Leitfaden für die Einführung eines Continuous-Auditing-Systems

Lösungsansätze und Best-Practice-Erfahrungen

Erarbeitet im DIIR-Arbeitskreis Continuous Auditing

Version 1.0
Stand 26.04.2021

DIIR
Deutsches Institut für
Interne Revision e.V.

Inhalt

1 Einleitung

Der stetig wachsende Druck, Prüfungen effizient durchzuführen und Prüfungsergebnisse zeitnah zu erzielen, stellt die Interne Revision vor ernstzunehmende Herausforderungen. Gleichzeitig verstärkt die größer werdende Anzahl gesetzlicher und regulatorischer Anforderungen diesen Druck und verlangt eine agile Weiterentwicklung des methodischen Vorgehens, um diesen Anforderungen zu genügen.

Die steigende Geschwindigkeit wirtschaftlicher Veränderungen mit ihren Einflüssen auf die Geschäftsmodelle, zunehmende Komplexitäten und Risikoschwankungen und nicht zuletzt die Digitalisierung und Automatisierung von Geschäftsprozessen verlangen verstärkt nach einer vorausschauend planenden und gleichzeitig zeitnah reagierenden Internen Revision im Unternehmen. Daher ist es unabdingbar, dass sich die Interne Revision von einer statischen, zeitraumbasierten (ein bis fünf Jahre im Voraus erfolgenden) Risikobeurteilung und Prüfungsplanung hin zu einer direkt situativ-reaktiven Analyse von Risiken und Kontrollwirksamkeiten mit darauf aufbauender, rollierender Prüfungsplanung verändert.

Um vor diesem Hintergrund mögliche Lösungsansätze und Best Practice-Erfahrungen zielgerichtet in einem Leitfaden für die Einführung eines Continuous Auditing-Systems (CA-System) zu vermitteln, wurde 2015 der DIIR-Arbeitskreis Continuous Auditing gegründet. Die Teilnehmer des Arbeitskreises haben sich dazu in den vergangenen Jahren intensiv über ihre Erfahrungen in den unterschiedlichen Branchen (u. a. Banken, Chemie, Industrie) ausgetauscht und Erkenntnisse u. a. im Rahmen einer Artikelreihe veröffentlicht.

Die seit 2017 veröffentlichten Artikel haben sich dabei mit folgenden Themen auseinandergesetzt:

1. Antwort der Revision auf komplexere Prüfungsanforderungen: Continuous Auditing – Der Mehrwert von Continuous Auditing aus der Anwenderperspektive[1]
2. Einsatz von Continuous Auditing anhand eines Modellunternehmens – Der Mehrwert für die Prüfungsplanung und -vorbereitung[2]

---

[1] Vgl. Bauch, M. et al., ZIR 3/2017, Erich Schmidt Verlag Berlin, S. 130 ff.
[2] Vgl. Gorschenin, E. et al., ZIR 3/2018, Erich Schmidt Verlag Berlin, S. 140 ff.

3. Der Mehrwert von Continuous Auditing für die Prüfungsdurchführung, die Berichterstattung und das Follow-up – Einsatz von Continuous Auditing anhand eines Modellunternehmens[3]

4. Einsatz von Continuous Auditing – Herausforderungen und Blick in die Zukunft[4]

Darauf aufbauend sowie dem Wunsch folgend, ein zielgerichtetes Nachschlagewerk für die Einführung eines CA-Systems zu veröffentlichen, befasst sich der vorliegende Leitfaden mit einer aus Sicht der Arbeitskreisteilnehmer praktikablen Definition des Continuous Auditing (CA) in Abgrenzung zum Continuous Monitoring (CM). Daraus abgeleitet beschreibt der Leitfaden mögliche Ansätze und Anreize für die grundlegende Entscheidungsfindung, ob CA eingesetzt werden soll bzw. kann. Im weiteren Verlauf werden für die Revisions-Kernprozesse Prüfungsplanung, -vorbereitung und -durchführung Beispiele für den Einsatz von CA vorgestellt.

Abschließend werden derzeit am Markt zu erwerbende, bzw. von Teilnehmern eingesetzte Tools, die CA-Prozesse unterstützen können, kurz vorgestellt und die Vor- und Nachteile eines Tool-Einsatzes kurz zusammengefasst.

Da die Einführung eines CA-Systems und die damit verbundenen Entscheidungen je nach Branche sowie Größe des Unternehmens bzw. der Internen Revision völlig unterschiedliche Mehrwerte bringen können, weisen die Autoren darauf hin, dass die als Best Practice zu verstehenden Anregungen dieses Leitfadens nur bei einer Entscheidungsfindung helfen sollen, aber weder als Vorgabe, noch als abschließende Lösung zu verstehen sind.

In den folgenden Kapiteln werden zunächst Begriffsklärungen, -definitionen und Abgrenzungen, ergänzt um Annahmen und Grundprinzipien, erfolgen, um das Verständnis und die Sichtweise des DIIR-Arbeitskreises Continuous Auditing darzustellen und eine Grundlage für die weitere Bearbeitung zu legen. Zudem wird eine begriffliche Abgrenzung zwischen CA und CM vollzogen. Darauf basierend werden die Ziele und der Mehrwert durch den Einsatz von CA dargestellt, ergänzt um einige Annahmen und Grundprinzipien zu den nachfolgenden Ausführungen.

---

[3] Vgl. Jacka, C. et al., ZIR 5/2018, Erich Schmidt Verlag Berlin, S. 237 ff.
[4] Vgl. Bauch, M. et al., ZIR 6/2018, Erich Schmidt Verlag Berlin, S. 248 ff.

1.1 Begriffsklärung, Annahmen und Grundprinzipien

Der Erfahrungsaustausch im Arbeitskreis verdeutlicht, dass es stark heterogene Umsetzungsfortschritte von CA gibt. Wesentliche Unterschiede sind zudem in der Ergebnisdarstellung, der Risikoadressierung und dem nachgelagerten Workflow zum Umgang mit den Risiken ausgeprägt. Auch die technische Umsetzung ist dabei sehr individuell und sowohl vom bestehenden Toolset eines Unternehmens als auch von Marktentwicklungen geprägt: Wo vor kurzer Zeit noch Lösungen auf Basis eines eigenständigen Data Warehouse (DWH) priorisiert wurden, zeigt sich nun ein Trend hin zu Tools zur skalierbaren Umsetzung von Massendatenanalysen (ggf. cloudbasiert). Neben einer Komponente für die Datenhaltung gibt es meist eine Komponente für die Pflege der Analyselogik und eine Präsentationskomponente (Visualisierung) für die Ergebnisse, welche selbst ggf. noch Interaktionsmöglichkeiten für den Nutzer bietet.

Trotz der heterogen ausgeprägten CA-Ansätze im Arbeitskreis besteht Einigkeit darüber, dass eine CA-Analyse immer ein relevantes Risiko adressiert, eine konkrete Zielsetzung verfolgt, reproduzierbar sein muss und bei entsprechender Kritikalität eine Handlung (Information, Beurteilung, Kurz- oder Ad hoc-Prüfung etc.) auslöst.

Abb. 1: Continuous Auditing Grundsatzannahmen[5]

Die Kombination aus risikoorientierter Analyse und nachgelagerter Handlung kennzeichnet einen Key Risk Indicator (KRI). Alternativ besteht auch die Option, konkrete Performanceziele zu verfolgen, welche als Key Performance Indicator (KPI) ausgeprägt werden können. Durch die Kombination der beiden Indikatoren werden Auditziele, welche als Key Audit Indicators (KAI) bezeichnet werden können. Sie sind die Basis für die praktische Anwendbarkeit von Continuous Auditing. Die Anwendungsmöglichkeiten erstrecken sich über den gesamten Audit Lifecycle.[6]

Die abgeleiteten Ergebnisse aus dem CA-Einsatz dienen primär der Internen Revision zur risikoorientierten und effizienten Planung und Durchführung von Prüfungshandlungen. Bei der späteren Klärung von Auffälligkeiten mit den Fachbereichen können sie ebenfalls herangezogen und bei Interesse auch dem Fachbereich zur Verfügung gestellt werden. Sollte

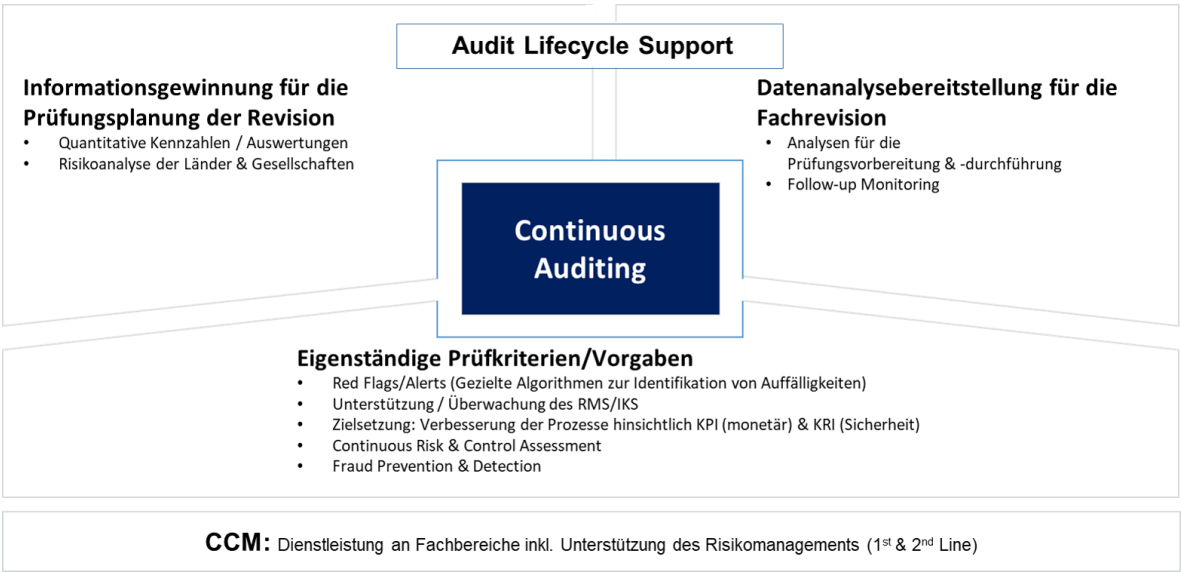
---

[5] Vgl. „Antwort der Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Verlag Berlin, S. 130 ff.

[6] Vgl. Kapitel 4.1.1 Audit Lifecycle-Support.

der Fachbereich weiterführende Analysen durchführen wollen, so sind diese Tätigkeiten von ihm selbst zu erbringen. Es wird klar darauf hingewiesen, dass die Interne Revision ihre Prüfungstätigkeit unabhängig und objektiv vollzieht und auch keine Auftragsarbeiten der Fachbereiche übernimmt, welche die Unabhängigkeit und Objektivität gefährden würden.[7] Möglichkeiten der Zusammenarbeit zwischen der Internen Revision und anderen (geprüften) Organisationseinheiten werden in Kapitel 3.3 Zusammenarbeitsmodelle dargestellt.

Abb. 2: Ausprägungen von CA-Systemen[8]



1.2 Ziele und Mehrwerte

Durch die stetige Digitalisierung und Automatisierung von Geschäftsprozessen und Transaktionen sowie die weitläufige Unterstützung durch IT-Services verfügt die Interne Revision heute über große Datenmengen, welche als Quelle für eine tiefergehende Datenanalyse verwendet werden können. Wegen der fortschreitenden Durchdringung von Produkten und Prozessen mit IT stehen völlig neue Kontroll- und Überwachungsmechanismen zur

[7] Vgl. Standards 1100 Unabhängigkeit und Objektivität in den Internationalen Standards für die berufliche Praxis der Internen Interne Revision 2017.

[8] Vgl. „Antwort der Interne Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Verlag Berlin, S. 130 ff.

Verfügung. Es entstehen zusätzlich neue Themenfelder, für welche geeignete Kontroll-, Steuerungs- und Überwachungsmechanismen umzusetzen sind.

Durch die Einführung und Verwendung des hier vorgestellten CA-Ansatzes ergeben sich eine Reihe von prüfungsbezogenen Verbesserungspotenzialen, welche im folgenden Schaubild dargestellt werden:

Abb. 3: Verbesserungspotenziale durch Continuous Auditing[9]

Zeit	➢ Kontinuierliche Risikobewertung und Follow-Up Verfolgung ➢ Zeitgerechte Erkennung von Schwachstellen im RMS / IKS ➢ Zeitnahe Ausführung von Analysen auf Basis von aktuellen und historischen Daten ➢ Reduzierung der Prüfungsdauer
Effizienz	➢ Konzentration auf wesentliche Sachverhalte ➢ Wiederverwendbarkeit ➢ Effiziente Ressourcennutzung
Qualität	➢ Erhöhung der Prüfungssicherheit ➢ Hohe Risikoabdeckung ➢ Reduktion von Fehlern
Mehrwert	➢ Kontinuierliches Monitoring führt zu zeitnahen Prozessverbesserungen ➢ Erhöhtes Gesamtprozesswissen stärkt die Fokussierung auf wesentliche Risikofelder ➢ Erhöhung des Abdeckungsgrads von Prüffeldern bzw. der Prüfungstiefe

Durch die Berücksichtigung als Adressat der Analysen kann CA zudem auch für die Fachbereiche der ersten und zweiten Linie[10] einen direkten Mehrwert liefern.

Der Einsatz von CA, speziell die fortlaufenden Kontroll- und Überwachungshandlungen bzw. Risikoeinschätzungen, führen zu:

- einer regelmäßigen Anpassung des Jahresprüfplans im Sinne einer effektiven rollierenden Prüfungsplanung aufgrund valider Informationen über Änderungen in der Risikolandschaft des Unternehmens,

[9] In Anlehnung an „Antwort der Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Verlag Berlin, S. 130 ff; RMS/IKS: Risikomanagement/Internes Kontrollsystem.

[10] Vgl. Drei-Linien-Modell im Positionspapier des IIA auf https://www.diir.de/fachwissen/iia-und-eciia-publikationen/ (Stand: 13.02.2021).

- zielgerichteter Definition des Prüfungsumfangs in den Standardprüfungen aus dem Jahresprüfplan, da bereits unterjährig erhobene Daten in der Internen Revision vorliegen,
- der Identifikation von notwendigen Ad-hoc-/Sonderprüfungen aufgrund von außergewöhnlichen Entwicklungen in Unternehmensbereichen und
- fortlaufender Kommunikation zwischen dem verantwortlichen Management der Geschäftsbereiche und der Internen Revision, die letztendlich zu einem besseren Verständnis der gegenseitigen Anforderungen und Aufgaben führt.[11]

1.3 Allgemeine CA-Definitionen

Die Verwendung des Begriffs CA hat bereits eine knapp 30-jährige Historie zu verzeichnen. So wurde bereits 1989 durch Vasarhelyi bei AT&T Bell Laboratories ein Continuous Process Auditing-System vorgestellt. Es diente der Analyse großer (papierloser) Datenbanken.[12] Eine erste Definition des Begriffs erfolgte durch die Verbände CICA/AICPA[13] in einem gemeinsamen Forschungsbericht 1999, welche als Grundlage des meistverbreiteten Verständnisses bzgl. Continuous Auditing angesehen wird.[14]

Dabei ist die Kernaussage, dass ein unabhängiger Prüfer durch CA in die Lage versetzt wird, mittels relevanter und aktueller Daten (auf Basis von überwachten Ereignissen) Handlungsnotwendigkeiten abzuleiten und spezifische Prüfungshandlungen durchzuführen. Spätere Veröffentlichungen zu CA-Definitionen führen ergänzend die Komponente Informationstechnologie ein, welche als wichtiger Bestandteil der fortlaufenden Datenerhebung und -verarbeitung im gegebenen Kontext dargestellt wird. Auch wird eine Erweiterung der Definition um Datenquellen und die Verwendung der Informationen im Zusammenspiel mit risikoorientierter Prüfungsplanung und -durchführung vollzogen.

Auch das IIA[15] führte im Zuge der Veröffentlichung des Global Technology Audit Guides zu Continuous Auditing (2nd Edition) in 2015 eine Definition ein: „Continuous auditing – the

---

[11] Vgl. Online-Revisionshandbuch, DIIR-Arbeitskreis MaRisk, Dezember 2017.
[12] Vasarhelyi, M. A.: The Continuous Audit of Online Systems (https://www.researchgate.net/publication/255667612_The_Continuous_Audit_of_Online_Systems, Stand: 14.08.2019).
[13] Canadian Institute of Accountants (CICA), American Institute of CPAs (AICPA).
[14] Vgl. Eulerich, M./Kalinichenko, A.: Die Continuous Auditing-Diskussion aus wissenschaftlicher Sicht, in: ZIR 01/2014, S. 34-44.
[15] The Institute of Internal Auditors (The IIA).

combination of technology-enabled ongoing risk and control assessments. Continuous auditing is designed to enable the internal auditor to report on subject matter within a much shorter timeframe than under the traditional retrospective approach."

Ergänzend wird dargestellt: „Continuous auditing comprises ongoing risk and control assessments, enabled by technology and facilitated by a new audit paradigm that is shifting from periodic evaluations of risks and controls based on a sample of transactions, to ongoing evaluations based on a larger proportion of transactions. Continuous auditing also includes the analysis of other data sources that can reveal outliers in business systems, such as security levels, logging, incidents, unstructured data, and changes to IT configurations, application controls, and segregation of duty controls."[16]

Obwohl CA bereits seit fast drei Jahrzehnten in der Literatur existiert, konnte sich keine allgemeingültige einheitliche Definition und zugehörig kein einheitliches Verständnis durchsetzen. So beinhalten die bestehenden Definitionen Unterschiede, welche abweichende Interpretationen zulassen. Daher hat sich der DIIR-Arbeitskreis Continuous Auditing entschlossen, eine eigene, auf der Darstellung des IIA aufbauende, praxisorientierte CA-Definition als Grundlage für die weiteren Ausführungen abzuleiten (vgl. Abbildung 4).

Abb. 4: Praxisorientierte CA-Definition des DIIR-Arbeitskreises Continuous Auditing[17]

Praxisorientierte CA-Definition des DIIR-Arbeitskreises Continuous Auditing
CA ist die Kombination von Risiko- und Kontroll-Assessments im gesamten Audit Lifecycle, welche maschinell unterstützt und in wiederholenden sowie von den eingesetzten Indikatoren und dem vorliegenden Risiko abhängigen Zeitabständen durchgeführt werden. *Die Anwendung von CA steigert die Effektivität und Effizienz der Internen Revision, indem es diese – gegenüber dem traditionellen Prüfungsansatz – zu einer früheren Identifikation der vom Soll-Zustand abweichenden Prüfungsgegenstände befähigt und bei einer schnelleren Durchführung von Prüfungen unterstützt.*

[16] Vgl. Institute of Internal Auditors (IIA): Global Technology Audit Guide (GTAG) Coordinating, Continuous Auditing and Monitoring to Provide Continuous Assurance, 2. Aufl., 2015 (https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG3.aspx, Stand: 14.08.2019).

[17] Ebd.

Darüber hinaus beinhaltet CA die Festlegung eines Adressatenkreises für die Übergabe der erlangten (Prüfungs-)Ergebnisse und Initialisierung von (Follow-up-)Maßnahmen.

Um die Vorteile von CA in vollem Umfang nutzen zu können, bedarf es der Durchführung regelmäßiger Reviews und notwendiger Anpassungen.

Ergänzend definiert der Arbeitskreis einen Indikator im Kontext der praxisorientierten CA-Definition als jegliche Ergebnisse, die auf Basis von festgelegten Parametern/Variablen unter Anwendung von Analyselogiken erzeugt werden.[18]

Ein Beispiel eines Indikators ist „Warenrückläufe > 5 Mio. €“. Hierbei bilden die 5 Mio. € den Parameter und das Zeichen „>“ die Analyselogik ab. Dabei lassen sich sowohl die Analyselogik als auch die Parameter beliebig erweitern.

Abschließend wird eine Abgrenzung zwischen CA und CM getroffen: Das IIA definiert CM als fortlaufende Tätigkeiten der ersten und zweiten Linie, um sicherzustellen, dass Regeln, Prozesse und Geschäftsabläufe als Bestandteile des Internen Kontrollsystems (IKS) effektiv umgesetzt bzw. durchgeführt werden. Die Tätigkeiten umfassen die Identifikation anwendbarer Kontrollziele und Bewertungskriterien sowie die Einführung automatisierter Testhandlungen, um Tätigkeiten und Transaktionen zu identifizieren, welche nicht den definierten Vorgaben entsprechen.[19] Die Unterscheidung liegt somit primär in dem verantwortlichen Personenkreis auf den unterschiedlichen Ebenen der drei Linien (vgl. auch Kapitel 3.2 „Einordnung in das Drei-Linien-Modell“).

Als wesentliche Bestandteile des CA sind das Continuous Controls Assessment (CCA) und das Continuous Risk Assessment (CRA) zu nennen. Das CCA liegt inhaltlich näher am CM, indem es die Bewertung der Wirksamkeit der wesentlichen Bestandteile des IKS beschreibt. Im CRA werden unter Berücksichtigung von Eintrittswahrscheinlichkeiten und Auswirkungen mögliche Risiken für das Unternehmen bewertet. Daraus werden notwendige Fokussierungen und Priorisierungen u. a. auch für die Tätigkeit der Internen Revision abgeleitet.

---

[18] Ebd.

[19] Vgl. Institute of Internal Auditors (IIA): Global Technology Audit Guide (GTAG) Coordinating, Continuous Auditing and Monitoring to Provide Continuous Assurance, 2. Aufl., 2015 (https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG3.aspx, Stand: 14.08.2019).

2 Rahmenbedingungen für CA-Systeme

Wie bereits in den vorherigen Kapiteln dargestellt, ist die Anwendung von CA-Methoden ein wichtiger Faktor, um die Interne Revision zukunftsfähig auszugestalten. Die Steigerung des Mehrwerts durch ein CA-System unter optimierten Bedingungen kann mehrfach begründet werden: Qualitativ bessere Erkenntnisse, eine damit verbundene höhere Validität der gezogenen Schlussfolgerungen und eine höhere Akzeptanz bei den Adressaten. Die Einführung eines CA-Systems ist aber auch mit grundsätzlichen Herausforderungen verbunden. Die folgenden Darstellungen spiegeln zum Teil Aspekte aus der Nutzung von Datenanalysen wider. Zunächst wird auf die notwendigen Voraussetzungen für die Anwendung von CA eingegangen.

Entscheidend ist im ersten Schritt die Definition des gewünschten Outputs (hier des KAI), welcher im zweiten Schritt Prüfungshandlungen anstoßen kann. Bei der Einführung von CA-Systemen wird primär auf strukturierte Daten aus bestehenden ERP-System und/oder Datenbanken zurückgegriffen.[20] Es können jedoch auch unstrukturierte Daten ausgewertet werden.

Beispiele für qualitative oder unstrukturierte Daten sind u. a. Bilder, Videoclips, eingescannte Geschäftsunterlagen, Notizen oder PowerPoint-Präsentationen, die sowohl aus internen als auch aus externen Datenquellen stammen können. Die kontinuierlich wachsende Nutzung sozialer Medien erzeugt Nachrichten, Kommentare, Chats oder Forenbeiträge in unstrukturierter oder zumindest semistrukturierter Form. Im Unterschied zu strukturierten Daten müssen unstrukturierte Daten zunächst in eine auswertbare, strukturierte Form überführt werden.

Sind die Hürden bei der Analyse von unstrukturierten Daten erst einmal überwunden, stehen dem Unternehmen (je nach analysierter Datenbasis) weitere relevante Informationen bspw. über Kunden, Geschäftspartner, die Branche oder die eigenen Geschäftsprozesse zur Verfügung. Die erhaltenen Informationen sind (z. B. aus betriebswirtschaftlicher Sicht) zu interpretieren, um daraus Erkenntnisse für den Audit Lifecycle abzuleiten. Dabei liefert die Kombination neuer Informationen mit den bereits bestehenden, strukturierten Daten (z. B. Unternehmensdaten, Wirtschaftsdaten, Marktdaten) weitere Analysemöglichkeiten.

---

[20] Beispiele sind Bestelldaten, Umsatzdaten oder Zugriffsberechtigungen von Benutzern.

Auch externe Datenquellen bieten ergänzende Informationen für mögliche CA-Szenarien, z. B. durch die Analyse von Diskussionen in sozialen Netzwerken über das eigene Unternehmen. Wird dabei ein wichtiges oder relevantes Thema identifiziert, kann dieses im Rahmen von neuen Revisionsprüfungen alsbald genauer untersucht werden. Auch Nachrichten und deren Effekte auf den eigenen Aktienkurs oder das Absatzverhalten von Produkten können im Rahmen von Analysen unstrukturierter Daten ermittelt werden. Aber auch bei internen Datenquellen gibt es diverse Möglichkeiten der Nutzung, z. B.:

- Analyse von eingereichten Schadensmeldungen in Verbindung mit genehmigten Ausgleichszahlungen im Hinblick auf Häufungen zur Aufdeckung von Betrugsversuchen von Mitarbeitern bei Versicherungen.
- Analyse von häufig auftretenden Incidents, z. B. bei der Hotline, die auf übergreifende Probleme hindeuten.
- Analyse auf Häufung der Änderung des Schutzbedarfs einer Anwendung/eines IT-Assets zur Identifikation von sich ändernden Funktionsumfängen oder unzureichendem Wissen bzgl. der verarbeiteten Informationen.

Die Menge an unstrukturierten Daten und die hohe Anzahl an Datenquellen wird in Zukunft weiterwachsen und die Fähigkeit, relevante Erkenntnisse aus solchen Daten ziehen zu können, wird dabei für Unternehmen zu einem immer wichtigeren potenziellen Wettbewerbsvorteil werden.

Grundsätzlich sind für den Einsatz von Continuous Auditing bestimmte Rahmenbedingungen zu beachten, die im folgenden Kapitel erläutert werden.

2.1 Rechtliche und organisatorische Rahmenbedingungen

CA-Aktivitäten dürfen nicht gegen geltendes Gesetz oder Rechtsnormen bzw. interne Regelungen verstoßen. Bestenfalls sind alle relevanten Regelungen vor Beginn eines produktiven CA-Betriebs bekannt und bereits auf Einhaltung geprüft. Bestehende Regelungslücken könnten bspw. mittels einer Betriebsvereinbarung geschlossen werden. Folgende Fragestellungen können dabei eine Orientierung geben:

- Existiert eine Betriebsvereinbarung, in der die Durchführung von (Massen-)Datenanalysen bereits geregelt worden ist? Beinhaltet diese Betriebsvereinbarung auch kontinuierliche Datenanalysen?
- Gibt es eine Zustimmung der Fachbereiche für die Verwendung der Daten in CA-Prozessen, welche für die Erzeugung der Daten organisatorisch zuständig sind?

- Widerspricht die zentrale Zusammenführung von Daten aus unterschiedlichen Quellsystemen in einem DWH (Data Warehouse) bestehenden Vereinbarungen/Regelungen? Ist der jederzeitige Zugriff der Revisionsmitarbeiter legitim?
- Bestehen für die zentrale Zusammenführung von Daten z. B. aus unterschiedlichen Ländern in einem DWH datenschutzrechtliche Restriktionen?
- Wurde für das ausgesuchte Verfahren im Rahmen eines CA-Systems eine ordnungsgemäße Dokumentation erstellt, um den gesetzlichen Nachweispflichten (EU-Datenschutzgrundverordnung) nachkommen zu können?

Neben den rechtlichen existieren auch organisatorische Herausforderungen. Für die Interne Revision könnte dies intern bedeuten, dass – sofern sich das CA von einer Regelprüfung unterscheidet – bestehende Ablaufregelungen erweitert werden sollten. In größeren Unternehmen könnte es zweckmäßig und sinnvoll sein, eine eigenständige CA-Einheit aufzubauen. Die Unterstützungsprozesse, Schnittstellen, Aufgaben und Verantwortlichkeiten sowie deren Abgrenzung zu den anderen Revisionseinheiten sollten in diesem Zusammenhang definiert werden. Da das CA unternehmensweite Einflüsse hat, sollten alle direkt und indirekt beteiligten Bereiche eines Unternehmens (u. a. Fachbereiche, IT, Compliance, Datenschutz, Betriebsrat) sowohl bei der Konzepterstellung als auch im operativen Einsatz einbezogen werden.

Bei der Ausgestaltung eines CA-Systems sind ggf. branchenspezifische regulatorische Vorgaben oder auch branchenübergreifende Standards zu berücksichtigen. Zu nennen sind u. a. die Internationalen Standards des Institute of Internal Auditors (IIA),[21] welche bspw. auf die Prozessunabhängigkeit der Internen Revision abzielen.

2.2 Inhaltliche und methodische Rahmenbedingungen

Im Rahmen der Einführung eines CA-Systems sind in einem ersten Schritt relevante KAIs zu identifizieren, fachlich sinnvoll zu definieren und deren Umsetzbarkeit zu prüfen. Dies stellt gleichzeitig auch eine der wichtigsten inhaltlichen Herausforderungen dar.

Unter „fachlich sinnvoll“ ist grundsätzlich zu verstehen, dass

[21] https://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2017_Standards__Version_6.1___20180110.pdf (Stand: 13.02.2021).

- ein KAI mit ausreichender Validität ein oder mehrere für das Unternehmen relevante Risiken und/oder Performanceziele misst („Kausalität“) und nicht nur ein mehr oder weniger durch Zufall bestehender Zusammenhang existiert („Korrelation“),
- ein vorgegebenes Ziel, bspw. aus der Unternehmensstrategie hergeleitet, zu realisieren ist, dessen Erreichungsgrad mittels des KAI gemessen werden kann (z. B. mindestens 75% aller Materialbestellungen sollen automatisiert erfolgen).

Unter „Umsetzbarkeit“ kann bspw. verstanden werden, dass

- die benötigten Daten in entsprechender Qualität, mit ausreichend langen Historien und in der Zukunft zuverlässig zur Verfügung stehen, und dass vorhandene Datenlücken angemessen geschlossen werden können. (So können auch bereits identifizierte Datenlücken und -wanderungen eine Feststellung sein.)
- der Einsatz für den Erhalt von Daten und die Validierung der Vertrauenswürdigkeit der Datenquellen akzeptabel ist.
- die benötigten fachlichen Datentransformationen und Berechnungen mit einem angemessenen (Zeit-)Einsatz stattfinden können.

Zudem sollte eine Übereinkunft zwischen Interner Revision und Fachbereich über die exakte Definition des KAI inklusive der Folgeaktivitäten bei Schwellenwertüberschreitung (bspw. Auslöser einer Sonderprüfung) bestehen, was wiederum die Akzeptanz für das gewählte Vorgehen erhöht.

Die zentrale methodische Herausforderung besteht darin, Schwellenwerte für die KAIs festzulegen. Die Schwellenwerte können entweder bestimmt (z. B. per Expertenschätzung oder Top-Down-Vorgabe) oder auf Basis vorhandener Daten mit statistischen Methoden kalkuliert werden. Schwellenwerte sollten im Praxisbetrieb regelmäßig (in definierten Intervallen) oder ggf. anlassbezogen überprüft und angepasst werden, denn

- ein zu geringer Schwellenwert verursacht zu viele Auffälligkeiten und damit ggf. einen zu hohen Aufwand/zu viele Nachfolgeaktivitäten,
- ein zu hoher Schwellenwert verursacht zu wenige Auffälligkeiten und damit ggf. eine zu niedrige Risikoabdeckung bzw. zu wenige Nachfolgeaktivitäten.

Idealerweise sollten deshalb die Mitarbeiter der Internen Revision über ein entsprechendes Statistik-Know-how für ein methodisch fehlerfreies Vorgehen verfügen.

2.3 Technische Rahmenbedingungen

Da zu Beginn die Verfügbarkeit von elektronischen Daten für die CA-Aktivitäten ggf. beschränkt ist, bestehen zentrale technische Herausforderungen in der Beschaffung, Aufbereitung und Vorhaltung aller notwendigen internen und ggf. externen Daten. Idealerweise stehen die Daten in einem revisionsinternen oder unternehmensweiten DWH zur Verfügung,

- in welchem die Daten dem Nutzungszweck entsprechend modelliert sind,
- in dem die Daten in angemessenen Zeitabständen aktualisiert werden,
- welches eine entsprechende (Daten-)Verarbeitungsgeschwindigkeit ermöglicht,
- dessen Datenanlieferung definiert und kontrolliert erfolgt, sodass Aussagen über die Qualität (z. B. Vollständigkeit, Richtigkeit, Integrität, Aktualität) jederzeit möglich sind.

Die Komplexität des Aufbaus und Betriebs eines DWH erhöht sich, wenn eine heterogene IT-Anwendungslandschaft (z. B. SAP, Non-SAP) im Unternehmen vorliegt oder Prozesse durch individuelle Datenverarbeitungen (z. B. Microsoft Excel) mit eigenen Datenhaushalten unterstützt werden. Aber auch im Fall einer homogenen Systemlandschaft ist die Datenmodellierung für das DWH komplex, wenn in unterschiedlichen Tochtergesellschaften zwar die gleichen Systeme betrieben werden, diese aber verschieden aufgebaut und/oder benutzt werden. Des Weiteren ist beim Betrieb des DWH zu beachten, dass sowohl bei Änderungen in der IT-Anwendungslandschaft (z. B. Abschalten/Releasewechsel bestehender oder Inbetriebnahme neuer Anwendungen) als auch bei anderen, die Datenerzeugung betreffenden Änderungen (z. B. Prozessänderungen), immer potenzielle Auswirkungen für das DWH untersucht und ggf. Anpassungen berücksichtigt werden müssen. Solche Gegebenheiten bewirken i. d. R. auch Anpassungen der automatisierten Analysen im Rahmen des CA (z. B. Änderung oder Austausch eines KAI).

Die Interne Revision sollte auch den Umgang mit Tools zur Visualisierung und Analyse (z. B. für Process Mining oder die Anwendung statistischer Verfahren) beherrschen, mit denen idealerweise direkt auf das DWH zugegriffen werden kann.

Eine alternative Möglichkeit der Datennutzung besteht in der Einrichtung und Verwendung von Lesezugriffen auf bereits bestehende Analysefunktionen in wesentlichen Kernsystemen oder Analysetools bzw. auf ein bereits existierendes DWH der ersten oder zweiten Linie.

2.4 Personelle Rahmenbedingungen

Die bisher gezeigten Rahmenbedingungen führen unausweichlich zu der Herausforderung, dass die Interne Revision über eine angemessene personelle Ausstattung mit entsprechenden Skillsets verfügen muss. Neben technischem und statistischem Wissen, Wissen über die Datenanalysetechniken und den Datenschutz sowie der Kenntnis der eigenen Unternehmensprozesse und dem Verständnis für das Geschäftsmodell, sind auch Fähigkeiten der Datenvisualisierung und der Kommunikation (hinsichtlich der Fachbereiche und Stakeholder) von großer Bedeutung. Aktuell haben sich die Bezeichnungen „Data Science“ (als Klammer über alle genannten Kompetenzbereiche) bzw. „Data Scientist“ (als korrespondierende Berufsbezeichnung) etabliert. Selbstverständlich kann und soll sich nicht jeder Revisor zum Data Scientist weiterqualifizieren, umgekehrt verfügt auch nicht jeder Data Scientist über eine umfassende Revisionserfahrung. Die Mischung in einem dazugehörigen Team – im Idealfall ergänzt um benötigtes Spezialwissen (z. B. Vertrieb, Bilanzierung) – und ein wechselseitiger Wissensaufbau erscheint sinnhaft bzw. notwendig.

Versierte Mitarbeiter für das eigene Unternehmen oder für die Interne Revision zu gewinnen, stellt derzeit vielfach eine große Herausforderung dar. Hier könnten CA-Projekte – quasi als positive Begleiterscheinung – aus Sicht von Data Scientists zur Verbesserung der Attraktivität der Tätigkeit in der Internen Revision beitragen.

2.5 Exkurs: Datenschutz/-sicherheit

Die (massenhafte) Verarbeitung von Daten erfordert auch eine Betrachtung der gesetzlichen Rahmenbedingungen. Dabei kann der Leitfaden des DIIR-Arbeitskreises Interne Revision & Datenschutz[22] hilfreich sein.

Grundsätzlich sollte die zu analysierende Datenmenge im jeweiligen Kontext möglichst abgegrenzt bzw. begrenzt sein (was ggf. dem Analyseziel entgegen steht), nur ein definierter Personenkreis sollte Zugang zu den Daten bekommen und es sollte ein Löschkonzept vorliegen. Bei der Durchführung ist außerdem auf eine ausreichende Dokumentation aller relevanten Schritte zu achten.

---

[22] Vgl. Leitfaden Interne Revision und Datenschutz auf https://www.diir.de/arbeitskreise/interne-revision-datenschutz/veroeffentlichungen/ (Stand: 13.02.2021)

Aus den bestehenden gesetzlichen Rahmenbedingungen lassen sich verschiedene Fragestellungen ableiten:

- Ist die Zweckbindung der Daten gewährleistet?
- Wurde analysiert, ob personenbezogene Daten oder sogar besondere Kategorien personenbezogener Daten verarbeitet werden?
- Wurde eine Abwägung der Interessen durchgeführt?
- Findet vor der Verarbeitung eine Anonymisierung oder wenigstens eine Pseudonymisierung personenbezogener Daten statt?
- Wird das Need-to-Know-Prinzip durchgängig eingehalten?
- Sind beim Einbezug externer Experten Verträge bzgl. Vereinbarungen zur Auftragsdatenverarbeitung notwendig?
- Wurde eine Datenschutz-Folgenabschätzung dort durchgeführt, wo sie verpflichtend ist?

Die Interne Revision sollte erwägen, ein grundsätzlich abgestimmtes Vorgehen mit dem Datenschutzbeauftragten und ggf. dem Betriebsrat zu vereinbaren, sowie sich mit diesen im Einzelfall abzustimmen. Dabei kann eine Betriebsvereinbarung den gewählten Rahmen definieren.

3 Die Rolle der Internen Revision

Die Interne Revision fungiert – unabhängig und objektiv – als Überwachungsfunktion des Unternehmens im Auftrag der Unternehmensleitung bzw. des Aufsichtsrats. Im folgenden Kapitel wird eine Einordnung dieser Aufgaben im Kontext des Drei-Linien-Modells vollzogen, um im Nachgang mögliche Ausprägungen von Zusammenarbeitsmodellen zu beleuchten.

3.1 Unterstützung der Unternehmensziele

In ihrer Funktion als dritte Linie ist es die Kernaufgabe der Internen Revision, Verbesserungspotenziale im Unternehmen aufzuzeigen und voranzutreiben. Dies wird insbesondere durch die Prüfung der Effektivität des IKS, des RMS und der Überprüfung der Ausgestaltung der ersten und zweiten Linie sichergestellt.

Durch den stetig wachsenden Druck, Prüfungen effizient durchzuführen und Prüfungsergebnisse zeitnah zu erzielen, muss die Interne Revision ihr methodisches Vorgehen anpassen, um den geforderten Beitrag zur Erreichung der Unternehmensziele leisten zu können.

3.2 Einordnung in das Drei-Linien-Modell

Das Drei-Linien-Modell bildet als Update des „Three-Lines-of-Defense-Modells“ seit 2020 einen organisatorischen Rahmen für die Ausgestaltung der Governance. Im Drei-Linien-Modell bildet die Interne Revision die sogenannte dritte Linie. In dieser Funktion beurteilt sie die Effektivität des IKS, RMS und der Überwachungsmaßnahmen in der ersten und zweiten Linie und ist zudem darauf ausgerichtet, Verbesserungspotenziale aufzuzeigen. Aufgrund ihrer Aufgaben im Unternehmen ist sie ein wesentlicher Treiber für die Imple-

mentierung von kontinuierlichen Prüfsystemen und periodischen Prüfmethoden, um fortlaufende Überwachungshandlungen und Risikoeinschätzungen effizient durchführen zu können.[23]

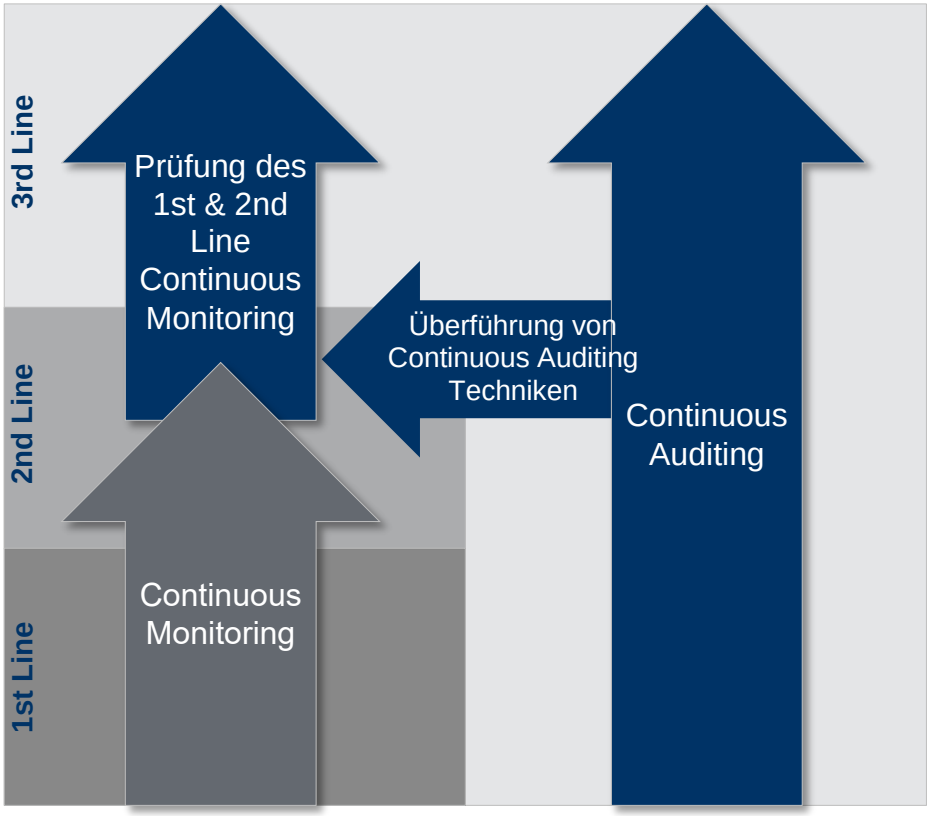


Abb. 5: CA im Kontext des Drei-Linien-Modells[24]

Jegliche Form der Zusammenarbeit der Internen Revision mit anderen Abteilungen ist möglich, so lange die Verantwortung der ersten und zweiten Linie (Definition der Prozesse, Bewertung der Risiken, Kontrolle der Compliance) nicht an die Interne Revision verlagert wird. Wenn die Kontaktpunkte zwischen der Internen Revision und den Abteilungen klar definiert sind, stärkt CA die unternehmensinterne Zusammenarbeit und Funktionsfähigkeit.

---

[23] Vgl. Online-Revisionshandbuch, DIIR-Arbeitskreis MaRisk, Dezember 2017.

[24] In Anlehnung an: Institute of Internal Auditors (IIA): Continuous Auditing: Coordinating Continuous Auditing and Monitoring to provide Continuous Assurance, 2nd Edition, S. 11.

Im nachfolgenden Kapitel werden einige mögliche Zusammenarbeitsmodelle genauer dargestellt.

3.3 Zusammenarbeitsmodelle

Die Einbindung der Fachbereiche in das CA-System und die damit in Verbindung stehende Rollenverteilung wird häufig kontrovers diskutiert. Konkret steht die Frage im Raum, ob die Interne Revision in Ihrer Rolle als dritte Linie Analyselogiken und -ergebnisse der ersten und zweiten Linie bereitstellen darf bzw. soll. Argumente, wie die Gefährdung der Unabhängigkeit der Internen Revision bzw. die mangelnde Prüfbarkeit und Verlässlichkeit von selbst entwickelten Analysen, stehen dem gemeinsamen Prozessverbesserungsgedanken sowie der Hebung von potenziellen Synergieeffekten durch die partnerschaftliche Kombination von Fachbereichs-Know-how und Sichtweise der Internen Revision oftmals entgegen.

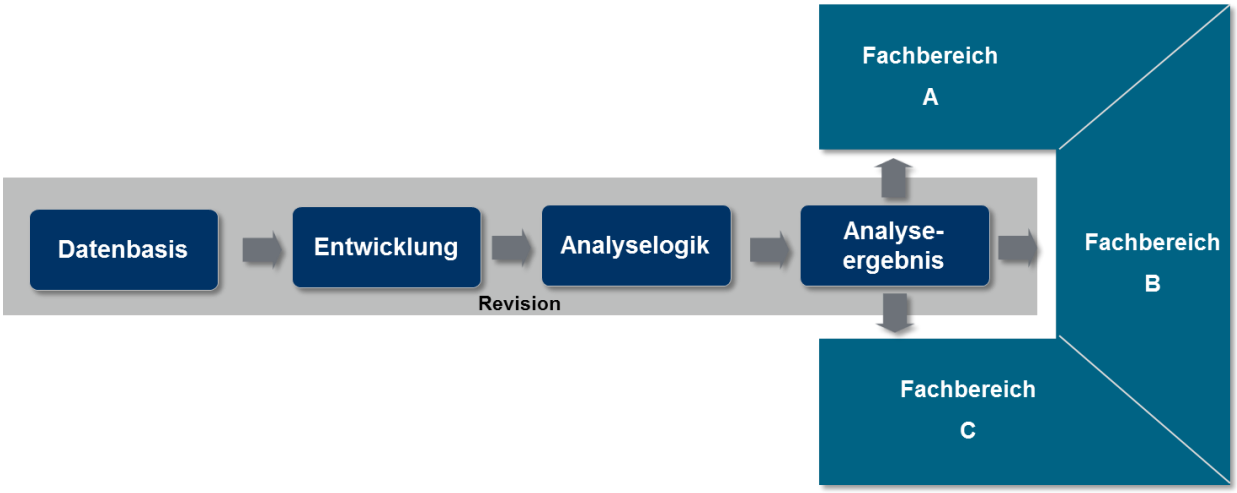
Bei der Implementierung eines CA-Ansatzes sind immer die wechselseitigen Abhängigkeiten zwischen den Ausprägungen von Continuous Monitoring-Prozessen durch einen Fachbereich in der ersten oder zweiten Linie und den Ausprägungen von CA durch die Interne Revision zu berücksichtigen. So ist speziell in Bereichen, in welchen kein ausgeprägtes CM im Fachbereich umgesetzt wurde, die Intensivierung von CA-Aktivitäten zielführend. Umgekehrt besteht diese Abhängigkeit genauso. Dabei ist unternehmensübergreifend immer zu analysieren, ob nicht Überwachungshandlungen doppelt ausgeprägt sind, welche die Prozess- und Kontrollsicherheit nicht erhöhen, sondern lediglich zusätzliche Kosten verursachen.

Die folgenden drei Szenarien für die Ausgestaltung der Zusammenarbeit unterscheiden sich im Wesentlichen in der Breite der Verantwortung für Prozessschritte und Ergebnisse. Dabei sind prinzipiell alle drei Szenarien anwendbar und in der Praxis vertreten. Bei der detaillierten Ausgestaltung von Zusammenarbeitsmodellen sollte die Maxime der Unabhängigkeit der Internen Revision leitender Gedanke sein.

Szenario 1: Interne Revision als Serviceprovider für Analyseergebnisse

Die Fachbereiche (z. B. Beschaffung, Produktion, Vertrieb, Personal) dienen als Empfänger der Analyseergebnisse, welche auf den in der Internen Revision entwickelten Analyse-Modellen basieren. Diese Analyseergebnisse können bspw. im Rahmen des Risikomanagements in der zweiten Linie die wirksame Kontrolldurchführung nachweisen oder das klassische operative IKS unterstützen.

Abb. 6: Interne Revision als Serviceprovider für Analyseergebnisse



Das Szenario 1 erfordert die Entwicklung eines Zusammenarbeitsmodells, welches die Verantwortlichkeiten klar abgrenzt, sowie die Aufgaben der Prozessbeteiligten eindeutig festlegt. Die von der Internen Revision entwickelten Analysen müssen zwingend verlässliche Ergebnisse liefern. Insbesondere sind die Vollständigkeit und die Richtigkeit der Datenbasis, welche den Analyseergebnissen zu Grunde liegt, mit größtmöglicher Sorgfalt durch die Interne Revision zu gewährleisten. Die Ergebnisbearbeitung erfolgt durch die Fachbereiche, allerdings werden sie verpflichtet, bei schwerwiegenden Beanstandungen auf die Interne Revision zuzugehen. Diese aktive Versorgung der ersten und zweiten Linie aus dem CA-System der Internen Revision erfordert bspw. eine strenge Separierung in einen CA-Workflow (Revisionsindikatoren) und einen CM-Workflow (Fachbereichsindikatoren).

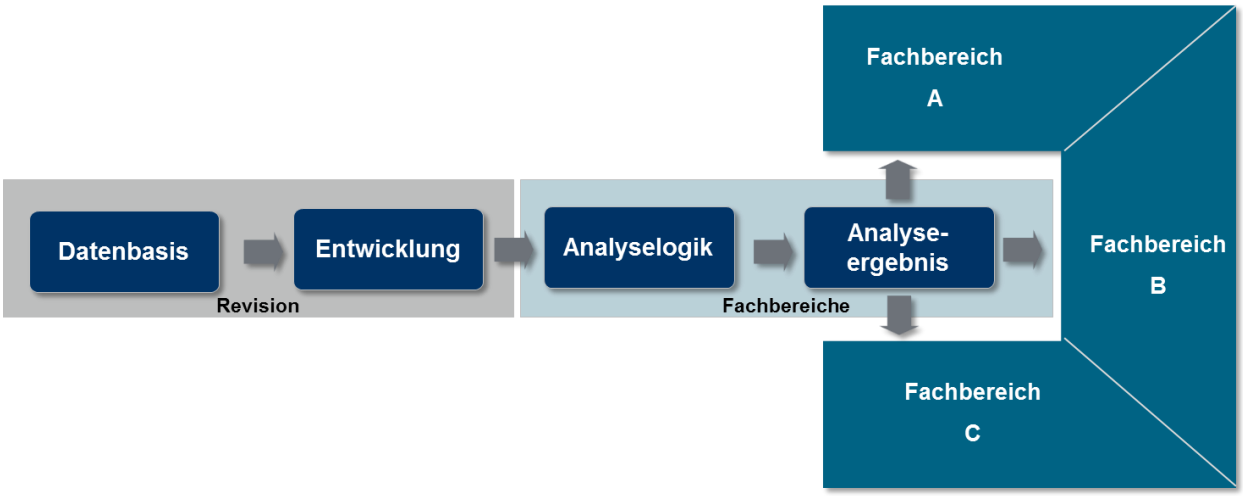
Bei einem solchen Servicemodell ist die Interne Revision ggf. nicht mehr unabhängig, wenn die inhaltliche Verantwortung der Analyseergebnisse von der ersten und zweiten Linie nicht übernommen wird. Definitiv besteht eine Unabhängigkeit, wenn die bereitgestellten Analyseergebnisse zusätzlich zu dem bestehenden IKS/RMS der ersten und zweiten Linie herangezogen werden oder die Analyseergebnisse im Rahmen von Prüfungen bereitgestellt werden. Eine Implementierungsvariante könnte sein, dass die Interne Revision mithilfe ihrer Analysetools eine Ergebnisliste (die z. B. falsch positive oder auch irrelevante Ergebnisse enthält) erstellt und diese der ersten und zweiten Linie zur weiteren Analyse zur Verfügung stellt. Die Prüfung der Ergebnisse könnte kontinuierlich erfolgen und in einem Revisionsbericht dokumentiert werden.

Szenario 2: Bereitstellung von entwickelten Analyselogiken an die Fachbereiche

Eine weitere Möglichkeit ist, dass die Fachbereiche von Erkenntnissen aus Prüfungen, in denen Datenanalysen eingesetzt wurden, profitieren können. Hierbei handelt es sich um

eine Bereitstellung der Analyselogiken z. B. in Form eines Indikatorensets zur vollständigen Übernahme in die Fachbereichssysteme bzw. genutzten Überwachungs-/Analysetools der ersten und zweiten Linie.

Abb. 7: Bereitstellung von entwickelten Analyselogiken an die Fachbereiche

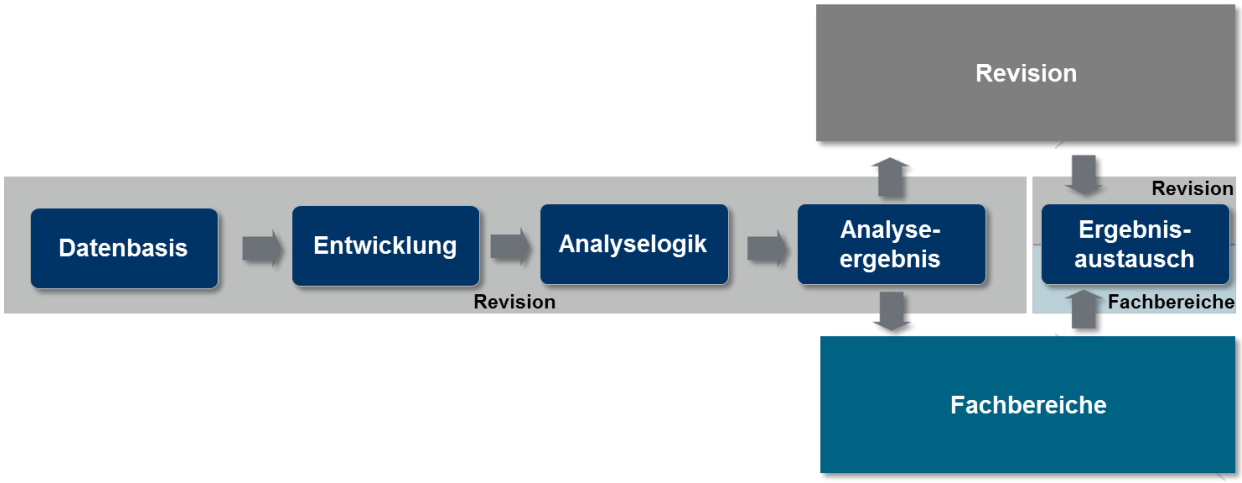


Bspw. wird der KAI „Rechnungseingang vor Bestellung“ in das Rechnungswesen übertragen und zukünftig kontinuierlich im kreditorischen ERP-System weiterverwendet. Hier ist allerdings entscheidend, dass die Verantwortung für die Richtigkeit und Vollständigkeit der Analyselogik an den Fachbereich übertragen wird. Die Weiterentwicklung der Analyselogik inklusive der Schwellenwertfestlegung bzw. die zukünftigen Anpassungen an Prozessänderungen sind ausschließlich durch den Fachbereich zu leisten. Somit wird gewährleistet, dass diese Prüffelder auch zukünftig ohne Interessenkonflikt geprüft werden können. Durch eine klare Verantwortungsübertragung ist sicherzustellen, dass die Interne Revision nicht Bestandteil des IKS des Fachbereiches wird.

Szenario 3: Partnerschaftlicher Ansatz

Neben den zuvor genannten Szenarien besteht die Möglichkeit, dass Analyseergebnisse sowohl von Fachbereichen als auch von der Internen Revision parallel genutzt werden. Die Interne Revision prüft neben klassischen Kontrollzielen auch Auditziele. Letztere kombinieren bspw. eine Risikoadressierung und Performanceziele oder legen den Fokus auf Schnittstellen zu anderen Fachbereichen. Der Fachbereich betrachtet jene Analyseergebnisse unter Einbezug seiner vordefinierten Kontrollziele bspw. der Einhaltung der Prozessvorgaben.

Abb. 8: Partnerschaftlicher Ansatz



Bei diesem Szenario werden fachbereichsübergreifende Prozessoptimierungspotenziale mit prozessintegrierten Fachbereichsaspekten kombiniert. Ein Austausch über die Ergebnisse ist zwingend erforderlich.

4 Unterstützender Einsatz von CA in der Audit-Praxis

Nach der Definition und Beschreibung von CA und dessen Einbettung in das Governance-Modell des Unternehmens, wird in den folgenden Kapiteln der Fokus auf die Anwendung von CA gerichtet. Dies erfolgt auf Basis von Beispielen zu verschiedenen Unterstützungsmöglichkeiten sowohl innerhalb als auch außerhalb des Standardrevisionsprozesses. Ziel der Darstellung ist es, konkrete Ideen und Einsatzmöglichkeiten zu vermitteln, um den beschriebenen Ansatz praxisbezogen und individuell adaptierbar nutzen zu können.

4.1 CA-Unterstützung im Standardrevisionsprozess

CA kann im Standardrevisionsprozess sowohl in einzelnen Phasen des Audit-Lifecycle[25] als auch durchgängig von der Planung bis zum Follow-up verwendet werden.

[25] Vgl. DIIR Positionspapier „Risikoorientierte Prüfungsplanung“, DIIR 2010.

4.1.1 Audit Lifecycle Support

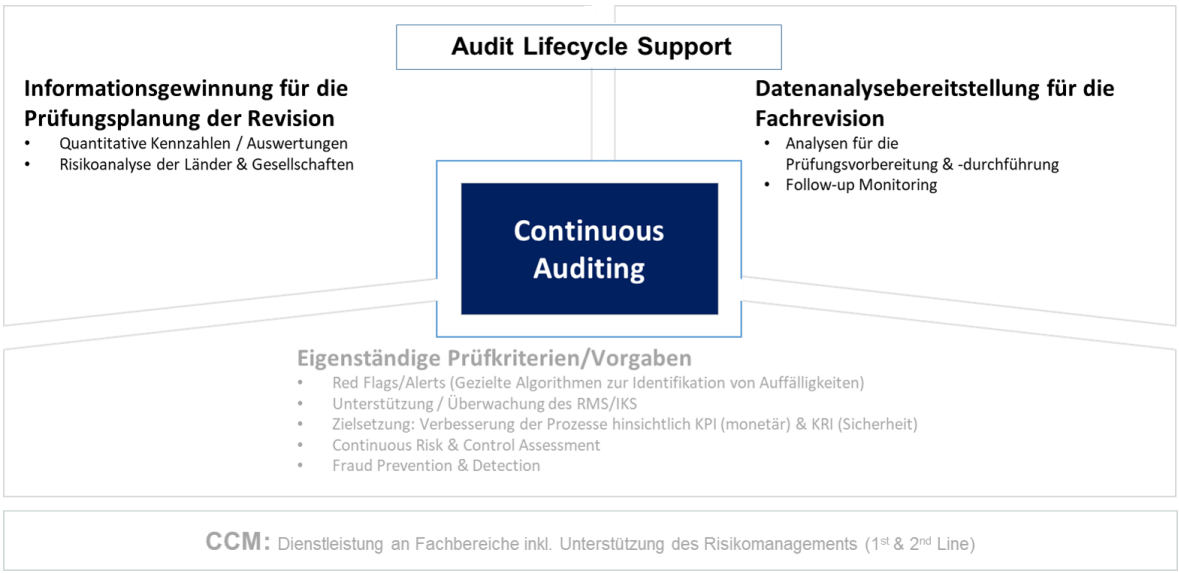


Abb. 9: Ausprägungen von CA-Systemen – Audit Lifecycle Support[26]

Planung

Die risikoorientierte Prüfungsplanung beinhaltet die Identifikation von Prüfungsobjekten, die Risikobewertung, die Priorisierung auf Basis des Risikos und die Ausgestaltung des Prüfungsprogramms.[27]

---

[26] Vgl. „Antwort der Interne Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Verlag Berlin, S. 130ff.

[27] Vgl. DIIR Positionspapier „Risikoorientierte Prüfungsplanung“, DIIR 2010.

Abb. 10: Der Mehrwert von CA für die Prüfungsvorbereitung[28]

Die Verwendung von CA führt auf Basis einer kontinuierlichen Risiko- und Kontrollbewertung zu einer zeitnahen Anpassung in der Prüfungsplanung. CA bietet sowohl bei der Identifikation von Prüfungsobjekten als auch bei der Risikobewertung Unterstützung. Die zur Planung benötigten Informationen werden aus verschiedenen Quellen erhoben, um entsprechende KAIs abzuleiten. Mit zunehmender Digitalisierung dienen als Quellen in erster Linie elektronische Informationen in bestehenden IT-Anwendungen, wobei die Datenqualität zu beachten ist. Eine Übersicht möglicher Informationsquellen ist in der Anlage 1 abgebildet.

Ergänzend erfolgt eine initiale Risikobewertung neu erkannter Prüfungsobjekte. Um Handlungsnotwendigkeiten aus den Risikowerten ableiten zu können, werden zusammen mit den KAIs Schwellenwerte definiert. Somit kann zwischen KAIs für die Identifikation von Prüfungsobjekten und Indikatoren zur Risikoanpassung unterschieden werden.

[28] Vgl. „Der Mehrwert von Continuous Auditing für die Prüfungsplanung und -vorbereitung“, Gorschenin, E. et al., ZIR 03/2018, Erich Schmidt Verlag Berlin, S. 140 ff.

Abb. 11: Beispiele für KAIs zur Identifikation neuer Prüfungsobjekte

KAIs zur Identifikation neuer Prüfungsobjekte
Anlage neuer Organisationseinheiten im elektronischen Organigramm
Freigabe eines neuen IT-Services in einer Configuration Management Database (CMDB)
Erfassung und Freigabe eines neuen externen Dienstleisters im Auslagerungsmanagementsystem
Genehmigung eines neuen Programms oder Projektes im Projektmanagement-System
Freigabe eines neuen Produktdatensatzes im ERP-System
Freigabe eines neuen Datensatzes im Stammdatenmanagementsystem

Abb. 12: Beispiele für KAIs zur Anpassung der Risikobewertung von Prüfungsobjekten im Einkaufsprozess

KAIs zur Anpassung der Risikobewertung von Prüfungsobjekten im Einkaufsprozess
Veränderung der Anzahl der Kunden
Erhöhung der Anzahl der Warenrückläufe
Erhöhung der Anzahl der Stornos im Einkaufsprozess
Erhöhung der durchschnittlichen Vertriebskosten
Erhöhung der Wareneingänge ohne Bestellung
Erhöhung der Bestellungen unterhalb von Freigabegrenzen

Wird der Schwellenwert eines KAI zur Identifikation von Prüfungsobjekten überschritten (z. B. Änderung auf >0), so ist das Prüfungsobjekt in das Prüfungsuniversum aufzunehmen und eine initiale Risikobewertung durchzuführen. Bei der Einstellung des Betriebs eines IT-Services lässt sich ebenfalls ein entsprechender Indikator (in diesem Falle <1) definieren, welcher einen Archivierungsprozess des zugehörigen Prüfungsobjektes anstoßen kann.

Für Risikoänderungsindikatoren können mehrere Schwellenwerte definiert werden (z. B. für eine Frühwarnung vs. direkte Handlungsnotwendigkeit). Die Frühwarnung kann als Auslöser für eine tiefere Betrachtung des Prüfungsobjekts dienen, während der Schwellen-

wert für die Handlungsnotwendigkeit eine Aktualisierung der Risikoeinstufung des Prüfungsobjektes auslöst. Die Grundlage bildet dabei das individuell ausgestaltete Risikomodell des anwendenden Unternehmens.

Bei der Ableitung eines KAI empfiehlt sich eine Überprüfung der Umstände, die zur Erreichung eines definierten Schwellenwertes geführt haben. Mit steigender Expertise und daraus erfolgten Anpassungen lassen sich Neubewertungen unter Berücksichtigung der Unternehmensgröße und des Einsatzzweckes ggf. auch sukzessive automatisieren. Eine spätere Integration von Prozessen des maschinellen Lernens zur weiteren Verfeinerung der Indikation ist möglich.

Beginnend mit einem (viertel-)jährlichen Rhythmus sollten die Aktualisierungszyklen für die Risikoneubewertung und entsprechende Anpassungen des Prüfungsplanes zunächst langsam verringert werden und die damit verbundenen Lerneffekte einfließen.

Die zielgerichtete Umsetzung von CA-Systemen führt durch kontinuierliche und detaillierte Informationen zu schnelleren Anpassungen in der risikobasierten Prüfungsplanung. Es bestehen Möglichkeiten, Risikobewertungen zeitnah zu aktualisieren und den risikoorientierten Prüfungsplanungsprozess zu automatisieren, um den internen Revisionsprozess insgesamt effektiver zu gestalten.

Vorbereitung

Abb. 13: Der Mehrwert von CA für die Prüfungsvorbereitung[29]

[29] Vgl. Der Mehrwert von Continuous Auditing für die Prüfungsplanung und -vorbereitung, Gorschenin, E. et al., ZIR 03/2018, Erich Schmidt Verlag Berlin, S. 140 ff.

In der Phase der Prüfungsvorbereitung wird das Scoping (der Prüfungsobjekte) detailliert und somit der genaue Prüfungsinhalt vor Beginn der Prüfungshandlungen festgelegt. Die Vorbereitungsphase endet beim klassischen Prüfungsvorgehen mit einem detaillierten Prüfungsplan,[30] welcher eine Priorisierung bzw. eine Auswahl durchzuführender Prüfungshandlungen enthält. Dies kann z. B. eine Vorauswahl von Kontrollen aus einer Risiko-Kontroll-Matrix sein. Die Prüfungsvorbereitung dient insbesondere der Entwicklung einer schriftlichen Planung bzgl. Zielen, Umfang, Zeitplan und zugeordneten Ressourcen (IIA-Standard 2200).[31] Die im Rahmen des CA-Systems verwendeten KAI unterstützen bei der Festlegung des Prüfungsinhalts u. a. durch Identifikation potenzieller Risikobereiche oder der Ableitung von Prüfungsfragen. Dies erhöht die Prüfungsqualität (siehe Anlagen 2-4).

CA ermöglicht hier auch eine Reduzierung des Prüfungsumfangs, z. B. durch Fokussierung auf risikorelevante Geschäftseinheiten, Geschäftsbereiche bzw. Geschäftsvorfälle. Sollte sich im Rahmen der Prüfungsdurchführung die Validität der KAIs nicht bestätigen, sind diese zu korrigieren oder zu verfeinern.

Auch bei einem agilen Prüfungsansatz kann CA den gesuchten Mehrwert liefern, indem eine risikobasierte Vorauswahl von Prüfungsobjekten durchgeführt wird. Durch gesammelte Erkenntnisse aus den ersten Sprints[32] können bei Bedarf Anpassungen an den KAIs vollzogen werden, um die weiteren Sprints zu priorisieren oder weitere relevante Prüfungsobjekte zu identifizieren bzw. bereits im Fokus stehende Prüfungsobjekte zu repriorisieren oder ggf. zu streichen.

Durchführung

Im Rahmen der Durchführung einer internen Revisionsprüfung kann ein CA-System erheblichen Mehrwert leisten, da dem Prüfungsteam durch die Analyse der KAIs bereits zu Beginn der Fieldworkphase vertiefte Erkenntnisse über einen Prüfungsgegenstand zur Verfügung stehen, die i. d. R. sonst nur zu einem späteren Zeitpunkt oder gar nicht vorliegen würden. In der Durchführungsphase sammelt das Prüfungsteam u. a. anhand von Interviews und einer Dokumentenanalyse weitere Informationen, erstellt Auswertungen und kann mit Hilfe dieser Informationen zudem die Geschäftsvorfälle nachvollziehen, welche auf der Grundlage von KAIs identifiziert wurden.

Durch die Kombination von bestehenden KAIs aus unterschiedlichen Bereichen, wie bspw.

---

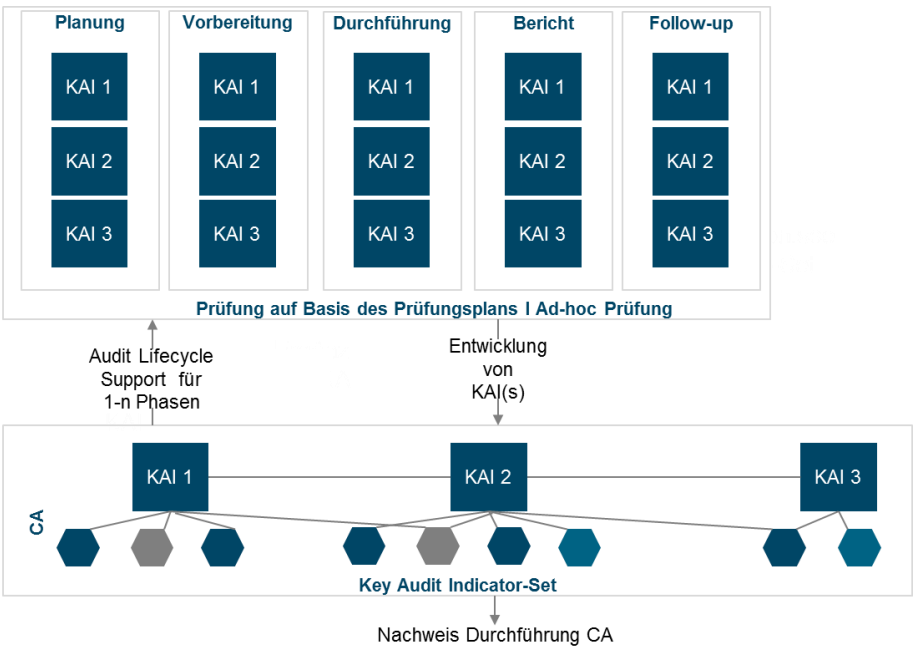
[30] Vgl. Amling, T./Bantleon, U., 2007, S. 75.

[31] Vgl. DIIR - Deutsches Institut für Interne Revision e.V., Internationale Standards für die berufliche Praxis der Internen Revision 2017, Standard 2200 Planung einzelner Aufträge.

[32] Ein Sprint ist hier als ein Durchlauf mit einem definierten Zeitraum zu verstehen, in dem ein festgelegter Plan zur Erreichung eines Ziels umgesetzt wird.

Finanzen und Beschaffung, kann zudem ein bereichsübergreifendes Verständnis geschaffen werden, welches ohne CA-System oder durch eine Fokussierung auf ein bestimmtes Prüffeld in einem Geschäftsbereich nicht möglich gewesen wäre. Dies kann die Ursachenanalyse für Auffälligkeiten erleichtern und die Identifikation von Prozessoptimierungspotenzialen gesamthaft für eine Prozesskette ermöglichen. Nach einer Analyse der KAIs kann ein Prüfungsteam seine Prüfungsfragen erweitern und auch gezielt die Selektion von auffälligen Einzelfällen vornehmen. Mit Hilfe eines etablierten CA-Systems stehen in der Regel die Datengrundlagen der KAIs zur Verfügung, sodass eine bewusste Stichprobenauswahl anhand von Auffälligkeitskriterien oder eine zufallsbasierte Auswahl basierend auf der ermittelten Grundgesamtheit erfolgen kann. Die Kombination von Indikatoren mit klassischen Prüfungshandlungen ist für die Durchführung von Prüfungen ein gesteigerter Mehrwert.

Abb. 14: Audit Lifecycle-Support durch ein Key Audit Indicator-Set.[33]



Für ein CA-System ist zudem die Phase der Durchführung essentiell wichtig, um ein bestehendes Indikatoren-Set anzupassen und/oder um dieses Set mit neuen KAIs zu erweitern. Durch den Einsatz von einmaligen Datenanalysen und durch die Analyse des Prüfungsgegenstands ergeben sich KAIs, die ggf. in Kombination mit den bestehenden KAIs künftig für die Phasen des Audit Lifecycle hilfreich sein werden. Die Durchführungsphase ist somit der Ideengeber für die (Weiter-)Entwicklung von KAIs.

[33] Vgl. Bauch, Kriegelstein: Die inverse Beziehung zwischen „Continuous Auditing und der Digitalisierung“, Fachvortrag DIIR Digitale Tage 2019.

Eine weitere Möglichkeit der Ausgestaltung in der Phase der Prüfungsdurchführung ist die prozessgestützte kontinuierliche Bereitstellung von Datenanalyselogiken und/oder -ergebnissen ggf. einer zentralen Datenanalyseabteilung innerhalb der Internen Revision. Entsprechend der CA-Definition des Arbeitskreises[34] ist die Wiederholfrequenz abhängig von dem zu Grunde liegenden Risiko und den eingesetzten Indikatoren. Dementsprechend stellt diese Bereitstellung bzw. dieser zentrale Zugriff eine weitere Variante dar, die zu einem Zusatznutzen für den bestehenden Audit Lifecycle führt. Beispielsweise wird bereits bei der Anlage einer Prüfung und der Auswahl des Prüfungsobjekts (Gesellschaft, Fachbereich, Prozess) bzw. entsprechender Systeme durch die Anfrage bestimmter Daten eine Datenanalyse generiert und an eine zentrale Datenanalyseeinheit versendet. Diese Einheit plausibilisiert die Analyseergebnisse und stellt wiederum dem Prüfungsteam die Ergebnisse für die Prüfungsdurchführung zur Verfügung. Wenn weiterführende oder eigenständige Datenanalysen in Prüfungen durchgeführt werden, ist die Bereitstellung eines an die bestehenden Unternehmensprozesse und Systemlandschaften angepassten Datenanalyseportfolios eine weitere mehrwertstiftende Aufgabe eines CA-Systems.

Abb. 15: Der Mehrwert von CA für die Prüfungsdurchführung[35]

Bericht

Im Rahmen einer Prüfung kann das klassische Berichtsformat in Textform auf der Basis eines KAI-Sets um Kennzahlen und Statistiken ergänzt werden, um den verantwortlichen

[34] Vgl. Kapitel 1.3, Abb. 4: Praxisorientierte CA-Definition des DIIR-Arbeitskreises Continuous Auditing.

[35] Vgl. „Der Mehrwert von Continuous Auditing für die Prüfungsdurchführung, die Berichterstattung und das Follow-up“, Jacka, C. et al., ZIR 05/2018, Erich Schmidt Verlag Berlin, S. 237 ff.

Bereichen und Vorständen eine visuelle Hilfestellung bei der Beurteilung der Feststellungen und Maßnahmen zu geben und das verbalisierte Prüfungsergebnis besser verstehen und einordnen zu können. Wenn bereits die Durchführung auf entsprechenden KAIs basiert, können die Ergebnisse übernommen und um Visualisierungen erweitert werden.

Zudem stellt die automatisierte Berichterstellung einen weiteren Anwendungsfall für die Unterstützung durch ein CA-System dar. Neben der Ergänzung eines bestehenden Reportings einer Internen Revision um ausgewählte KAIs kann auch ein Durchführungsnachweis generiert werden. Ein solches Reporting zeigt die Abdeckung von Prüfungsfeldern und Prozessen durch die vorhandenen KAIs und erläutert, wo sich Auffälligkeiten ergaben. Die Feststellungen und Empfehlungen der daraufhin initiierten Prüfungshandlungen u. a. in Form von künftigen Programmprüfungen und Ad- hoc-Prüfungen sind entsprechend in Verbindung mit relevanten KAIs zu setzen.

Abb. 16: Der Mehrwert von CA für den Prüfungsbericht[36]

Grundsätzlich kann der Einsatz einer erhöhten Anzahl von bestehenden KAIs dazu führen, dass die klassischen Prüfungshandlungen und -ergebnisse reduziert werden können. Je mehr KAIs eingesetzt werden, desto stärker kann eine weitestgehend automatisierte Berichterstattung verfolgt werden, die sogar eine Echtzeitanalyse von Unternehmensindikatoren darstellen könnte und Handlungsfelder aufzeigt. Im Idealfall können kontinuierlich aktuelle Ergebnisse in einem Dashboard oder einer Performance Scorecard – ggf. ergänzt um

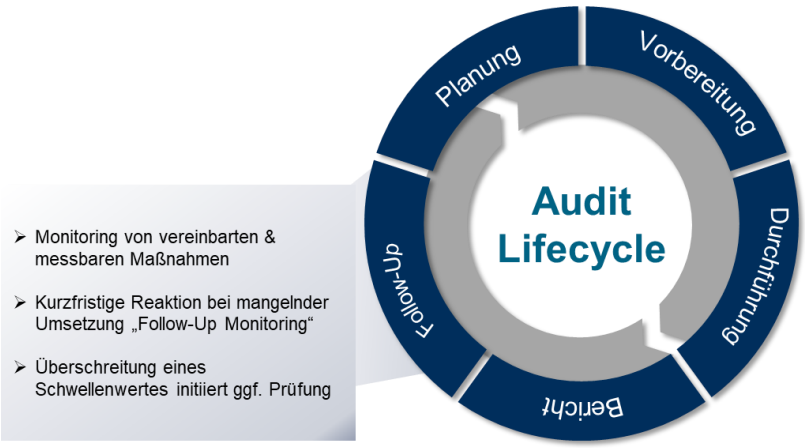
[36] Ebd.

Unternehmens- oder Industriebenchmarks – visualisiert und bei Bedarf gezielt mittels E-Mail-Benachrichtigung versendet werden. So werden Prüfungsleiter mit Informationen über ihre Prüfungsgebiete versorgt und bspw. Adressaten im Fachbereich zeitgleich über Auffälligkeiten per E-Mail benachrichtigt, die zu analysieren sind. Neben einer prüfungsgegenstandsbezogenen Einzeldarstellung, die es zu automatisieren und zu standardisieren gilt, sollte auch die übergeordnete Berichterstattung an die Unternehmensführung bzw. die Stakeholder berücksichtigt werden.

Follow-up

Wenn im Rahmen von internen Revisionsprüfungen Datenanalysen verwendet werden, können die für den Prüfungsgegenstand einmalig entwickelten Datenanalyselogiken im Rahmen eines Follow-up erneut genutzt werden, um eine gemeldete Maßnahmenumsetzung messbar bzw. überprüfbar zu machen.

Abb. 17: Der Mehrwert von CA für das Follow-up[37]



Durch den Anstieg der zu einer Prüfung zugeordneten KAIs kann zudem eine mangelnde Umsetzung vor der Meldung einer Umsetzung oder nach Abschluss der Maßnahmenverfolgung sichtbar werden, sodass kurzfristig auf diese Veränderungen reagiert werden kann. Somit können nach der Vereinbarung von Maßnahmen eben diese KAIs herangezogen werden, um die nachhaltige Realisierung von Maßnahmen zu überwachen. Bei einem erhöhten Anstieg von Auffälligkeiten kann mit einer Handlung wie bspw. der Aktualisierung

[37] Vgl. „Der Mehrwert von Continuous Auditing für die Prüfungsdurchführung, die Berichterstattung und das Follow-up“, Jacka, C. et al., ZIR 05/2018, Erich Schmidt Verlag Berlin, S. 237ff. und Bauch, M., Kriegelstein-Sternfeld H., Die inverse Beziehung zwischen Continuous Auditing und der Digitalisierung, Fachvortrag DIIR Digitale Tage 2019.

der Risikobewertung oder der Initiierung einer Ad-hoc-Prüfung reagiert werden. Die kontinuierliche Weiterverwendung der KAIs kann zur Initiierung einer Follow-up Prüfung und auch der erneuten Aufnahme eines Prüfungsobjektes in die Jahresplanung führen. Damit besteht die Möglichkeit, auch nach Abschluss der Maßnahmenverfolgung frühzeitig einen Anstieg eines zugeordneten Risikos zu erkennen und schneller mit Handlungen zu reagieren. Im Rahmen des Einsatzes von Kennzahlen für das Follow-up ist die Festlegung von unterschiedlichen Schwellenwerten eine Möglichkeit, in Abhängigkeit des Risikos eine Prüfungshandlungstiefe festzulegen. Nicht jede Auffälligkeit sollte automatisch zu einer Eskalation in Form einer Follow-up-Prüfung führen. Die Abbildung 18 zeigt, wie in Abhängigkeit von Schwellenwerten abgestufte Maßnahmen festgelegt werden können.

Abb. 18: Schwellenwerte, die unterschiedliche Maßnahmen nach sich ziehen[38]

Maßnahme	Schwellen-wert	Maßnahmenbeschreibung
Sonderprüfung	> 6%	Fachbereich wird informiert, dass Handlungsbedarf besteht. Initiierung einer zeitnahen Sonderprüfung.
Prüfung auf Basis der Prüfungsplanung	>3%	Fachbereich wird informiert, dass Handlungsbedarf besteht. Fachbereich erhält Rückmeldung. Erstellung Prüfungsvorschlag.
Begleitung	>2%	Fachbereich wird informiert, dass Handlungsbedarf besteht. Sondierungsgespräch. Fachbereich erhält Rückmeldung.
Monitoring	>1%	Fachbereich wird informiert, dass Handlungsbedarf besteht. Fachbereich erhält Rückmeldung.
Erste Linie Abdeckung	<=1%	Kein Handlungsbedarf. Fachbereich führt parallel eigenständige kontinuierliche Kontrollhandlungen durch.

Durch die Kombination bereits implementierter Indikatoren mit neuen KAIs werden ggf. zuvor nicht sichtbare Zusammenhänge transparent, was die Identifikation von Verbesserungspotenzialen ermöglicht. Der Aufbau von KAIs für das Follow-up bietet zudem die Chance, die Prüfungsplanung der Folgeperioden mit quantitativen Kennzahlen zu unterstützen. Jene Kennzahlen ermöglichen, wie bereits zuvor erläutert, eine erhöhte unterjährige Flexibilität, um zeitnah auf Veränderungen im Zusammenhang mit den Prüffeldern reagieren zu können.

[38] Vgl. „Der Mehrwert von Continuous Auditing für die Prüfungsdurchführung, die Berichterstattung und das Follow-up“, Jacka, C. et al., ZIR 05/2018, Erich Schmidt Verlag Berlin, S. 237 ff.

4.1.2 Audit Workflow Support

Während sich der Audit Lifecycle Support auf KAIs, die ergänzend zu den klassischen Prüfungshandlungen (u. a. Interview, Prozess Walkthrough) heranzuziehen sind oder diese Prüfungshandlungen zu einem gewissen Maße oder vollständig ersetzen, bezieht, liefert die Verwendung eines CA-Systems für den Audit Workflow-Support u. a. Kennzahlen, die zur Unterstützung des Prüfungsprozesses als solchem herangezogen werden.

Mit Hilfe von Steuerungsgrößen wie bspw. Prüfungsdauer, -zeitverbrauch, -status und Abweichung zur Vorgabe kann jedem Prüfungsleiter ein Dashboard zur internen Steuerung seiner Prüfungen bereitgestellt werden. Aufgrund einer kontinuierlichen Aktualisierung der Kennzahlen, kann dieser somit auf jegliche Änderungen ad hoc reagieren und bspw. seine zur Verfügung stehenden Ressourcen anders zuordnen. Der manuelle Kontroll- und Steuerungsbedarf kann durch den Einsatz von CA-Methoden reduziert werden. Durch die Kombination dieser internen Steuerungskennzahlen mit weiteren Kennzahlen wie bspw. der Anzahl offener Follow-up-Punkte[39] oder deren Kritikalität kann zudem ein vollumfängliches KAI-Reporting aufgebaut werden, welches der Revisionsleitung, der Geschäftsführung oder den Vorständen zu jedem Zeitpunkt bereitgestellt werden kann. Ziel sollte es sein, ein standardisiertes Reporting-Dashboard je Berichtsebene zu implementieren, welches – ohne manuell eingreifen zu müssen – kontinuierlich aktualisiert wird. Die aufwändige manuelle Erstellung von komplexen Präsentationen je Berichtsebene zu unterschiedlichen Anlässen kann somit reduziert werden. Dadurch können freigesetzte Ressourcen anders eingesetzt werden.

[39] Anzahl der offenen vereinbarten Maßnahmen und Empfehlungen aus durchgeführten Prüfungen.

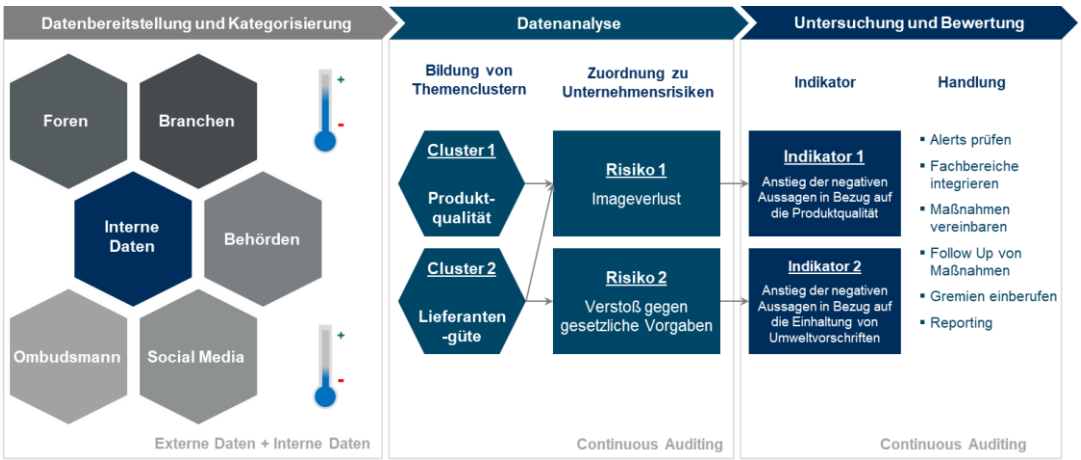
Abb. 19: Beispiele für einen Audit Workflow-Support

Agile Planung & Steuerung	Individuelle Dashboards zur internen Prüfungssteuerung je Prüfungsleiter unter Verwendung von Steuerungskennzahlen wie bspw. Prüfungsdauer und Prüfungszeitverbrauch
Continuous Management Dashboard	Standardisierte Management Dashboards je Berichtsebene (u.a. Revisionsleiter und Vorstand) Kombination von internen Steuerungs- und weiteren Kennzahlen wie bspw. die Anzahl offener Maßnahmen
Automated Approval Workflow	Automatisierung von Workflows zur Genehmigung von Meilensteinen
Automated Quality Management	Automatisierung von Kontrollen des Internen Kontrollsystems der Internen Revision / Quality Gates Automatisierte Quality-Checks bspw. hinsichtlich von Doppelungen und Arbeitsfehlern in Dokumenten
Automated Issue Management	Automatisiertes tägliches Screening von Informationen aus unterschiedlichen Datenquellen (u.a. Internet, externe Datenbanken) mit Hilfe von Text-Mining zur Verbesserung der Prüfungsplanung & -vorbereitung
Knowledge Search	Aufbau von Suchfunktionalitäten, um Inhalte aus Audits, Wissensdatenbanken für alle Prüfer gezielt zugänglich zu machen
Digital Audit Approach	Digitalisierung von Prüfleitfäden/-checklisten & Analyse der Prüfungsanforderungen hinsichtlich der Automatisierung oder Unterstützung durch Datenanalyselogiken
Sample Selection Tool	Stichprobenauswahl anhand von Auffälligkeitskriterien
Automated document tray	Automatisierte systematische Ablage von Dokumenten, die bspw. vom Geprüften bereitgestellt werden.
Unstructured Data Analyzing	Automatisierte Analyse bspw. von Lieferanten- & Kundenverträgen hinsichtlich bestimmter Prüfkriterien (Beispiel: 2 Unterschriften mit entsprechenden Berechtigungen vorhanden)
Automated Text-Mapping / Generation	Automatisierte Zuordnung von fest definierten Themen zu Feststellungen / Generierung von Schlag-/Stichwörtern für Textpassagen und Berichte

In Abhängigkeit des Nicht-/Vorhandenseins einer IT-Infrastruktur bspw. in der Ausprägung eines Audit Management Systems kann auch die Anforderung bestehen, den manuellen Genehmigungsworkflow von der Planung bis zum Follow-up zu automatisieren. Jener Genehmigungsworkflow geht einher mit der Qualitätssicherung über sogenannte Quality-Gates, die mit bestimmten Meilensteinen im Prozess gleichzusetzen sind. Über einen automatisierten Workflow können somit je Prüfung entsprechende Genehmigungsschritte historisiert, ohne Systembrüche und unveränderbar aufbewahrt werden.

Eine weitere Variante eines Workflow-Supports stellt das automatisierte Issue Management dar. Dies beinhaltet ein kontinuierliches automatisiertes Screening von externen Informationen aus unterschiedlichen Datenquellen (u. a. Internet, externe Datenbanken), welches mit Hilfe von Text-Mining-Methoden ermöglicht wird.

Abb. 20: Kombination von internen & externen Daten zur Bildung von KAIs[40]



Durch die Kombination von externen Informationen wie bspw. News über Schlüsselliefe-ranten (u. a. über Qualitätsprobleme, Rohstoffengpässe), Unternehmens-/Industriebench-marks und geopolitische Risiken mit internen Informationen kann das Resultat durch den Prüfungsleiter für die Prüfungsplanung in Form von Kennzahlen oder Risikohinweisen her-angezogen werden. Im Rahmen der Prüfungsvorbereitung können zudem pro Prüffeld auf-bereitete Informationen die Erstellung eines Arbeitsprogramms verbessern. Weiterhin kön-nen Text-Mining-Algorithmen auch für die automatisierte Zuordnung von fest definierten Themen (Zuordnung zu Prüffeldern, Zuordnung von Key-Words) zu Feststellungen ver-wendet werden. Anhand historischer Daten kann ein Algorithmus angelernt werden, um Schlagwörter zu generieren, die entsprechend zugeordnet werden. Diese Stichwortgene-rierung kann natürlich auch für jegliche Textpassagen oder vollständige Berichte verwen-det werden.

Ergänzend zu einem CA-System im engeren Sinne unter Verwendung von standardisier-ten KAIs, können auch Dokumente des Geprüften, die über einen zentralen Ablageort (Laufwerk, Dokumentenmanagementsystem) eingehen, automatisiert und systematisch weiterverarbeitet werden. Neben Ablegen, Ergänzung von Informationen (z. B. Bereitstel-lungsdatum) oder Entpacken kann auch eine Ablageübersicht erstellt werden, die als zent-rales Trackingdokument verwendet werden kann. Hier könnte zudem ein automatisierter Abgleich mit der Dokumentenanforderung hergestellt werden. Weiterhin kann auch eine Update-E-Mail-Funktion implementiert werden, die die Prüfungsteams täglich darüber in-formiert, ob die angeforderten Dokumente vollständig und fristgerecht bereitgestellt wurden bzw. noch ausstehen, obwohl die Bereitstellungsfrist erreicht wurde.

---

[40] Bauch M., Kriegelstein-Sternfeld H.: Antwort der Revision auf komplexere Prüfungsanforderungen: Conti-nuous Auditing, DIIR Kongress, 15. November 2017.

Die Verwendung eines CA-Systems in Form des Audit Workflow-Supports bedeutet im weitesten Sinne, dass der Grad der Automatisierung in den Support-Prozessen erhöht wird, um die Effektivität und Effizienz einer Internen Revision zu steigern. Ziel ist es hierbei, eine toolbasierte ganzheitliche Betrachtung der internen Revisionsprozesse herzustellen. Ein Mittel zum Zweck ist die sogenannte Robotic Process Automation (RPA), bei der manuelle Tätigkeiten durch Softwareroboter, auch Bots genannt, erlernt werden und künftig kontinuierlich und automatisiert ausgeführt werden.[41]

4.2 CA-Unterstützung außerhalb des Standardprozesses der Internen Revision

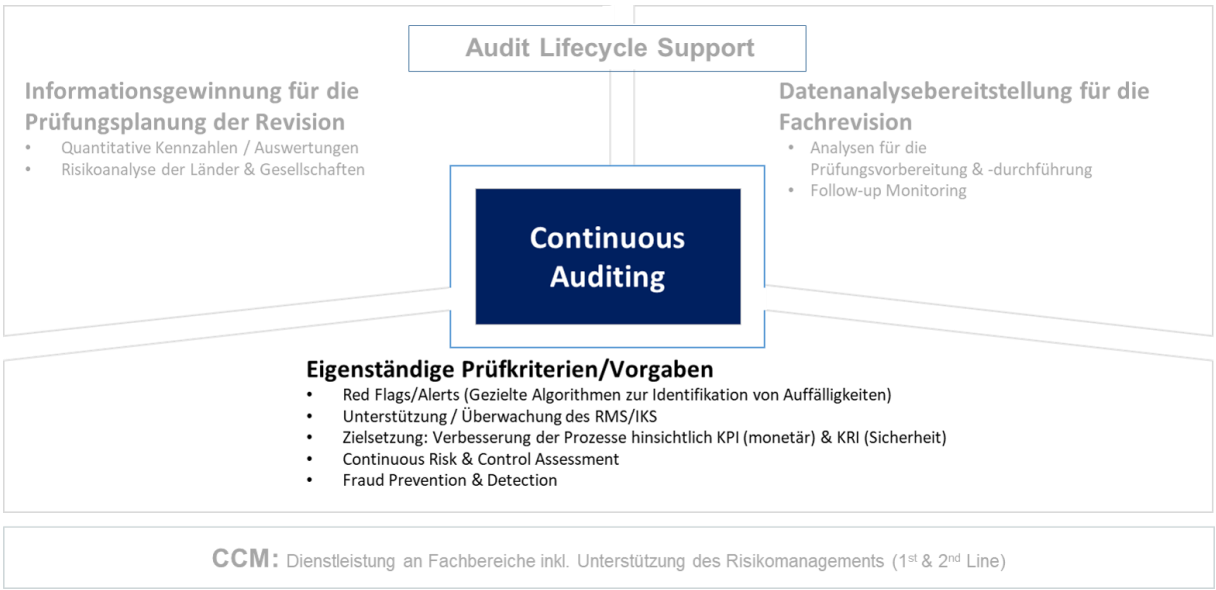
4.2.1 Übersicht eigenständiger Prüfkriterien/Vorgaben

Eine wesentliche Ausprägung eines CA-Systems stellt die Verwendung eigenständiger Prüfkriterien/Vorgaben dar: Darunter sind letztendlich jegliche KAIs zu verstehen, die nicht den regulären Audit Lifecycle unterstützen, sondern zusätzlich hierzu und eigenständig verwendet werden. In der Regel stellen strukturierte Daten aus im Unternehmen eingesetzten ERP-Systemen und/oder Datenbanken die Grundlage eines solchen eigenständigen CA-Systems dar. Verwendet werden zumeist KAIs mit dem Charakter eines Red Flags/Alerts. Hierbei handelt es sich um gezielte Algorithmen zur Identifikation von Auffälligkeiten in Prozessen. Eine Auffälligkeit zu definieren, stellt eine der größten Herausforderungen dar. Sie kann sich aus einem KAI oder aus der Kombination von KAIs ergeben, für die Schwellenwerte zu hinterlegen sind. Auch bei einem solchen eigenständigen CA-System ist es entscheidend, dass diese Auffälligkeiten analysiert bzw. geprüft werden und entsprechende Maßnahmen/Handlungen abgeleitet werden. In Abhängigkeit des Zusammenarbeitsmodells kann eine Auffälligkeit von der Internen Revision und/oder durch verantwortliche Fachbereiche (gemeinsam) analysiert werden. Ein mögliches Zielszenario für den Einsatz eigenständiger Prüfkriterien/Vorgaben ist, dass fachbereichsübergreifend das RMS/IKS unterstützt oder überwacht wird (Continuous Risk & Control Assessment), um u. a. Risiken zu identifizieren, die letztendlich durch die nachgelagerte Umsetzung von Maßnahmen künftig beherrscht werden sollen (Risikosteuerung und -

[41] Vgl. Christian Czarnecki, Gunnar Auth: Prozessdigitalisierung durch Robotic Process Automation. In: Digitalisierung in Unternehmen: Von den theoretischen Ansätzen zur praktischen Umsetzung (= Angewandte Wirtschaftsinformatik). Springer Fachmedien Wiesbaden, Wiesbaden 2018, ISBN 978-3-658-22773-9, S. 113-131, doi:10.1007/978-3-658-22773-9_7 (springer.com [abgerufen am 14. August 2019]).

minimierung). Durch die Abbildung des implementierten IKS können Kontrolllücken und -schwächen identifiziert werden. Ein weiteres Ziel ist es, Verbesserungspotenziale in Bezug auf monetäre Aspekte zu heben. Ein wesentlicher Erfolgsfaktor eines CA-Ansatzes auf Basis von Prüfkriterien ist es, Daten aus unterschiedlichen Systemquellen zu kombinieren, um fachbereichsübergreifende Prozesslücken & -schwächen zu identifizieren. Je nach CA-Ausgestaltung können z. B. Auffälligkeiten bei Security Levels, Logging, Incidents, IT-Konfigurationen, Applikationskontrollen oder Funktionstrennungsaspekte überwacht und somit betrügerische Aktivitäten[42] frühzeitig erkannt werden.[43]

Abb. 21: Ausprägungen von CA-Systemen[44]



4.2.2 Initiierung von Ad-hoc-Prüfungen durch die Anwendung eines CA-Systems

Neben der Verwendung von KAIs für den Audit Lifecycle stellt ein CA-System auf Basis von Prüfkriterien einen erheblichen Vorteil für die Initiierung von Ad-hoc- bzw. Sonderprü-

---

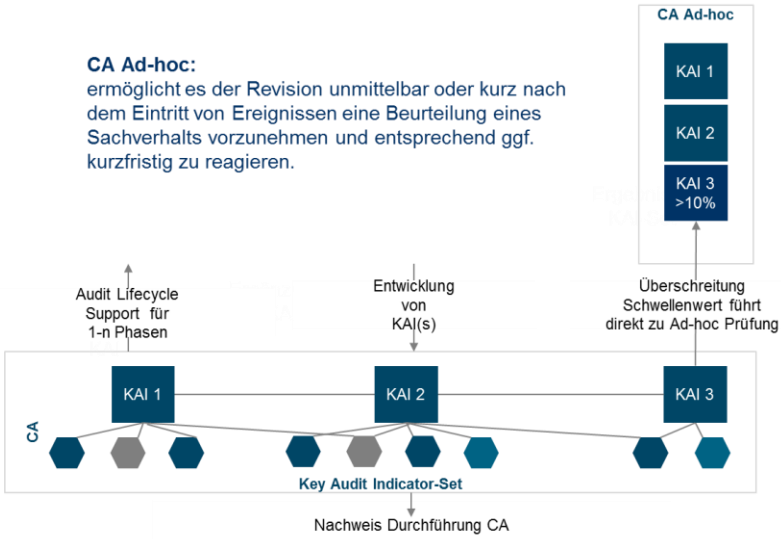
[42] Vgl. Kapitel 4.2.4 Fraud Prevention & Detection.

[43] Vgl. IIA, GTAG Global Technology Audit Guide, Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance, 2nd Edition, March 2015.

[44] Vgl. „Antwort der Interne Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Verlag Berlin, S. 130 ff.

fungen dar. Durch die Entwicklung eines Kennzahlensystems (z. B. aus vergangenen Prüfungen bzw. Datenanalysen) wird eine Interne Revision bei kontinuierlicher Verwendung dazu befähigt, unmittelbar oder kurz nach Eintritt von Ereignissen bzw. Identifikation von Auffälligkeiten eine Beurteilung eines Sachverhalts vorzunehmen und ggf. kurzfristig zu reagieren.

Abb. 22: Interaktion von CA mit und zusätzlich zum Audit Lifecycle[45]



Dies geschieht in der Regel durch das Überschreiten von Schwellenwerten bestimmter KAIs oder einer Kombination von KAIs. Basierend auf dieser Überschreitung kann zudem eine unterjährige Adjustierung der Jahresplanung erfolgen oder dazu führen, dass eine zusätzliche Prüfung initiiert wird, da in einem bestimmten Bereich bzw. für ein Prüfungsobjekt ein erhöhter Risikowert besteht.

Letztendlich werden zeitnah Ressourcen zu den risikoreichsten Prüfungsobjekten zugeordnet oder dafür eingesetzt, um auffälligkeitsbasierten Hinweisen im Rahmen einer Ad hoc-Prüfung nachzugehen. Dabei ist nicht zwingend eine Prüfung zu initiieren. Alternativ kann auch in Abhängigkeit des Risikos der Fachbereich per Workflow- oder E-Mail-Benachrichtigung darum gebeten werden, diese Auffälligkeit zu prüfen. Z. B. könnte bei einer Überschreitung der tolerierbaren Ausfallquote der geleisteten Anzahlungen um mehr als 10% eine Aufforderung an das verantwortliche Management mit der Bitte um Stellungnahme erfolgen. Bei mehr als 25% Überschreitung oder bei Auffälligkeiten von weiteren KAIs könnte das Interne Revisionsmanagement entscheiden, eine Ad-hoc-Prüfung zu initiieren.

---

[45] Vgl. „Der Mehrwert von Continuous Auditing für die Prüfungsdurchführung, die Berichterstattung und das Follow-up“, Jacka, C. et al., ZIR 05/2018, Erich Schmidt Verlag Berlin, S. 237 ff.

4.2.3 Newsscreening/Issue Management mit Textmining

Beim Einsatz von CA-Systemen können neben im Unternehmen vorliegenden Daten, auch so genannte unstrukturierte Daten, wie bspw. Bilder, Videos, eingescannte Geschäftsunterlagen, Notizen oder PowerPoint-Präsentationen verwendet werden. Zusätzlich hierzu sind Informationen aus dem Internet bzw. den sozialen Medien (u. a. Nachrichten, Kommentare, Chats, Forenbeiträge) zu nennen, die der Kategorie unstrukturierter Daten bzw. semistrukturierter Daten zugeordnet werden. Unstrukturierte Daten müssen mithilfe von Modellen zunächst in ein verarbeitbares, einheitliches Format gebracht werden, um hinsichtlich bestimmter Fragestellungen analysiert werden zu können. Zusammengefasst werden qualitative Daten durch ausgewählte Datenanalysetechniken wie bspw. die Methode des Textminings in quantitative Daten überführt und auswertbar gemacht. Die Automatisierung des Newsscreening bzw. Issue Management in der Internen Revision durch den Einsatz von Text-Mining-Methoden stellt einen konkreten Anwendungsfall dar.[46]

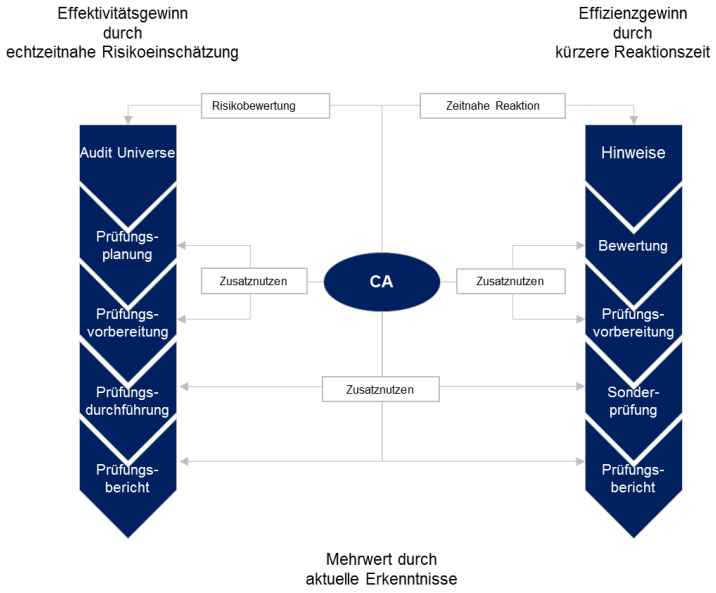
Für die initiale, risikoorientierte Prüfungsplanung und die unterjährige Anpassung dieser Planung aufgrund von Sondersituationen stellen Nachrichten bspw. über das eigene Unternehmen, seine Lieferanten, Kunden, die Konkurrenz, gesetzliche Veränderungen oder Änderungen der Marktsituation entscheidende Faktoren dar. Ein sogenanntes Issue Management bezeichnet das Risiken- und Chancen-Management von Organisationen. Ein Issue stellt ein bestimmtes Thema, einen Aspekt oder Ereignis dar (innere oder äußere Entwicklung/Veränderung), das dazu geeignet ist, erfolgskritischen Einfluss auf die Handlungsfähigkeit einer Organisation bzw. die Zielerreichung zu nehmen.[47] Organisationsrelevante Ereignisse sollen frühzeitig erkannt werden, um kurzfristig reagieren zu können. In vielen Internen Revisionen wird ein solches Management in manueller Form durchgeführt, um bestimmte Aspekte in die Prüfungsplanung einfließen zu lassen.

---

[46] Vgl. „Einsatz von Continuous Auditing: Einsatz von Continuous Auditing: Herausforderungen und Blick in die Zukunft, Bauch, M. et al., ZIR 06/2019, Erich Schmidt Verlag Berlin, S. 248 ff.

[47] Vgl. Gabler Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/issues-management-52703.

Abb. 23: Der Mehrwert von CA durch aktuelle Erkenntnisse[48]



Durch die Möglichkeit, unter Einhaltung der Datenschutzgesetze, interne und externe, unstrukturierte Daten mit der Methode des Text Mining auswertbar zu machen, kann dieser manuelle Prozess automatisiert werden, um durch bestimmte Informationen eine (echt-) zeitnahe Risikoeinschätzung für die Prüfungsplanung durchzuführen oder bei der Häufung von textuellen Hinweisen eine Ad-hoc-Prüfung zu initiieren.

4.2.4 Fraud Prevention & Detection

Fraud Prevention & Detection hat die frühzeitige Erkennung potenzieller Betrugsfälle zum Ziel und versucht, weitere Betrugsversuche zu unterbinden. Einen Einstieg bildet auch hier die kontinuierliche Überwachung von KAIs, welche zielführend zur Identifikation von Prozessabweichungen oder der Häufung von bestimmten Ereignissen eingesetzt wurden. So kann z. B. eine Versicherungsgesellschaft eingereichte Schadensmeldungen systematisch untersuchen, um Betrugsversuche aufzudecken. In diesem Zusammenhang kann es ggf. notwendig sein, weitere Details zu erheben und Themenkomplexe/Aggregationen über Schadensmeldungen zu bilden. Dabei ist das Vorgehen bei der Aggregation, d. h. die bewusste, zielführende Kombination einzelner Informationsbausteine, für die Aussagekraft der Analyseergebnisse ausschlaggebend. So kann eine Häufung von Schadensfällen unmittelbar unterhalb bestehender Freigabegrenzen eine erste Indikation darstellen, welche

[48] Vgl. „Antwort der Interne Revision auf komplexere Prüfungsanforderungen: Continuous Auditing“, Bauch, M. et al., ZIR 03/2017, Erich Schmidt Verlag Berlin, S. 130 ff.

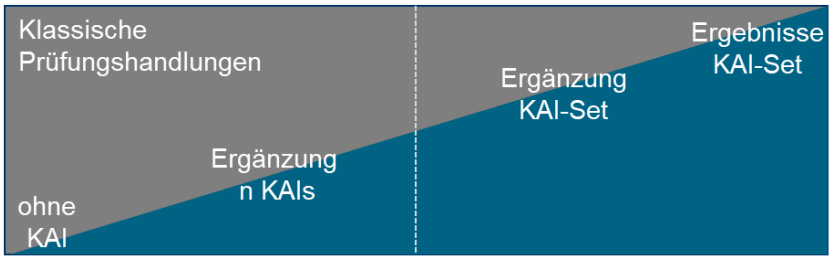
genauer zu betrachten ist. Durch die Ergänzung um Bearbeitungs- oder Buchungszeitpunkte sowie ggf. pseudonymisierte Antragssteller und/oder Sachbearbeiter lassen sich weitere zielführende Indikationen realisieren.

Die unterschiedlichen Datenanalysetools am Markt bieten hier bereits standardisierte Auswertungsmöglichkeiten, z. B. Lückenanalysen (Beleg- oder Sortierungslücken), Benford-Analysen (Abweichungsanalyse als Vergleich von Ziffernmustern in Datenbeständen mit der Erwartungshaltung des Benfordschen Gesetzes) oder Doppelbelegungsanalysen. Einige Toolanbieter und Berater haben darüber hinaus bereits eine Vielzahl von Fraud-Indikatoren entwickelt, welche meist auf ERP-Systemdaten und den Standard-Workflows in ERP-Systemen aufbauen. Sollte eine hohe Anzahl spezifischer Anpassungen an ERP-Standprozessen und -einstellungen im Unternehmensumfeld realisiert worden sein, so können diese standardisierten Analysen ggf. nicht ohne ebenfalls notwendige Anpassungen verwendet werden.

4.2.5 Vollautomatisiertes CA-System ohne Interaktion mit dem Audit Lifecycle

Bei der Darstellung der Zusammenarbeitsmodelle wurde bereits ausgeführt, dass es unterschiedliche Szenarien gibt. Des Weiteren variiert die Anzahl vorhandener KAIs in einem CA-System und das Verhältnis zwischen der Verwendung der KAI-Ergebnisse zu den klassischen Prüfungshandlungen einer Internen Revision.

Abb. 24: Automatisierungs- und Verwendungsgrad eines CA-Systems[49]



Die Erhöhung des Automatisierungs- und Verwendungsgrad der vorhandenen KAIs führt dazu, dass klassische, oft manuelle und zeitintensive individuelle Prüfungshandlungen reduziert werden können.

[49] Bauch, M., Kriegelstein-Sternfeld H., Die inverse Beziehung zwischen Continuous Auditing und der Digitalisierung, Fachvortrag DIIR Digitale Tage 2019,16.05.2019.

So ist es möglich, dass durch die Interne Revision entwickelte KAIs vollautomatisiert auf Basis eines Zeitplans durchgeführt werden. Dabei können bestimmte Analysen aufeinander aufbauen und vorhergehende Ergebnisse im Rahmen nachgelagerter Analysen verwendet werden. Beispielhaft können Prüfroutinen genannt werden, welche automatisiert zu festen, regelmäßigen Zeitpunkten durchgeführt und zur Bearbeitung weitergeleitet werden. Anschließend werden die Ergebnisse um weitere Informationen bzgl. Zeitpunkt und Prozessfluss ergänzt. Es ist vorab zu klären, wer der Empfänger der hier erzeugten Ergebnisse sein soll (Interne Revision und/oder die Fachabteilung). Bei einer exklusiven Verwendung der Ergebnisse durch Adressaten im Fachbereich besteht die Notwendigkeit, dass dieser die inhaltliche Verantwortung der Analysen und Ergebnisse (auch in Form einer Qualitätssicherung) übernimmt (vgl. Kapitel 3.3 Zusammenarbeitsmodelle). Es muss sichergestellt sein, dass der Fachbereich die Prüfmethodik kennt, um die Ergebnisse korrekt interpretieren zu können. Dabei können und müssen sie regelmäßig auf Aktualität geprüft werden. Anpassungen an den Prozessen oder den Datenmodellen der unterstützenden Systeme erfordern möglicherweise eine Anpassung der KAIs. Da es im Kontext ggf. keinen Rückfluss von Informationen zur Internen Revision gibt bzw. die Ergebnisse nicht ergänzend auch durch die Interne Revision verwendet werden, können diese auch keinen Einfluss auf den Audit Lifecycle nehmen. Hier wird in Abhängigkeit der Prozessverantwortung ggf. auch die Grenze vom CA hin zum CM überschritten (vgl. auch Kapitel 1.4 Allgemeine Definitionen).

Ein vollautomatisiertes CA ohne Interaktion mit dem Audit Lifecycle bedeutet dementsprechend, dass ein umfangreiches KAI-Set vollumfänglich und eigenständig implementiert ist und Analyseergebnisse automatisiert erstellt und direkt zur Umsetzung per Workflow an die Empfänger adressiert werden. Die Umsetzung bzw. die durchgeführten Handlungen werden anschließend an das CA-System gemeldet.

Die folgenden Veränderungen können somit mit einem vollautomatisierten CA für die Interne Revision eintreten:

- Kontinuierliche und damit weitestgehend automatisierte Überwachung der Kontrollen und Prozesse eines Unternehmens
- Realtime Abbildung wichtiger Unternehmensindikatoren
- KAIs ersetzen klassische Prüfungshandlungen zu 100%
- Workflow und/oder E-Mail-Benachrichtigung bei Überschreiten von Schwellenwerten
- Prüfungsberichte/-ergebnisse werden automatisiert erstellt und in digitaler Form adressiert
- Implementierung von workflowbasierten Freigaben
- Prüfungsdurchführung vor Ort ist nicht immer notwendig, sodass Reisezeit und Reisekosten eingespart werden können. Die Prüfung kann teilweise oder vollständig aus der Ferne erfolgen.

Als Einschränkung ist hervorzuheben, dass je höher der Automatisierungs- und Verwendungsgrad eines CA-Systems ist, desto mehr Wissen und Transparenz gehen über die Geschäftsprozesse durch fehlende Beobachtung und Befragung verloren. Das beste CA-System kann derzeit, auch unter Einbezug der Erfahrungen der Sondersituation während der Pandemie, nicht die fachlichen und sozialen Kompetenzen eines Revisors ersetzen. Die Disposition- und Steuerungsfähigkeiten wie auch das Urteilsvermögen des qualifizierten Revisors sind vermeintlich unverzichtbar.

4.2.6 Risikofrüherkennung/Präventive Ansätze

Wie an verschiedenen vorhergehenden Stellen bereits dargestellt, dient die kontinuierliche Überwachung der KAIs auch der frühzeitigen Identifikation von Risiken. So kann z. B. ein tieferliegendes Problem durch die Auswertung von Kundenbeschwerden erkannt werden, sollte ein Sachverhalt gehäuft oder häufiger als zuvor auftreten. Hierzu ist es ggf. wiederum notwendig, weitere Details zu erheben und Kundenbeschwerden zu aggregieren. Dabei liegen wahrscheinlich unstrukturierte Daten (z. B. aus Freitextfeldern) vor, welche zunächst umzuwandeln sind.

Bei einer übergreifenden Feldanalyse ist es z. B. möglich, Reklamationen auf bestimmte Produktgruppen, Produkte oder noch feiner granuliert auf bestimmte Bauteile zu referenzieren. Durch die Aggregation von Informationen zu messbaren Umgebungsfaktoren (z. B. Nutzungsdauer, Temperaturen, Chargennummern, Lieferantennummern, Zeitpunkte) lassen sich zielgerichtete Cluster bilden. Dies kann präventiv als Ausgangspunkt für eine Qualitätsüberprüfung dienen, bei welcher sowohl Roh- und Betriebsstoffe, Zulieferteile oder auch Prozessabläufe und Kontrollen durch die Qualitätssicherung eines produzierenden Unternehmens fokussiert werden können. Aber auch im Handel oder bei Dienstleistern können entsprechende Analysen umgesetzt werden.

Die verwendeten Risikoindikatoren und die Erhöhung der entsprechenden Risikowerte veranlassen ggf. auch die Interne Revision, eine Anpassung an der Prüfungsplanung vorzunehmen. Die Ergebnisse dieser Untersuchungen dienen auch dazu, möglichen rechtlichen und regulatorischen Verstößen sowie wirtschaftlichen Schäden und Reputationsschäden entgegen zu wirken.

5 Software-Unterstützung in CA-Systemen

5.1 Software-Architekturmodelle

Der Aufbau eines CA-System im eigenen Unternehmen steht in Abhängigkeit u. a. zu der Governance-Struktur, der Auslegung der Rolle der Internen Revision im Unternehmen, der vorhandenen IT-Infrastruktur, IT-Systemen, Datenquellen, Datenmengen und der etablierten CM-Systeme in der ersten und zweiten Linie. Wichtig ist hervorzuheben, dass ein CA-System bei jedem Unternehmen anders ausgeprägt sein kann. Ausgehend von den individuellen Rahmenbedingungen und einer Kosten-/Nutzenanalyse kann ein CA-System auf Excel, Datenanalyse- oder -Miningtools, Datenbankabfragen bis hin zu Process-Miningtools und eigenen programmierten Systemen basieren. In Abhängigkeit der zu verarbeitenden Datenmenge bspw. im Big-Data-Umfeld und der Umwandlung von unstrukturierten in strukturierte Daten sind zudem entsprechende Software Frameworks, Hardware und Architekturen aufzubauen bzw. vorhandene IT-Infrastrukturen, Datenbanken und/oder Data Lakes[50] zu nutzen.

Um alle Vorteile von CA-Systemen auszuschöpfen, ist die Anwendung passender Software empfehlenswert. Die damit verbundene Automatisierung ist dabei nicht nur auf die Analyse von Daten begrenzt, sondern mag sich auch über mögliche, vorgelagerte Schritte, bspw. die Datenextraktion erstrecken. Aufgrund der vielfältigen Anwendungsgebiete existieren am Markt viele verschiedene IT-Lösungen, die sich zur Automatisierung von CA-Systemen eignen. Trotz dieser Vielfältigkeit unterscheiden Theorie und Praxis bei der technischen Umsetzung von CA-Systemen im Wesentlichen zwischen zwei systemseitigen Architekturen: Embedded Audit Modules (EAM) und Monitoring Control Layer (MCL).

- **EAM-Architektur:** Kern der EAM-Architektur ist ein Prüfungsmodul, welches in ein bereits bestehendes IT-System (welches den Prüfungsgegenstand digital abbildet) eingebettet und somit Teil dieses Systems ist. Um eine technische Kompatibilität zu gewährleisten, muss bei der Einbettung die gleiche Programmiersprache und -logik verwendet werden. Dies ermöglicht auch bei großen Datenmengen sehr kurze Verarbeitungszeiten. Prüfmodule in einer EAM-Architektur gliedern sich aus Anwendersicht

[50] Vgl. Gartner.com: Ein Data Lake ist ein Konzept, das aus einer Sammlung von Speicherinstanzen verschiedener Datenbestände besteht. Diese Assets werden in einer nahezu exakten oder sogar exakten Kopie des Quellformats gespeichert und sind eine Ergänzung zu den ursprünglichen Datenspeichern. (https://www.gartner.com/en/information-technology/glossary/data-lake).

vergleichsweise nahtlos in das bestehende System ein, sodass der Anwender aufgrund der funktionalen und visuellen Ähnlichkeit zum bestehenden System nur eine vergleichsweise kurze Eingewöhnungsphase benötigt. Datenzugriff und Datenextraktion erfolgen nach den bekannten Vorgehensweisen.

In EAM-Architekturen verlassen die zu analysierenden Daten in der Regel das eigentliche IT-System nicht und müssen somit keinen zusätzlichen Security- bzw. Datenschutzanforderungen unterworfen werden. Jedoch liegt der Betrieb des IT-Systems und somit auch die Hoheit über Zugriffsrechte und Security-Parameter häufig im Verantwortungsbereich von Fachabteilungen (CM).

- **MCL-Architektur:** MCL-Architekturen hingegen umfassen als wesentlichen Bestandteil ein außerhalb des bestehenden IT-Systems gelagertes, eigenständiges Prüfsystem, das relevante Informationen aus dem bestehenden IT-System extrahiert und extern analysiert. Das Prüfsystem stellt in dieser Architekturvariante somit eine eigene Schicht dar, die Aufgaben wie Datenextraktion, Datenfilterung, Datenharmonisierung, Datenanalyse und Ergebnisaufbereitung übernehmen kann. Aufgrund seiner unabhängigen Natur kann das Prüfsystem leichter Daten aus verschiedenen Quellen verwerten und bietet sich somit für Unternehmen mit vielen IT-Systemen bzw. mit einer heterogenen IT-Landschaft ganz besonders an. Dem Prüfer selbst bietet sich bei einem eigenständigen Prüfsystem (bspw. ein Revisions-DWH) die Möglichkeit, Parameter und andere Einstellung selbst zu setzen.

  MCL-Architekturen hingegen fallen oftmals in den Verantwortungsbereich der Internen Revision und lassen somit einen höheren Grad der Unabhängigkeit und Selbstbestimmung seitens der Prüfer zu. Aufgrund ihrer „externen“ Lage bedürfen diese allerdings häufig einer Berücksichtigung verschärfter Datenschutz- und Security-Vorgaben, insbesondere dann, wenn Daten außerhalb der bestehenden IT-Infrastruktur (z. B. direkt beim Anbieter oder in einer externen Cloud) gespeichert oder verarbeitet werden. Viele Systeme bieten entsprechende Datensicherheits- und Verschlüsselungsfunktionalitäten an.

Neben diesen beiden Architekturmodellen finden sich in der Praxis eine Reihe von Hybridvarianten in unterschiedlichen Ausprägungen. Die Auswahl der Architekturausprägung bzw. der spezifischen Anwendung sollte daher generell situationsabhängig geschehen. Zu berücksichtigende Faktoren sind dabei u. a. die Beschaffenheit der bestehenden IT-Infrastruktur, Zielsetzung und Umfang der geplanten CA-Aktivitäten, sowie die Erfahrung des Prüfers mit derartigen IT-Anwendungen. Etwaige Voraussetzungen, bspw. hinsichtlich der Verfügbarkeit von Daten auf der einen Seite, sowie der Verschlüsselung von Daten und der Einhaltung von Security-Parametern auf der anderen Seite sollten vollumfänglich identifiziert und berücksichtigt werden.

5.2 Einsatzszenarien der Datenanalyse für die Interne Revision

Für die Zwecke der Prüfungs- und Beratungstätigkeiten des Revisors stellen neben Dokumenten und Nachweisen die Daten des Unternehmens eine belastbare Informationsquelle dar. Die Datenanalyse unterstützt den Revisor in der Prüfung, Beratung und der Ermittlung von Schwellenwerten der Key Audit Indicators (KAIs), die für das Continuous Auditing Anwendung finden können.

Im Folgenden werden nach der Definition die Methoden und Einsatzmöglichkeiten der Datenanalyse im CA-System beschrieben.

Definition der Datenanalyse

Datenanalyse[51] wird definiert als Methode, mit der aus Einzeldaten zusammenfassende Informationen (Kenngrößen) gewonnen und tabellarisch oder grafisch dokumentiert werden. Datenanalysen können in folgende Bereiche eingeteilt werden:

- **Deskriptive Datenanalyse:** Bei einer Totalerhebung oder einem Datensatz kann die deskriptive Datenanalyse Informationen verdichten und Wesentliches mit Hilfe von Tabellen, graphischen Darstellungen und charakteristischen Maßzahlen darstellen.
- Die **inferenzielle Datenanalyse** ermöglicht die Übertragung von Stichprobenbeständen auf die Grundgesamtheit.
- Mit der **explorativen Datenanalyse** werden Datenmengen verarbeitet, um Strukturen und Zusammenhänge zu zeigen und zu entdecken.[52]
- Anhand der **konfirmatorischen Datenanalyse** lassen sich Zusammenhänge überprüfen (z. B. Regressionsanalyse).

Revisorische Methoden der Datenanalyse

Manuelle Ad hoc-Datenanalyse

Revisoren können sich sowohl bei Regel-, Sonderprüfungen als auch bei Themen, die sich nur mit der Auseinandersetzung der vorliegenden Daten erschließen lassen, der Ad-hoc-Datenanalyse bedienen. Die Ad-hoc-Datenanalyse ermöglicht dem Revisor belastbare Er-

---

[51] https://wirtschaftslexikon.gabler.de/definition/datenanalyse-30331, 02.09.2019.
[52] Vgl. Kapitel 7. Process Mining.

gebnisse und Erkenntnisse des konkret zu untersuchenden Themenkomplexes zu ermitteln. Aufgrund der meist einmaligen bzw. spezifischen Durchführung handelt es sich um eine klassische, nicht standardisierte Datenanalyse.

Bei Ad-hoc-Datenanalysen können Revisoren auf Themenbereiche aufmerksam werden, die als KAIs für ein CA-System nützlich sind. Zum Beispiel führt eine Datenanalyse im Bereich Accounts Payable zum Ergebnis, dass Lieferanten Rechnungen zu Bankverbindungen in dem Land ihres Firmensitzes, aber auch zusätzlich zu Bankverbindungen in potenziellen Steuerhäfen (Tax Havens) stellen. Diese Information könnte daher in ein CA-System einfließen und ein KAI pro Quartal anzeigen, wie viele Rechnungen und welche Rechnungssummen auf potenziell kritische Bankverbindungen überwiesen wurden.

Mögliche Software-Tools für die manuelle Datenanalyse sind IDEA, ACL oder Standard-Makros, z. B. von Excel.[53]

Halbautomatisierte Datenanalyse

Die halbautomatisierte Datenanalyse kennzeichnet sich durch die Kombination von manuellen Handlungen wie einen manuellen Start des Prozesses durch Personen und von automatisch ausgeführten Datenanalyselogiken wie bspw. Skripte. Revisoren können zum Beispiel zu definierten Themenfeldern (z. B. Einkaufsprozesse, die nicht dem Standardprozess folgen) ein automatisches Skript zur Verfügung haben, das ihnen eine fundierte und brauchbare Analyse ermöglicht. Im Rahmen von Revisionsprüfungen fragen Revisoren entweder bei dem jeweils zu prüfenden Fachbereich oder durch eigenen direkten Systemzugriff manuell die benötigten Daten, wie bspw. Zahlungs- oder Einkaufsdaten ab. Für die erhaltenen Daten liefern nach der erforderlichen Datenaufbereitung die automatischen Skripte die Ergebnisse der Datenanalyse.

Ein Hauptgrund bzw. Vorteil des Einsatzes von halbautomatisierten Datenanalysen im Vergleich zur vollautomatisierten Datenanalyse ist die geringere Komplexität der Skripterstellung. Auch wenn die Analysedurchführung teilweise von menschlichen Schritten abhängig ist, gilt diese Variante als kostengünstig und passender für bestimmte Einsatzzwecke (z. B. für kleinere Unternehmen, spezifische Prozessanforderungen). Viele Interne Revisionen, die u. a. aufgrund der Unternehmenskomplexität eine entsprechende Größe aufweisen, implementieren zur Erstellung von Datenanalyselogiken, -module und ggf. zur Aufbereitung von Analyseergebnissen zentrale Datenanalyse-Abteilungen, um Revisoren im Rahmen von Revisionsprüfungen zu versorgen.

---

[53] Diese Aufzählung ist nicht abschließend und nicht als Empfehlung zu interpretieren.

Vollautomatisierte Datenanalyse

Bei der vollautomatisierten Datenanalyse findet die Ausführung von zeitlich gesteuerten Datenanalyselogiken wie bspw. Skripten statt. Diese Methode der Datenanalyse ist vollständig in die IT-Prozessumgebung integriert. Aufgrund der meist komplexen Umsetzung handelt es sich dabei um eine kostenintensivere Lösung, bei der in der Konzeptionsphase eine Kosten-/Nutzenanalyse sinnvoll ist, um den Mehrwert bestimmen zu können.

Vollautomatisierte Datenanalysen finden in einem vollständig eigenständigen Prozess statt. Der Aufruf der zu analysierenden Daten kann zum Beispiel monatlich erfolgen. Für festgelegte Kenngrößen wie Unter-/Überschreitungen oder aktueller Stand werden die Informationen per E-Mail oder Dashboard den relevanten Personen angezeigt. Zum Beispiel werden Revisoren im definierten Zeitabstand die Ergebnisse eines besonders risikoreichen Prozesses des Unternehmens dargestellt, um die Ergebnisse der analysierten Daten auswertbar zu machen.

Datenanalyse in CA-Systemen

Zur Anwendung von CA-Methoden sind für den Revisor manuelle und automatisierte Datenanalysen, wie im Folgenden exemplarisch beschrieben, relevant.

Identifikation von KPIs und Errechnung deren Schwellenwerte

Der Revisor bzw. Ersteller eines CA-Systems wendet die manuelle Datenanalyse an, um für einen definierten Themenbereich die identifizierten KPIs zu erstellen. Auf Basis der Auswertung spezifischer Daten können relevante Messgrößen und Schwellenwerte für die identifizierten KPIs erhoben werden. Es ergeben sich Messgrößen und Schwellenwerte, die einen entsprechenden Soll-Wert darstellen. Im CA-System laufen dann aktuelle Zahlen gegen den festgelegten Soll-Wert und zeigen ein positives (im Soll-Bereich) oder ein negatives Ergebnis (außerhalb des Soll-Bereiches) an.

Regelmäßige Datenanalysen im CA-System

Ein implementiertes CA-System ermöglicht den kontinuierlichen Vergleich von KPIs anhand festgelegter Messgrößen und Schwellenwerte. Dabei werden Unternehmensdaten analysiert, aggregiert und aufbereitet. Das Ziel ist die Ermittlung der Ist-KPIs und dementsprechend des Ist-Zustands der Daten des Unternehmens.

6 Entwicklung und Validierung von KAIs inklusive Schwellenwerten

Dieses Kapitel beschreibt, wie KAIs inklusive Schwellenwerten entwickelt und validiert werden können.

Abb. 25: Definition Key Audit Indicators (KAI)

Definition Key Audit Indicators (KAI)
KAIs sind quantitative Messgrößen, deren aktuelle Werte bzw. Ausprägungen und zeitliche Entwicklungen in einem erkennbaren Kausalitäts-Zusammenhang mit der Eintrittswahrscheinlichkeit der Prüffeld-Risiken und/oder mit der Chance zur Erreichung der Prüffeld-Performance-Ziele stehen.

Überschreitungen der festgelegten Schwellenwerte lösen (angemessene) Aktivitäten zur Ursachenbestimmung (bspw. weiterführende, vertiefende Datenanalysen, Dokumentensichtung, Gespräche mit dem Fachbereich, Sonderprüfung) und ggf. in der Folge oder sofort die Feststellung eines Mangels aus. Die Fachbereiche sollten die KAIs und die für die KAIs aktuell festgelegten Schwellenwerte kennen.[54]

Die Schwellenwerte stellen die Soll-Werte dar, gegen die in einem KAI-basierten CA-System regelmäßig geprüft wird. Die häufige (und regelmäßige) Berechnung des KAI-Werts (Ist-Wert) und der Vergleich mit dem Schwellenwert (Soll-Wert) stellen also de facto eine (automatisierte bzw. perspektivisch automatisierbare) kontinuierliche Prüfungshandlung dar.

Je größer die Steuerungswirkung der KAIs und ihrer Schwellenwerte für die Aktivitäten der Internen Revision im Audit Lifecycle insgesamt ist, desto nachvollziehbarer und begründeter sollte die Wahl eines Schwellenwertes sein. Insbesondere bei der Festlegung der Schwellenwerte spiegelt sich die Verantwortung wider, die die Interne Revision bzgl. eines risikoorientierten und in einem ausgewogenen Aufwand-Nutzen-Verhältnis stehenden Vorgehens im CA-System übernimmt.

[54] Vgl. Kapitel 2.2 Inhaltliche und methodische Rahmenbedingungen und 4.1.1 Audit Lifecycle-Support.

Bei Eignung für das CA-System kann die Interne Revision vom Fachbereich verwendete Indikatoren (z. B. Key Risk Indicators und Key Performance Indicators) als KAIs – ggf. sachgerecht bzgl. des Audit-Ziels modifiziert und/oder kombiniert – nutzen. Durch die Wahl der Schwellenwerte drückt sich dann die unabhängige Einschätzung der Internen Revision hinsichtlich der Bedeutung des Untersuchungsgegenstands für das Unternehmen aus. I. d. R. liegt die Interne Revisionsschwelle im Sinne einer Frühwarnung angemessen unterhalb der Fachbereichsschwelle. Für die Entwicklung von KAI hat sich eine Berücksichtigung von Prüffeld-Risiken und Prüffeld-Performance-Zielen bewährt.[55]

Die Beschreibung eines KAI muss neben der Definition insbesondere die Angabe eines Schwellenwertes enthalten, mittels dessen festgelegt ist, ab wann die o. g. Eintrittswahrscheinlichkeit bzw. Chance als so erhöht bzw. verringert angenommen wird, dass seitens der Internen Revision eine Aktivität zu starten ist.[56]

Ein quantitativer KAI kann auf verschiedene Arten definiert werden:

Absolut (Anzahl, Betrag, andere einheitenbehaftete Größen), bspw.:

- Anzahl überfälliger Rechnungen, z. B. 13
- Anzahl Mitarbeiter in Abt. 4711, z. B. 8
- Summe Doppelzahlungen, z. B. 1000 EUR
- Mittelwert Doppelzahlungen, z. B. 500 EUR
- FX-Kurs, z. B. 1,0 EUR/USD

Relativ, bspw.:

- Durchschnittliche Anzahl Mitarbeiter pro Team im letzten Quartal, z. B. 12
- Eigenkapitalrendite (ROE) im letzten Jahr, z. B. 10%
- Scoring: Kombination mehrerer einzelner Indikatoren zu einem KAI.

Ein KAI darf auf Basis von (aggregierten) (Risiko-)Kennzahlen gebildet werden, z. B. „Auffälliger Sprung der mittleren Ausfallwahrscheinlichkeit“.[57]

Die Verwendung relativer Größen (z. B. Indizes) bietet gegenüber absoluten Größen den entscheidenden Vorteil, dass eine Vergleichbarkeit der KAI-Werte gegeben ist, auch wenn

---

[55] Vgl. Anlage 2: Berücksichtigung von Prüffeld-Risiken und Prüffeld-Performance-Zielen.
[56] Vgl. Anlage 3: KAI-Beschreibung.
[57] Vgl. Anlage 4: KAI auf Basis von Kennzahlen.

sich die absolute Bezugsgröße im Laufe der Zeit ändert. Relative Kennzahlen sind absoluten Größen bei der KAI-Bildung daher i. A. vorzuziehen.

Ein quantitativer KAI ist einem qualitativen KAI vorzuziehen, um mittel- bis langfristig die Möglichkeit zur Automatisierung der Ermittlung des aktuellen KAI-Wertes sicherzustellen. Bspw. könnte das Risiko einer im Fachbereich unsachgemäß durchgeführten Qualitätskontrolle, das sich intuitiv eher durch einen qualitativen KAI beschreiben lässt, durch einen quantitativen KAI abgebildet werden, der die Zeitdauer der Durchführung der Qualitätskontrolle misst, sofern zwischen Dauer und Qualität dieser Tätigkeit ein Kausalzusammenhang angenommen werden kann.

Bei der Verwendung eines quantitativen KAI sollte die Datenqualität im Rahmen der KAI-Validierung regelmäßig überprüft bzw. beurteilt werden.[58]

Sollen für die Berechnung des KAI-Wertes Daten eines historischen Zeitraums verwendet werden (z. B. kurzfristiges vs. langfristiges Mittel), ist die Auswirkung der Länge des betrachteten historischen Zeitraums auf die KAI-Werte zu untersuchen und die Wahl der Länge des Zeitraums (z. B. 1 Quartal, 1 Jahr, 2 Jahre, …) nachvollziehbar zu begründen. Insbesondere wenn eine Zeitreihe von Daten, die in die KAI-Berechnung einfließen, im Zeitverlauf einen Sprung aufweist, ist zu analysieren, inwieweit ältere Werte berücksichtigt werden dürfen. Dabei ist die Vollständigkeit der Daten sicherzustellen.[59]

Auch bei der Verwendung eines qualitativen KAI muss eine angemessene Qualität der Informationen, auf denen der KAI basiert, gegeben sein, d. h., es muss Transparenz bzgl. der Zuverlässigkeit, der Korrektheit, der Zugänglichkeit, der Verfügbarkeit und der Aktualität der benötigten Informationen herrschen.

Die KAI-Definitionen sollten unbedingt mit den Fachbereichen inhaltlich reflektiert werden, da nur durch ausreichende Transparenz des Vorgehens ein für den Erfolg des KAI-basierten CA-Ansatzes notwendiges Akzeptanzniveau im Fachbereich erreicht werden kann.[60]

Für die konkrete Operationalisierung des CA-Systems wird für jeden KAI eines Prüffelds ein Indikatorwert festgelegt, oberhalb dessen die Eintrittswahrscheinlichkeit des Risikos als wesentlich erhöht (und damit als kritisch) angenommen wird.[61] Dieser Wert wird als Schwellenwert bezeichnet. Umgekehrt wird die Eintrittswahrscheinlichkeit des Risikos nicht

---

[58] Vgl. Anlage 5: KAI-Datenqualität.

[59] Vgl. Anlage 6: Daten-Vollständigkeit bei historischem Zeitraum.

[60] Vgl. Kapitel 3.3 Zusammenarbeitsmodelle.

[61] Die Darstellung des Überschreitens eines Schwellenwertes gilt analog für die Unterschreitung eines Schwellenwertes, falls niedrigere Indikatorwerte (statt höhere Werte) höhere Eintrittswahrscheinlichkeiten des Risikos bedeuten.

als wesentlich erhöht angenommen, wenn der aktuelle Indikatorwert unterhalb des Schwellenwertes liegt. Die Überschreitung (bzw. Unterschreitung) eines Schwellenwertes wird häufig als Schwellenwertbruch oder als „Red Flag“ bezeichnet.

In der Praxis liegt i. d. R. keine ideale Situation vor, in der sich gute Indikatorwertbereiche von schlechten Bereichen exakt trennen ließen und sich ein Schwellenwert daher einfach bestimmen ließe. D. h., es kommt prinzipiell zu gelegentlichen Fehleinschätzungen, weil

- Situationen mit erhöhter Eintrittswahrscheinlichkeit des Risikos vorliegen können, in denen der aktuelle Wert des KAI (ggf. knapp) unterhalb des Schwellenwertes liegt. Der KAI schlägt also fälschlicherweise nicht an (falsch negativ).
- Situationen mit geringer Eintrittswahrscheinlichkeit des Risikos vorliegen können, in denen der aktuelle Wert des KAI (knapp) oberhalb des Schwellenwertes liegt. Der KAI schlägt also fälschlicherweise an (falsch positiv).

Ein Schwellenwert ist also meistens nicht zwingend eindeutig festlegbar. Diese Nicht-Eindeutigkeit bietet einen Spielraum, der eine sorgsame Abwägung/Entscheidung verlangt, denn

- ein zu niedriger Schwellenwert bedeutet: Es werden zwar nur wenige (oder sogar keine) Situationen mit erhöhter Eintrittswahrscheinlichkeit des Risikos verpasst, aber viele Schwellenwertüberschreitungen verursachen viel Aufwand/hohe Bearbeitungskosten.
- ein zu hoher Schwellenwert bedeutet: Wenige Schwellenwertüberschreitungen verursachen zwar wenig Aufwand/niedrige Bearbeitungskosten, aber viele (vielleicht die meisten oder sogar alle) Situationen mit erhöhter Eintrittswahrscheinlichkeit des Risikos werden verpasst.

Abwägungskriterien bei der Schwellenwertfestlegung können sein:

- Konservativität: Besser (zu viele) Fehlalarme als ein verpasster Schaden.
- Progressivität: Besser verpasste Schäden als (zu) großer Aufwand (in der Internen Revision und im Fachbereich).
- Ausgewogenes Verhältnis: Fehleinschätzungen kommen in beiden Richtungen ungefähr gleich häufig vor.

Das gewählte Abwägungskriterium bei der konkreten Festlegung eines Schwellenwertes ist zu dokumentieren.[62]

---

[62] Vgl. Anlage 7: Arten von Schwellenwerten.

Die Frequenz, mit der ein Schwellenwert festgelegt bzw. angepasst wird, kann statisch, anlassbezogen oder automatisch definiert werden.[63]

Neben den einfachen Schwellenwerten für einen KAI sind folgende Varianten bei der Schwellenwertfestsetzung und -anwendung möglich:

- Es kann ein Korridor definiert werden, d. h. eine Kombination aus einem unteren und einem oberen Schwellenwert. Eine Aktivität würde seitens der Internen Revision also dann gestartet werden, wenn der KAI einen Wert annimmt, der außerhalb des Korridors liegt.[64]
- Es können mehrere Schwellenwerte festgelegt werden. Deren Überschreitung kann nacheinander unterschiedliche Aktivitäten auslösen. Bspw. würde der KAI-Wert 13 eine andere Aktivität zur Folge haben, als der KAI-Wert 11, wenn der Wert 10 als erster Schwellenwert und der Wert 12 als zweiter Schwellenwert festgelegt worden sind.
- Ein Schwellenwert muss mehrmals nacheinander überschritten werden, bevor eine Aktivität gestartet wird. Bspw. würde eine Aktivität erst dann ausgelöst werden, wenn der KAI zweimal hintereinander (z. B. in zwei aufeinander folgenden Monaten bei monatlicher Betrachtungsfrequenz) den Schwellenwert überschreitet.
- Bei länger anhaltender Schwellenwertüberschreitung und bereits erfolgter Aktivität wird in einem Folgezeitraum keine weitere Aktivität durchgeführt.[65]
- Ein KAI kann der Schwellenwert eines anderen KAI sein (z. B. kann der 6M-Euribor als Schwellenwert des 3M-Euribor definiert werden. Dann würde eine Auffälligkeit vorliegen, wenn der 3M-Euribor größer als der 6M-Euribor wird).

KAI-Schwellenwerte, die im CA-System Anwendung finden sollen, sowie deren Herleitung sollten wie die KAIs selbst mit dem betroffenen Fachbereich reflektiert werden.

Die Verwendung eines durch eine Expertenschätzung[66] gewonnenen Schwellenwertes wird grundsätzlich als zulässig angesehen, insbesondere bei der Neueinführung eines KAI.[67] Jedoch ist möglichst anzustreben, Schwellenwerte (zumindest langfristig) per Datenanalyse zu ermitteln.

---

[63] Vgl. Anlage 8: Frequenz, mit der ein Schwellenwert festgelegt wird.

[64] Auch der umgekehrte Fall ist denkbar: Der KAI soll sich außerhalb des Korridors bewegen, d. h., eine Auffälligkeit liegt vor, wenn der KAI innerhalb des Korridors liegt.

[65] Die Länge eines solchen Zeitraums kann fest definiert oder dynamisch bestimmt werden, z. B. durch die vom Fachbereich für die Behebung eines Mangels benötigte Zeit.

[66] Als Experte wird hier z. B. der Verantwortliche für das zugehörige Prüffeld in der Internen Revision angesehen.

[67] Vgl. Anlage 9: Vor- und Nachteile einer Expertenschätzung.

Für die Bestimmung des Schwellenwertes eines KAI gibt es verschiedene Anlässe.[68] Um mit angemessenem Aufwand und zeitnah einen KAI für ein Prüffeld definieren zu können, gilt:

- Ein Kausalzusammenhang zwischen einem prüffeldthemen-spezifischen Risiko und einem zugeordneten KAI muss qualitativ nachvollziehbar sein. Die Höhe der Korrelation muss nicht quantifiziert werden.
- Anzahl- und Volumenbetrachtungen stellen in vielen Fällen einen zielführenden Ansatz für KAIs dar, um einen KAI zu definieren, z. B.:
  - Anzahl Schadenfälle,
  - Anzahl neuer Geschäfte,
  - Volumen der Schadenfälle in EUR,
  - Volumen neuer Geschäfte in EUR.
- Anzahl- und Volumenbetrachtungen können insbesondere auf zwei Arten von Veränderungen abzielen, da ein Mangel deren Ursache sein könnte:
  - Vergleich mit der längeren Vergangenheit (1 Jahr oder mehr): Eine wesentliche Änderung im Vergleich zur längeren Vergangenheit stellt eine untersuchungswerte Auffälligkeit dar.
  - Vergleich mit der jüngeren Vergangenheit (1 Monat bis ein 1 Jahr): Eine starke Änderung (Sprung) im Vergleich zur jüngeren Vergangenheit stellt eine untersuchungswerte Auffälligkeit dar.

Für jedes Prüffeld sollte einmal pro Kalenderjahr eine Validierung durchgeführt und angemessen dokumentiert werden, in deren Rahmen

- die wesentlichen prüffeldthemen-spezifischen Risiken, die KAIs und deren Schwellenwerte hinsichtlich mehrerer Aspekte zu überprüfen sind,
- notwendiger Änderungsbedarf bzgl. der KAIs und/oder deren Schwellenwerte zu identifizieren ist,
- entsprechende Maßnahmen abzuleiten sind und
- der Status der Maßnahmen der vorausgegangenen Validierung zu reflektieren ist.

Dem ggf. resultierenden Maßnahmenplan muss entnommen werden können,

---

[68] Vgl. Anlage 10: Anlässe für die Bestimmung eines Schwellenwertes.

- welche Maßnahmen nicht umgesetzt werden sollen und warum nicht, und welche Risiken mit einer Nicht-Umsetzung der Maßnahmen verbunden sind,
- welche Maßnahmen bis wann und wie umgesetzt werden sollen, und welche Risiken bzw. Schwächen während der Dauer der Umsetzung existieren.

Um diese Ziele zu erreichen, muss eine turnusmäßige Validierung mindestens bestimmte Validierungshandlungen umfassen.[69]

Hat die Validierung Änderungsbedarf für einen KAI und/oder seinen Schwellenwert ergeben und wird der KAI auch in einem weiteren Prüffeld verwendet, ist zu prüfen, ob die Änderungen auch für die Anwendung in dem anderen Prüffeld gelten sollen oder sogar müssen. Ggf. ist also der für das andere Prüffeld verantwortliche Auditor über den möglichen Änderungsbedarf zu informieren.

Am Ende einer turnusmäßigen Validierung kann je KAI eine Beurteilung mittels Vergabe einer Farbe aus der im Anhang dargestellten Farbskala[70] vorgenommen werden.

Für die Ausgestaltung und Validierung der KAIs besteht die Notwendigkeit der Dokumentation. Die Dokumentation sollte im Audit-System grundsätzlich im Prüfungskonzept des CA-Prüfungsauftrags (Dauerauftrag oder jährlicher Auftrag) erfolgen. Für die Dokumentation der Validierungen kann ein separater übergreifender Auftrag verwendet werden.[71]

---

[69] Vgl. Anlage 11: Validierungshandlungen.
[70] Vgl. Anlage 12: Farbskala für Ergebnis einer Validierung.
[71] Vgl. Anlage 13: Dokumentation der Validierung.

7 Process Mining

Die Eingabe und Verarbeitung von Daten in digitalen Systemen wird in Form eines technischen Aktivitätsprotokolls aufgezeichnet. Die Aktivitäten hinterlassen damit sozusagen digitale Fußspuren. Process-Mining ist ein Verfahren, welches diese digitalen Spuren so visualisiert, dass der Betrachter Rückschlüsse auf den internen Verlauf der Businessprozesse treffen kann.

Ziel von Process-Mining ist die Identifikation der unternehmerischen Ist-Prozesse und ihrer Varianten. Die Methode kann in unterschiedlichen Phasen einer revisorischen Prüfung eingesetzt werden:

- Zum Zeitpunkt der Prüfungsplanung hilft es dem Revisor, einen Gesamtüberblick über die Prozesse des zu prüfenden Unternehmensbereichs zu gewinnen. Der Revisor sieht dadurch nicht nur die typischen und am häufigsten anzutreffenden Aktivitäten und Prozessverläufe, sondern er sieht auch selten bis sehr selten auftretende Aktivitäten (z. B. Reaktivierung stornierter Belege) und auch selten auftretende Aktivitätsverläufe (z. B. Einkaufsbelege, bei denen die Aktivität Rechnungseingang zeitlich vor der Aktivität Anlage des Einkaufsbelegs vorkam).
- Während der Prüfungsdurchführung kann der Revisor mittels Process Mining einen Gesamtüberblick der Prozesse gewinnen, den identifizierten Ist-Zustand mit dem Soll-Zustand vergleichen und explorativ in die detaillierteren Tiefen der Belege eintauchen.
- In der Berichtsphase können die aus dem Process Mining gewonnenen Grafiken in der Regel exportiert und im Prüfbericht aufgeführt werden.

Zusammenhang Process Mining und Continuous Auditing

Das Process Mining Verfahren ist ein exploratives Instrument mit sehr flexiblen Einsatzmöglichkeiten. Es kann auch unabhängig von den bekannten Process Mining Tools realisiert werden.

Die typische Vorgehensweise innerhalb von Continuous Auditing besteht u. a. darin, im Vorfeld definierte KAIs kontinuierlich im Auge zu behalten, um beim Über- oder Unterschreiten kritischer Schwellenwerte auch unterjährig reagieren zu können. Der wesentliche Aspekt an dieser Stelle ist die kontinuierliche Betrachtung derselben KAIs.

Die Process Mining-Methode eignet sich im Vorfeld der Einrichtung eines CA-Systems, um kritische Prozessrisiken zu identifizieren und richtige KAIs zu definieren. Die mittels Process Mining gewonnenen Erkenntnisse bieten also Rückschlüsse auf gute KAIs. Damit eignet es sich sehr gut für revisorische Tätigkeiten.

Hervorzuheben ist, dass auf der Grundlage eines Process-Mining Tools auch kontinuierliche CA-Systeme realisiert werden können, da nach der Definition von den Soll-Ist-Abweichungen der Prozesse, diese als KAIs abgebildet und kontinuierlich überprüft werden können.

8 Maschinelles Lernen

Hinter dem Maschinellen Lernen (ML) steckt die Idee, Maschinen durch geeignete Algorithmen, die Fähigkeit zu verleihen, aus Daten und Erfahrungen zu lernen. Die Maschinen leiten aus den Informationen ein statistisches Modell ab. Ein künstliches System lernt somit aus den gelieferten Informationen und kann diese nach Abschluss der Lernphase verallgemeinern.

Bei diesem Vorgang werden die Beispiele nicht einfach auswendig gelernt, sondern es werden Muster und Gesetzmäßigkeiten in den Lerndaten erkannt. Dadurch können die Maschinen ein Modell ihrer Welt aufbauen und die ihnen zugedachten Aufgaben besser lösen.

Im besten Fall ist es der Maschine möglich unbekannte Daten zu beurteilen und einen Lerntransfer herzustellen. Im schlechtesten Fall ist aber auch ein Scheitern am Lernen unbekannter Daten möglich. ML-Verfahren können daher nicht selbstständig operieren, sondern müssen von Spezialisten aufgesetzt, angewandt und evaluiert werden.

Die Implementierung erfolgt in drei Phasen.

- Phase 1 – Lern- bzw. Trainingsphase (Modellierung),
- Phase 2 – Testphase (Qualitätssicherung und Bewertung),
- Phase 3 – Anwendung auf unbekannte Daten (Prognosen).

Die unterschiedlichen Anwendungen von ML können wie folgt gruppiert werden:

- Datentypen werden unterschieden in Text, Sprache und Bilddaten.
- Lernaufgaben werden unterschieden in Klassifikation, Regression und Clustering.
- Algorithmen sind die technische Lösung des Problems.

Diese Kategorien stehen oftmals in Abhängigkeit zueinander: So lassen sich bspw. sehr unterschiedliche Lernaufgaben mit sehr ähnlichen Algorithmen lösen. Für bestimmte Datentypen können spezielle Algorithmen angewandt werden, die bei anderen Ausprägungen zu keinen sinnvollen Ergebnissen führen.

Typische Anwendungen von maschinellen Lernverfahren z. B. im Finanzsektor sind:

- Bonitätsbewertung,
- Kreditkartenbetrug,

- Aktienmarktanalysen,
- Kundensegmentierung.

ML kann nach erfolgreicher Implementierung als Methode angewandt werden, um in diesen und weiteren Bereichen Auffälligkeiten und Unregelmäßigkeiten zu identifizieren. Insofern eignet es sich möglicherweise als Kontrollinstrument und ist damit u. a. als Werkzeug der ersten Linie geeignet.

Allerdings ergeben sich in der ML-Praxis für die Interne Revision diverse Herausforderungen, welche den Einsatz von ML als eher schwierig gestalten:

- Der Einsatz von ML setzt sehr große Datenbewegungen voraus.
- Die Einführung von ML erfordert eine entsprechende technische und personelle Ausstattung (leistungsstarke Server, datenwissenschaftlich ausgebildetes Personal).
- Der Aufwand für ML ist vergleichsweise hoch.
- Der Erfolg von ML lässt sich nicht klar vorhersagen.
- Die False-Positive-Quote ist bei ML vergleichsweise hoch.
- Wird ein Sachverhalt als auffällig markiert und gemeldet, so fehlt oft das Verständnis dafür, warum die Maschine diesen als Auffälligkeit deklariert.

Bei CA geht es im Wesentlichen darum, regelmäßig aktualisiert fest definierte KAI zu ermitteln, mit ihren jeweiligen Sollwerten zu vergleichen und im Falle signifikanter Abweichungen Handlungen abzuleiten. ML stellt eine Möglichkeit dar, nach der Implementierung eines kennzahlenbasierten CA-Systems dieses entsprechend zu erweitern.

9 Anlagen

9.1 Mögliche Datenquellen

Abb. 26: Datenquellen[72]

Datenquelle	Beispiele für erhobene Informationen
IT-Asset-Register	Bezeichnungen/IDs von IT-Assets, deren Lebenszyklus und prozessbasierte Termine; Abhängigkeiten zw. IT-Assets (Informationsverbund)
elektronische Organigramme/Organisationsstrukturen	Änderungen an der Organisationsstruktur, ReOrg-Maßnahmen, Änderungen an Bezeichnungen; Rollen und Zuständigkeitsänderungen
Risikomanagementsysteme	Veränderung (prozessbasierter) Risikobewertungen; Eintritt und Bearbeitungsstatus von Risiken, ggf. Schadenshöhen, Prozesszuordnungen
internes und externes Berichtswesen	Feststellungen und Maßnahmen aus JAP-Berichten oder Berichten externer Aufsichts-/Kontrollorgane (BaFin, EZB, Landes- oder Bundesdatenschutz, Prüfberichte von Dienstleistern)
Projektmanagementsysteme	Projekte und deren Rahmendaten (Budget, Genehmigungen, Organe, Ziele, Meilensteine, Rollen, Verantwortlichkeiten, Risikobewertungen, Wirtschaftlichkeitsbewertungen)
Knowledge-Management-Systeme	Prozessinformationen, Schwachstellen, Bewertungen, Verbesserungen, Lösungen, diverse Analysen
Produktdatenbanken/-kataloge	Produkte und deren Daten (Bezeichnungen, Abhängigkeiten, Verknüpfung zu rechtlichen Rahmenbedingungen, Lebenszyklus, Beschreibungen, Verknüpfungen zu Controlling-Informationen)
Protokolle von Gesprächen mit Fach- und Führungskräften	Geplante Veränderungen von Prozessen und Zuständigkeiten, Risikobewertungen durch Fachbereiche, Identifikation von Prüfungsobjekten, Prüfungs- und Beratungswünsche

[72] Die Auflistung ist nicht vollständig. Sie wird im Rahmen von weiteren Überarbeitungen des Leitfadens aktualisiert.

elektronische Prozessdokumentation	Prozesse und deren Daten (Bezeichnungen, Abhängigkeiten, Verantwortlichkeiten, Lebenszyklus, Beschreibungen, Kontrollen, Kontrollziele, ggf. Ergebnisse und Belege durchgeführter Kontrollhandlungen der ersten und zweiten Linie); ggf. Ergebnisse aus Process-Mining-Analysen
ERP-Systeme/DWHs	Prozess- und Produktinformationen, Kontrollinformationen, Analysen/Auswertungen, ggf. Ergebnisse aus Process-Mining-Analysen, Controlling-Informationen, diverse Analysemöglichkeiten durch Kombination verschiedener Datenquellen
Providermanagementsysteme	Provider mit deren Kontaktdaten, Ansprechpartnern, Risikobewertungen, Notfallinformationen, Informationen aus dem Überwachungsprozess, Prüfungsberichte, ggf. eigene Prüfungsberichte, Gesprächsprotokolle, KPIs aus der Überwachung, Vertragsinformationen
Security Information and Event Management	Use Cases, Security Events mit deren Risikobewertung und Status der Bearbeitung
Personalmanagementsysteme	Personaldaten, Eintritts- und Austrittstermine, Gehaltsinformationen, Schulungsinformationen
Stammdatenmanagementsysteme	Personaldaten, Berechtigungsinformationen, User Accounts und deren Status, Eintritts- und Austrittstermine
Identity- and Access-Management	Berechtigungsinformationen und -kompositionen, User Accounts und deren Status, Befristungen, Rezertifizierungen, Freigabeebenen, Anträge und Änderungen mit zugehörigen Rahmendaten

9.2 Berücksichtigung von Prüffeld-Risiken und Prüffeld-Performance-Zielen

Um KAIs zu entwickeln, ist es empfehlenswert, für jedes Prüffeld, das im CA-System der Internen Revision berücksichtigt werden soll, zunächst die **Prüffeld-Risiken** und **Prüffeld-Performance-Ziele** schriftlich zu fixieren und dabei eine Aufteilung in „wesentlich“ und „nicht wesentlich“ sowie in „prüffeldthemen-spezifisch“ und „prüffeldthemen-unspezifisch“ vorzunehmen. Die damit verbundene Vergegenwärtigung der wesentlichen Risiken und Performance-Ziele unterstützt den Auditor bei der Definition der KAIs und dem zügigen Aufbau des KAI-basierten CA-Systems.

Zuerst sollten **KAIs für die wesentlichen prüffeldthemen-spezifischen Risiken** und Performance-Ziele gebildet werden. Im Laufe der Zeit können dann mittels weiterer KAIs auch die anderen Risiken und Performance-Ziele, z. B. in der Reihenfolge

I. wesentliche prüffeldthemen-unspezifische Risiken (bspw. unangemessene Personalausstattung, unzureichende IT-Verfügbarkeit.) und wesentliche prüffeldthemen-unspezifische Performance-Ziele,

II. nicht wesentliche prüffeldthemen-spezifische Risiken und nicht wesentliche prüffeldthemen-spezifische Performance-Ziele

III. sowie nicht wesentliche prüffeldthemen-unspezifische Risiken und nicht wesentliche prüffeldthemen-unspezifische Performance-Ziele kontinuierlich geprüft werden.

Die Formulierung der (wesentlichen) Risiken und Performance-Ziele sollte unbedingt mit den involvierten Fachbereichen inhaltlich reflektiert werden, um ein gemeinsames Verständnis bzgl. der Prüffeldinhalte und deren Gewichtung zu erreichen.

9.3 KAI-Beschreibung

Eine KAI-Beschreibung sollte folgende Angaben enthalten:

- **Indikatorname**: Der KAI soll einen aussagekräftigen Namen erhalten.
- **Bereich**: Der Bereich, in dem der KAI Verwendung findet, ist zu nennen (z. B. Finanzen).
- **Prüfungsfrequenz**: Die Frequenz, mit der der KAI betrachtet werden soll, ist festzulegen (z. B. monatlich).
- **Risiken, Performance-Ziele**: Der Bezug zum abgedeckten (wesentlichen) Risiko bzw. Performance-Ziel ist herzustellen.
- **Abhängigkeiten**: Mögliche Abhängigkeiten des KAI zu anderen KAIs sind zu nennen.
- **Beachtenswertes**: Es sollte festgehalten werden, auf was bei der Verwendung des KAI geachtet werden muss.
- **Besonderheiten**: Die Quellen, aus denen die für den KAI benötigten Informationen/Daten bezogen werden, sind zu nennen; ebenso Alternativquellen, falls vorhanden.
- **Aggregationslevel**: Wenn der KAI für verschiedene Aggregationslevel (z. B. Organisationseinheit, Kontinent, Produktart) verwendbar ist, ist dies anzugeben.

9.4 KAI auf Basis von Kennzahlen

Beispiel für ein KAI: Im Prüffeld Rating-Verfahren existiert das Risiko „Die Ratingverfahren liefern keine validen und damit objektiven Ergebnisse für Ausfallwahrscheinlichkeit eines Kreditnehmers.“ Es wird der KAI „Auffälliger Sprung der mittleren Ausfallwahrscheinlichkeit (aller oder eines Teil-Portfolios)“ definiert.

Dieser KAI motiviert sich dadurch, dass eine erhebliche Änderung (Sprung) der durchschnittlichen Ausfallwahrscheinlichkeit aller mit einem bestimmten Rating-Modul bewerteten Engagements selten zu erwarten ist und daher im Fall einer erheblichen Veränderung dieser Kennzahl eine Auffälligkeit vorliegt. Für eine solche Auffälligkeit kann es neben natürlichen Ursachen diverse Gründe geben, bspw. Mängel in der Rating-Berechnung oder bei der ordnungsgemäßen Rating-Anwendung. Somit ist eine erhebliche Veränderung des Indikatorwertes sowohl nach oben als auch unten auffällig.

Das Prinzip dieses KAI, d. h. die Reaktion auf die erhebliche Veränderung einer Kennzahl, bei der keine Sprünge zu erwarten sind, ist sehr gut auf andere Prüffelder übertragbar.

9.5 KAI-Datenqualität

Bei der Verwendung eines quantitativen KAI ist bzgl. der Qualität der für die KAI-Berechnung benötigten Daten Folgendes zu betrachten:

- Vollständigkeit der benötigten Daten,
- Zuverlässigkeit der benötigten Daten (d. h., ist die Entstehung der Daten nachvollziehbar bspw. mittels eines Fachkonzeptes oder einer Prozesslandkarte?)
- ggf. Konsistenz der benötigten Daten über verschiedene Systeme bzw. Quellen hinweg,
- Korrektheit und ggf. Exaktheit der benötigten Daten,
- Zugänglichkeit der benötigten Daten (aktuell und langfristig), z. B.:
  - eigene System- oder Datenbank-Berechtigung,
  - Zulieferung vom Fachbereich oder von IT,
  - Internet (www.destatis.de, …),
- Verfügbarkeit der benötigten Daten (aktuell und auch langfristig, d. h., werden die benötigten Daten langfristig produziert?),

- Aktualität der benötigten Daten (d. h., werden die benötigten Daten zeitlich dann produziert und/oder stehen sie genau dann zur Verfügung, wenn sie für die KAI-Berechnung benötigt werden? Und wenn nicht, ist die Verwendung von Daten, die bereits ein gewisses Alter aufweisen, akzeptabel, d. h., können die Continuous Auditing-Ziele erreicht werden?).

9.6 Daten-Vollständigkeit im historischem Zeitraum

Insbesondere wenn eine Zeitreihe von Daten, die in die KAI-Berechnung einfließen, im Zeitverlauf einen Sprung aufweist, ist zu analysieren, inwieweit ältere Werte berücksichtigt werden dürfen. Bzgl. der Vollständigkeit der Daten ist wie folgt vorzugehen:

- Nur mit vollständigen oder mit sachgerecht vervollständigten Daten darf ein KAI-Wert verwendet werden.
- Sind Datenlücken im gewählten historischen Zeitraum vorhanden, kann die Datenqualität dennoch angemessen sein, nämlich wenn die vorhandenen Daten korrekt sind und die Datenlücken sachgerecht gefüllt werden können.
- Das Füllen der Datenlücken kann auf verschiedene Arten geschehen:
  - Idealerweise lassen sich die fehlenden Daten doch noch (mit angemessenem Aufwand) beschaffen (z. B. aus anderen Quellen) oder produzieren.
  - Per Expertenschätzung, wofür allerdings gesichertes Expertenwissen im Fachbereich und/oder in der Internen Revision vorhanden sein muss.
  - Per konstanter Fortsetzung an den Rändern im Fall einer Zeitreihe: Fehlen am Anfang und/oder am Ende des gewählten historischen Zeitraums Daten, kann die Datenreihe mit dem jeweils letzten vorhandenen Datum vervollständigt werden, sofern dies sachgerecht ist und nachvollziehbar begründet werden kann.
  - Per Interpolation:
    - Stückweise lineare Interpolation: Alle Daten, zwischen denen Daten fehlen, werden mittels einer Geraden verbunden, woraus sich die fehlenden Werte ergeben.
    - Andere Interpolationsverfahren wie höhergradige Polynome, kubische Spline-Interpolation oder die Gaußprozess-Regression sind i. d. R. aufwendig. Sie sollten nur verwendet werden, falls eine lineare Interpolation offensichtlich zu unangemessenen Ergebnissen führt.

9.7 Arten von Schwellenwerten

Beispiele für Arten von Schwellenwerte sind

- für qualitative KAIs:
  - Ja/Nein bzw. 0/1.
- für quantitative KAIs:
  - 0, falls Null-Toleranz.
  - Vorgabe aus
    - Gesetz, Verordnung,
    - Geschäftsstrategie,
    - Schriftlich fixierte Ordnung/Anweisungswesen, Fachkonzepte.
  - Schwellenwert aus einer Vorgabe abzüglich (bzw. zuzüglich) eines von Experten geschätzten (i. d. R. konservativen) Add-on (absolut oder relativ).
  - Expertengeschätzter quantitativer Wert.
  - Durchschnitt der KAI-Werte eines relevanten/fachlich sachlich angemessen langen Zeitraums in der Vergangenheit.
  - Durchschnitt minus (oder plus) n Standardabweichungen der KAI-Werte eines relevanten/fachlich sachlich angemessen langen Zeitraums in der Vergangenheit.
  - Quantil, sofern bekannt ist, wie die historischen KAI-Werte verteilt sind (bspw. 95%-Quantil im Fall einer Normalverteilung)

9.8 Frequenz, mit der ein Schwellenwert festgelegt wird

Bzgl. der Frequenz, mit der ein Schwellenwert festgelegt wird, sind folgende Varianten möglich:

- Statisch: Der Schwellenwert wird festgelegt und bleibt b. a. w. konstant. Eine Überprüfung, die zu einer Änderung führen kann, findet aber auf alle Fälle im Rahmen der KAI-Validierung statt, d. h., die Überprüfungs- bzw. Anpassungsfrequenz entspricht der Validierungsfrequenz.
- Anlassbezogene Anpassung: Neben der Überprüfung, die regelmäßig im Rahmen der KAI-Validierung erfolgt, kann der Schwellenwert anlassbezogen geändert werden, was zu begründen und zu dokumentieren ist. Anlässe können bspw. sein:

    - Ein KAI hat seinen Schwellenwert überschritten, aber die Folgeaktivität (z. B. Gespräch mit dem Fachbereich) hat gezeigt, dass sich die Eintrittswahrscheinlichkeit des Risikos nicht (wesentlich) erhöht hat. Dann könnte der Schwellenwert angepasst (in diesem Fall erhöht) werden.
    - Die Interne Revision hat Kenntnis über die (wesentliche) Erhöhung der Eintrittswahrscheinlichkeit eines Risikos erlangt, aber der zugehörige KAI hat seinen Schwellenwert nicht überschritten. Dann kann der Schwellenwert angepasst (in diesem Fall gesenkt) werden.
- Dynamisch/automatische Anpassung: Wird der Schwellenwert mittels einer Betrachtung eines historischen Verlaufs der KAI-Werte in einem Zeitraum ermittelt, sind zwei Varianten möglich:
    - Der historische Zeitraum besteht aus n ganzen Kalenderjahren vor dem aktuellen Kalenderjahr. Dann wird der Schwellenwert immer zu Beginn eines Kalenderjahrs auf Basis der KAI-Daten des neuen Zeitraums bestimmt (während eines Kalenderjahres ist der Schwellenwert dann konstant).
    - Der historische Zeitraum (z. B. l Monate, m Quartale, n Jahre) beginnt stets direkt vor dem aktuell betrachteten Zeitraum (z. B. aktueller Monat, aktuelles Quartal), d. h., der Schwellenwert wird zu jedem Betrachtungszeitpunkt (Berechnungszeitpunkt des KAI) neu bestimmt und unmittelbar angewendet.

Der Vorteil einer dynamischen Anpassung des Schwellenwertes bzw. der Anwendung eines dynamisch ermittelten Schwellenwertes besteht darin, dass stets die unmittelbar jüngste Vergangenheit und somit die aktuelle Entwicklung des durch den KAI abgebildeten Sachverhalts berücksichtigt werden. Allerdings ist diese Variante mit Bedacht anzuwenden, da ein Trend, der mit der Erhöhung der Eintrittswahrscheinlichkeit des Risikos einhergehen könnte, eventuell verpasst wird.

Im Fall einer Zeitreihe ist – z. B. mittels Visualisierung der Daten – zu prüfen, ob im gewählten historischen Zeitraum ein Trend und/oder eine Saisonalität vorhanden sind, die bei der Ermittlung eines Schwellenwertes berücksichtigt werden sollten.

9.9 Vor- und Nachteile einer Expertenschätzung

Vorteile einer Expertenschätzung:

- In der Praxis sind Verfahren zur quantitativen Bestimmung eines optimalen Schwellenwertes häufig nicht trivial. Ist der Aufwand unverhältnismäßig, ist die Expertenschätzung eine zunächst kostengünstige Alternative, die die sofortige Anwendung eines KAI erlaubt.

- Liegen die notwendigen Daten für die Anwendung eines quantitativen oder visuellen Verfahrens für die Schwellenwertbestimmung gar nicht oder nicht in ausreichender Menge oder Qualität vor,[73] ist die Expertenschätzung eine zunächst kostengünstige Alternative. Sind die notwendigen Daten nur mit unverhältnismäßigem Aufwand oder gar nicht beschaffbar, ist die Expertenschätzung ggf. zunächst die einzige Möglichkeit, einen Schwellenwert festzulegen.

Nachteile einer Expertenschätzung:

- Menschen überschätzen häufig die Wahrscheinlichkeit seltener Ereignisse und unterschätzen die Wahrscheinlichkeit häufig vorkommender Ereignisse. Die Herleitung eines Schwellenwertes aus einer Datenanalyse liefert dagegen Ergebnisse, die nicht oder weniger subjektiv verzerrt sind.
- Aufgrund des subjektiven Anteils bei einer Expertenschätzung ist die Nachvollziehbarkeit des Ergebnisses i. d. R. geringer als bei einer Berechnung.
- Im Gegensatz zur Herleitung eines Schwellenwertes aus einer Datenanalyse lässt sich eine Expertenschätzung nicht automatisieren.

Aufgrund der genannten Nachteile ist möglichst anzustreben, Schwellenwerte (zumindest langfristig) per Datenanalyse zu ermitteln.

9.10 Anlässe für die Bestimmung des Schwellenwertes

Für die Bestimmung des Schwellenwertes eines KAI gibt es verschiedene Anlässe:

- Start des CA-Systems: Zum Zeitpunkt des Starts des CA-Systems sind de facto alle KAIs neue KAIs. ➔ Die Bestimmung von Schwellenwerten ist notwendig.
- Neuer KAI in einem bestehenden Prüffeld: Das KAI-Set eines bestehenden Prüffelds wird um einen neuen KAI erweitert. ➔Die Bestimmung eines Schwellenwertes ist notwendig.
- Neues Prüffeld: Dem Audit Universe wird ein neues Prüffeld hinzugefügt.

---

[73] Dass historische Daten gar nicht bzw. nicht in ausreichender Menge oder Qualität vorliegen, wird bei einem neuen KAI relativ häufig der Fall sein (d.h. bei vielen KAIs zum Zeitpunkt des Starts des CA-Systems). Im Laufe der Zeit sollte sich diese Situation deutlich verbessern, da die Einführung eines KAI die Produktion der notwendigen Daten durch den Fachbereich (oder auch durch die Interne Revision selbst) bewirken wird.

    - Die wesentlichen Risiken des neuen Prüffeldes werden ganz oder teilweise durch neue KAIs abgebildet. ➔ Die Bestimmung von Schwellenwerten ist notwendig.
    - Die wesentlichen Risiken des neuen Prüffeldes werden ganz oder teilweise durch KAIs abgebildet, die auch in anderen Prüffeldern verwendet werden. ➔ Die Bestimmung eines Schwellenwertes ist dann notwendig, wenn die in den anderen Prüffeldern für die bestehenden KAIs verwendeten Schwellenwerte nicht ebenfalls im neuen Prüffeld verwendet werden sollen.
- Geänderter KAI in einem bestehenden Prüffeld: Aufgrund nicht beeinflussbarer Umstände ergibt sich die Notwendigkeit für die Änderung eines KAI (z. B. Produktion der benötigten Daten wird eingestellt), d. h., seine Datengrundlage und/oder seine Berechnungslogik werden geändert (dann handelt es sich eventuell sogar um einen neuen KAI). ➔ Die Bestimmung eines neuen Schwellenwertes ist notwendig.
- Validierung: Aus der turnusmäßigen Validierung eines KAI und seines Schwellenwertes ergibt sich die Notwendigkeit für die Neubestimmung des Schwellenwertes.

Wenn notwendig, werden neue KAIs in das CA-System aufgenommen. Die erste Zeit nach der Aufnahme eines KAI in das CA-System wird als Einführungsphase bezeichnet. In dieser Phase, die bis zu einem Jahr dauern darf, können bzgl. der Anpassung des Schwellenwertes eines KAI reduzierte formale Anforderungen gelten.[74]

- Der Schwellenwert darf grundsätzlich das Ergebnis einer Expertenschätzung sein, auch wenn die Datenlage eine Schwellenwertbestimmung per Datenanalyse erlauben würde.
- Der Schwellenwert darf mehrfach per Expertenschätzung angepasst werden, insbesondere wenn die Analyse der Ursache einer auftretenden Schwellenwertüberschreitung zu der Erkenntnis führt, dass eine Fehleinschätzung vorliegt.
- Der Anlass für die Anpassung muss jeweils dokumentiert werden. Dies muss den Grund für die Richtung der Anpassung (größerer oder kleinerer Schwellenwert als vorher) beinhalten.
- Die Höhe einer Änderung muss nur qualitativ begründet werden.

Nach der Einführungsphase sollte die Expertenschätzung – falls möglich – durch eine Datenanalyse abgelöst werden.

---

[74] Der Validierungsturnus beträgt generell 1 Jahr (s. Abschnitt 9.11 Validierung), d. h., spätestens 1 Jahr nach der Einführung des neuen KAI findet eine Regelvalidierung des KAI inkl. der Überprüfung seines Schwellenwertes statt.

9.11 Validierungshandlungen

Um die KAI-Ergebnisse zu verifizieren, muss eine turnusmäßige Validierung mindestens folgende Handlungen umfassen:

- bzgl. der wesentlichen prüffeldthemen-spezifischen Risiken:
  - Es ist zu untersuchen, ob die prüffeldthemen-spezifischen Risiken vollständig benannt worden sind, d. h., ob
    - Risiken und somit ggf. KAIs ergänzt werden müssen,
    - Risiken (und somit ggf. KAIs), die nicht mehr wesentlich sind, wegfallen.
  - Es ist zu untersuchen, ob die Formulierung der wesentlichen prüffeldthemen-spezifischen Risiken angepasst werden muss oder wenigstens geschärft werden sollte.
- bzgl. der KAIs:
  - Es ist zu untersuchen, ob zwischen Risiko und KAI weiterhin eine Kausalität angenommen werden kann.
  - Es ist – unter Einbeziehung der im Validierungszeitraum aufgetretenen Schwellenwertüberschreitungen – zu untersuchen, ob die Beobachtungsfrequenz des KAI geändert werden sollte (d. h. häufigere oder seltenere KAI-Berechnungen).
  - Es ist zu untersuchen, ob die Qualität der für die Berechnung des Wertes eines quantitativen KAI verwendeten Daten weiterhin angemessen ist. Insbesondere ist darauf zu achten, dass die Ergänzung von Daten im Fall lückenhafter Daten weiterhin sachgerecht erfolgt.
  - Es ist zu untersuchen, ob die Qualität der Informationen, auf der qualitative KAIs basieren, weiterhin angemessen ist.
  - Es ist zu untersuchen, ob die KAI-Berechnungslogik geändert werden müsste. Eine Änderung ist sorgsam abzuwägen, da dies de facto die Einführung eines neuen KAI mit den entsprechenden Konsequenzen (Abstimmung mit dem Fachbereich, neuer Schwellenwert, idealerweise Berechnung historischer KAI-Werte u. a.) bedeutet.
  - Wird ein Tool (z. B. ein Excel-Sheet mit Formeln) für die Berechnung und Visualisierung eines KAI verwendet, ist ein Tool-Review durchzuführen, um die Korrektheit der Berechnungen sicherzustellen. Dafür ist u. a. zu untersuchen, ob die im Tool enthaltenen Testfälle auch weiterhin eine ausreichende Testabdeckung sicherstellen oder ob weitere Testfälle ergänzt werden müssen. Im Fall eines Excel-Sheets sollte ein Tool-Review zudem u. a. folgende Aktivitäten umfassen:
    - Es ist zu untersuchen, ob Formeln Fehlerwerte ausgeben, die nicht mit einem sachgerechten Fehler-Handling verarbeitet werden.

    - Es ist zu untersuchen, ob kopierte Formeln korrekt kopiert worden sind (z. B., wenn Datenreihen verlängert wurden, um den Folgezeitraum abzudecken).
    - Es ist zu untersuchen, ob die in den Formeln ggf. angesprochenen Zellbereiche korrekt sind (z. B., wenn Zellbereiche erweitert wurden, um den Folgezeitraum abzudecken).
    - Es ist zu untersuchen, ob in Grafiken alle relevanten Daten dargestellt werden (z. B., wenn Datenreihen verlängert wurden, um den Folgezeitraum abzudecken).
- bzgl. der Schwellenwerte der KAIs:
    - Es ist zu untersuchen, ob die Anzahl und Höhe der im Validierungszeitraum aufgetretenen Schwellenwertüberschreitungen angemessen war. Ggf. sollte der Schwellenwert angepasst werden.
    - Es ist zu untersuchen, ob die Reaktion der Internen Revision bei den im Validierungszeitraum aufgetretenen Schwellenwertüberschreitungen angemessen war. Ggf. sollte die geplante Reaktion angepasst werden und/oder es könnten mehrere Schwellenwerte mit jeweils einer anderen Reaktion eingeführt werden.
    - Es ist zu untersuchen, ob die Methode, mit der der Schwellenwert bestimmt wird, geändert werden sollte bzw. könnte (z. B. Datenanalyse statt Expertenschätzung).
    - Der Zeitverlauf des KAI (inkl. einer Darstellung des Schwellenwertes) sollte – wenn sinnvoll und möglich und noch nicht geschehen – visualisiert werden, um die Nachvollziehbarkeit bzgl. aller im Validierungszeitraum durchgeführten und auf den KAI-Beobachtungen basierenden Aktivitäten bzw. aller nicht durchgeführten Aktivitäten zu steigern.
    - Sind Umstände bekannt geworden, bei denen eine Reaktion der Internen Revision sinnvoll bzw. notwendig gewesen wäre, aber nicht erfolgt ist und keine Schwellenwertüberschreitung gemessen wurde, ist zu untersuchen, ob der Schwellenwert angepasst werden sollte.
    - Wird für die Bestimmung des Schwellenwertes ein Tool verwendet, z. B. ein Excel-Sheet mit Formeln, ist ein Tool-Review durchzuführen, um die Korrektheit der Berechnungen sicherzustellen.

Existieren bzgl. der wesentlichen prüffeldthemen-spezifischen Risiken, der KAIs und/oder ihrer Schwellenwerte unterschiedliche Sichtweisen zwischen Fachbereich und Interner Revision, sollte die Validierung erneut zum Anlass genommen werden, die Sichtweise der Internen Revision mit dem Fachbereich zu reflektieren und im optimalen Fall Konsens mit dem Fachbereich herzustellen.

Für jede Validierungshandlung gilt,

- dass nachvollziehbar zu dokumentieren ist, warum sie ggf. nicht durchgeführt wird,
- dass nachvollziehbare Begründungen formuliert werden müssen (z. B. „Risiko X ist nicht länger wesentlich, weil …“, „die Berechnungslogik eines KAI wird geändert, weil …“).

Besteht relativ kurze Zeit nach einer turnusmäßigen Validierung (d. h. vor Ablauf von 9 Monaten nach der Validierung) die Notwendigkeit für eine weitere Validierung, kann wie folgt vorgegangen werden (anlassbezogene Validierung):

- Es wird eine verkürzte Validierung durchgeführt, z. B. nur für einen KAI statt für alle KAIs. Dafür ist zu entscheiden, welche Validierungshandlungen einer regelmäßigen Validierung (s. o.) mindestens notwendig sind, um das CA-System für das Prüffeld mittels KAIs auch zukünftig zu gewährleisten. Diese werden dokumentiert. In diesem Fall stellt nicht das Ende der anlassbezogenen Validierung, sondern das Ende der letzten turnusmäßigen Validierung den Bezugszeitpunkt für den Beginn der nächsten turnusmäßigen Validierung dar.
- Es wird eine Validierung durchgeführt, die bzgl. ihres Umfangs einer turnusmäßigen Validierung entspricht. In diesem Fall stellt nicht das Ende der turnusmäßigen Validierung, sondern das Ende der anlassbezogenen Validierung den Bezugszeitpunkt für den Beginn der nächsten turnusmäßigen Validierung dar.

9.12 Farbskala für Ergebnis einer Validierung

Am Ende einer turnusmäßigen Validierung kann je KAI eine Beurteilung mittels Vergabe einer Farbe aus der folgenden Farbskala vorgenommen werden:

Grün

- KAI wird weiterhin verwendet,
- Berechnungslogik unverändert oder angepasst,
- Schwellenwert unverändert oder angepasst.

Gelb

- KAI weiterhin verwendbar, aber die Verwendung wird ausgesetzt, bis der notwendige Änderungs- bzw. Korrekturbedarf (z. B. angemessene Datenqualität ist herzustellen, Schwellenwert ist neu zu berechnen und abzustimmen) umgesetzt ist (➔ Maßnahmenplan),

- erneuter Einsatz geplant ab …

Rot

- KAI kann/soll nicht mehr verwendet werden, weil …

Blau

- Neuer KAI,
- Einsatz ab sofort bzw. Einsatz ab …

9.13 Dokumentation der Validierung

Die Dokumentation der KAIs und Schwellenwerte sollte grundsätzlich im Prüfungskonzept des CA-Prüfungsauftrags (Dauerauftrag oder jährlicher Auftrag) erfolgen. Für die Dokumentation der Validierungen kann ein separater übergreifender Auftrag verwendet werden. Auf diese Weise entsteht folgende mögliche Aufteilung:

Dokumentation der KAIs und Schwellenwerte im Prüfungskonzept des CA-Prüfungsauftrags

KAIs

- Die Dokumentation der Ausgestaltung der KAIs muss ergänzend zur Definition eines KAI nachvollziehbare Begründungen für die konkrete Ausgestaltung enthalten.
- Die Eigenschaften eines KAI[75] können in einem Anhang zum Prüfungskonzept dargestellt werden.
- Dabei soll die Verbindung zu den zu betrachtenden Risiken/Performance-Zielen des per CA zu bewertendem Prüffeldes hergestellt werden.

Schwellenwerte

- Die Dokumentation der Schwellenwerte muss nachvollziehbare Begründungen für die konkrete Ausgestaltung enthalten.

[75] Vgl. Anlage 3: KAI-Beschreibung.

- Dabei soll auf das Abwägungskriterium bei der Schwellenwertfestlegung eingegangen werden (Konservativität, Progressivität, …).
- Anlassbezogene, unterjährige Änderungen.

Dokumentation der Validierung in einem separaten übergreifenden Auftrag

- Dieser Auftrag gliedert sich in die im CA betrachteten Prüffelder. Je Prüffeld sind für alle KAIs die Durchführung und die Ergebnisse der notwendigen Validierungshandlungen sowie ggf. resultierende Maßnahmen zu dokumentieren.
- Dateien, aus denen Validierungsergebnisse abgeleitet werden (bspw. Excel-Dateien), stellen Anhänge des Validierungsauftrags dar.

Herausgeber

Dieser Leitfaden wurde im DIIR-Arbeitskreis Continuous Auditing erarbeitet und herausgegeben vom DIIR – Deutsches Institut für Interne Revision e.V.

Zur Webseite des Arbeitskreises.

Veröffentlichung am 26.04.2021 auf www.diir.de.

Das DIIR bedankt sich bei den Mitgliedern des Arbeitskreises Continuous Auditing und dem Arbeitskreisleiter, Herrn Michael Bauch, für die Erstellung der Veröffentlichung.

Frankfurt am Main, 26. April 2021

DIIR – Deutsches Institute für Interne Revision e.V.
Theodor-Heuss-Allee 108
60486 Frankfurt am Main