

CHE WHITEPAPER 2026

# Risikomanagement, interne Kontrollsysteme und digitale Prozessprüfungen in Kommunalverwaltungen

---

*Wissenschaftlich orientiertes Konzept für die kommunale Rechnungsprüfung  
· Risiko-Kontrollmatrizen · digitale Evidenz · Process Mining*

**Leitgedanke** Die Prüfung der Wirksamkeit interner Kontrollen ist in NRW eine gesetzliche Aufgabe der örtlichen Rechnungsprüfung. Prüfbar wird das IKS erst, wenn Prozess, Risiko, Kontrollziel, Ausführung, Verantwortung, Nachweis und Wirksamkeit verbunden sind.

Stand: 1. September 2026

Adressaten: Kommunale Rechnungsprüfung, Interne Revision, Kämmerei, Kasse, Organisation, IT und Beteiligungsmanagement

# Inhaltsverzeichnis

|                                                                                |           |
|--------------------------------------------------------------------------------|-----------|
| <b>Abstract.....</b>                                                           | <b>4</b>  |
| <b>1. Problemstellung, Erkenntnisinteresse und rechtliche Einordnung .....</b> | <b>4</b>  |
| 1.1 Problemstellung und Zielsetzung .....                                      | 4         |
| 1.2 Gesetzlicher Prüfungsauftrag (Nordrhein-Westfalen).....                    | 4         |
| 1.3 Abgrenzung unterschiedlicher Prüfungssituationen .....                     | 5         |
| <b>2. Grundlagen der Prüfung.....</b>                                          | <b>5</b>  |
| 2.1 Risikomanagement, interne Kontrolle und Prüfung .....                      | 5         |
| 2.2 Steuerungs- und Prüfungskreislauf.....                                     | 6         |
| 2.3 Risikobewertung.....                                                       | 6         |
| <b>3. Gesamtkonzeption einer IKS-Prüfung.....</b>                              | <b>7</b>  |
| 3.1 Einordnung in die risikoorientierte Prüfungsplanung .....                  | 7         |
| 3.2 IKS-Prüfungsphasen .....                                                   | 7         |
| 3.3 Prüfungsobjekt und Aussageform .....                                       | 8         |
| 3.4 Rollenmodell und Unabhängigkeit .....                                      | 8         |
| <b>4. Ansatzpunkte zur Prüfung des Risikomanagementsystems.....</b>            | <b>9</b>  |
| 4.1 Kommunale Beispiele für Risiken und Kontrollen .....                       | 9         |
| 4.2 Typische Prüfungshandlungen.....                                           | 11        |
| <b>5. Digitale IKS-Prüfung .....</b>                                           | <b>11</b> |
| 5.1 Prüfungsdimensionen digitaler Kontrollen.....                              | 12        |
| 5.2 Informationssicherheit nach IDR-L 113-1 .....                              | 12        |
| 5.3 Notfallmanagement nach IDR-L 113-2 .....                                   | 13        |
| 5.4 Vom Fragebogen zum Wirksamkeitstest.....                                   | 13        |
| 5.5 Digitale Risiko-Kontrollmatrix für IT-Sicherheit und Notfallvorsorge ..... | 13        |
| 5.6 Digitale Prozessprüfungen und Process Mining .....                         | 14        |
| 5.6.1 Drei Analysearten und ihr Prüfungsnutzen.....                            | 14        |
| 5.6.2 Eventlog als prüferischer Datenvertrag .....                             | 15        |
| 5.6.3 Prüfungsablauf: acht Arbeitsschritte .....                               | 15        |
| 5.6.4 Verbindung von Risiko-Kontrollmatrix und Process Mining .....            | 16        |
| 5.6.5 Kommunale Praxisevidenz .....                                            | 16        |
| 5.6.6 Grenzen, Datenschutz und Beweiswert.....                                 | 17        |
| 5.6.7 Mindest-Arbeitspapier für eine digitale Prozessprüfung.....              | 17        |
| <b>6. IKS-Risikoprüffelder (Auswahl).....</b>                                  | <b>17</b> |
| <b>7. Aufbau einer prüffähigen Risiko-Kontrollmatrix je Prüffeld .....</b>     | <b>18</b> |
| <b>8. Praxisfall: Kreditorenrechnung bis Auszahlung .....</b>                  | <b>19</b> |

|                                                                          |           |
|--------------------------------------------------------------------------|-----------|
| 8.1 Risiko-Kontrollmatrix .....                                          | 20        |
| 8.2 Vertiefung der Schlüsselkontrolle: Änderung der Bankverbindung ..... | 21        |
| <b>9. Datenanalytische Kontrollen und NKF-Kontierung.....</b>            | <b>21</b> |
| 9.1 NKF-Kontenrahmen als digitales Prüfungsuniversum .....               | 21        |
| 9.2 Digitale Kontierungsprüfungen.....                                   | 22        |
| <b>10. Prüfung der Kontrollen .....</b>                                  | <b>22</b> |
| 10.1 Vier Prüfungsstufen .....                                           | 22        |
| 10.2 Muster eines Kontrolltests .....                                    | 23        |
| 10.3 Feststellungen und Gesamturteil .....                               | 23        |
| <b>11. Umsetzungsempfehlung für Rechnungsprüfungen .....</b>             | <b>24</b> |
| <b>12. Dokumentierte kommunale Praxisbeispiele .....</b>                 | <b>24</b> |
| 12.1 KGSt, Kiel und Dortmund .....                                       | 24        |
| 12.2 Stadt München – steuerliches IKS .....                              | 24        |
| 12.3 Weitere kommunale Beispiele .....                                   | 24        |
| <b>13. Limitationen, Entwicklungsbedarf und Fazit .....</b>              | <b>25</b> |
| <b>14. Literatur- und Quellenverzeichnis .....</b>                       | <b>25</b> |
| 14.1 Rechtsgrundlagen und kommunale Ausgangsmaterialien .....            | 25        |
| 14.2 Rahmenwerke und Prüfungsstandards .....                             | 26        |
| 14.3 Informationssicherheit und Business Continuity.....                 | 26        |
| 14.4 Lehrbücher und Handbücher zur Vertiefung.....                       | 27        |
| 14.5 Veröffentlichte kommunale Praxisfundstellen .....                   | 27        |
| 14.6 Process Mining und digitale Prozessprüfung.....                     | 27        |

## Abstract

Die Digitalisierung kommunaler Verwaltungsprozesse verändert Gegenstand und Methodik der Rechnungsprüfung. Kontrollen werden zunehmend in Fachverfahren, Workflows, Schnittstellen und Berechtigungssystemen ausgeführt. Das vorliegende Papier entwickelt ein integriertes Konzept zur Prüfung kommunaler Risikomanagement- und interner Kontrollsysteme. Es verbindet den gesetzlichen Prüfungsauftrag, internationale Rahmenwerke, prozessorientierte Prüfungsmethodik, Risiko-Kontrollmatrizen, digitale Evidenz und Process Mining. Konzeptioneller Kern ist ein geschlossener Nachweisweg vom kommunalen Ziel über Risiko und Kontrollziel bis zur tatsächlichen Kontrollausführung, zum manuellen oder digitalen Nachweis und zu einer in ihrer Reichweite ausdrücklich begrenzten Prüfungsaussage.

Schlüsselbegriffe: Kommunale Rechnungsprüfung; internes Kontrollsystem; Risikomanagement; digitale Prüfung; Process Mining; Eventlog; Risiko-Kontrollmatrix; Kontrollwirksamkeit; Datenqualität; Conformance Checking.

## 1. Problemstellung, Erkenntnisinteresse und rechtliche Einordnung

### 1.1 Problemstellung und Zielsetzung

Ausgangspunkt ist ein methodisches Grundproblem: Das Vorhandensein einer Dienstanweisung, Freigaberegeln oder technischen Funktionen erlaubt noch keine Aussage darüber, ob eine Kontrolle angemessen gestaltet, tatsächlich eingerichtet und während des Prüfungszeitraums verlässlich ausgeführt wurde. Ebenso belegt eine grafisch auffällige Prozessvariante noch keinen Rechts- oder Kontrollverstoß. Erforderlich ist nach der hier vertretenen Auffassung ein Prüfungsmodell, das normative Anforderungen, reale Prozessausführung, Datenqualität und fachliche Würdigung zusammenführt.

### 1.2 Gesetzlicher Prüfungsauftrag (Nordrhein-Westfalen)

§ 104 Abs. 1 Nr. 6 GO NRW ordnet die Prüfung der Wirksamkeit interner Kontrollen im Rahmen des internen Kontrollsystems als Aufgabe der örtlichen Rechnungsprüfung an. Die Vorschrift wurde durch das Zweite NKF-Weiterentwicklungsgesetz neu gefasst und trat zum 1. Januar 2019 in Kraft. Der Prüfungsauftrag betrifft damit nicht nur das Vorhandensein formaler Regelungen, sondern ausdrücklich deren Wirksamkeit.<sup>1</sup>

| Normativer Bezug          | Bedeutung für den Prüfungsansatz                                                                                                                                                                      |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| § 102 GO NRW              | Jahresabschluss und Lagebericht sind vor Feststellung zu prüfen; die Buchführung ist einzubeziehen. Wesentliche Unrichtigkeiten und Verstöße sollen bei gewissenhafter Berufsausübung erkannt werden. |
| § 104 Abs. 1 Nr. 1 GO NRW | Laufende Prüfung der Vorgänge in der Finanzbuchhaltung zur Vorbereitung der Jahresabschlussprüfung.                                                                                                   |
| § 104 Abs. 1 Nr. 2 GO NRW | Dauernde Überwachung der Zahlungsabwicklung und Vornahme der Prüfungen.                                                                                                                               |
| § 104 Abs. 1 Nr. 3 GO NRW | Prüfung von Programmen der DV-Buchführung vor ihrer Anwendung.                                                                                                                                        |
| § 104 Abs. 1 Nr. 5 GO NRW | Prüfung von Vergaben.                                                                                                                                                                                 |
| § 104 Abs. 1 Nr. 6 GO NRW | Prüfung der Wirksamkeit interner Kontrollen im Rahmen des IKS.                                                                                                                                        |

Rechtsstand und Quelle: GO NRW, Fassung ab 1. Januar 2026; <https://recht.nrw.de/lrgv/gesetz/01012026-gemeindeordnung-fuer-das-land-nordrhein-westfalen-bekanntmachung-der/>

---

<sup>1</sup> Gemeindeordnung für das Land Nordrhein-Westfalen (GO NRW), § 104 Abs. 1 Nr. 6, aktuelle Fassung; Rechtsportal NRW, <https://recht.nrw.de/>.

## 1.3 Abgrenzung unterschiedlicher Prüfungssituationen

IKS-Prüfungen können grundsätzlich in folgenden Prüfungssituationen beziehungsweise mit folgendem Prüfungsumfang durchgeführt werden:

| Situation                           | Ziel                                                                                                                           | Reichweite des IKS-Bezugs                                                                                                                                                                |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jahresabschlussprüfung              | Prüfungsurteil über die Zuverlässigkeit des Rechnungswesens und der Erstellung von Jahresabschluss und Lagebericht.            | Verständnis des rechnungslegungsrelevanten IKS zur Risikobeurteilung und Planung geeigneter Prüfungshandlungen. Daraus folgt nicht automatisch ein Gesamturteil zur Wirksamkeit des IKS. |
| Eigenständige IKS-Prüfung           | Prüfungsurteil bzw. belastbare Aussage über Angemessenheit, Implementierung und operative Wirksamkeit ausgewählter Kontrollen. | Prozess- oder themenbezogener Prüfungsgegenstand mit ausdrücklich definiertem Zeitraum, Kriterien und Kontrollpopulationen.                                                              |
| Prüfung des Risikomanagementsystems | Beurteilung, ob wesentliche Verwaltungsrisiken systematisch erkannt, bewertet, gesteuert, überwacht und berichtet werden.      | Organisationsweite oder bereichsbezogene Systemprüfung; rechtliche Grundlage und örtlicher Auftrag sind gesondert festzulegen.                                                           |

Übersicht 1: Abgrenzung unterschiedlicher Prüfungssituationen der IKS-Prüfung

**Wesentliche Abgrenzung** Die Abschlussprüfung nutzt das IKS als Teil ihres risikoorientierten Prüfungsansatzes. Eine eigenständige IKS-Prüfung untersucht dagegen gezielt die Wirksamkeit der Kontrollen selbst. Prüfungsziel und Berichtsaussage dürfen nicht vermischt werden.

## 2. Grundlagen der Prüfung

### 2.1 Risikomanagement, interne Kontrolle und Prüfung

Der Zusammenhang von Risikomanagement, internen Kontrollen und Prüfungstätigkeiten interner oder externer Prüfer/-innen wird durch den gesetzlichen und fachlichen Leistungsauftrag kommunaler Verwaltungen (z. B. § 75 Abs. 1 GO NRW) geprägt. Alles, was die dauerhafte Leistungsfähigkeit einer Kommunalverwaltung gefährden könnte, soll identifiziert und kontrolliert werden.

Da es sich um jeweils durchaus komplexe Subsysteme einer Verwaltung handelt, sind grundsätzliche Regelungen zur Ausgestaltung dieser Systeme erforderlich. Die in Schrifttum und Praxis herausgebildeten Systeme sind bekanntlich das Risikomanagementsystem, das Interne Kontrollsystem und das auf gesetzestreue ausgerichtete Compliance Management System, das zuletzt v.a. im Wege der steuerlichen Kontrollsysteme (Tax Compliance Management Systeme (TCMS)) Verbreitung gefunden hat.

Folgende Übersicht stellt die drei zentralen Systeme im Zusammenhang dar. Man kann sie sich durchaus als ein in der Realität integriertes – jedenfalls stark wechselseitig abhängiges – Gesamtsystem (=Governance) vorstellen. Die in der Literatur entwickelte Dreiteilung wird zunehmend kritisch beurteilt und sollte unseres Erachtens nicht überbewertet werden.

Unter "Good Governance" kann man dann ein effizientes und wirksames lokales Gesamtsystem verstehen, das die Aufgaben Risikokontrolle und Rechtstreue zuverlässig umsetzt.

| System                            | Funktion                                                                              | Leitfrage                                                    |
|-----------------------------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------|
| Risikomanagementsystem            | Zukünftige Ereignisse identifizieren, bewerten, steuern und überwachen.               | Was kann die kommunalen Ziele gefährden?                     |
| Internes Kontrollsystem (IKS)     | Fehler, Rechtsverstöße, Vermögensschäden oder Manipulation verhindern bzw. aufdecken. | Welche Kontrolle reduziert das konkrete Prozessrisiko?       |
| Compliance Management             | Einhaltung externer und interner Regeln organisatorisch absichern.                    | Welche Regelpflichten sind wie umgesetzt?                    |
| Rechnungsprüfung/Interne Revision | Angemessenheit, Implementierung und Wirksamkeit unabhängig beurteilen.                | Ist die Kontrolle richtig gestaltet und nachweisbar wirksam? |

Übersicht 2: (Teil-)Systeme der lokalen Governance

**Merksatz** Das Compliance- & Risikomanagement bestimmt, was (rechtlich) gefährlich ist. Das IKS legt fest, was dagegen getan wird. Die unabhängige Prüfung beurteilt, ob dies tatsächlich funktioniert.

## 2.2 Steuerungs- und Prüfungskreislauf

Nach herrschender Meinung wird die Tätigkeit im Bereich Governance durch einen wiederkehrenden Steuerungs- und Prüfungskreislauf bestimmt, der wie folgt beschrieben werden kann:

1. Kommunale Ziele und kritische Prozesse bestimmen.
2. Risikoereignisse und Ursachen identifizieren.
3. Bruttoisiken bewerten.
4. Bestehende Kontrollen erfassen und Kontrolllücken erkennen.
5. Restrisiken sowie zusätzliche Maßnahmen festlegen.
6. Durchführung und Kontrollnachweise überwachen.
7. Wirksamkeit unabhängig prüfen und Maßnahmen nachhalten.

## 2.3 Risikobewertung

Risikobewertungen in kommunalen Verwaltungen dienen der Priorisierung knapper Steuerungs- und Prüfungsressourcen. Sie sind kein Selbstzweck und ersetzen weder Szenarioanalyse noch fachliche Beurteilung. Insbesondere die häufig verwendete Multiplikation ordinaler Stufen für Wahrscheinlichkeit und Schadensausmaß erzeugt keinen mathematisch exakten Erwartungswert; sie liefert lediglich einen transparenten Rangbeziehungsweise Priorisierungswert.

Ein stark vereinfachter Bewertungsmaßstab verwendet Eintrittswahrscheinlichkeit  $W$  und Schadensausmaß  $S$  mit jeweils fünf Stufen. Der Priorisierungswert ergibt sich aus  $R = W \times S$ . Für wesentliche kommunale Risiken sind neben finanziellen Schäden insbesondere Rechtmäßigkeit, Versorgungssicherheit, Reputation, Datenschutz und Auswirkungen auf Menschen zu berücksichtigen.<sup>2</sup>

Methodischer Hinweis: Bei fünfstufigen, ordinalen Skalen ist das Produkt  $W \times S$  kein mathematisch exakter Erwartungswert. Es dient der transparenten Priorisierung. Skalenanker, Zeithorizont, Risikoperspektive (brutto/netto), Abhängigkeiten und Eskalationsschwellen sind deshalb vorab festzulegen; bei wesentlichen Risiken sind Szenarioanalysen und Bandbreiten ergänzend einzubeziehen.

<sup>2</sup> Die Multiplikation ordinaler Kategorien ist als transparenter Priorisierungsscore, nicht als metrischer Erwartungswert zu interpretieren. Vgl. Diederichs, M. (2023): Risikomanagement und Risikocontrolling, 5. Aufl., Vahlen.

| Risiko-Score | Einstufung | Reaktion                                                         |
|--------------|------------|------------------------------------------------------------------|
| 1–4          | niedrig    | Beobachten; Regelkontrollen genügen häufig.                      |
| 5–9          | mittel     | Kontrolle dokumentieren und periodisch überwachen.               |
| 10–15        | hoch       | Schlüsselkontrolle und Verantwortlichkeit verbindlich festlegen. |
| 16–25        | sehr hoch  | Sofortige Behandlung, Eskalation und enges Monitoring.           |

Übersicht 3: Beispiel für Stufen des Risiko-Scoring

## 3. Gesamtkonzeption einer IKS-Prüfung

### 3.1 Einordnung in die risikoorientierte Prüfungsplanung

Die örtliche Rechnungsprüfung kann nicht sämtliche Prozesse und Kontrollen jährlich vollständig prüfen. Erforderlich ist ein risikoorientiertes Prüfungsuniversum: Prozesse, Organisationseinheiten, IT-Verfahren, Haushaltsvolumina, Rechtsrisiken, frühere Feststellungen und Veränderungsereignisse werden zu prüfbaren Einheiten zusammengeführt und in eine mehrjährige Planung überführt.

| Planungsgegenstände                | Ergebnis                                                                                                           |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Prüfungsuniversum (Audit Universe) | Vollständige, strukturierte Übersicht der wesentlichen Prozesse und (IT-)Systeme.                                  |
| Risikobewertung                    | Priorisierung nach Auswirkung, Wahrscheinlichkeit, Veränderungsdynamik, Kontrollreife und früheren Feststellungen. |
| Mehrjahresplanung                  | Abdeckung wesentlicher IKS-Felder in einem nachvollziehbaren Zyklus.                                               |
| Jahresplanung                      | Konkrete Prüfungen mit Ressourcen, Zeitfenster und Berichtsadressaten.                                             |
| Einzelauftrag                      | Abgegrenzter Prüfungsgegenstand, Ziel, Kriterien, Zeitraum und Vorgehen.                                           |

Übersicht 4: Planungsgegenstände der IKS-Prüfung

### 3.2 IKS-Prüfungsphasen

So wie die risikoorientierte Prüfung generell unterliegt auch die spezifische IKS-Prüfung (gedacht als ein Teilsystem risikoorientierter Prüfungen) einem strukturierten Vorgehensmodell. Es hat sich eingebürgert solche Konzepte als Phasenmodelle zu bezeichnen und zu beschreiben. Das gilt damit auch für die IKS-Prüfung. Gesucht ist also ein risikoorientiertes Phasenmodell für IKS-Prüfungen.

Die Zahl und Abgrenzung der Phasen kann je nach Prüfungsansatz variieren. Unverändert bleibt das Grundkonzept risikoorientierter Prüfungen: man geht von eher allgemeinen, teilweise extern dominierten Kriterien (Risiken) über intern-systemorientierte "globale" Risiken zu einzelnen Teilbereichen bzw. Fallgruppen über und beurteilt zunächst die insoweit noch eher allgemeinen Risiken vorläufig. Anschließend werden dann diese vorläufigen Beurteilungen zumeist mit Stichproben und ausgewählten Einzelfällen vertieft und durch detaillierte Beurteilung entweder revidiert oder bestätigt. Das alles wird abschließend zu einem prüferischen Gesamturteil zusammengeführt. Im Falle von IKS-Prüfungen stehen dabei Risiken, Kontrollen, Prozesse und Wirksamkeitstests im Vordergrund.

| Phase                            | Kernhandlungen                                                                                         | Arbeitsergebnis                                         |
|----------------------------------|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| 1 Auftrag und Abgrenzung         | Prüfungsziel, Gegenstand, Zeitraum, Kriterien, Rollen und Berichtsempfänger festlegen.                 | Prüfungsauftrag/Scoping-Memo                            |
| 2 Prozess- und Risikoverständnis | Interviews, Unterlagen, Walkthroughs, Daten- und Systemlandschaft sowie eventfähige Quellen auswerten. | Prozessbild, Risikoinventar und vorläufiges Datenmodell |
| 3 Soll-Konzeption                | Kontrollziele und erforderliche Kontrollen aus Risiken und Regelwerk ableiten.                         | Soll-Risiko-Kontrollmatrix                              |
| 4 Design und Implementierung     | Kontrollgestaltung beurteilen und tatsächliche Einrichtung nachvollziehen.                             | Design-/Implementierungsurteil                          |
| 5 Wirksamkeitstest               | Kontrollpopulation bestimmen, Stichprobe oder Vollprüfung durchführen, Abweichungen bewerten.          | Testbogen und Evidenz                                   |
| 6 Gesamtbewertung                | Einzelermängel, Kompensationskontrollen und Kombinationseffekte beurteilen.                            | Prozess-/Systemurteil                                   |
| 7 Bericht und Follow-up          | Ursache, Risiko, Feststellung, Empfehlung, Maßnahme und Frist vereinbaren/nachhalten.                  | Prüfungsbericht und Maßnahmenregister                   |

Übersicht 5: Ein risikoorientiertes Phasenkonzept für die IKS-Prüfung

### 3.3 Prüfungsobjekt und Aussageform

Prüfungsumfang und Aussageform müssen zusammenpassen. Eine Prozessprüfung ausgewählter Schlüsselkontrollen erlaubt regelmäßig kein Gesamturteil über das gesamte IKS der Kommune. Kriterien, Zeitraum, Population, Stichprobe und etwaige Einschränkungen sind im Prüfungsauftrag und im Bericht ausdrücklich zu benennen.

- Prüfungsobjekt: eindeutig benannter Prozess oder Teilprozess einschließlich Systeme, Schnittstellen und Organisationseinheiten.
- Prüfungszeitraum: Stichtagsprüfung für Design/Implementierung oder Zeitraumprüfung für operative Wirksamkeit.
- Prüfungskriterien: Gesetz, Satzung, Dienstanweisung, Prozessziel, Kontrollstandard und anerkannte methodische Grundsätze.
- Aussagegrenze: keine pauschale Bestätigung des gesamten IKS, wenn nur einzelne Prozesse oder Kontrollen geprüft wurden.
- Wesentlichkeit: finanzielle und nichtfinanzielle Auswirkungen sowie qualitative Nulltoleranzbereiche berücksichtigen.

**Key-Controls** Für jede Schlüsselkontrolle ("Key-Control") müssen Population, Kontrollfrequenz, Verantwortlichkeit, erwarteter Nachweis und zulässige Abweichung vor Beginn des Wirksamkeitstests feststehen.

### 3.4 Rollenmodell und Unabhängigkeit

Wie auch in anderen risikoorientierten Prüfungen müssen auch bei IKS-Prüfungen betroffene oder handelnde Personen durch Rollen definiert und in ihrer Unabhängigkeit von der Prüfungsdurchführung bestätigt sein. Wesentliche Rollen sind dabei regelmäßig die folgenden (siehe Übersicht6):

| Rolle | Verantwortung |
|-------|---------------|
|-------|---------------|

| Rolle                          | Verantwortung                                                                                                         |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Verwaltungsleitung/Führung     | Ziele, Risikobereitschaft, Organisation und wirksame Kontrollen verantworten.                                         |
| Prozessverantwortliche         | Risiken und Kontrollen im Prozess gestalten, durchführen und dokumentieren.                                           |
| Querschnittsfunktionen         | Methoden, Compliance, Informationssicherheit, Datenschutz, Steuer- oder Risikomanagement unterstützen und überwachen. |
| Örtliche Rechnungsprüfung      | Unabhängig prüfen; nicht selbst für Aufbau oder Durchführung der geprüften Kontrollen verantwortlich werden.          |
| Rechnungsprüfungsausschuss/Rat | Prüfungsergebnisse beraten und die Umsetzung wesentlicher Maßnahmen begleiten.                                        |

Übersicht 6: Rollenmodelle und Unabhängigkeit in der IKS-Prüfung

## 4. Ansatzpunkte zur Prüfung des Risikomanagementsystems

### 4.1 Kommunale Beispiele für Risiken und Kontrollen

Wesentliche Beispiele für die Kombination "Risiken und Kontrollen" zeigt die nachstehende Tabelle:

| Risikofeld                | Konkretes Risiko                                             | Praktische Kontrollen                                                                                                                                 |
|---------------------------|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zahlungsverkehr           | Unberechtigte oder manipulierte Auszahlung                   | Funktionstrennung zwischen Anordnung, Freigabe und Zahlung; Vier-Augen-Freigabe; Bankkonten-Whitelist; Tageshöchstgrenzen; nachträgliche Datenanalyse |
| Debitoren und Forderungen | Forderungen werden nicht oder verspätet erhoben              | Soll-Ist-Abgleich Fachverfahren/Hauptbuch; Fälligkeits- und Mahnlisten; Überwachung von Niederschlagungen und Erlassen                                |
| Kreditoren                | Doppelzahlungen, Scheinrechnungen, falsche Bankverbindungen  | Dublettenprüfung; Abgleich IBAN/Kreditor; Änderungsprotokoll bei Stammdaten; Rückruf beim Lieferanten bei IBAN-Änderung                               |
| Buchführung               | Unzulässige oder ungewöhnliche Buchungen                     | Kontierungsvorgaben; Gegenkontenanalyse; Journal-Entry-Testing; Freigabe manueller Abschlussbuchungen; Perioden- und Betragsgrenzen                   |
| Jahresabschluss           | Unvollständige Rückstellungen oder falsche Abgrenzungen      | Abschlusskalender; Verantwortlichkeitsmatrix; Saldenbestätigungen; Rückstellungsmeldungen der Fachämter; zentrale Plausibilitätsprüfungen             |
| Haushaltswirtschaft       | Überschreitung von Ansätzen und Budgets                      | Monatliches Plan-Ist-Monitoring; Forecast; Sperren; Ampelberichte; Pflicht zur Gegensteuerungsmaßnahme                                                |
| Liquidität                | Zahlungsunfähigkeit oder übermäßige Kassenkredite            | Rollierende Liquiditätsplanung; Mindestliquidität; Kreditlinienmonitor; Stressszenarien; täglicher Finanzstatus                                       |
| Vergabe                   | Manipulation, unzulässige Direktvergabe, Interessenkonflikte | Zentrale Vergabestelle; Vier-Augen-Prinzip; Vergabevermerk; Schwellenwertkontrolle; Erklärung zu Interessenkonflikten; Bieterrotation                 |

| Risikofeld              | Konkretes Risiko                                          | Praktische Kontrollen                                                                                                        |
|-------------------------|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Zuwendungen             | Doppelförderung oder zweckwidrige Mittelverwendung        | Förderakte; Verwendungsnachweis; Meilensteinzahlungen; Stichproben/Vor-Ort-Kontrollen; Abgleich mit anderen Förderprogrammen |
| Sozialleistungen        | Mehrfach- oder Fehlzahlungen                              | Identitäts- und Haushaltsabgleich; automatisierte Plausibilitätsregeln; Wiedervorlagen; Stichproben nach Risikoklassen       |
| Gebühren                | Gebühren werden nicht vollständig oder zu niedrig erhoben | Abgleich Leistungsmenge/Gebührenbescheid; Gebührenkalkulation; Kontrollsummen; Vollständigkeitsabgleich mit Fachverfahren    |
| Personal                | Unberechtigte Zahlungen oder Interessenkonflikte          | Stellenplanabgleich; Personalstammänderungen mit Vier-Augen-Freigabe; Austrittskontrolle; Nebentätigkeitsanzeigen            |
| Korruption              | Bevorzugung einzelner Anbieter oder Antragsteller         | Gefährdungsatlas; Rotation; Funktionstrennung; Hinweisgebersystem; Korruptionsbeauftragter; anlassbezogene Prüfungen         |
| IT und Cybersecurity    | Ransomware, Datenverlust, Systemausfall                   | Rollen- und Berechtigungskonzept; MFA; Backup und Rücksicherungstest; Notfallhandbuch; Krisenstab; Wiederanlaufübungen       |
| Datenschutz             | Unzulässiger Datenzugriff oder Datenabfluss               | Berechtigungskontrollen; Protokollierung; Löschkonzept; Datenschutz-Folgenabschätzung; Auswertung von Zugriffslogs           |
| Bau und Investitionen   | Kostensteigerungen, Nachträge, Terminverzug               | Risikoregister je Großprojekt; Kostenreserve; Nachtragsprüfung; Meilensteinfreigaben; unabhängiges Projektcontrolling        |
| Beteiligungen           | Verluste oder Haftungsrisiken kommunaler Unternehmen      | Quartalsberichte; Kennzahlen- und Covenant-Monitoring; Risikoberichte; Zustimmungsvorbehalte; Mandatsträgerbetreuung         |
| Krisen und Katastrophen | Ausfall kritischer Verwaltungsleistungen                  | Krisenorganisation; Ersatzarbeitsplätze; Priorisierung kritischer Dienstleistungen; Einsatzteams; Praxis-Übungen             |

Das Risikomanagementsystem ist erkennbar weiter gefasst als das rechnungslegungs- und prozessbezogene IKS. Es soll sicherstellen, dass wesentliche strategische, finanzielle, rechtliche, operative, personelle sowie daten- und informationstechnische Risiken – insbesondere Cyber-Sicherheit - rechtzeitig erkannt und kontrolliert werden. Die Prüfung kann organisationsweit oder für einen abgegrenzten Bereich erfolgen, für einzelne Fachverfahren oder für umfassende Querschnittsaufgaben wie Finanzen, Personal- oder IT-Wirtschaft.<sup>3</sup>

<sup>3</sup> Vgl. ISO 31000:2018, Risk management – Guidelines, sowie COSO (2017), Enterprise Risk Management – Integrating with Strategy and Performance.

| Prüffeld             | Leitfragen                                                                                               | Mögliche Nachweise                                  |
|----------------------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Governance           | Sind Ziele, Rollen, Eskalationswege und Risikobereitschaft festgelegt?                                   | Richtlinie, Geschäftsverteilung, Gremienprotokolle  |
| Risikoidentifikation | Werden wesentliche Risiken vollständig und anlassbezogen erhoben?                                        | Risikokatalog, Workshops, Umfeldanalyse             |
| Bewertung            | Sind Skalen, Zeithorizonte, Brutto-/Nettorisiko und Abhängigkeiten definiert?                            | Bewertungsmethodik, Risikomatrix, Szenarien         |
| Steuerung            | Sind Maßnahmen, Verantwortliche, Fristen und Ressourcen festgelegt?                                      | Maßnahmenregister, Beschlüsse, Projektpläne         |
| Überwachung          | Werden Frühindikatoren, Maßnahmenstatus und Restrisiken verfolgt?                                        | Kennzahlen, Dashboards, Quartalsberichte            |
| Berichterstattung    | Erreichen wesentliche Risiken rechtzeitig die zuständigen Entscheidungsträger?                           | Risikoberichte, Eskalationen, Vorlagen              |
| Integration          | Ist Risikomanagement mit Haushalt, Zielen, Projekten, Beteiligungen, IKS und Krisenmanagement verbunden? | Planungsunterlagen, Prozesslandkarte, Berichtswesen |
| Verbesserung         | Werden Vorfälle, Prüfungsfeststellungen und Beinahe-Schäden ausgewertet?                                 | Lessons Learned, Follow-up, Reifegradanalyse        |

Übersicht 7: Prüffelder der IKS-Prüfung

## 4.2 Typische Prüfungshandlungen

Typische Prüfungshandlungen sind:

- Risikomanagement-Richtlinie und örtliche Zuständigkeiten gegen tatsächliche Praxis spiegeln.
- Risikoinventur vom Entstehungsprozess bis zur Berichterstattung nachvollziehen.
- Ausgewählte Top-Risiken rückwärts auf Quellen, Annahmen und Maßnahmen prüfen.
- Bekannte Schadensfälle, Prüfungsfeststellungen und Haushaltsrisiken mit dem Risikoregister abgleichen.
- Bewertungsunterschiede zwischen Fachbereichen analysieren und Kalibrierung beurteilen.
- Prüfen, ob überfällige Maßnahmen, hohe Restrisiken und Schwellenwertüberschreitungen eskaliert wurden.

## 5. Digitale IKS-Prüfung

Die zuvor beschriebenen Prüfungshandlungen werden angesichts der fortschreitenden Digitalisierung kommunaler Verwaltungsprozesse zunehmend durch technisch gestützte und datenorientierte Verfahren ergänzt. Dazu zählen insbesondere Datenanalysen, digitale Fernprüfungen und automatisierte Auswertungen von System- und Ereignisdaten.

Digitale Verwaltungsprozesse verlagern Kontrollen zunehmend in Fachverfahren, Schnittstellen, Berechtigungssysteme und automatisierte Workflows. Die Prüfung muss deshalb organisatorische, technische und prozessuale Kontrollen gemeinsam betrachten. Prüfungsnachweise entstehen nicht nur in Akten, sondern insbesondere in Parameterlisten, Konfigurationen, Protokoll- und Ereignisdaten, Rollenmodellen, Änderungsverläufen, Monitoringberichten und maschinell bestimmaren Kontrollpopulationen.

Systemischer Ansatz der IDR-Leitlinien: Die Rechnungsprüfung soll nicht sämtliche Anforderungen des BSI-Grundschatzes technisch im Detail nachprüfen. Sie beurteilt systemisch, ob die Verantwortlichen wesentliche Bausteine betrachtet und elementare technische, organisatorische, infrastrukturelle und personelle Maßnahmen initiiert und wirksam umgesetzt haben.

## 5.1 Prüfungsdimensionen digitaler Kontrollen

In der Regel werden die folgenden Prüfungsdimensionen digitaler Kontrollen unterschieden:

| Dimension              | Prüfungsgegenstand                                                                       | Typische digitale Evidenz                                     |
|------------------------|------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Governance             | Strategie, Leitlinien, Rollen, Verantwortlichkeiten und Berichtswesen.                   | Beschlüsse, Richtlinien, Tickets, Managementberichte          |
| Identitäten und Rechte | Zutritt, Zugang, Zugriff, privilegierte Rechte und Funktionstrennung.                    | Benutzer-/Rollenexporte, Änderungslogs, Rezertifizierungen    |
| IT-Betrieb             | Verfügbarkeit, Monitoring, Patchen, Schadsoftware, Redundanz und Dienstleistersteuerung. | Monitoringlogs, Patchstatus, Alarm- und Serviceberichte       |
| Datenintegrität        | Vollständige und richtige Verarbeitung, Schnittstellen und Stammdaten.                   | Kontrollsummen, Fehlerlogs, Änderungsverläufe, Reconciliation |
| Datensicherung         | Sicherung, Auslagerung, Zugriffsschutz und Wiederherstellbarkeit.                        | Backup-Logs, Restore-Protokolle, Aufbewahrungsnachweise       |
| Änderungsmanagement    | Genehmigte, getestete und nachvollziehbare Systemänderungen.                             | Change-Tickets, Test-/Freigabenachweise, Transportlogs        |
| Kontinuität            | Kritische Prozesse, Ausfalltoleranzen, Notfallorganisation und Wiederanlauf.             | BIA, Notfallhandbuch, Übungen, Wiederanlaufprotokolle         |

Übersicht 8: Prüfungsdimensionen digitaler Kontrollen

## 5.2 Informationssicherheit nach IDR-L 113-1

Die IDR-Prüfungsleitlinie 113-1 stellt die Schutzbedarfe Verfügbarkeit, Vertraulichkeit und Integrität einschließlich Authentizität in den Mittelpunkt. Ihre Checkliste umfasst Technikräume und Infrastruktur, Sicherheitsmanagement, organisatorische Maßnahmen, Virenschutz und Datensicherung.<sup>4</sup>

| Prüffeld                | Ausgewählte Prüffragen                                                                         | Wirksamkeitsnachweis                                  |
|-------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Technikräume            | Zutritt, Brand/Wasser, Strom, USV, Klima, Redundanz und Störungsmeldung geregelt?              | Zutrittslogs, Alarmtests, Wartungen, Vor-Ort-Begehung |
| Sicherheitsorganisation | Leitlinie, Sicherheitsbeauftragte, Sicherheitskonzept, Ziele und Managementberichte vorhanden? | Freigaben, Organigramm, Berichte, Maßnahmenstatus     |
| Berechtigungen          | Vergabe von Zutritt, Zugang und Zugriff geregelt, dokumentiert und periodisch überprüft?       | Rollenexport, Genehmigung, Rezertifizierungsprotokoll |
| Personalmaßnahmen       | Einweisung, Verpflichtung, Schulung und geregelter Austritt wirksam?                           | Teilnahmenachweise, Austrittstickets, Rechteentzug    |
| Virenschutz             | Konzept, zentrale Aktualisierung, Erkennung, Dokumentation und Meldekette wirksam?             | Managementkonsole, Update-/Incident-Logs              |
| Datensicherung          | Konzept, Turnus, geschützte Aufbewahrung und regelmäßige Wiederherstellungstests?              | Backup- und Restore-Logs, Testprotokolle              |

Übersicht 9: IKS-Prüfung der Informationssicherheit nach IDR L 113-1

Für ein heutiges BCM/Notfallmanagement ist der finale BSI-Standard 200-4 (2023) die maßgebliche BSI-Referenz. Ältere Verweise auf BSI 100-4 sind historisch einzuordnen. Die IDR-Leitlinie ist eine Prüfungshilfe, keine eigenständige Rechtsnorm; örtliche Rechts-, Sicherheits- und Organisationsvorgaben bleiben maßgeblich.<sup>5</sup>

<sup>4</sup> Institut der Rechnungsprüfer (IDR), Prüfungsleitlinie IDR-L 113-1 – Informationssicherheit, Stand 09/2023.

<sup>5</sup> Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standard 200-4 – Business Continuity Management, finale Fassung 2023.

## 5.3 Notfallmanagement nach IDR-L 113-2

Notfallmanagement beziehungsweise Business Continuity Management soll die Handlungsfähigkeit bei länger andauernden Ausfällen mit hohen Auswirkungen erhalten. Die Leitlinie unterscheidet Störung, Notfall, Krise und Katastrophe und verbindet präventive Notfallvorsorge mit organisierter Notfallbewältigung.

| Kernelement                   | Prüfungsfokus                                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Business Impact Analyse (BIA) | Kritische Fachprozesse, Fachverfahren, Ressourcen, Abhängigkeiten, Auswirkungen und maximal tolerierbare Ausfallzeiten vollständig bestimmen.     |
| Risikoanalyse                 | Bedrohungen, Schwachstellen, örtliche Besonderheiten, Wahrscheinlichkeit und Schadensfolgen bewerten.                                             |
| Notfallvorsorgekonzept        | Infrastrukturelle, technische, organisatorische und personelle Präventionsmaßnahmen verbindlich festlegen.                                        |
| Notfallhandbuch               | Notfallorganisation, Rollen, Alarmierung, Kommunikation, Kontaktdaten, Geschäftsfortführung, Wiederanlauf und Wiederherstellung dokumentieren.    |
| Übungen und Tests             | Systemausfall, Datenwiederherstellung und Wiederanlauf praktisch testen, dokumentieren und auswerten.                                             |
| Verfügbarkeitsanforderungen   | Maximal tolerierbare Ausfallzeiten mit Verwaltungs- und Fachbereichsleitung vereinbaren und in Service-, Redundanz- und Ersatzplanung überführen. |

Übersicht 10: IKS-Prüfung des Notfallmanagements nach IDR-L 113-2

## 5.4 Vom Fragebogen zum Wirksamkeitstest

Ein ausgefüllter Fragebogen belegt zunächst nur eine Selbstausskunft oder das Vorhandensein einer Regelung. Für eine Wirksamkeitsaussage muss die Rechnungsprüfung die Aussage mit digitaler Evidenz verbinden.

| Prüfschritt      | Beispiel Datensicherung                                                                            |
|------------------|----------------------------------------------------------------------------------------------------|
| Soll-Anforderung | Kritische Daten werden täglich gesichert und quartalsweise wiederhergestellt getestet.             |
| Design           | Backupverfahren, Verantwortlichkeit, Aufbewahrung und Fehlerbehandlung sind geeignet festgelegt.   |
| Implementierung  | Jobs, Speicherziele, Zugriffsschutz und Benachrichtigung sind tatsächlich eingerichtet.            |
| Population       | Sämtliche Backup-Jobs und Restore-Tests des Prüfungszeitraums werden vollständig exportiert.       |
| Test             | Fehlgeschlagene Jobs, verspätete Behebung, Sicherungslücken und Restore-Ergebnisse auswerten.      |
| Urteil           | Kontrolle wirksam, teilweise wirksam oder unwirksam; Auswirkungen auf kritische Prozesse ableiten. |

Übersicht 11: Vom Fragebogen zum Wirksamkeitstest

## 5.5 Digitale Risiko-Kontrollmatrix für IT-Sicherheit und Notfallvorsorge

Eine Risiko-Kontrollmatrix (RKM) für den Bereich IT-Sicherheit und Notfallvorsorge könnte wie folgt aussehen:

| ID    | Risiko                    | Schlüsselkontrolle                                                   | Evidenz/Test                                                     |
|-------|---------------------------|----------------------------------------------------------------------|------------------------------------------------------------------|
| IT-01 | Unberechtigter Zugriff    | Periodische Rezertifizierung privilegierter Rechte.                  | Vollständiger Rollenexport; Abgleich Personal und Genehmigungen. |
| IT-02 | Rechte nach Austritt      | Automatisierter Austrittsworkflow mit Rechteentzug.                  | Personal-/Benutzerabgleich; Zeitdifferenz bis Sperrung.          |
| IT-03 | Unbemerkter Systemausfall | Zentrales Monitoring mit Ruf- und Eskalationskette.                  | Alarmstichprobe; Reaktions- und Behebungszeiten.                 |
| IT-04 | Schadsoftware/Ransomware  | Zentraler Virenschutz mit aktuellen Signaturen und Incident-Prozess. | Konsolenexport, Updatequote, Incidents und Eskalationen.         |

| ID     | Risiko                                 | Schlüsselkontrolle                                         | Evidenz/Test                                            |
|--------|----------------------------------------|------------------------------------------------------------|---------------------------------------------------------|
| IT-05  | Datenverlust                           | Automatisierte Sicherung mit geschützter Auslagerung.      | Jobpopulation, Fehlerquote und Nachbearbeitung.         |
| IT-06  | Nicht wiederherstellbare Sicherung     | Regelmäßige dokumentierte Restore-Tests.                   | Testumfang, Ergebnis, Abweichung und Maßnahmen.         |
| BCM-01 | Kritischer Prozess nicht erkannt       | Periodische BIA unter Beteiligung der Fachbereiche.        | Prozess-/Verfahrensabgleich und Freigaben.              |
| BCM-02 | Unrealistische Ausfalltoleranz         | MTA/RTO durch Leitung festgelegt und technisch gespiegelt. | Abgleich BIA, SLA, Redundanz und Wiederanlauf.          |
| BCM-03 | Notfallorganisation nicht einsatzfähig | Aktuelles Notfallhandbuch und erreichbare Rollen.          | Dokumentenprüfung und unangekündigter Alarmierungstest. |
| BCM-04 | Wiederanlauf scheitert                 | Szenariobasierte Übungen und technische Tests.             | Übungsprotokoll, Zielerreichung, Lessons Learned.       |

Übersicht 12: Beispiel RKM für IT-Sicherheit und Notfallvorsorge

## 5.6 Digitale Prozessprüfungen und Process Mining

Process Mining wird im Folgenden nicht als Visualisierungsinstrument, sondern als prüferische Analysemethode verstanden. Ihr Erkenntniswert entsteht erst aus der Verbindung von Prüfungsziel, Sollprozess, Eventlog-Datenvertrag, populationsbezogener Vollständigkeit, reproduzierbarer Transformation, Abweichungsanalyse und fachlichem Nachtest. Die Methode erweitert die Reichweite der Risikoanalyse; sie erzeugt für sich genommen weder einen Kontrollnachweis noch ein Prüfungsurteil.

Process Mining rekonstruiert und untersucht digital-systemseitig tatsächlich protokollierte Prozessabläufe aus Ereignisdaten (=Eventlogs). Für die Rechnungsprüfung ist es kein eigenständiges Prüfungsurteil, sondern eine datenanalytische Methode innerhalb des risikoorientierten Prüfungsansatzes. Sie kann Prozessverständnis, Risikoanalyse, Auswahl von Einzelfällen und Wirksamkeitsprüfungen wesentlich unterstützen.<sup>6</sup>

### 5.6.1 Drei Analysearten und ihr Prüfungsnutzen

Man unterscheidet grundsätzlich die folgenden drei Analyseschritte.

| Analyseschritt                            | Prüferische Fragestellung                                                              | Typische Ergebnisse                                                                    |
|-------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Process Discovery                         | Wie läuft der Prozess nach den protokollierten Daten tatsächlich ab?                   | Ist-Modell, Varianten, Schleifen, Übergänge, seltene Pfade                             |
| Conformance Checking (Prozess-Compliance) | Entsprechen reale Abläufe dem Sollprozess und den Kontrollregeln?                      | fehlende, verfrühte oder verspätete Aktivitäten; Regelverstöße; Alignment-Abweichungen |
| Performance/Enhancement                   | Wo entstehen Wartezeiten, Engpässe, Wiederholungen oder auffällige Bearbeitungsmuster? | Durchlauf- und Liegezeiten, Rework-Quoten, Bottlenecks, Ressourcen- und Zeitmuster     |

Übersicht 13: Analysearten und ihr Prüfungsnutzen von Process-Mining-Analysen

Prüferischer Schwerpunkt ist nicht die möglichst umfassende oder grafisch komplexe Prozessdarstellung, sondern die aus Prüfungsziel und Risiken abgeleitete Analysefrage, etwa ob Prozessverzögerungen zu Vermögensschäden führen könnten. Discovery liefert zunächst Hypothesen; Conformance- und Detailprüfungen müssen klären, ob Abweichungen zulässig, fehlerhaft oder kontrollrelevant sind.

<sup>6</sup> Van der Aalst, W. M. P. (2016): Process Mining – Data Science in Action, 2. Aufl., Springer, DOI 10.1007/978-3-662-49851-4.

## 5.6.2 Eventlog als prüferischer Datenvertrag

Ein klassisches Eventlog benötigt mindestens eine eindeutige Fall-ID, eine fachlich definierte Aktivität und einen belastbaren Zeitstempel. Für prüferische Zwecke sind regelmäßig weitere Attribute erforderlich. Der Datenvertrag muss Quelle, Transformation, fachliche Bedeutung, Gültigkeitsregeln und Abstimmung zur Grundgesamtheit dokumentieren.<sup>7</sup>

| Feld          | Mindestanforderung                                                        | Kommunales Beispiel/Prüfrisiko                                                                                     |
|---------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Case-ID       | identifiziert den geprüften Fall über alle relevanten Systeme eindeutig   | Kassenzeichen, Vorgangs-, Beleg- oder Rechnungsnummer; Geschäftspartnernummer allein kann mehrere Fälle vermischen |
| Activity      | fachlich verständliche, konsistent abgeleitete Prozessaktivität           | Anlage Steuerfall, Bescheid, Rechnungseingang, sachliche Freigabe, Zahlung                                         |
| Timestamp     | Zeitpunkt, ggf. Start und Ende, mit Zeitzone und definierter Granularität | gleiche Zeitstempel können Reihenfolgen unentscheidbar machen; Batchläufe verzerren Bearbeitungszeiten             |
| Resource/Role | ausführende Stelle oder pseudonymisierte Rolle, soweit erforderlich       | Funktionstrennung, Selbstfreigabe, auffällige Vertretungs- oder Nachtmuster                                        |
| Object/Bezug  | weitere Objekte und Schlüssel für End-to-End-Verknüpfung                  | Bestellung, Rechnung, Wareneingang, Zahlung; bei 1:n/n:m-Beziehungen ggf. objektzentrierter Ansatz                 |
| Attributes    | risikorelevante Merkmale mit Herkunft und Datentyp                        | Betrag, Wertgrenze, Buchungskreis, Organisationseinheit, Status, Änderungsgrund                                    |

Übersicht 14: Bedeutung von Eventlogs

Vollständigkeitsnachweis: Die Anzahl und – soweit sinnvoll – die Wertsumme der Fälle und Ereignisse sind zu Quellsystem, Nebenbuch/Hauptbuch oder einem unabhängigen Kontrolltotal abzustimmen. Ohne diesen Nachweis beschreibt Process Mining nur den gelieferten Datenausschnitt; eine Aussage über die vollständige Population ist dann nicht zulässig.

## 5.6.3 Prüfungsablauf: acht Arbeitsschritte

Der generelle Ablauf einer Process-Mining-Analyse kann wie folgt beschrieben werden:

1. Prüfungsziel, Prozessgrenzen, Zeitraum, Kriterien und erwartete Aussage festlegen.
2. Sollprozess, Schlüsselkontrollen, zulässige Varianten und Eskalationsregeln aufnehmen.
3. IT-Landschaft, Tabellen, Schnittstellen und fachliche Schlüssel gemeinsam mit Fachbereich und IT identifizieren.
4. Eventlog-Datenvertrag erstellen; Extraktion und Transformation reproduzierbar dokumentieren.
5. Datenintegrität, Vollständigkeit, Eindeutigkeit, Zeitlogik und fachliche Plausibilität validieren.
6. Ist-Prozess entdecken und Komplexität durch prüfungszielbezogene Filter oder Meilensteine beherrschbar machen.
7. Soll-Ist-Abweichungen, Kontrollregeln, Varianten, Zeit- und Ressourcenmuster untersuchen und risikoorientiert Einzelfälle auswählen.
8. Treffer mit Belegen, Konfigurationen, Interviews und Nachtests validieren; Ursache, Reichweite und Kontrollwirkung beurteilen.

**Hinweis: wegen der in der Regel erkennbaren Betroffenheit einzelner Arbeitsplätze sollten die Analysen zumindest auf Teamebene durchgeführt oder – wenn nicht anders möglich – maximal anonymisiert durchgeführt werden, da ansonsten datenschutzrechtliche Aspekte berührt werden.**

<sup>7</sup> Van der Aalst, W. M. P.; Carmona, J. (Hrsg.) (2022): Process Mining Handbook, Springer, insbesondere die Beiträge zu Event Log Engineering und Data Challenges.

## 5.6.4 Verbindung von Risiko-Kontrollmatrix und Process Mining

Die Erkenntnisse aus Process-Mining-Analysen und der Risiko-Kontrollmatrix werden im Rahmen der IKS-Prüfungen wie folgt zusammengeführt:

| Risiko/Kontrollziel    | Aus Ereignisdaten prüfbare Regel                                                    | Erforderlicher Nachtest                                                         |
|------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Zahlung ohne Freigabe  | Freigabe muss vor Zahllauf liegen; definierte Wertgrenzen und Rollenfolge einhalten | Berechtigung, Freigabebeleg und Systemkonfiguration prüfen                      |
| Umgehung Wareneingang  | Rechnung/Zahlung ohne protokollierten Wareneingang oder zulässigen Ausnahmegrund    | klären, ob Dienstleistung, Teilrechnung oder fehlende Protokollierung vorliegt  |
| Selbstfreigabe/SoD     | gleiche Person oder unvereinbare Rolle führt kritische Aktivitäten aus              | Rollenmodell, Vertretung, Notfallrechte und tatsächliche Nutzerzuordnung prüfen |
| Nachträgliche Änderung | Stammdaten- oder IBAN-Änderung kurz vor Rechnung/Freigabe/Zahlung                   | Änderungslog, Rückrufnachweis, Genehmigung und Zahlungsempfänger abgleichen     |
| Frist-/Leistungsrisiko | ungewöhnliche Liegezeiten, Schleifen oder wiederholte Rückgaben                     | Ursache, Fallkomplexität, Organisationsengpass und Folgen bewerten              |
| Kontrollumgehung       | seltene Variante überspringt Schlüsselkontrolle oder kehrt Reihenfolge um           | Zulässigkeit der Variante und kompensierende Kontrolle anhand Einzelfall prüfen |

Übersicht 16: Verbindung von Risiko-Kontrollmatrix und Process Mining

Wesentlich: Eine fehlende Aktivität im Eventlog beweist nicht automatisch, dass die fachliche Handlung unterblieben ist. Sie kann außerhalb des Systems, in einem anderen Fachverfahren, als Sammelbuchung oder ohne geeignete Protokollierung erfolgt sein. Umgekehrt beweist ein technisches Ereignis nicht ohne Weiteres die sachliche Qualität der Kontrolle.

## 5.6.5 Kommunale Praxisevidenz

Beispiel Wien – Purchase-to-Pay (Beschaffungsprozess): Der Stadtrechnungshof Wien integrierte Process Mining in einen risikoorientierten Prüfungsablauf. Aus SAP- und ergänzenden Systemdaten wurden Prozess- und Datenmodell, Eventlog und Ist-Prozess aufgebaut. Analysiert wurden unter anderem Vollständigkeit, Kontrollschritte, Varianten, Wertgrenzen, Durchlaufzeiten und Engpässe. Die Studie zeigt zugleich, dass Datenbeschaffung, Mapping und Validierung einen erheblichen Anteil der Prüfung ausmachen.<sup>8</sup>

Kommunales Pilotprojekt Hundesteuer (ifV/CHE): Im ifV-Pilotprojekt wurden Ereignisdaten aus dem kommunalen Steuerverfahren und SAP-FI zusammengeführt. Als wesentliche Lernpunkte ergaben sich die frühe Festlegung geeigneter Case-IDs, die eindeutige Benennung von Aktivitäten, belastbare Zeitstempel, die Abstimmung zwischen Rechnungsprüfung, Fachbereich und Rechenzentrum sowie die Grenzen verdichteter Hauptbuchdaten. Geschäftspartnernummern waren nur ersatzweise nutzbar; Kassenzahlen wurden als prozessnähere Fall-ID identifiziert.<sup>9</sup>

<sup>8</sup> Stadtrechnungshof Wien: Prüfungen mit Process Mining; ausgewertete deutschsprachige Projektstudie zum Purchase-to-Pay-Prozess der Wiener Stadtwerke.

<sup>9</sup> CHE-Kommunalberatung/ifV (2025): Pilotprojekt Journal Entry Testing und Process Mining in der kommunalen Praxis, kommunaler Anwendungsfall Hundesteuer.

Beschaffungsbeispiel aus den Anlagen: Bei 29.680 Fällen entsprach nur ein Teil dem erwarteten Hauptpfad; weitere Varianten enthielten fehlende oder anders gereichte Aktivitäten sowie Ausreißer bei Durchlaufzeiten. Die fachliche Würdigung zeigte, dass Abweichungen nicht automatisch Mängel sind. Gerade seltene, risikoreiche Varianten können jedoch in klassischen Stichproben unentdeckt bleiben und sollten gezielt nachgeprüft werden.

### 5.6.6 Grenzen, Datenschutz und Beweiswert

Aus den dargestellten Praxisbeispielen lassen sich unter Beachtung ihrer begrenzten Übertragbarkeit folgende Schlussfolgerungen ableiten:

- Process Mining sieht nur digital protokollierte Ereignisse. Medienbrüche, Telefonate, Papierbelege und nicht integrierte Fachverfahren erzeugen kritische Blindstellen.
- Die Wahl der Case-ID bestimmt die Prozesssicht. Ungeeignete Schlüssel können Fälle unzulässig zusammenfassen oder künstlich aufspalten.
- Filter, Aktivitätsmapping und Meilensteinbildung sind prüferische Modellentscheidungen und müssen versioniert, begründet und reproduzierbar sein.
- Kennzahlen zu Varianten und Durchlaufzeiten sind deskriptiv. Wesentlichkeit, Ursache und Kontrollmangel erfordern fachliche Würdigung und Nachweise.
- Personen- und Leistungsdaten sind auf Rechtsgrundlage, Zweckbindung, Datenminimierung, Rollen-/Berechtigungskonzept, Aufbewahrung und möglichst Pseudonymisierung zu prüfen. Datenschutz und Personalvertretung sind frühzeitig einzubeziehen.<sup>10</sup>
- Process Mining ersetzt weder Walkthrough, Systemprüfung, Belegprüfung noch prüferisches Ermessen. Es erweitert die Reichweite der Risikoanalyse und verbessert die Auswahl risikobehafteter Fälle.

### 5.6.7 Mindest-Arbeitspapier für eine digitale Prozessprüfung

Wegen der erheblichen Komplexität örtlicher Prozess- und Systemlandschaften sollten Arbeitspapiere für digitale Prozessprüfungen mindestens folgende Inhalte aufweisen:

- Prüfungsziel, Prozessgrenze, Zeitraum, Sollmodell und relevante Kontrollregeln
- System- und Datenquellenkarte einschließlich Schnittstellen und Datenverantwortlichen
- Eventlog-Datenvertrag mit Feldkatalog, Mapping, Extraktions- und Transformationsschritten
- Abstimmung der Population sowie dokumentierte Datenqualitäts- und Integritätstests
- Version der Software, Parameter, Filter, Modellierungs- und Vereinfachungsentscheidungen
- Varianten-, Conformance-, Zeit- und Ressourcenanalysen mit reproduzierbaren Ergebnissen
- Trefferliste, Auswahlbegründung, Einzelfallnachweise, Gegenbelege und Fehlerklassifikation
- Beurteilung von Ursache, Reichweite, Kontrollwirkung, Restrisiko und erforderlichem Follow-up

## 6. IKS-Risikoprüffelder (Auswahl)

Eine besondere Herausforderung liegt in der Definition und Auswahl der IKS-Prüffelder. Prozesse, Organisationseinheiten, Querschnittsaufgaben, thematische Schwerpunkte oder Einzelthemen (z. B. Fraud-Risiken) können Ansatzpunkte des konkreten Prüfauftrags sein.

Die nachstehende Übersicht liefert einen ersten, notwendigerweise unvollständigen Themenkatalog.

---

<sup>10</sup> Vgl. Verordnung (EU) 2016/679 (DSGVO), insbesondere Grundsätze der Zweckbindung, Datenminimierung, Speicherbegrenzung und Integrität/Vertraulichkeit.

| Risikofeld       | Beispielrisiko                                | Typische Kontrolle                                                           |
|------------------|-----------------------------------------------|------------------------------------------------------------------------------|
| Zahlungsverkehr  | Unberechtigte/manipulierte Auszahlung         | Funktionstrennung; Vier-Augen-Bankfreigabe; Limits; Analysen                 |
| Forderungen      | Nicht- oder verspätete Erhebung               | Soll-Ist-Abgleich; Fälligkeitslisten; Überwachung von Erlass/Niederschlagung |
| Kreditoren       | Doppelzahlung; falsche Bankverbindung         | Dublettencheck; IBAN-Verifikation; Stammdatenprotokoll                       |
| Buchführung      | Unzulässige oder ungewöhnliche Buchung        | Kontierungsregeln; Gegenkontenanalyse; Journal Entry Testing                 |
| Jahresabschluss  | Unvollständige Rückstellungen/Abgrenzungen    | Abschlusskalender; Meldeverfahren; Salden- und Plausibilitätskontrollen      |
| Haushalt         | Budgetüberschreitung; strukturelles Defizit   | Plan-Ist; Forecast; Sperren; Ampelbericht; Gegensteuerung                    |
| Liquidität       | Zahlungsengpass; hohe Liquiditätskredite      | Rollierende Planung; Limits; Stressszenarien; Tagesfinanzstatus              |
| Vergabe          | Manipulation; Aufteilung; Interessenkonflikt  | Zentrale Vergabe; Wertgrenzenkontrolle; Erklärung; Vier-Augen-Prinzip        |
| Zuwendungen      | Doppelförderung; Fehlverwendung               | Verwendungsnachweis; Meilensteinzahlung; Vor-Ort-/Stichprobenkontrolle       |
| Sozialleistungen | Mehrfach- oder Fehlzahlung                    | Identitäts-/Haushaltsabgleich; Plausibilitätsregeln; Risikostichproben       |
| Gebühren         | Unvollständige oder falsche Festsetzung       | Leistungs-/Bescheidabgleich; Gebührenkalkulation; Kontrollsummen             |
| Personal         | Unberechtigte Zahlungen; Rechte nach Austritt | Stellenplanabgleich; Stammsfreigabe; Austrittskontrolle                      |
| Korruption       | Bevorzugung; Vorteilsannahme                  | Gefährdungsatlas; Rotation; Funktionstrennung; Hinweisgebersystem            |
| IT/Cyber         | Ransomware; Datenverlust; Ausfall             | MFA; Rollen; Offline-Backup; Rücksicherungstest; Notfallübung                |
| Bau/Investition  | Kosten-, Termin- und Nachtragsrisiko          | Projekt-Risikoregister; Kostenreserve; Meilenstein-/Nachtragsprüfung         |
| Beteiligungen    | Verluste; Haftung; Zielverfehlung             | Quartalsbericht; Kennzahlen; Risikobericht; Zustimmungsvorbehalt             |

Übersicht 17: Themenkatalog für IKS-Prüffelder (Auswahl)

## 7. Aufbau einer prüffähigen Risiko-Kontrollmatrix je Prüffeld

Für jedes ausgewählte Prüffeld sollte eine Risiko-Kontrollmatrix aufgestellt werden. Ihre Ausgestaltung richtet sich nach Prüfungsziel, Prozesskomplexität und örtlichen Gegebenheiten; sie sollte mindestens die nachfolgend dargestellten Elemente enthalten:

| Pflichtfeld          | Inhalt                                                                |
|----------------------|-----------------------------------------------------------------------|
| Prozess/Teilprozess  | Eindeutige Zuordnung zum Verwaltungsablauf.                           |
| Prozessziel          | Erwartetes rechtmäßiges, wirtschaftliches und verlässliches Ergebnis. |
| Risikoereignis       | Konkrete Zielabweichung; nicht nur ein abstraktes Themenwort.         |
| Ursache/Folge        | Warum kann das Ereignis eintreten und welche Wirkung entsteht?        |
| Bruttoisiko          | Bewertung vor Berücksichtigung vorhandener Kontrollen.                |
| Kontrollziel         | Was muss verhindert oder rechtzeitig erkannt werden?                  |
| Kontrollbeschreibung | Wer prüft was, womit, wann und wie?                                   |
| Kontrollart          | Präventiv/detektiv; manuell/automatisch; Schlüsselkontrolle.          |
| Frequenz/Auslöser    | Je Vorgang, täglich, monatlich oder ereignisbezogen.                  |
| Verantwortung        | Ausführende und überwachende Rolle; Vertretung.                       |
| Nachweis             | Systemlog, Checkliste, Freigabe, Bericht oder dokumentierte Ausnahme. |
| Restrisiko           | Bewertung nach wirksamer Kontrolle.                                   |
| Wirksamkeitstest     | Prüfhandlung, Population, Stichprobe, Toleranz und Ergebnis.          |

| Pflichtfeld | Inhalt                                            |
|-------------|---------------------------------------------------|
| Maßnahme    | Lücke, Verantwortlichkeit, Frist und Nachprüfung. |

Übersicht 18: Aufbau einer prüffähigen Risiko-Kontrollmatrix

**Qualitätskriterium** „Vier-Augen-Prinzip vorhanden“ ist keine ausreichende Kontrollbeschreibung. Benötigt werden Gegenstand, Rollen, Zeitpunkt, Entscheidungskriterium, Ausnahmebehandlung und Kontrollnachweis.

## 8. Praxisfall: Kreditorenrechnung bis Auszahlung

Die nachfolgende Matrix ist ein realitätsnahes kommunales Muster. Sie ist nicht als unveränderte interne Matrix einer bestimmten Stadt zu verstehen. Örtliche Dienstanweisungen, Fachverfahren, Wertgrenzen und Organisationsstrukturen müssen ergänzt werden.

## 8.1 Risiko-Kontrollmatrix

| ID  | Teilprozess      | Risikoeignis                             | Brutto | Schlüsselkontrolle                                         | Art               | Frequenz      | Verantwortlich        | Nachweis                   | Rest |
|-----|------------------|------------------------------------------|--------|------------------------------------------------------------|-------------------|---------------|-----------------------|----------------------------|------|
| R01 | Rechnungseingang | Nicht-/Mehrfacherfassung                 | 3×3=9  | Zentrale elektronische Erfassung mit Beleg-ID              | autom.; präventiv | je Rechnung   | Rechnungseingang      | Zeitstempel/Beleg-ID       | 3    |
| R02 | Rechnungsprüfung | Zahlung ohne Leistung                    | 3×5=15 | Sachliche und rechnerische Feststellung durch Berechtigte  | man.; präventiv   | je Rechnung   | Fachamt               | elektronische Feststellung | 5    |
| R03 | Rechnungsprüfung | Kontrolle eigener Bestellung/Leistung    | 3×4=12 | Trennung Bestellung, Leistungsbestätigung und Freigabe     | organisatorisch   | ständig       | Fachbereichsleitung   | Rollenmatrix               | 4    |
| R04 | Kontierung       | Falsches Konto/Produkt                   | 4×3=12 | Plausibilitätsprüfung gegen Produkt- und Kontenplan        | autom./man.       | je Buchung    | Geschäftsbuchhaltung  | Prüfprotokoll              | 6    |
| R05 | Umsatzsteuer     | Falscher Steuerschlüssel/Vorsteuerabzug  | 3×4=12 | Steuerregeln; neue Sachverhalte durch Steuerstelle         | präventiv         | je neuer Fall | Steuerstelle          | Steuerprüfbogen            | 4    |
| R06 | Budget           | Keine Haushaltsmittel                    | 2×4=8  | Automatische Mittelprüfung; Freigabe üpl./apl. Ausgabe     | automatisch       | je Buchung    | Budgetverantwortung   | Systemlog/Beschluss        | 2    |
| R07 | Vergabe          | Aufteilung zur Wertgrenzenumgehung       | 3×5=15 | Kumulierung nach Lieferant, Warengruppe, Einheit, Zeitraum | datenanalytisch   | monatlich     | Vergabestelle         | Analysebericht             | 8    |
| R08 | Kreditorenstamm  | Fiktiver/doppelter Kredit                | 2×5=10 | Zentrale Stammdatenanlage mit Dublettenprüfung             | präventiv         | je Anlage     | Stammdatenstelle      | Freigabeprotokoll          | 3    |
| R09 | Bankverbindung   | Manipulierte IBAN                        | 3×5=15 | Unabhängiger Rückruf; Vier-Augen-Freigabe                  | präventiv         | je Änderung   | Stammdatenstelle      | Rückrufprotokoll           | 5    |
| R10 | Bankverbindung   | IBAN bei mehreren Partnern/Beschäftigten | 3×5=15 | IBAN-Abgleich über Kreditoren, Debitoren, Personal         | detektiv          | wöchentlich   | Compliance/Kasse      | Treffer-/Fallliste         | 6    |
| R11 | Anordnung        | Unberechtigte Freigabe                   | 2×5=10 | Rollenmodell und periodische Rezertifizierung              | präventiv/det.    | quartalsweise | Fachadministration    | Rollenreview               | 4    |
| R12 | Zahlungslauf     | Alleinige End-to-End-Ausführung          | 3×5=15 | Technische Funktionstrennung und zweite Bankfreigabe       | präventiv         | je Lauf       | Kassenleitung         | Bank-Freigabelog           | 3    |
| R13 | Zahlungslauf     | Doppelzahlung                            | 3×4=12 | Dublettenprüfung über Kredit, Nr., Betrag, Datum, IBAN     | automatisch       | je Lauf       | Kreditorenbuchhaltung | Ausnahmeliste              | 3    |
| R14 | Zahlungslauf     | Hohe/Eilzahlung ungeprüft                | 2×5=10 | Zusätzliche Freigabe ab Schwellenwert; Begründung          | präventiv         | je Fall       | Kassenleitung         | Freigabe/Begründung        | 4    |
| R15 | Empfänger        | Zahlung an gesperrten Empfänger          | 2×5=10 | Kreditorensperre und Ausschlussprüfung                     | autom./man.       | je Zahlung    | Kasse/Vergabe         | Systemlog                  | 3    |
| R16 | Nachkontrolle    | Fehler trotz formaler Freigabe           | 3×5=15 | Vollständige Zahlungsanalyse mit Risikoscoring             | detektiv          | monatlich     | RPA/Revision          | Analyse-/Fallprotokoll     | 6    |
| R17 | Berechtigung     | Rechte nach Beschäftigungsende           | 3×5=15 | Austrittsworkflow; Abgleich Personal-/Benutzerstamm        | präventiv/det.    | monatlich     | Personal/IT           | Abgleichprotokoll          | 4    |
| R18 | Protokollierung  | Änderung nicht nachvollziehbar           | 2×4=8  | Unveränderbare Audit-Logs kritischer Daten                 | automatisch       | ständig       | IT                    | Audit-Log                  | 2    |

Übersicht 19: Beispiel einer RKM

## 8.2 Vertiefung der Schlüsselkontrolle: Änderung der Bankverbindung

| Merkmal               | Festlegung                                                                                                      |
|-----------------------|-----------------------------------------------------------------------------------------------------------------|
| Kontrollziel          | Zahlungen erfolgen nur auf eine vom tatsächlichen Kreditor bestätigte Bankverbindung.                           |
| Risiko                | Gefälschte E-Mail, kompromittiertes Lieferantenkonto oder interne Manipulation.                                 |
| Kontrollhandlung      | Zweite Person verifiziert die IBAN durch Rückruf über bereits bekannte oder unabhängig ermittelte Kontaktdaten. |
| Auslöser              | Neuanlage oder Änderung von IBAN, Kontoinhaber oder Zahlungsweg.                                                |
| Unvereinbare Funktion | Prüfende Person darf die Änderung nicht selbst erfasst haben.                                                   |
| Nachweis              | Datum, Prüfer, Gesprächspartner, verwendete Telefonnummer und Ergebnis.                                         |
| Ausnahme              | Keine Freigabe ohne Verifikation; Eskalation an Kassenleitung.                                                  |
| IT-Unterstützung      | Workflow, Historie alter/neuer IBAN und Auszahlungssperre bis Freigabe.                                         |
| Wirksamkeitstest      | Stichprobe aller Änderungen; Abgleich mit Rückrufnachweis und Folgezahlungen.                                   |

Übersicht 20: Vertiefung der KM einer Schlüsselkontrolle

## 9. Datenanalytische Kontrollen und NKF-Kontierung

Organisatorische Kontrollen sollten bei großen Buchungsvolumina durch vollständige oder risikoorientierte Datenanalysen ergänzt werden. Treffer sind zunächst Auffälligkeiten und keine Feststellung eines Fehlers oder einer Manipulation. Die Bearbeitung folgt dem Prinzip „Comply or explain“.

| Regel | Prüfung                                               | Reaktion                                 |
|-------|-------------------------------------------------------|------------------------------------------|
| DA01  | Gleiche Rechnungsnummer und gleicher Kreditor         | Zahlungssperre bzw. Dublettenklärung     |
| DA02  | Gleicher Betrag, Kreditor und Rechnungsdatum          | Warnung und Belegvergleich               |
| DA03  | Zahlung kurz nach Änderung der IBAN                   | Zusätzliche Freigabe                     |
| DA04  | Gleiche IBAN bei mehreren Kreditoren                  | Fallprüfung                              |
| DA05  | Kreditoren-IBAN entspricht Beschäftigten-IBAN         | Sofortige Eskalation                     |
| DA06  | Buchende Person änderte zuvor den Kreditorenstamm     | SoD-Prüfung                              |
| DA07  | Rechnungen knapp unter Vergabeschwellenwert           | Kumulierung mit verwandten Beschaffungen |
| DA08  | Buchung/Zahlung am Wochenende oder nach Dienstschluss | Plausibilisierung                        |
| DA09  | Manuelle Zahlung ohne Rechnungs-/Bestellbezug         | Begründungs- und Belegprüfung            |
| DA10  | Storno und Neuzahlung an abweichende IBAN             | Sofortige Eskalation                     |

Übersicht 21: Datenanalytische RKM

### 9.1 NKF-Kontenrahmen als digitales Prüfungsuniversum

Die Anlagen 19 und 20 zum kommunalen Haushaltsrecht enthalten den haushaltsrechtlichen NKF-Kontenrahmen und die Zuordnungsvorschriften des kommunalen Kontierungsplans. Sie sind keine IKS-Prüfleitlinien. Für die digitale IKS-Prüfung bilden sie jedoch einen normativen Ordnungsrahmen, gegen den örtliche Kontenpläne, Buchungsregeln und Datenbestände gespiegelt werden können.

| Kontenklasse | Prüfungsrelevanter Schwerpunkt                   | Beispiel digitaler Kontrolle                                                                                    |
|--------------|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| 0/1          | Anlagevermögen, Forderungen, liquide Mittel, RAP | Anlagenzugänge, Forderungsarten und Bank-/Kassenbestände auf zulässige Kontierung und Vollständigkeit prüfen.   |
| 2            | Eigenkapital, Sonderposten und Rückstellungen    | Unbelegte Gruppen 22/24/29; Wertberichtigungen ohne Bilanzausweis; Rückstellungsbewegungen plausibilisieren.    |
| 3            | Verbindlichkeiten und passive RAP                | Kreditarten, Liefer-/Transferverbindlichkeiten und wirtschaftlich gleichkommende Vorgänge trennen.              |
| 4/5          | Erträge und Aufwendungen                         | Ungewöhnliche Gegenkonten, periodenfremde Buchungen, Kontenwechsel und manuelle Abschlussbuchungen analysieren. |
| 6/7          | Ein- und Auszahlungen                            | Ergebnis-/Finanzrechnung abstimmen; zahlungswirksame und nicht zahlungswirksame Vorgänge unterscheiden.         |
| 8            | Eröffnungs-, Abschluss- und Korrekturkonten      | Buchungen auf Abschluss- und Korrekturkonten vollständig und berechtigungsbezogen prüfen.                       |
| 9            | Kosten- und Leistungsrechnung                    | Örtliche Ausgestaltung, Überleitungen und interne Leistungsbeziehungen nachvollziehen.                          |

Übersicht 22: Datenanalytische Auswertung von Kontenklassen

## 9.2 Digitale Kontierungsprüfungen

Typische datenanalytische Prüfungshandlungen im Zusammenhang mit Kontierungen sind folgende.

- Örtlichen Kontenplan maschinell gegen NKF-Kontenrahmen und Zuordnungsvorschriften mappen.
- Buchungen auf nicht belegten Kontengruppen sowie technisch neu angelegten Konten aussteuern.
- Ungewöhnliche oder unzulässige Soll-/Haben- und Gegenkontenkombinationen identifizieren.
- Ergebnis- und Finanzrechnung auf sachgerechte Zuordnung zahlungswirksamer Vorgänge abstimmen.
- Manuelle Buchungen auf Abschluss-, Korrektur-, Rückstellungs- und Rechnungsabgrenzungskonten risikoorientiert prüfen.
- Kontenstammänderungen, Kontierungsfreigaben und Buchungsberechtigungen miteinander verknüpfen.
- Treffer als Auffälligkeiten behandeln und nach dem Prinzip „Comply or explain“ fallbezogen aufklären.

**Prüferische Folgerung** Der Kontenrahmen liefert den normativen Erwartungsraum. Erst die Verbindung mit Buchungsjournal, Stammdaten, Benutzer-/Rolleninformationen, Änderungslogs und Belegen ermöglicht eine digitale Prüfung der Kontrollwirksamkeit.

## 10. Prüfung der Kontrollen

### 10.1 Vier Prüfungsstufen

Da der Kernauftrag von IKS-Prüfungen die Erzeugung von Nachweisen zur Wirksamkeit von Kontrollen (=Wirksamkeitstest) ist, wird die Aufgabe des Wirksamkeitstests in vier Stufen erledigt:

| Stufen | Prüfungsfrage                                                             | Beispiel                                                                                                                      |
|--------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Design | Kann die Kontrolle das Risiko grundsätzlich reduzieren? Ist sie geeignet? | Eine computergestützte Fristenkontrolle zum Schutz vor Verjährungen ist grundsätzlich geeignet Vermögensschäden zu verhindern |

| Stufen          | Prüfungsfrage                                                 | Beispiel                                                                                                         |
|-----------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Implementierung | Ist die Kontrolle organisatorisch und technisch eingerichtet? | Workflow, Zuständigkeit und Zugriff (Sperrung) sind nachweislich vorhanden.                                      |
| Durchführung    | Wurde sie im Prüfungszeitraum tatsächlich ausgeführt?         | Prüfprotokoll der Fristenkontrolle liegt für jede Forderung vor.                                                 |
| Wirksamkeit     | Hat sie konsistent funktioniert und Ausnahmen behandelt?      | Stichprobe ist ohne unaufgeklärte Abweichung; Treffer (=Fristenkontrolle hat trotzdem versagt) wurden eskaliert. |

Übersicht 23: Prüfungsstufen des Kontrolltests

## 10.2 Muster eines Kontrolltests

Zur Feststellung der operativen Wirksamkeit sind Kontrolltests durchzuführen. Bei standardisierten, wiederkehrenden Kontrollen kann hierzu eine Attribut- beziehungsweise Merkmalsstichprobe (Attribute Sampling) eingesetzt werden. Das nachfolgende Muster beschreibt die wesentlichen Schritte eines solchen Kontrolltests:

| Prüffeld                             | Festlegung                                                                                                     |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Population definieren                | Sämtliche Änderungen von Kreditorenbankverbindungen im Prüfungsjahr.                                           |
| Stichprobe erstellen                 | Risikoorientiert: alle Hochbetragsfälle plus Zufallsstichprobe der übrigen Änderungen. Nach Paretoprinzip      |
| Prüfnachweise erzeugen               | Änderungslog, Freigabe, Rückrufdokumentation und erste Folgezahlung.                                           |
| Abweichungen feststellen (=Findings) | Fehlender Nachweis, identische Erfasser/Freigeber, Nutzung einer nicht erlaubten Berechtigung                  |
| Toleranzgrenzen beachten             | Bei Schlüsselkontrollen gegen Zahlungsmanipulation regelmäßig sehr geringe oder keine tolerierbare Abweichung. |
| Ergebnis beurteilen                  | Wirksam, teilweise wirksam oder unwirksam; Ursache und Reichweite dokumentieren.                               |
| Follow-up entscheiden                | Maßnahme, Verantwortlicher, Frist und Nachprüfung festlegen.                                                   |

Übersicht 24: Muster eines Kontrolltests

## 10.3 Feststellungen und Gesamturteil

Kontrollabweichungen werden nicht allein gezählt. Zu beurteilen sind Ursache, Häufigkeit, mögliche Auswirkung, systematische Reichweite, kompensierende Kontrollen und das Risiko einer Außerkraftsetzung durch Führungskräfte (Management Override). Eine klare Feststellung trennt Prüfungsmaßstab, Sachverhalt, Ursache, Risiko beziehungsweise Folge und Empfehlung.

| Bewertung                   | Orientierung                                                                                                                  |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Geringfügiger Mangel        | Einzelfall ohne wesentliche Auswirkung; Kontrolle insgesamt weiterhin wirksam.                                                |
| Kontrollmangel              | Design, Implementierung oder Durchführung ist beeinträchtigt; Risiko wird nicht verlässlich reduziert.                        |
| Wesentlicher Kontrollmangel | Es besteht eine begründete Möglichkeit, dass ein wesentliches Risiko nicht rechtzeitig verhindert oder aufgedeckt wird.       |
| Systemischer Mangel         | Mehrere Kontrollen oder Prozesse sind aufgrund gemeinsamer Ursachen betroffen; übergreifende Steuerungsmaßnahme erforderlich. |

Übersicht 25: Feststellungen und Gesamturteil

## 11. Umsetzungsempfehlung für Rechnungsprüfungen

Aus den oben dargestellten Gründen ergibt sich schlüssig folgende Umsetzungsempfehlung für örtliche Rechnungsprüfungen:

1. Ein kommunales Prüfungsuniversum und eine mehrjährige risikoorientierte IKS-Prüfungsplanung aufbauen.
2. Mit drei bis fünf kritischen Prozessen pilotieren, statt sofort eine flächendeckende Vollerhebung anzustreben.
  1. Prüfungsziel und Aussageform vor Beginn eindeutig festlegen.
  2. Prozessverantwortliche für Walkthrough und Evidenzgewinnung einbinden, ohne die Unabhängigkeit der Prüfung aufzugeben.
3. Nur risikorelevante Schlüsselkontrollen intensiv testen; Routinekontrollen angemessen bündeln.
4. Kontrollpopulationen möglichst aus Systemdaten bestimmen und deren Vollständigkeit nachweisen.
5. Automatisierte Datenkontrollen und wiederholbare Analysen für laufende Prüfung und Follow-up nutzen.
6. Mängelursachen und systemische Wirkungen stärker gewichten als reine Abweichungszahlen.
7. Maßnahmen, Verantwortliche, Fristen und Nachprüfungen in einem verbindlichen Workflow führen.
8. Methoden, Arbeitspapiere und Erfahrungswerte aus abgeschlossenen Prüfungen in einer kommunalen IKS-Prüfbibliothek sichern.

**Zielbild** Ein integriertes kommunales System verbindet Zielregister, Risikoinventar, Risiko-Kontrollmatrizen, Maßnahmenverfolgung, Datenanalysen und risikoorientierte Prüfung. Ein isoliertes Risikohandbuch genügt nicht.

## 12. Dokumentierte kommunale Praxisbeispiele

### 12.1 KGSt, Kiel und Dortmund

Die KGSt weist kommunale Arbeitshilfen aus, darunter eine Anleitung zur IKS-Risikokontrollmatrix, Risiko-Kontrollmatrizen für Teilprozesse des Jahresabschlusses und der Aufnahme von Liquiditätskrediten sowie eine Musterdokumentation der Stadt Dortmund. Die Matrizen zu Jahresabschluss und Liquiditätskrediten wurden nach KGSt-Angaben gemeinsam mit einer Arbeitsgruppe und der Stadt Kiel entwickelt. Vollzugriff kann eine KGSt-Mitgliedschaft erfordern.

Quelle: <https://www.kgst.de/risikomanagement>

### 12.2 Stadt München – steuerliches IKS

Die Stadt München plante für ihr steuerliches IKS ausdrücklich Prozessbeschreibungen und Risiko-Kontrollmatrizen für Umsatz- und Ertragsteuer. Das Beispiel zeigt die typische Verbindung von Prozessaufnahme, Risikoanalyse, Kontrollgestaltung und Dokumentation.

Quellen: <https://risi.muenchen.de/risi/dokument/v/4734181> und <https://risi.muenchen.de/risi/dokument/v/4734183>

### 12.3 Weitere kommunale Beispiele

- Gemeindeverwaltungsverband Hardheim-Walldürn: TCMS mit Risiko-Kontrollmatrix zur Bewertung steuerlicher Risiken.

- Landkreis Lüneburg: Erstellung und laufende Fortführung der steuerlichen Risiko-Kontrollmatrix als Verwaltungsaufgabe.
- Einwohnergemeinde Recherswil (Schweiz): öffentliches IKS-Konzepthandbuch mit Prozess-, Risiko- und Kontrollsystematik.
- Stadtwerke München: halbjährliche Risikoinventuren, Risikoberichterstattung und COSO-orientiertes IKS mit präventiven und detektiven Kontrollen.

Fundstellen siehe Quellenverzeichnis. Operative, vollständig ausgefüllte kommunale Matrizen werden aus Sicherheits- und Vertraulichkeitsgründen nur selten vollständig veröffentlicht.

## 13. Limitationen, Entwicklungsbedarf und Fazit

Das Konzept besitzt vier wesentliche Grenzen. Erstens unterscheiden sich Rechtsgrundlagen und Organisationsmodelle zwischen Ländern und Kommunen. Zweitens hängt die digitale Prüfbarkeit von Protokollierung, Datenzugang, semantischer Qualität und Schnittstellen ab. Drittens können automatisierte Analysen komplexe rechtliche und fachliche Bewertungen nicht ersetzen. Viertens ist die veröffentlichte empirische Basis vollständiger kommunaler IKS- und Process-Mining-Prüfungen bislang begrenzt.

Die kommunale IKS-Prüfung entwickelt sich von einer regelungs- und aktenorientierten Prüfung zu einer integrierten System-, Prozess- und Datenprüfung. Risiko-Kontrollmatrizen bilden das fachliche Bindeglied; digitale Analysen und Process Mining erweitern Reichweite und Präzision. Ihre Aussagekraft bleibt jedoch an Datenvollständigkeit, Modellentscheidungen und fachliche Validierung gebunden. Ein belastbares Prüfungsmodell verbindet deshalb kommunalrechtliche Maßstäbe, Prozessverständnis, IT- und Datenkompetenz sowie unabhängiges prüferisches Ermessen.

## 14. Literatur- und Quellenverzeichnis

### 14.1 Rechtsgrundlagen und kommunale Ausgangsmaterialien

Gemeindeordnung für das Land Nordrhein-Westfalen (GO NRW), insbesondere §§ 102 und 104, aktuelle Fassung. Rechtliche Grundlage für Jahresabschlussprüfung und örtliche Rechnungsprüfung; die Pflicht zur Prüfung der Wirksamkeit interner Kontrollen nach § 104 Abs. 1 Nr. 6 ist landesspezifisch einzuordnen. <https://recht.nrw.de/>

Zweites NKF-Weiterentwicklungsgesetz Nordrhein-Westfalen, GV. NRW. 2018 S. 759. Gesetzgebungsgeschichtlicher Bezug zur Aufwertung der IKS-Prüfung. <https://recht.nrw.de/gvnw/2018-s759-0>

IDR: Prüfungsleitlinie IDR-L 113-1 – Informationssicherheit, Stand 09/2023, sowie IDR-L 113-2 – Notfallmanagement, Stand 09/2023. Ausgewertete Prüfungshilfen für die digitale IKS-Prüfung; keine Rechtsnormen.

VV Muster zur GO NRW, Anlagen 19 und 20: haushaltsrechtlicher NKF-Kontenrahmen und Zuordnungsvorschriften. Hochgeladene Materialien als Grundlage für kontierungsbezogene Datenanalysen.

KGSt: Risikomanagement – kommunale Arbeitshilfen und Praxisbeispiele. Besonders geeignet für kommunale Einführung, Risikoinventur und organisatorische Verankerung. <https://www.kgst.de/risikomanagement>

## 14.2 Rahmenwerke und Prüfungsstandards

COSO (2013): Internal Control – Integrated Framework. International verbreitetes Referenzmodell mit fünf Komponenten; als Strukturierungsrahmen nutzbar, aber an kommunales Recht und örtliche Organisation anzupassen. <https://www.coso.org/guidance-on-ic11>

COSO (2017): Enterprise Risk Management – Integrating with Strategy and Performance. Referenz für die Verbindung von Zielen, Strategie, Leistung und Risiken. <https://www.coso.org/enterprise-risk-management>

ISO 31000:2018: Risk management – Guidelines. Grundsätze, Rahmen und Prozess des Risikomanagements; Leitlinie, keine Zertifizierungsnorm. <https://www.iso.org/standard/65694.html12>

INTOSAI GOV 9100 und 9130: Guidelines for Internal Control Standards for the Public Sector sowie ergänzende Hinweise zum Enterprise Risk Management. Öffentlicher-Sektor-Perspektive auf IKS und Risikomanagement. <https://www.issai.org/themes/internal-control/13>

The Institute of Internal Auditors (IIA): The Three Lines Model, 2020, aktualisierte Fassung/Terminologie beachten. Orientierung für Verantwortung, Überwachung sowie unabhängige Prüfungs- und Beratungsleistungen. <https://www.theiia.org/en/resources/statements-of-position/>

IDW PS 981 (Stand 03.03.2017): Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen; IDW PS 982 (Stand 03.03.2017): Prüfung des IKS des internen und externen Berichtswesens. Methodische Referenzen, deren Anwendungsbereich und Aussageform nicht ungeprüft auf kommunale Prüfungen übertragen werden dürfen. <https://www.idw.de/idw/idw-verlautbarungen/14>

DIIR-Revisionsstandard Nr. 2: Prüfung des Risikomanagementsystems durch die Interne Revision, Version 2.2 (08/2026), einschließlich Prüfungsleitfaden. Praxisnaher Referenzrahmen; kommunaler Prüfungsauftrag und örtliche Satzung bleiben vorrangig. <https://www.diir.de/arbeitskreise/interne-revision-und-risikomanagement/veroeffentlichungen/>

## 14.3 Informationssicherheit und Business Continuity

BSI-Standards 200-1 (ISMS), 200-2 (IT-Grundschutz-Methodik), 200-3 (Risikoanalyse) und 200-4 (Business Continuity Management, 2023). Systematische Referenzen für digitale Kontrollziele und Prüfungsnachweise. <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/>

BSI: IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung sowie BSI/BBK: Kommunale IT-Krisen – Handlungsfähigkeit sichern. Kommunalspezifische Hilfen für Mindestabsicherung, Krisenorganisation und Wiederanlauf.

ISO/IEC 27001:2022: Information security management systems – Requirements, und ISO/IEC 27002:2022: Information security controls. Internationale Referenzen für ISMS und Kontrollgestaltung; Lizenz- und Urheberrechtsbedingungen beachten. <https://www.iso.org/isoiec-27001-information-security.html>

---

11 Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013): Internal Control – Integrated Framework.

12 International Organization for Standardization (ISO) (2018): ISO 31000 – Risk management – Guidelines.

13 INTOSAI GOV 9100: Guidelines for Internal Control Standards for the Public Sector; INTOSAI GOV 9130: Further Information on Entity Risk Management.

14 Institut der Wirtschaftsprüfer (IDW), IDW PS 981 und IDW PS 982, jeweils Stand 03.03.2017.

## 14.4 Lehrbücher und Handbücher zur Vertiefung

Bungartz, Oliver (2026): Handbuch Interne Kontrollsysteme (IKS) – Steuerung und Überwachung von Unternehmen, 7., völlig neu bearbeitete und erweiterte Auflage, Erich Schmidt Verlag, Berlin, ISBN 978-3-503-24078-4. Umfassendes Praxis- und Nachschlagewerk zu Aufbau, Dokumentation und Überwachung von IKS.

Diederichs, Marc (2023): Risikomanagement und Risikocontrolling, 5., vollständig überarbeitete und ergänzte Auflage, Verlag Franz Vahlen, München, ISBN 978-3-8006-6931-8. Fundierte Einführung in Organisation, Instrumente, Bewertung und Reporting.

Gleißner, Werner (2022): Grundlagen des Risikomanagements – Handbuch für ein Management unter Unsicherheit, 4. Auflage, Verlag Franz Vahlen, München. Vertiefung insbesondere zu Risikoquantifizierung, Aggregation und entscheidungsorientiertem Risikomanagement.

## 14.5 Veröffentlichte kommunale Praxisfundstellen

Stadt München: Einführung eines Tax Compliance Management Systems einschließlich Prozessbeschreibungen und Risiko-Kontrollmatrizen. <https://risi.muenchen.de/risi/dokument/v/4734181> und <https://risi.muenchen.de/risi/dokument/v/4734183>

Gemeindeverwaltungsverband Hardheim-Walldürn: Beschlussunterlage zur Einführung eines Tax Compliance Management Systems; Landkreis Lüneburg: Aufgaben der Steuerorganisation; Einwohnergemeinde Rechterswil (Schweiz): IKS-Konzepthandbuch. Die Übertragbarkeit ist jeweils anhand von Rechtslage, Größe und Organisation zu prüfen.

Hinweis zur Nutzung: Normen und berufsständische Standards sind methodische Referenzen, soweit der kommunale Prüfungsauftrag nichts Abweichendes vorgibt. Die veröffentlichten Praxisbeispiele belegen reale Ansätze; die vollständige Fallmatrix dieses Whitepapers ist eine fachlich abgeleitete Mustermatrix und örtlich zu validieren. Abruf der Onlinequellen: 1. September 2026.

## 14.6 Process Mining und digitale Prozessprüfung

Van der Aalst, Wil M. P. (2016): Process Mining – Data Science in Action, 2. Auflage, Springer, Berlin/Heidelberg. Grundlegendes Lehrbuch zu Discovery, Conformance und Enhancement. <https://link.springer.com/book/10.1007/978-3-662-49851-415>

Van der Aalst, Wil M. P.; Carmona, Josep (Hrsg.) (2022): Process Mining Handbook, LNBIP 448, Springer, Cham, Open Access. Vertiefung zu Discovery, Conformance, Eventlog Engineering, Enhancement und Anwendungen. <https://link.springer.com/book/10.1007/978-3-031-08848-3>

IEEE Task Force on Process Mining (2011): Process Mining Manifesto. Grundlegende Leitprinzipien und Qualitätsanforderungen für Ereignisdaten und Process-Mining-Projekte. <https://www.processmining.org/>

Object-Centric Event Log Standard: OCEL 2.0. Referenz für Prozesse mit mehreren verknüpften Objekttypen und komplexen 1:n-/n:m-Beziehungen. <https://www.ocel-standard.org/16>

Ausgewertete Anlage 2: Process Mining Shortpaper; Anlage 3: Anwendungsbeispiel zur IKS-Prüfung im Beschaffungsprozess; Anlage 4: Studie des Stadtrechnungshofs Wien zum Einsatz von Process Mining in Prüfungen.

---

15 Van der Aalst, W. M. P. (2016), a. a. O.; ergänzend IEEE Task Force on Process Mining (2011): Process Mining Manifesto.

16 Object-Centric Event Log Standard, OCEL 2.0, <https://www.ocel-standard.org/>.

Ausgewertete Anlage 5 und Anlage NN: Checklisten zu digitalen Prüfansätzen bzw. digitalen Prozessprüfungen; verwendet für Prozessabgrenzung, Datenquellen, Eventlog, Modellierung und Ergebnisadressaten.

Ausgewerteter Schlussbericht ‚ifV Pilotprojekte 2024 – Journal Entry Testing und Process Mining in der kommunalen Praxis‘, Fassung 15.03.2025; kommunaler Pilotfall Hundesteuer mit Fachverfahren und SAP-FI.

Ausgewertete Anlage ‚Process Mining in Kommunen‘; Überblick zu Nutzen, Voraussetzungen, Datenschutz und kommunalen Anwendungsfeldern.