängt nicht allein von der Auswahl und Leistungsfähigkeit der Algorithmen ab, sie ist auch von der Datenqualität maßgeblich bestimmt. Lückenhafte Daten schmälern die Aussagekraft der abgeleiteten Zusammenhänge. Beispiele für Predictive Analytics sind Verfahren zu Prognosen, Machine-Learning und regelbasierten Ansätzen. Exemplarische Tools: KNIME, Alteryx.

d) *Prescriptive Analytics:* Verwendung analytischer Verfahren zur Entscheidungsvorbereitung (bspw. anhand unterschiedlicher Szenarien)

Prescriptive Analytics nutzt Daten, maschinelles Lernen und Optimierungsalgorithmen, um Entscheidungen vorzubereiten. Somit sollen Verhalten und Ergebnisse durch automatisierte Entscheidungen verbessert werden. Oftmals werden hierfür verschiedene Szenarien modelliert. Beispiele für Prescriptive Analytics sind Entscheidungsunterstützungs- oder auch sog. prädiktive Wartungssysteme. Anwendungsfeld dieser Verfahren kann bspw. die Entwicklung von Prozessoptimierungen sein. Exemplarisches Tool: ACL Robotics.

Tabelle 1 zeigt eine zusammenfassende Darstellung von beispielhaft strukturierten Methoden und typischen Anwendungsfällen. Tabelle 2 führt die Prüfungsziele, die Komplexität der Anwendung und beispielhafte Tools auf. Die Zusammenstellungen zielen dabei nicht auf qualitative Aussagen bezüglich der Beispiele oder gar eine Vollständigkeit gängiger Verfahren, Tools o. Ä. ab. Es geht vielmehr um eine grundlegende Orientierung bzgl. bekannter Tools und datenanalytischer Verfahren. Ebenso werden die Tools schwerpunktmäßig den Methoden zugeordnet. Die Verwendung mit anderem methodischem Schwerpunkt ist abhängig von der gewählten Zielsetzung der Analyse möglich.

Tab. 1: Methoden und typische Anwendungsfälle

Methode und exemplarische Verfahren	**Typische Anwendungsfälle**
Descriptive	
Beschreibung von Daten und Datenstrukturen	Identifizierung auffälliger Datenmuster
Visualisierung	Darstellung von Daten für eine leichtere Interpretation
Datenkonsolidierung	Konsolidierung von Daten verschiedener Quellen
Zeitreihenanalyse	Identifikation von Anomalien
Korrelationsanalysen	Aufdeckung von Zusammenhängen zwischen Transaktionen
Diagnostic	
Regressionsanalysen	Identifikation von Zusammenhängen zwischen Faktoren
Ursache-Wirkungs-Analysen	Identifikation von Ursachen oder Faktoren, die zu Fraud führen
Varianzanalyse	Identifikation signifikanter Unterschiede in Transaktionsmustern
Clusteranalysen, Klassifikationsanalysen	Identifikation von Gruppen mit ähnlichen Mustern
Predictive	
Prognosen	Prognose, wann und wo betrügerische Aktivitäten wahrscheinlicher auftreten
Regelbasierte Analysen	Identifikation von Transaktionen zu ungewöhnlichen Zeiten oder über einen bestimmten Schwellenwert hinausgehend
Maschine Learning	Identifikation von Transaktionen auf Grundlage von Merkmalen und Mustern
Neuronale Netzwerke	Identifikation von subtilen Mustern oder Anomalien
Entscheidungsbäume	Erstellung von Regeln zur Identifikation betrügerischer Aktivitäten
Prescriptive	
Entscheidungsunterstützung	No Code- oder Low Code-Plattformen ermöglichen die einfache Entwicklung von Systemen zur Entscheidungsunterstützung.
Prozessoptimierungen	Reduktion repetitiver und manueller Tätigkeiten durch Prozessautomatisierungen
Simulationen	Simulation von Prozessen und Identifikation von Schwachstellen
Szenarioanalysen	Entdeckung von Betrugsrisiken sowie Testing von Kontrollsystemen

Tab. 2: Methoden, Ziele, Komplexität und Tools

Methode und exemplarische Verfahren	Prevention	Detection	Investigation	Komplexität	MS Standard	Statistiktools	Regelbasierte Systeme	Programmierung o. ä. Abbildung
Descriptive					Excel Power BI	Stata R Process Mining		Python (z. B. Matplotlib, Scikit, Learn, Tensorflow)
Beschreibung von Daten und Datenstrukturen	x	x		Niedrig				
Visualisierung	x	x	x	Niedrig				
Datenkonsolidierung		x	x	Niedrig				
Zeitreihenanalyse	x	x	x	Mittel				
Korrelationsanalysen		x	x	Mittel				
Diagnostic								
Regressionsanalysen		x		Hoch				
Ursache-Wirkungs-Analysen		x		Hoch				
Varianzanalyse		x	x	Hoch				
Clusteranalysen, Klassifikationsanalysen		x	x	Hoch				
Predictive							KNOW Alteryx	
Prognosen			x	Mittel	MS Power Platform Power BI			
Regelbasierte Analysen	x	x	x	Mittel				
Maschine Learning	x	x		Hoch				
Neuronale Netzwerke		x	x	Hoch				
Entscheidungsbäume		x	x	Mittel				
Prescriptive								ACL Robotics SQL Operations Research
Entscheidungsunterstützung			x	Mittel				
Prozessoptimierungen	x		x	Mittel				
Simulationen		x	x	Mittel				
Szenarioanalysen	x	x		Mittel				

Die dargelegten Analyseverfahren verdeutlichen, mit welchen Einsatzmöglichkeiten vorliegende oder zu generierende Datenbestände genutzt werden können. Gleichzeitig wird transparent, dass vorliegende Daten ohne definiertes Analyseziel und die damit verbundene Festlegung auf das erforderliche Verfahren noch keine sinnvollen Ergebnisse garantieren. Vielmehr sind die Verwendungszwecke der identifizierten und erschlossenen Daten klar abzugrenzen. Die Auswahl des angestrebten Verfahrens muss dann gleichzeitig die Analyseziele unterstützen. In der Arbeit der Internen Revision werden dabei häufig deskriptive Methoden angewandt. Die vorgenannten Beispiele zeigen sinnvolle weiterführende Möglichkeiten in Verbindung mit den bestehenden Potenzialen auf. Auch sollte bei einzusetzenden Methoden bzw. Tools das Augenmerk auf eine nicht zu hohe Komplexität

gelegt werden. Andernfalls könnten Komplexität und Präferenzen der Prüfungsleitung zu verzerrten Beurteilungen von Prüfungsnachweisen führen.[22]

Um die praktischen Vorgehensweisen bei Datenanalysen weiter zu konkretisieren, folgt eine Erläuterung der Analyseprozesse unter Differenzierung nach präventiven, detektiven oder investigativen Zielsetzungen.

[22] Vgl. Koreff et al., 2023.

5 Vorgehensweise bei der Datenanalyse

5.1 Wichtige Rahmenbedingungen für die Analytik

Im Folgenden wird ein Überblick über Kernelemente zur Durchführung der Datenanalytik gegeben. Ziel ist die Darstellung wichtiger Schritte von der Planung über die Umsetzung der Datenanalyse bis zu notwendigen Abstimmungs- bzw. Qualitätssicherungsschritten. In allen beschriebenen Fällen sollten die Ergebnisse der Datenanalytik anhand der bestehenden Prozesse zumindest initial auch mit den verantwortlichen Fachbereichen qualitätsgesichert werden (wenn nicht der konkrete Zweck und Gegenstand investigativer Analysen dagegenspricht). Die Fachbereiche kennen im Regelfall aus dem praktischen Tagesgeschäft resultierende Konstellationen und Beschränkungen. Die Qualitätssicherung hilft, wenig praxisrelevante Konstellationen auszuschließen bzw. die Menge eventuell unzutreffender Analyseergebnisse (false positives) zu reduzieren. Fehlt die Abstimmung, kann dies ggf. zu strittigen Ergebnissen führen, die zu Zweifeln an der Sinnhaftigkeit von Datenanalysen führen können.

5.2 Generische Prozesselemente der Datenanalyse

Abbildung 1 zeigt eine grundlegende Übersicht über die anzuwendende Vorgehensweise zur Vorbereitung und Durchführung einer Datenanalyse.

Abb. 1: Vorgehensweise bei Vorbereitung und Durchführung einer Datenanalyse

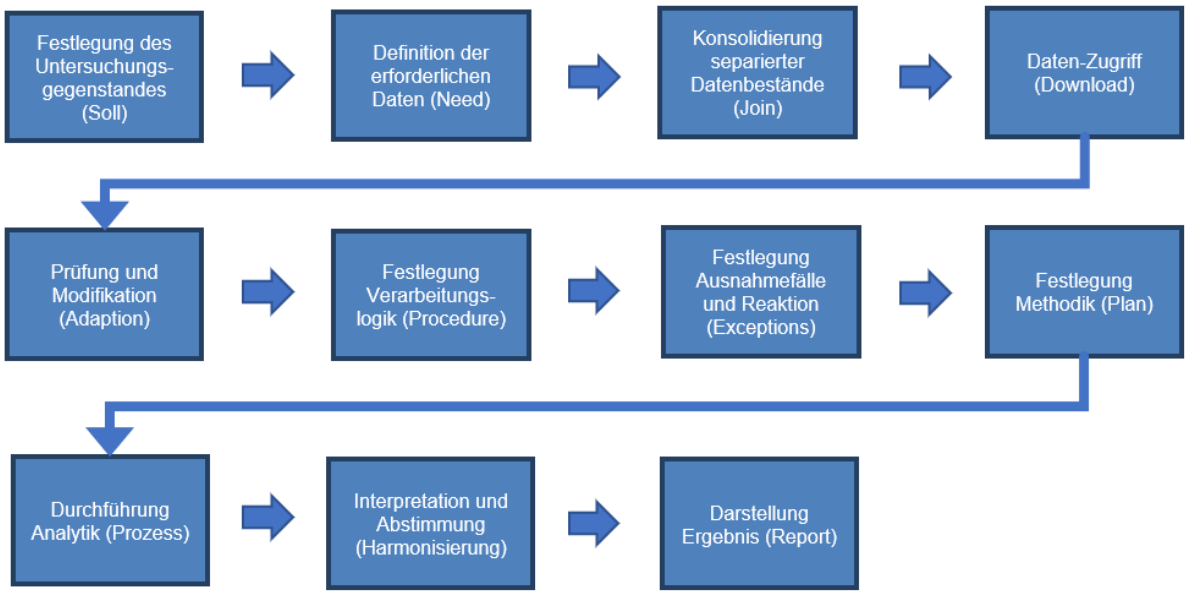

Tabelle 3 liefert eine generische Übersicht und strukturierte Abbildung der Vorgehensweise bei der Analyse unter der jeweiligen Zielsetzung Prevention, Detection und Investigation.

Tab. 3: Vorgehen bei Prevention, Detection und Investigation

	Prevention	Detection	Investigation
SOLL			
Vorliegen eines Sollkonzepts Um Abweichungen zu identifizieren, ist ein Soll-Maßstab erforderlich. Auf dieser Grundlage können die folgenden Schritte konkreter benannt werden.	X	X	
Festlegung Schwerpunkt Detection Bspw. eingehende/ausgehende Zahlungen in andere Länder als bei den bisherigen Lieferungen. Erforderlich ist die Zielsetzung der Analyse. Erst dann können		X	

	Prevention	Detection	Investigation
die relevanten (Teil-)Prozesse und die benötigten Daten eindeutig benannt werden.			
Ausgangspunkt: Verdacht Ausgangspunkt ist in der Regel ein zu konkretisierender bzw. zu belegender Verdacht. Dies bedeutet, dass der Verdacht so eindeutig bzw. spezifisch wie möglich beschrieben sein sollte. Erst dann ist eine verlässliche Basis für die durchzuführenden Analysen vorhanden.			X
Identifikation der risikobehafteten Bereiche bzw. Prozesse Welche Unternehmensbereiche oder welche risikobehafteten Prozesse sollen einer besonderen Überwachung durch Datenanalysen unterworfen werden?	X	X	
NEED			
Identifikation relevanter Datenbestände Im Zusammenhang mit der Identifikation der risikobehafteten Bereiche: Welche Datenbestände/Datenbanken/Anwendungen werden von den identifizierten Prozessen/Teilprozessen verwendet? Eventuell liegen Beschränkungen bei Zugriffsberechtigungen vor. Dies ist zu lösen, andernfalls kann die angestrebte Analyse ggf. nicht gelingen oder zu unerwünschten Ergebnissen führen.	X	X	X
Ergänzung separierter Daten Sind für die Zwecke der Datenanalyse originär separierte Datenbestände notwendig (bspw. aus Finanzbuchhaltung und Materialwirtschaft oder Einkauf), so sollte geklärt werden, ob ggf. die Zusammenführung bestimmter identifizierter Daten in zuvor getrennten Beständen sinnvoll ist.	X	X	X
JOIN			
Datenaufbereitung (bspw. join getrennter Daten, cleansing) Dies gilt für den Fall, wenn erst zusammengeführte Daten erlauben, das zu betrachtende Feld zu erschließen (bspw. Bestellsystem- und Warenwirtschaftsdaten, um unzulässige Bestellungen zu identifizieren). Regelmäßig sollte dabei das Risiko eines Datenschutz-Verstoßes bedacht werden.	X	X	X
DOWNLOAD			
Zugriff auf die benötigten oder für die Analyse festgelegten Daten Grundsätzlich besteht die Möglichkeit, der Revision den benötigten Zugriff auf die Daten zu gewähren. Dies erfordert Zugriffsberechtigungen, aber auch die Einweisung in den technischen Zugriff auf die Daten (Training). Möglich ist, dass die IT-Abteilung die Daten in verarbeitbarer Form zur Verfügung stellt. Dies hat den Nachteil, dass sich die Revision in Abhängigkeit zu der Verfügbarkeit der IT und	X	X	X

	Prevention	Detection	Investigation
des IT-Personals begibt, was inhaltliche oder zeitliche Beschränkungen zur Folge haben kann.			
ADAPTION			
Festlegung kritischer Konstellationen und Prozessschritte Welche Konstellationen machen es erforderlich, vor Durchführung der Analyse eventuell Datenbereinigungen oder zusätzliche Downloads durchzuführen? Datenformate und Relationen müssen bekannt sein. Bei lückenhaften Daten oder bei im vorangegangenen Schritt erkanntem Verbesserungsbedarf ist es sinnvoll, Lösungsmöglichkeiten zur Sicherstellung korrekter Daten zu finden. Andernfalls kann der gewünschte Zweck der Analyse ggf. nicht erreicht werden.	X	X	X
PROCEDURE			
Festlegung des anzuwendenden Verfahrens Zur Erreichung des angestrebten Ziels ist die Festlegung der Verarbeitungslogik vor Beginn der Analyse notwendig. Andernfalls kann die Verarbeitung (und damit das Analyseergebnis) von der Form oder Verfügbarkeit der vorliegenden Daten beeinflusst werden. Die Objektivität der Ergebnisse könnte ggf. gefährdet sein.	X	X	X
EXCEPTIONS			
Festlegung der Verarbeitungsregeln für Besonderheiten Vor Beginn der Datenanalyse sollte (nachvollziehbar) festgelegt werden, wie mit unerwarteten Datenkonstellationen umgegangen werden soll. Dies betrifft insbesondere false positives. Sonst entsprechen die ausgewiesenen Ergebnisse der Analyse nur vordergründig dem angestrebten Ziel und sind nicht objektiv. Dies erfordert ggf. die Eingrenzung der definierten Zielmenge (Orientierung an Adaption und Procedure). Auch eine zu umfangreiche Ergebnismenge, z. B. weil die Analyse unzureichend eingegrenzt wurde, erfordert zusätzliche Maßnahmen. Ansonsten können Ergebnisse ggf. nicht weiterverwendet werden.	X	X	X
PLAN			
Festlegung der Datenverarbeitungsmethodik Abhängig vom angestrebten Ziel (Soll) und den verfügbaren Daten sollte die Methodik (deskriptiv, diagnostisch, prädiktiv, präskriptiv) für die Analyse festgelegt werden.	X	X	X
Wahl des einzusetzenden Tools Mit der Festlegung auf die relevante Methodik kann die Festlegung auf das zu verwendende Tool erfolgen. Wenn die Voraussetzungen aufgrund fehlender Lizenz nicht gegeben sind, kann das Ziel der Analyse ggf. nicht erreicht werden. Die Methode kann bestimmend für die zu verwendenden Tools sein. Oder die	X	X	X

	Prevention	Detection	Investigation
verfügbaren Tools bestimmen umgekehrt die im Unternehmen erzielbaren Analysezwecke.			
PROCESS			
Analytik Durchführung der Analyse unter Kenntnis des vorliegenden Datenmaterials. Überlegungen zum angestrebten Output unter Beachtung der identifizierten Daten. Sicherstellung der Berücksichtigung der mit der Analytik angestrebten Zielsetzung.	X	X	X
HARMONISIERUNG			
Modifikationen Sollten die erzielten Ergebnisse nicht eindeutig sein, d. h. eine unerwünscht große Trefferzahl liefern oder dem gewünschten Analysezweck nicht entsprechen, so kann eine Abwandlung des gewählten Ansatzes, die Verwendung weiterer oder anderer Daten oder die Konkretisierung des angestrebten Ergebnisses sinnvoll sein. Auf keinen Fall sollten nicht befriedigende Ergebnisse ohne weiteres Nachfassen zum Abbruch der vorgesehenen Datenanalyse führen.	X	X	X
Feedback Die vorliegenden Ergebnisse sollten hinsichtlich ihrer Güte oder eines eventuellen Nachbesserungsbedarfs überprüft werden. Inwiefern sind die Ergebnisse ausreichend, um die angestrebten Ziele zu erreichen und zu dokumentieren?			X
Evaluation der Ergebnisse Die gewonnenen Ergebnisse sollten mit den Prozessverantwortlichen besprochen werden. Dies dient der Qualitätssicherung. Falsche Rückschlüsse können ggf. vermieden, die Erkenntnisse in den richtigen Kontext gestellt und zielgerichtet bzw. priorisiert die notwendigen Verbesserungsmaßnahmen vereinbart werden. Außerdem ist eine Abstimmung häufig ein notwendiger Schritt, um die erzielten Ergebnisse korrekt zu interpretieren.	X	X	
Evaluation der Ergebnisse mit Dritten Abstimmung der erzielten Ergebnisse mit den Auftraggebern: Passen die Ergebnisse zum angestrebten Analyseziel? Spiegeln sich die originär erhobenen Vorwürfe in den ermittelten Analyseergebnissen wider?			X
Interpretation der Daten Sind die Ergebnisse stichhaltig in Bezug auf die angestrebten Ziele und liegt die erforderliche Dokumentation vor? Sollten die Ergebnisse nicht hinreichend sein, sind mit dem Auftraggeber ggf. zusätzliche Analysen oder Nachdokumentationen	X	X	X

	Prevention	Detection	Investigation
zu vereinbaren. Daher sollten diese Punkte frühzeitig geklärt werden. Dies gilt insbesondere bei investigativen Untersuchungen für die Berücksichtigung gesetzlicher Fristen.			
Aufklärungsgespräche Da Ergebnisse investigativer Analysen häufig weiterführender Klärung mit Beteiligten, Informationsgebern und Verdächtigten bedürfen, sollten die Anforderungen seitens beteiligter anderer Parteien dafür frühzeitig bekannt sein.			X
REPORT			
Berichterstattung Die Analyseergebnisse sollten adressatengerecht aufbereitet und kommuniziert werden. Mögliche weitergehende Analyseerfordernisse (bspw. aus den ermittelten Ergebnissen entstehender zusätzlicher Analysebedarf) sollten transparent gemacht werden, auch, um die Erwartung an die Leistungsfähigkeit analytischer Verfahren korrekt einordnen zu können.	X	X	X
Dokumentation Die Dokumentation der durchgeführten Arbeiten sollte vollständig sein, so dass der gewählte Ansatz und die Vorgehensweise auch nachvollziehbar sind.	X	X	X
Verwendung durch Dritte Die Dokumentation muss so strukturiert sein, dass sie vollständig die Anforderungen an Gerichtsverwertbarkeit erfüllt.			X

In allen Fällen ist für eine erfolgreiche Anwendung von Datenanalysen zu beachten, dass die verwendeten Daten per se noch keine Erkenntnisse liefern. Erst die detaillierte Analyse und anschließende Interpretation liefert die notwendigen Rückschlüsse und damit die gewünschte Information.

6 Herausforderungen/Kritische Parameter bei Datenanalysen

Die folgenden Ausführungen zeigen dem Anwender datenanalytischer Methoden, Verfahren und Tools zu beachtende kritische Fragestellungen auf. Sie können für eine erfolgreiche Anwendung bzw. Umsetzung von Bedeutung sein. Hierbei zeigt sich deutlich die Vielzahl und die hohe Komplexität zu beachtender Fragestellungen bei der Einführung oder dem Ausbau datenanalytischer Verfahren. Die angesprochenen Themen sollten zunächst geklärt und bei der praktischen Anwendung regelmäßig hinterfragt werden. Zu berücksichtigen sind dabei insbesondere organisatorische und technische, aber auch rechtliche Aspekte. Der Datenschutz spielt eine wesentliche Rolle. Weiterhin ist besonderes Augenmerk auf die datenanalytischen Kenntnisse der Prüferinnen und Prüfer zu lenken und für eine ausreichende Ausbildung zu sorgen. Dies gilt sowohl für die Verwendung der Verfahren als auch für die Interpretation der generierten Ergebnisse. Ebenso sind die Kennnisse über die zu verwendenden Datenbestände und der für die Analysezwecke benötigten Datenfeldinhalte entscheidend.

Organisatorische und prozessuale Fragestellungen

- Gibt es aus anderen Bereichen (z. B. Controlling) bereits bestehende analytische Verfahren, von denen die Revision profitieren kann? Ggf. ist ein Combined-Assurance-Ansatz in Erwägung zu ziehen.
- Welche Erfahrungen bestehen im IT-Bereich (Tabellenstrukturen, bestehende Abfragen)? Ggf. ist ein Combined-Assurance-Ansatz in Erwägung zu ziehen.
- Wie erfolgt die Abgrenzung der Aufgaben innerhalb des Drei-Linien-Modells? Wer ist für die Analysen zuständig, auch hinsichtlich der Ergebnisse? Es ist eine Abgrenzung zwischen Continuous Monitoring und Continuous Auditing zu treffen.
- Welche Empfehlungen können für die Interaktion zwischen den beteiligten Parteien abgeleitet werden? Was wären bestimmende Faktoren oder KPIs?
- Wie wird die Aufgabe organisatorisch abgebildet? (ein Experte, alle Mitarbeiter als Experten oder ggf. eine Make-or-Buy-Entscheidung)
- Was passiert mit den Ergebnissen, bspw. wenn zu viele Treffer erzielt werden?
- Gibt es eine Erwartungslücke? Was kann Ergebnis sein, was nicht?
- Welche Datenquellen stehen zur Verfügung? Wer kann bei der Datenbeschaffung behilflich sein?
- Wer darf in einem Fraud-Verdachtsfall informiert werden? Wie wird sichergestellt, dass bei der Datenbeschaffung die Datenintegrität gewahrt wird?

Anforderungen aus Technik und Datenstruktur

- Welchen Einfluss hat die bestehende Datenstruktur auf die Anwendbarkeit von Datenanalysen? (homogene Daten oder Datenintegration)
- Welche Daten werden für die jeweilige Analyse benötigt (bspw. Datenpool für Process Mining vs. punktuelle Datenbestände)?
- Welche logischen Verknüpfungen bestehen zwischen den Daten und müssen ggf. berücksichtigt werden?
- Welcher Ressourcenbedarf resultiert aus der Datenstruktur? (Zugriff und Datendownload nur unter Einbeziehung Dritter, Laufzeit von Downloads oder Analysen, Speicherplatzbedarf)

Berücksichtigung relevanter rechtlicher Rahmenbedingungen

- Welche Fragen des Datenschutzes und unterschiedlicher Rechtsnormen in verschiedenen Jurisdiktionen müssen initial geklärt werden?
- Wie können Anforderungen des Datenschutzes in der Prüfungspraxis eingehalten werden?
- Gibt es branchenspezifische Anforderungen, z. B. Versicherungsaufsichtliche Anforderungen an die IT (VAIT)? Resultieren hieraus besondere Anforderungen, z. B. an die Informationssicherheit?
- Gibt es weitere Anforderungen, z. B. Mitbestimmungsrechte der Arbeitnehmervertretung?

Dokumentationserfordernisse

- Welche besonderen Dokumentationsanforderungen bestehen für unterschiedliche Anwendungsziele? Zeichnet sich bspw. ab, dass die Nachweisführung als Beweismittel im Rahmen straf-, arbeitsrechtlicher oder ziviler Klagen verwendet wird, sind die Grundsätze einer gerichtsfesten Dokumentation zu erfüllen.
- Unterliegen die Unterlagen einer besonderen Aufbewahrungsfrist?

Anforderungen an die Qualifikation der Anwender

- Welche Qualifikation ist für die Aufgaben erforderlich?
- Wie sind die Qualifikationsanforderungen an die Datenanalysen zu erfüllen?
- Wie wird sichergestellt, dass das erforderliche Verständnis für Datenanalyseinstrumente und -methoden und den praktischen Einsatz besteht?
- Welche Prozess- und welche Fraud-Expertise wird von den verantwortlichen Prüferinnen und Prüfern erwartet?

- Welche Abstimmung der ermittelten Ergebnisse mit den Prozessexperten ist erforderlich?
- Handelt es sich um große Datenmengen, die z. B. mit Hilfe eines bestimmten Verfahrens übertragen werden müssen? Welche Expertise ist diesbezüglich erforderlich?

Fragen zum anwendbaren Verfahren/Tool

- Genügt ein unspezifisches Tool für die Analyse der Daten (bspw. MS-Excel oder ein vorgefertigter Pool an Analysen unter Verwendung von ACL) oder ist eine Spezialanwendung erforderlich? Ist diese Spezialanwendung aufgrund ihres spezifischen Datenbedarfs ggf. eigenständig zu entwickeln?
- Welche Kosten sind zu erwarten? (Entscheidungsvorbereitung zur Anwendung des Tools)
- Gibt es Einflüsse auf die Zusammenarbeit mit dem Abschlussprüfer und sonstigen Stakeholdern? (Co-Sourcing der Internen Revision)
- Was zeichnet eine zu identifizierende Abweichung aus, bzw. was ist noch in Ordnung? (Toleranzbereich)
- Wie ist mit red flags umzugehen? Wer muss ggf. beim Vorliegen sofort informiert werden?
- Welche Überlegungen gibt es zur Abwägung der Eingrenzung von red flags?

7 Datenanalysen und Datenschutz

Spätestens mit der Einführung der EU-DSGVO, die seit dem 25. Mai 2018 anzuwenden ist, hat der Datenschutz eine wichtige Rolle bei der Verwendung personenbezogener Daten in den betrieblichen Abläufen erlangt. Wichtige Anhaltspunkte für die Berücksichtigung datenschutzrechtlicher Themenfelder in der Revisionsarbeit liefert der „Leitfaden Interne Revision und Datenschutz“ des DIIR-Arbeitskreises „Datenschutz und Data Governance“.[23]

Neben Beschäftigtendaten (Kapitel 2.3) enthält der Leitfaden ein Kapitel zu unternehmensinternen Ermittlungen (Kapitel 2.4). Die Berücksichtigung des Leifadens wird in Ergänzung zu diesem Fachbeitrag dringend empfohlen, um datenschutzrechtlich konforme Analysen sicherzustellen.

[23] Vgl. DIIR, 2021. Für datenanalytische Verfahren im Zusammenhang mit Prevention, Detection und Investigation sollten regelmäßig datenschutzkonforme Vorgehensweisen etabliert sein, um erzielte Ergebnisse (insbesondere für die Investigation) nicht angreifbar zu machen. Wesentliche Beachtung verdienen daher die folgenden Anforderungen an die Datenverarbeitung:

- Rechtmäßigkeit (Verarbeitung nach Treu und Glauben, Transparenz),
- Zweckbindung (Erhebung nur für definierte Zwecke),
- Datenminimierung (Zweckangemessenheit),
- Speicherbegrenzung (Dauer), Integrität und Vertraulichkeit (Zweckbindung) sowie sachliche Richtigkeit (dem Verarbeitungszweck dienend).

8 Beispiele für praktische Fallkonstellationen: Zu verwendende Datenbestände

Für den Erfolg des Einsatzes datenanalytischer Verfahren ist die gezielte und systematische Verwendung spezifischer Datenbestände sowie die Qualität der Daten (bspw. Vollständigkeit, Eindeutigkeit) entscheidend. Je nach Zweck der Verarbeitung bzw. angestrebten Ergebnissen kann es sinnvoll oder sogar notwendig sein, Auszüge von bestehenden Datenbeständen oder die Kombination verschiedener Datenbestände zu generieren. Darüber hinaus bedingt die Vielfalt betrügerischer Handlungsmöglichkeiten eine Vielzahl potenziell heranzuziehender unterschiedlicher Datenquellen, um nach Indizien für Fraud suchen zu können.

Die Arbeitsgruppe Datenanalysen des DIIR-Arbeitskreises Anti-Fraud-Management, Compliance und Interne Revision hat in der Tabelle 4 eine Liste ausgewählter Beispiele für zu Analysezwecken verwendbare Datenquellen zusammengestellt. Mit dieser Aufstellung wird interessierten neuen Anwendern datenanalytischer Verfahren, aber auch Erfahrenen, eine Anregung zu Themenfeldern für Analysen gegeben. Ausgehend von einer etablierten Kategorisierung des ACFE[24] finden sich zudem Beispiele zu unterschiedlichen Vorgängen doloser Handlungen. Diese beschreiben Datenbestände, die für eine Suche nach geeigneten Indizien für Fraud herangezogen werden können. Sofern möglich, werden die genannten Datenbestände um praxisbezogene Hinweise zu Konstellationen, die aus dem Datenmaterial erschlossen werden können, ergänzt.

Die Benennung der Datenquellen ist generisch und software- bzw. systemunabhängig. Für Interessierte ist (in Absprache mit der IT-Abteilung) eine Präzisierung auf die eigenen unternehmensinternen Datenquellen möglich. Ziel muss es sein, die lokalen Gegebenheiten präzise zu erfassen und die verfügbaren Datenstrukturen konkret zu benennen. Hieraus ist die Zugriffslogik (Extrakt, Download, Schaffung eines Zwischenspeichers oder einer eigenen Verarbeitungsdatenbank) abzuleiten.

[24] Vgl. ACFE, 2022.

Tab. 4: Beispiele für zu Analysezwecken verwendbare Datenquellen

Typ			Datenquellen	Relevante Auffälligkeit/red flags
I. VERMÖGENSSCHÄDIGUNGEN				
I.1 Cash				
a. Kassenbestand			Daten aus Kassenbuch oder Kassenkonto: Kassentransaktionssalden, Kasseninventurdifferenzen, Einzahlungs- und Auszahlungsbelege	Ausbuchung von Zähldifferenzen
b. Geldeingänge				
Abschöpfung (Skimming)	Umsätze	nicht erfasste	Daten aus FiBu zu Umsätzen und Beständen	Abgleich Umsätze und Bestände
	Umsätze	unterbewertete	Daten aus FiBu zu Umsätzen	Ungewöhnliche Rabatte oder Preisnachlässe
	Forderungen	Abschreibungen	Daten aus FiBu zu: Forderungsbestand, Veränderungen der Forderungsbestände zu definierten Stichtagen, Abschreibungen, Abschreibungsbeträge zu definierten Stichtagen, Zuordnung oder Referenzierungsdaten der Abschreibungen zu den Forderungen	Auffällige Abschreibungsbeträge intransparente Abschreibungen (Buchungstext) fehlende eindeutige Zuordnung der Abschreibungen zu Forderungen Abschreibungsbeträge gleicher Höhe oder wiederholte Abschreibung gleicher Beträge
	Forderungen	Überlagerungen (Kumulationen)	Daten aus der Debitorenbuchhaltung (Einzelpostenebene), insb. Stornierungen und Gutschriften Daten zu Zahlungsmittelzuflüssen und deren Kontierung	Unangemessene Darstellung der Werthaltigkeit von Forderungen: fiktive Zahlungen auf überfälligen Debitorenkonten Stornierung und erneutes Einbuchen falsche Darstellung der Altersstruktur
	Forderungen	Offene		
	Rückerstattungen			

Typ			Datenquellen	Relevante Auffälligkeit/red flags
Bargeld-Diebstahl i. S. v. Veruntreuung			Daten aus Kassenbuch oder Kassenkonto: Kassentransaktionssalden, Kasseninventurdifferenzen, Einzahlungs- und Auszahlungsbelege Berechtigungsdaten und Änderungslogs	Auffällige oder fehlende Buchungstexte SoD-Konflikte: Bereicherung durch Vereinigung der Berechtigungen für Kassenbuchungen, Kreditorenbuchungen, Reisekostenbuchungen, Autorisierung von Zahlungstransaktionen (Bankvollmacht)
c. Auszahlungsbetrug				
Rechnungsstellung	Briefkastenfirma		Daten aus FiBu: Kreditorenstammdaten und Rechungskopfdaten, Änderungsbelege (Stammdatenänderungen)	Kreditorenstammdaten und Rechnungsdaten laufen auf eine PO-Box-Adresse, es liegt keine andere Adresse vor Adressdaten eines inaktiven Kreditors wurden nach längerer Inaktivität auf PO-Box-Adresse umgestellt Lieferantenkategorie bzw. -branche ist untypisch für Briefkastenadressen, z. B. produzierendes Gewerbe (Teillieferant)
	Lieferant		Daten aus FiBu: Kreditorenstammdaten, Bestell-, Wareneingangs-, Rechnungs- und Zahlungstransaktionsdaten, Änderungsbelege (Bankstammdatenänderungen)	Überzahlungen Doppelzahlungen: Transaktionen mit gleicher Rechnungsnummer, gleichem Rechnungsbetrag am gleichen Tag (an einen oder mehrere Kreditoren) Wrong vendor scheme: Doppelte Adressen in Lieferantenstammdaten Ausreißer in Beträgen, die in Rechnung gestellt wurden, glatte Beträge Zahlungen ohne Bestellung Zahlungen an Lieferanten, die nicht als Kreditor angelegt sind

Typ			Datenquellen	Relevante Auffälligkeit/red flags
	Privateinkäufe		Daten FiBu zu Kassenbuchungen: Kassentransaktionen, Rechnungs- und Lieferungskopfdaten Daten aus FiBu zu Reisekosten und Geschenkekonten): Reisekostenabrechnungen, Rechnungsdaten Daten aus dem Warenbestellsystem wie Bestellung und Bestellender Daten über die den Warenempfang bestätigenden Person aus dem Warenlagermanagement-System Daten des definierten Warenkatalogs	Rechnungs- oder Lieferadresse ist keine Firmenadresse Wiederkehrende Ausgaben mit scheinbarem generischen Geschäftsbezug (bspw. Kunden-, Messebesuch, branchenuntypische Geschenke für Geschäftspartner), jedoch Privatcharakter, z. B. Supermärkte, Baumärkte, bei denen die Lieferantenadresse mit der Mitarbeiteradresse übereineinstimmt Geschäftsessen an Wochenenden/am Freitagabend mit jeweils einem Geschäftspartner Fehlendes 4-Augen-Prinzip, Hierarchielevel Einkäufe um die Weihnachtszeit Fehlende Funktionstrennung zwischen Bestellendem und Warenempfänger Rechnungsfreigabe vor Wareneingangsbestätigung: häufige Warenbestandskorrekturen Bestellung von Artikeln abweichend vom definierten Warenkatalog Lieferadresse weicht von der Adresse des bestellenden Unternehmens ab fehlende Bestellanforderung Wareneingang ohne Bestellung
Gehaltsabrechnung	Fiktiver Beschäftigter (Lohn- und Gehaltszahlungen auf den Namen fiktiver oder		Daten aus Personalakte (E-Akte) bzw. Personalstammdaten, Personalzeitwirtschaftssystem, und -abrechnungssystem, Active	Unstimmigkeiten zwischen bilanziellen und unternehmensinternen Informationen

Typ			Datenquellen	Relevante Auffälligkeit/red flags
	ausgeschiedener Mitarbeiter)		Directory Einträge oder andere IT-Systeme zur Regelung von Zugriff und Zutritt (Bewegungsdaten) Daten aus Personalmanagement-System wie Personalstammdaten, elektronische Personalakte Daten aus Zeiterfassungssystemen Daten aus den Systemen zur Freigabe von Urlaubsanträgen	Fehlende Dokumente/Anlagen in Personalakte Fehlende Adressdaten in Personalstammdaten Ungültige oder fehlende Sozialversicherungsnummer Wiederkehrende oder identische Zeiteinträge im Zeitwirtschaftssystem Ausschließlich manuelle Zeiteinträge/-korrekturen im Zeitwirtschaftssystem bei elektronischer Erfassung Keine Krankheits- oder Urlaubseinträge in PT Fehlende Abzüge in Gehaltsabrechnung zur Sozialversicherung Eintrag im Zutrittssystem erfolgt ohne korrespondierende UserID/E-Mail-Adresse/PC-Login Doppelte Mitarbeiter-Bankverbindungen Unvollständige Personalstammdaten (z. B. Kostenstelle, Abteilung, Urlaubsanspruch) Unvollständige (elektronische) Personalakte (z. B. unterzeichneter Arbeitsvertrag, Ausweiskopie) Mitarbeiter mit kumulierten Urlaubsansprüchen Abweichung der Anzahl der Personen zwischen Personalmanagement-System und Zeiterfassungssystem Urlaubsanträge von Mitarbeitern werden nicht im definierten Freigabesystem erfasst.

Typ			Datenquellen	Relevante Auffälligkeit/red flags
	Falschabrechnungen		Daten aus Personalzeitwirtschaftssystem (PT), Personalabrechnungssystem (PY)	Regelmäßige Überstunden über einem bestimmten Stundensatz (z. B. 48 h) oder prozentual über vertraglich vereinbarter Arbeitszeit (z. B. wöchentliche Arbeitszeitüberschreitung um 20 %) Manipulierte Zeiteinträge im Zeitwirtschaftssystem, z. B. über konsistente Muster der Zeiteinträge Abweichungen zwischen Stechzeiten am Zeiterfassungssystem und Stundenberechnung in Payroll (PY und PT stimmen nicht überein bzw. sind nicht überführbar)
	Provisionsschemata			
Auslagenerstattungen	Falschdeklaration		Daten aus Kassenbuch/Kassenkonto/Spenden- und Sponsoringkonten/Reisekostenabrechnung	Tarnung einer privaten Ausgabe als geschäftlich veranlasste Ausgabe: Rechnungsdatum stimmt nicht mit Reise- oder Entertainmentdatum (Zweck) überein Deklaration oder Buchung von Ausgaben als Spenden und Sponsoringaktivitäten, obwohl es sich nicht um Spenden handelt oder privater Natur sind (z. B. Eigentümerspende an Kirche zu Weihnachten)
	Überhöhte Auslagen		Daten aus FiBu insb. zu Stornierungen, Belegen	Manipulierte Belege Eigenbelege anstelle von Originalbelegen Stornierungen des Kaufs einer teureren Leistung und Kauf eines ähnlichen Produkts zu einem geringeren Wert, aber Einreichung der höheren Rechnung zur Erstattung

Typ			Datenquellen	Relevante Auffälligkeit/red flags
	Fiktive Auslagen		Daten aus Kassenbuch/Kassenkonto/Reisekostenabrechnung: Barvorschussbuchungen, Eigenbelegerstattungen	Barvorschüsse als Kurzzeitkredit und Erstattung fiktiver Auslagen über Eigenbelege (z. B. Einreichung über Reisekostenabrechnung): Barvorschuss wird innerhalb kürzester Zeit in voller Höhe zurückerstattet und im gleichen Zeitraum erfolgt die Einreichung von Eigenbelegen Eigenbelege über untypische Positionen oder in ähnlicher Höhe wie der Barvorschuss
	Mehrfacherstattungen		Daten aus FiBu: Doppelte Rechnungen (Betrag, Rechnungsdatum, Lieferant, Position(en) sind gleich)	Supervisor swap scheme (hierzu Kostenstellenanalyse)
Scheck- und Zahlungsbetrug	Gefälschter Aussteller			
	Gefälschte Vermerke			
	Geänderter Zahlungsempfänger		Daten aus Zahllaufsystemen, wie Zahlungsvorschlagsliste, Zahllaufliste, elektronischer Bankkontoauszug	Manuelle Zahlläufe für Standardtransaktionen Verwendete Bankverbindung weicht von Lieferantenstammdaten ab Häufiger Abbruch von Zahlungsvorschlagslisten
	Autorisierter Aussteller			
Rückerstattungen	Fingierter Beleg		Daten aus der Buchhaltung (Belegebene)	Falsche Datierung oder Belegfälschung Abgleich von Belegnummern, Sichtprüfung ob Auffälligkeiten (z. B. eingescannte Unterschriften o. Ä.) bestehen Doppelprüfung
	Fingierte Erstattung			

Typ			Datenquellen	Relevante Auffälligkeit/red flags
	Konto pro Diverse (CPD)		Buchhaltung	Z. B. häufige Nutzung, wiederholte Kreditoren/Bankverbindungen
d. Versicherungsbetrug				
Beanspruchung von Versicherungsleistungen in betrügerischer Absicht	Fingierte Schäden		Verträge, Vorschäden, Vertragsänderungen, Zahlungsverhalten, Schadenunterlagen, Schadenanzeigen, Belege und Rechnungen	Atypische Schadenverläufe (außergewöhnliche Schadenhäufung in einem bestimmten Zeitraum)
	Vorsätzliche Herbeiführung		Belege und Rechnungen	Besondere Schadenverläufe (Überschreitung einer gewissen Schadenhöhe, z.B. Fahrzeugschäden, die fiktiv auf Basis eines Gutachtens oder eines Kostenvoranschlags abgerechnet werden)
	Übertreibung		Zahlungen	Auffälligkeiten im Schaden- oder Leistungsfall (Schadenhergang)
	Umdefinitionen		Verträge, Vertragsänderungen	Abgeschlossene Lebens- und Berufsunfähigkeitsversicherungen (Überversicherung)
e. Krediterschleichung (Insolvenzverschleierung)			Dokumentenmanagementsystem	Unstimmigkeiten bei Buchungsroutinen und Zahlungsvorgängen mit Auswirkung auf das Controlling
f. Geldwäsche				

Typ			Datenquellen	Relevante Auffälligkeit/red flags
Zahlungstransfers zum Zweck der Geldwäsche			Buchhaltung (Belegebene), Zahlungstransaktionsdaten, Kreditoren- und Debitorenstammdaten (insb. Bankstammdaten), Kontoauszüge	Zahlungen an Empfänger in einem anderen Land als dem Ursprungsland von bezogenen Waren und Dienstleistungen Smurfing: Aufteilung des Geldbetrags in mehrere kleine Tranchen Verschleierung der ausgehenden Zahlung über Versicherungsprodukte (sofortige oder aufgeschobene Annuitäten), investmentbezogene Transaktionen (z. B. Sicherheiten), Nutzung von nichtbankbezogenen Finanzdienstleistungen Zahlungen an Länder, die es erlauben, dass der Kontoinhaber keiner natürlichen Person zugeordnet werden kann Zahlungen an Vermittler, Treuhänder oder Mantelgesellschaften mit Auslandsbankkonten in Steuerparadiesen oder Ländern mit strengen Bankgeheimnisgesetzen Zahlungen mit digitalen Währungen
g. Diebstahl				
Bestellanforderung				
Fingierter Umsatz und Versand			Daten aus Beschwerdemanagement-System Daten aus Carrier System Daten aus FiBu: Abschreibung von Forderungen, Ausbuchung von Forderungen, Altersstruktur von Forderungen, manuelle Umsatzbuchungen	Anstieg von Kundenbeschwerden über fehlende/unvollständige Warenlieferung Inkonsistenz zwischen aufgezeichneten Warenausgängen und Speditionsdaten Wertberichtigung/Ausbuchung von Forderungen ohne relevanten Hintergrund Überfällige Forderungen: Bei manueller Umsatzbuchung wird

Typ			Datenquellen	Relevante Auffälligkeit/red flags
				als Gegenkonto ein Konto außerhalb der definierten Kontenklasse verwendet, z. B. Aufwandskonto.
Bestellung und Wareneingang			Daten aus Bestellsystemen Daten über den Besteller aus dem Warenbestellsystem Daten über die den Warenempfang bestätigenden Person aus dem Warenlagermanagement-System	Umgehen der Bestellsysteme (z. B. Privatbuchen von Hotels) Fehlende Funktionstrennung zwischen Besteller und Warenempfänger: Rechnungsfreigabe vor Wareneingangsbestätigung Häufige Warenbestandskorrekturen
Offener Diebstahl				
I.2 Weitere Bilanzpositionen				
Abschreibung von Verbindlichkeiten			Abschreibungskonten, movement types	Wiederholte und (hohe) Wertberichtigungen bei Verbindlichkeiten, Buchungen kurz vor und nach den Abschlüssen
Wertberichtigungen			Wertberichtigungskonten, movement types	Wiederholte und (hohe) Wertberichtigungen von Warenbeständen, Buchungen kurz vor und nach den Abschlüssen
II. KORRUPTION				
II.1 Interessenkonflikte				
a. Einkaufskanäle			Preisspiegel, Vertragsunterlagen, Kreditorendaten	Eigentumswechsel bspw. durch Kauf von Gebäuden oder Grundstücken durch einen Mitarbeiter oder verbündeten Dritten, der wusste, dass das Unternehmen, bei dem er angestellt ist oder zu dem eine Verbindung besteht, Interesse an einem Kauf zeigt. Anschließend Verkauf an das Unternehmen zu einem höheren Preis.

Typ		Datenquellen	Relevante Auffälligkeit/red flags
b. Vertriebskanäle		Verkaufspreise, Rabattstaffelung, Verkaufsdokumente (z. B. Rechnung), Debitorenstammdaten	Verkäufe zu niedrigeren Preisen oder höheren Rabatten (z. B. Abzug eines Volumenrabatts, obwohl Volumen nicht erreicht ist). Häufig sind Empfänger der Organisation oder einem Mitarbeiter nahestehende Unternehmen.
II.2 Bestechung			
a. (Rechnungs-)Kickbacks		Daten aus FiBu: Rechnungsdaten, wie Rechnungspositionen und deren Konkretisierung oder Nachweis, Zahlungsdaten, Lieferungsdaten	Versteckter Ausweis in Pauschale Beschaffung und Anlieferung über dritten Lieferanten Fehlende Stundennachweise zu Rechnungen, unstimmige Zeitangaben oder doppelte Abrechnung von Mitarbeitern Sehr zeitnahe Bezahlung der Rechnungen Starke Abweichung von Zahlungszielen (gemäß General Terms & Conditions) Fehlende Nachweise für Provisionsleistungen
b. Angebotsmanipulation			
II.3 Illegale Zuwendungen		Daten aus FiBu: bspw. Aufwendungen für Mitgliedschaften, Beiträge, Bankkontodaten	Zahlungen an Vereinigungen oder Organisationen ohne bestehende Mitgliedschaft bzw. welche nicht existieren Die Bankbuchung erfolgt direkt gegen eine Aufwandsposition.
II.4 (Wirtschaftliche) Erpressung			
II.5 Vorteilsgewährung: Bevorteilung eines Lieferanten oder Geschäftspartners			
a. Gewährung von Vorteilen für Amtsträger oder Geschäftspartner			
Vorteilsnahme im Amt (öffentlicher Dienst)	Fehlende oder zielgerichtete Ausschreibung, Umgehung von Vergaberichtlinien, Nepotismus	Ausschreibungen bei Vergaben, Auftragsvergaben	Auffällige Häufungen von Auftragsvergaben an einzelne Institutionen (ohne sonstige Begründung)

Typ		Datenquellen	Relevante Auffälligkeit/red flags
	(Interessenkonflikte, wenn Freunde oder Verwandte bevorzugt werden)		
b. Eigene Beschäftigte lassen sich (finanzielle oder sachliche) Vorteile zukommen gegen Auftragsvergabe		Auftragsvergaben allgemein	Wiederkehrende Vergabe an einzelne Personen ohne besondere Begründung
III. RECHNUNGSLEGUNGSBETRUG			
III.1 Überbewertung, überhöhter Ausweis			
a. Zeitversatz			
b. Fiktive Erträge/Umsatzrealisierung		Umsatzerlöse, Ausgangsrechnungen, Zahlungsziele Umsatzerlösbuchungen und Zahlungsmittelzuflüsse Saldenbestätigungen	Falsche bzw. manipulierte Umsatzrealisierung (Cut-Off), z. B. Realisierung von Umsatzerlösen bereits zum Zeitpunkt der Bestellung oder betrügerische Vorfakturierung in Absprache mit Kunden Anstieg realisierter Umsätze vor den Abschlüssen (Belege bei stichtagsnahen Geschäften, Stornierung von Umsatzgeschäften nach einem Stichtag) Unzutreffender Ausweis von Kapitalzuflüssen als Umsatzerlöse Ausweis eines Konsignationslagers als Umsatzerlöse
c. Eigentümerfraud			
Verdeckte Privatentnahmen: Abrechnung von Aufwendungen für die private Lebensführung über die Firma und Verbuchung als Betriebsausgaben		Bilanz und Informationen aus dem Controlling	Die Buchungen erfolgen zu einer ungewöhnlichen Tageszeit bzw. außerhalb der regulären Arbeitszeit.
Scheingeschäfte mit fiktiven Partnern, z. B. fingierte Eingangsrechnungen		Datenabgleich: Bilanz und Informationen aus dem Controlling Dokumentenmanagementsystem	Die Buchungen beinhalten runde Beträge oder gleichbleibende Endnummern. Es gibt keinen Buchungstext oder nur unzureichende Erläuterungen. Häufig haben diese Buchungen Auswirkungen auf die Umsatzerlöse. Zu Beginn der Folgeperiode werden sie häufig storniert.

Typ	Datenquellen	Relevante Auffälligkeit/red flags
d. Verdeckte Verpflichtungen und Ausgaben		
e. Falsche Bewertungen von Vermögensgegenständen	Daten aus der Anlagenbuchhaltung	Zu niedrige Abschreibung durch überhöht angesetzte Nutzungsdauer bzw. fehlender oder inadäquater Impairment-Test
f. Falsche Veröffentlichungen		
g. Gefälschte Bestätigungen bzw. Gefälligkeitsgutachten	Dokumentenmanagementsystem Daten aus der Anlagenbuchhaltung	Unstimmigkeiten bei den unternehmensinternen Informationen (z. B. zukünftiger Nutzen oder Veräußerbarkeit des aktivierten Vermögensgegenstandes ist nicht plausibel)
h. Zu hoher Ausweis selbsterstellter immaterieller Vermögensgegenstände	Bilanz und Informationen aus dem Controlling Daten aus der Anlagenbuchhaltung Inventurunterlagen	Unstimmigkeiten zwischen bilanziellen und unternehmensinternen Kennzahlen Zu niedrige Abschreibung durch überhöht angesetzte Nutzungsdauer bzw. fehlender oder inadäquater Impairment-Test
i. Bewertung der selbsterstellten Anlagen zu überhöhten Herstellungskosten	Dokumentenmanagementsystem Daten aus dem Rechnungswesen Daten zum Vorratsvermögen	Fehlende interne Belege zu den Annahmen und eingesetzten Methoden Manipulation von Preisen bei Anschaffungs- und Herstellungskosten oder bei internen Kalkulationen wie der meist individuellen Standardkostenermittlung
j. Gefälschte Dokumente, z. B. falsche Angaben auf Rechnungen	Dokumentenmanagementsystem Daten zum Vorratsvermögen	Unstimmigkeiten zwischen bilanziellen und unternehmensinternen Informationen Unrichtige Bezeichnung oder Bezifferung von Kosten(-bestandteilen) in Rechnungen zum Zweck der Aktivierung oder unsachgemäße Aktivierung von Instandhaltungsaufwendungen Manipulierte Unterlagen über Qualität von Vorräten, Verwertungschancen oder

Typ	Datenquellen	Relevante Auffälligkeit/red flags
		Verschrottungsabsichten oder z. B. Nichtvorlage von Unterlagen, die auf Qualitätsmängel und Abwertungsbedarf schließen lassen
k. Auslagerung nicht werthaltiger Fixed Assets auf Zweckgesellschaften	Bilanz und Informationen aus dem Controlling	Unstimmigkeiten zwischen bilanziellen und unternehmensinternen Informationen
l. Unzulässige Sale-and-Lease-Back-Gestaltungen, z. B. Mehrfachabschlüsse von Sale-and-Lease-back-Verträgen über die gleichen Vermögensgegenstand	Dokumentenmanagementsystem	Unstimmigkeiten zwischen bilanziellen und unternehmensinternen Informationen
III.2 Unterbewertung/verkürzter Ausweis		
a. Zeitversatz		
b. Unterbewertete Erträge		
c. Nichterfassung von Verbindlichkeiten (Schuldentarnung): Aufnahme von Darlehen über SPE, die im Konzernabschluss nicht konsolidiert werden	Dokumentenmanagementsystem	Unstimmigkeiten zwischen bilanziellen und unternehmensinternen Kennzahlen
d. Falsche Bewertungen von Vermögensgegenständen	Abschreibungen	Bewusste Unterlassung erforderlicher außerplanmäßiger Abschreibungen (bspw. Verkauf gebrauchter Maschinen als fabrikneu)
e. Fälschung von unternehmensinternen Kennzahlen, z. B. im Personalwesen		
Trotz Erteilung von rechtsverbindlichen Pensionszusagen an Mitarbeiter Unterlassung der Bildung der erforderlichen Pensionsrückstellungen Keine Weitergabe der schriftlichen Zusagen an den versicherungsmathematischen Gutachter	Dokumentenmanagementsystem	Unstimmigkeiten zwischen bilanziellen und unternehmensinternen Kennzahlen
Noch im alten Jahr mündliche Mitteilung der Erhöhung der Pensionszusagen an die Mitarbeiter sowie Erstellung der Zusageschreiben, aber Vordatierung der schriftlichen Erhöhenszusagen auf ein Datum im neuen Jahr und Berechnung der Pensionsrückstellungen ohne Berücksichtigung der Erhöhungen.	Dokumentenmanagementsystem	Unstimmigkeiten zwischen bilanziellen und unternehmensinternen Informationen
f. Falsche Veröffentlichungen		
IV. UNERLAUBTE BEANSPRUCHUNG STAATLICHER LEISTUNGEN, Z.B. INVESTITIONSZULAGEN		
IV.1 Nicht bestimmungsgemäße Verwendung staatlicher Fördermittel		

Typ	Datenquellen	Relevante Auffälligkeit/red flags
a. Weitergabe der erhaltenen Subventionen als Darlehen an Kunden und Ausweis in der Bilanz als Beteiligungen	Dokumentenmanagement-system	Fehlende interne Belege zu den Annahmen und eingesetzten Methoden

9 Literaturverzeichnis

ACFE (2022): Occupational Fraud 2022: A Report to the nations®. https://legacy.acfe.com/report-to-the-nations/2022/.

Barr-Pulliam, Dereck/Brazel, Joseph F./McCallen, Jennifer/Walker, Kimberly (2020): Data Analytics and Skeptical Actions: The Countervailing Effects of False Positives and Consistent Rewards for Skepticism (October 19, 2020). http://dx.doi.org/10.2139/ssrn.3537180.

Barr-Pulliam, D., Brown-Liburd, H. L., & Carlson, A. G. (2023): Do Audit Data Analytics Influence Juror Perceptions of Audit Quality and Auditor Negligence? Current Issues in Auditing, P1-P10.

Brown-Liburd, Helen/Issa, Hussein/Lombardi, Danielle (2015): Behavioral Implications of Big Data's Impact on Audit Judgment and Decision Making and Future Research Directions. Accounting Horizons, 29(2): 451-468. https://doi.org/10.2308/acch-51023.

Bünis, Michael/Gossens, Thomas (2022): Please Mind The Gap: Die Digitalisierung fordert die Interne Revision heraus. Zeitschrift Interne Revision, 57(2): 64-76.

Cao, Min, Roman Chychyla, and Trevor Stewart (2015): "Big data analytics in financial statement audits." Accounting Horizons 29.2: 423-429.

Christ, Margaret H./Eulerich, Marc/Krane, Ronja/Wood, David A. (2020): New Frontiers for Internal Audit Research. (June 8, 2020). Available at SSRN: https://ssrn.com/abstract=3622148 or http://dx.doi.org/10.2139/ssrn.3622148.

Dai, Jun, and Miklos A. Vasarhelyi (2020): "Continuous audit intelligence as a service (CAIaaS) and intelligent app recommendations." Journal of Emerging Technologies in Accounting 17.2: 1-15.

Deloitte (2023): https://www2.deloitte.com/de/de/pages/trends/data-analytics.html.

DIIR (2023): Deutsches Institut für Interne Revision e. V. (Hrsg.): Enquete 2023 - Die Interne Revision in Deutschland, Österreich und der Schweiz. Frankfurt: DIIR. https://www.diir.de/fileadmin/fachwissen/downloads/Enquete-Broschuere_2023.pdf.

DIIR (2021): Deutsches Institut für Interne Revision e. V. (Hrsg.): Leitfaden Interne Revision und Datenschutz; DIIR-Arbeitskreis Interne Revision & Datenschutz.

Earley, Christine E. (2015): "Data analytics in auditing: Opportunities and challenges.", https://doi.org/10.1016/j.bushor.2015.05.002.

Eulerich, Marc/Georgi, Christine/ Schmidt, Alexander (2020): "Continuous auditing and risk-based audit planning—An empirical analysis." Journal of Emerging Technologies in Accounting 17.2: 141-155.

Eulerich, Marc/Kalinichenko, Artur (2018): The Current State and Future Directions of Continuous Auditing Research: An Analysis of the Existing Literature. Journal of Information Systems, 32(3): 31-51. https://doi.org/10.2308/isys-51813.

Eulerich, Marc/Masli, Adi./Pickerd, Jeffrey/Wood, David A. (2020): The Impact of Audit Technology on Audit Outcomes: Technology-Based Audit Techniques‘ Impact on Internal Auditing (August 28, 2019). https://ssrn.com/abstract=3444119 or http://dx.doi.org/10.2139/ssrn.3444119.

EY (2023): https://www.ey.com/de_de/big-data-analytics.

Gepp, Adrian, et al. (2018) "Big data techniques in auditing research and practice: Current trends and future opportunities." Journal of Accounting Literature 40: 102-115.

Gutzmer, Martin (2021): Heute, morgen, übermorgen - die Interne Revision im Wandel. Zeitschrift Interne Revision, 56(3): 118-122.

Haas, Ulrike/Schreckenberger, Alexander/Stottrop, Jan (2022): Die neue Revision spricht IT. Zeitschrift Interne Revision, 57(4): 156-164.

Kalinichenko, Artur (2016): Continuous Auditing im Kontext der Internen Revision. Dissertation. Universität Duisburg-Essen.

Kim, Yongbum, and Miklos A. Vasarhelyi (2012): "A model to detect potentially fraudulent/abnormal wires of an insurance company: An unsupervised rule-based approach." Journal of Emerging Technologies in Accounting 9.1: 95-110.

Koreff, J., & Perreault, S. (2023): Is sophistication always better? Can perceived data analytic tool sophistication lead to biased judgments?. Journal of Emerging Technologies in Accounting, 20(1), 91-110.

KPMG (2023): https://kpmg.com/de/de/home/themen/uebersicht/data-und-analytics.html.

Kümpel, Thomas, Kohlhoff, Kristina (2007): “Dolose Handlungen (Fraud) in Industrieunternehmungen.“ Controller Magazin 2/07: 109-117.

Odenthal, Roger/Odenthal, Kay (2023): KI-Techniken und Digital Audit. Zeitschrift Interne Revision, 58(3): 125-135.

PWC (2023): https://www.pwc.de/de/im-fokus/data-und-analytics.html.

Wagner, Johannes M. (2017): Empirische Studie zum Umsetzungsgrad von Continuous Auditing in deutschen Innenrevisionen. In: Zeitschrift Interne Revision, 52(1): 14-25.

Autoren

Arbeitsgruppe „Datenanalysen“ im DIIR-Arbeitskreis „Anti-Fraud-Management, Compliance und Interne Revision“

Veröffentlicht auf www.diir.de

Frankfurt am Main, Dezember 2023

DIIR – Deutsches Institut für Interne Revision e.V.

Theodor-Heuss-Allee 108

60486 Frankfurt am Main