Dienstleistungsbezogenes IKS: Praxisleitfaden für Aufbau, Prüfung und Nachweis

Vorwort:

Dienstleister übernehmen zunehmend zentrale Aufgaben in den Wertschöpfungsketten ihrer Kunden. Damit steigt die Erwartung, dass Leistungen kontrolliert, nachvollziehbar und prüfbar erbracht werden.

Ein dienstleistungsbezogenes Internes Kontrollsystem (IKS) schafft dafür die Grundlage. Es stellt sicher, dass Risiken erkannt, Prozesse beherrscht und Kontrollen wirksam umgesetzt werden. Doch viele Dienstleister stehen vor der Frage, wie ein solches System strukturiert, dokumentiert und prüfbar aufgebaut werden kann.

Dieses Whitepaper soll Orientierung geben. Es beschreibt praxisnah den Aufbau eines IKS, erläutert die relevanten Prüfungsrahmen nach ISAE 3402 und IDW PS 951 n.F. und zeigt, wie Dienstleister damit Vertrauen schaffen und ihre Marktposition stärken können.

R3 Audit & Assurance GmbH
Wirtschaftsprüfungsgesellschaft

Inhalt

1. Einleitung und Hintergrund

Dienstleister übernehmen heute in nahezu jeder Branche zentrale Aufgaben für ihre Kunden. Damit tragen sie maßgeblich zur Qualität, Verfügbarkeit und Sicherheit der Leistungen ihrer Auftraggeber bei.

Mit dieser Rolle wächst die Erwartung, dass der Dienstleister seine Prozesse **nachvollziehbar steuert, überwacht und dokumentiert**. Auftraggeber müssen nachvollziehen können, ob Leistungen zuverlässig, sicher und regelkonform erbracht werden.

Ein **dienstleistungsbezogenes Internes Kontrollsystem (IKS)** bildet dafür den strukturierten Rahmen. Es beschreibt, wie der Dienstleister seine Dienstleistung erbringt, Risiken für die Leistungsgüte erkennt, angemessene Kontrollen implementiert und die Wirksamkeit dieser Kontrollen sicherstellt. Das System dient drei Zielen:

1. **Qualitätssicherung:** Vermeidung bzw. Aufdeckung von Fehlern und Ineffizienzen in der Leistungserbringung.
2. **Transparenz:** Nachvollziehbarkeit der Prozesse und Verantwortlichkeiten gegenüber Kunden und Prüfern.
3. **Vertrauen:** Nachweis, dass Dienstleistungen unter beherrschten Bedingungen erbracht werden.

Wichtig ist dabei die **Rollenabgrenzung**:

Der Auftraggeber bleibt stets verantwortlich für die ordnungsgemäße Steuerung der ausgelagerten Aufgaben. Der Dienstleister muss jedoch sicherstellen, dass seine eigenen Prozesse und Kontrollen so gestaltet sind, dass der Auftraggeber sich auf sie stützen kann.

Die Implementierung eines dienstleistungsbezogenen IKS ist daher kein rein regulatorisches Thema. Auch nicht regulierte Unternehmen stehen zunehmend unter **Nachweisdruck;** sei es aufgrund vertraglicher oder branchenspezifischer Anforderungen, oder um überhaupt als Dienstleister in bestimmten Märkten in Betracht zu kommen. Ein dokumentiertes und geprüftes IKS wird damit zum **Qualitätsmerkmal** und **Wettbewerbsvorteil**: Es signalisiert Zuverlässigkeit, senkt Prüfungsaufwände auf Kundenseite und stärkt die Position in Ausschreibungen.

2. Prüfungs- und Nachweisrahmen für dienstleistungsbezogene IKS

Assurance-Berichte ersetzen kein Vertrauen – sie machen es belegbar.

Um dem Nachweisdruck zu begegnen, sind Assurance-Berichte von unabhängigen Prüfern die bevorzugte Wahl. Berichte von Wirtschaftsprüfern sind dabei erste Wahl, da diese aufgrund der strengen berufsrechtlichen Vorgaben besondere Beweiskraft entfalten.

Ein formalisierter, nach gängigen Prüfungsstandards erstellter **Assurance-Bericht** liefert dem Auftraggeber eine nachvollziehbare, von unabhängiger Seite geprüfte Bestätigung über die **Angemessenheit und ggf. Wirksamkeit** des Kontrollsystems.

In der Praxis werden solche Berichte auf Basis des internationalen Prüfungsstandards ISAE 3402 oder nach dessen deutscher Adaption IDW PS 951 n.F. (03.2021) erstellt.

2.1 ISAE 3402

Der von der **International Federation of Accountants (IFAC)** herausgegebene Standard **ISAE 3402 „Assurance Reports on Controls at a Service Organization“** bildet die **weltweit anerkannte Grundlage** für die Prüfung von Dienstleistungsunternehmen.

Er beschreibt, wie ein unabhängiger Prüfer beurteilt, ob das interne Kontrollsystem des Dienstleisters

- **angemessen ausgestaltet** ist (Design) und
- **wirksam funktioniert** (Operating Effectiveness).

Im Ergebnis wird ein **Assurance-Bericht** erstellt, der die Kontrollelemente des Dienstleisters beschreibt und eine Prüfungsfeststellung enthält. Dieser Bericht dient den Kunden und deren Prüfern als Nachweis, dass die Leistungen des Dienstleisters unter einem funktionsfähigen Kontrollsystem erbracht wurden.

Der ISAE 3402 ist **branchenunabhängig** einsetzbar und wird insbesondere dann verwendet, wenn die Dienstleistung international angeboten wird.

2.2 IDW PS 951 n.F.

Der vom **Institut der Wirtschaftsprüfer (IDW)** herausgegebene **IDW Prüfungsstandard: Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen (IDW PS 951 n.F. (03.2021))** ist die **deutsche Adaption des ISAE 3402**.

Er übernimmt die internationalen Grundsätze, konkretisiert sie jedoch für den deutschen Rechts- und Prüfungskontext. Der Standard legt fest,

- welche Inhalte eine prüfungsfähige **IKS-Beschreibung** enthalten muss,
- wie die **Kontrollziele und -maßnahmen** darzustellen sind, und
- nach welchen Kriterien der Prüfer die **Angemessenheit und ggf. Wirksamkeit** des IKS beurteilt.

2.3 Vergleich von ISAE 3402 und IDW PS 951 n.F.

Obwohl IDW PS 951 n.F. auf ISAE 3402 aufbaut, sind die Anforderungen nicht vollständig identisch.

Die wichtigste Gemeinsamkeit der beiden Standards ist das zweistufige Vorgehen und die daraus folgende Art der Berichterstattung:

1. **Prüfung der Angemessenheit / Design (Gegenstand des Typ-1-Berichts und Grundlage für den Typ-2-Bericht):**

   Beurteilung, ob die beschriebenen Kontrollen geeignet sind, die definierten Kontrollziele zu erreichen.

2. **Prüfung der Wirksamkeit / Operating Effectiveness (Gegenstand des Typ-2-Berichts):**

   Beurteilung, ob die Kontrollen über den Prüfungszeitraum tatsächlich wirksam ausgeführt wurden.

Die nachfolgende Tabelle stellt die wichtigsten Unterschiede und Gemeinsamkeiten dar:

Merkmal	**ISAE 3402**	**IDW PS 951 n.F.**
Herausgeber	International Federation of Accountants (IFAC)	Institut der Wirtschaftsprüfer (IDW)
Standardtyp	International Standard on Assurance Engagements (ISAE)	Deutscher Prüfungsstandard
Geltungsbereich	Weltweit, insbesondere bei internationalen Dienstleistungsbeziehungen	Deutschland, deutscher Rechts- und Prüfungskontext
Sprache und Berichtsgestaltung	I.d.R. Englisch (international üblich)	Deutsch
Adressaten	Internationale Mandanten und deren Prüfer	Deutsche Mandanten und Prüfer
Struktur der IKS-Beschreibung	Freier Rahmen, orientiert an Kontrollzielen	Detaillierte Mindestinhalte nach Tz. 21 ff. IDW PS 951 n.F.
Subdienstleister-Darstellung	inclusive / carve-out-Methode	inclusive / carve-out-Methode
Ergebnis	Assurance-Bericht (Typ 1 oder Typ 2)	Assurance-Bericht (Typ 1 oder Typ 2)

3. Grundlagen eines dienstleistungsbezogenen IKS

Ein IKS ist kein Dokument, sondern ein lebendes System aus Verantwortung, Risiko und Kontrolle.

3.1 Abgrenzung des dienstleistungsbezogenen IKS

Das Interne Kontrollsystem (IKS) eines Dienstleisters umfasst grundsätzlich **alle organisatorischen Regelungen, Verfahren und Kontrollen**, die sicherstellen sollen, dass Geschäftsprozesse ordnungsgemäß, effizient und risikobewusst ablaufen.

Nicht alle diese Kontrollen sind jedoch für die Kunden oder deren Prüfer von Bedeutung.

Man unterscheidet daher zwischen zwei Betrachtungsebenen:

1. **Nicht-dienstleistungsbezogenes IKS**
   umfasst interne Themen, die keinen unmittelbaren Bezug zu den an Kunden erbrachten Leistungen haben (z. B. allgemeine Finanzbuchhaltung, Personalverwaltung, Marketing oder interne Budgetkontrolle).

2. **Dienstleistungsbezogenes IKS**
   bezieht sich ausschließlich auf die Kontrollen, die **unmittelbar oder mittelbar** die Qualität, Sicherheit und Ordnungsmäßigkeit der **vertraglich geschuldeten Leistungen** betreffen.

Die Abgrenzung ist entscheidend, weil nur das dienstleistungsbezogene IKS Gegenstand einer Prüfung nach ISAE 3402 oder IDW PS 951 n.F. ist. Ein häufiger Fehler in der Praxis besteht darin, das gesamte unternehmensinterne IKS als Prüfungsgegenstand zu verstehen. Dies führt zu unnötigem Mehraufwand und verwässert den Fokus auf jene Kontrollen, die tatsächlich für die Auftraggeber relevant sind.

3.2 Grundelemente eines IKS

Ein wirksames dienstleistungsbezogenes IKS besteht aus mehreren, aufeinander abgestimmten Elementen. Sie definieren die organisatorische Basis, auf der Prozesse gesteuert, Risiken erkannt und Kontrollen wirksam umgesetzt werden.
Die folgende Struktur orientiert sich an bewährten Frameworks (z. B. COSO) und den Vorgaben des IDW PS 951 n.F.:

1. **Kontrollumfeld**

   Das Kontrollumfeld beschreibt die Rahmenbedingungen, unter denen Kontrollen wirken.

   Für Dienstleister bedeutet das:

   - **Verantwortlichkeiten und Zuständigkeiten** sind klar festgelegt.
   - Führung und Kultur vermitteln, dass Kontrolle **Teil des Arbeitsalltags** ist.
   - Governance-Strukturen stellen sicher, dass Risiken und Kontrollergebnisse **bis zur Geschäftsleitung kommuniziert** werden.

2. **Risikobeurteilung**

   Das IKS baut auf einer fundierten Risikoanalyse auf.

   Für Dienstleister bedeutet das:

   - Risiken werden **prozessbezogen identifiziert**, also entlang der tatsächlich erbrachten Dienstleistung.
   - Die Bewertung orientiert sich an **Eintrittswahrscheinlichkeit und Auswirkung** von Fehlern auf die Dienstleistungsqualität.
   - Ziel ist es, die **wesentlichen Risiken herauszufiltern,** um darauf abgestimmte Kontrollen zu entwickeln („Kontrolle folgt Risiko“).

3. **Kontrollaktivitäten**

   Kontrollen sind die operativen Maßnahmen, mit denen Risiken beherrscht werden. Sie bilden den Kern des IKS und entscheiden über dessen tatsächliche Wirksamkeit.

   Für Dienstleister gilt:

   - **Kontrollen sind in die Prozesse integriert** und nicht nachgelagerte Prüfungen. Eine Kontrolle ist dann wirksam, wenn sie im Ablauf verankert ist und Fehler präventiv verhindert oder frühzeitig erkennt.
   - **Automatisierte und manuelle Kontrollen** ergänzen sich: Automatisierte Kontrollen sind reproduzierbar, effizient und dokumentierbar (z. B. Berechtigungsprüfungen, Plausibilitätskontrollen). Manuelle Kontrollen sind dort erforderlich, wo fachliche Beurteilung oder Entscheidungsspielraum besteht (z. B. Freigaben, Reviews, Eskalationen).

- **Schlüsselkontrollen** (Key Controls) stehen im Fokus: Das sind jene Kontrollen, deren Funktionsfähigkeit für die Erreichung der Kontrollziele wesentlich ist. Sie adressieren wesentliche Risiken direkt und müssen nachvollziehbar dokumentiert und prüfbar sein.
- **Verantwortlichkeiten sind klar zugeordnet**. Für jede Kontrolle muss feststehen, wer sie durchführt, wer Ergebnisse überwacht und wer bei Abweichungen reagiert („Control Owner").

Wirksame Kontrollaktivitäten zeichnen sich nicht durch ihre Anzahl, sondern durch **Risikoorientierung, Prozessintegration und Nachvollziehbarkeit** aus.

4. **Information und Kommunikation**

   Ein IKS funktioniert nur, wenn Informationen **vollständig, zeitgerecht und adressatengerecht** fließen.

   Für Dienstleister bedeutet das:

   - Innerhalb des Unternehmens müssen Kontrollergebnisse, Prozessänderungen und Auffälligkeiten dokumentiert und weitergeleitet werden.
   - Gegenüber Kunden sind bei wesentlichen Vorkommnissen Transparenzpflichten zu beachten (z. B. im Rahmen von SLAs oder Berichtswegen).
   - Die IKS-Kommunikation sollte dokumentiert, nachvollziehbar und rollenbezogen erfolgen.

5. **Überwachung (Monitoring)**

   Die Überwachung dient der Sicherstellung, dass das IKS dauerhaft funktioniert.

   Für Dienstleister bedeutet das:

   - **Die Wirksamkeit der Kontrollen wird regelmäßig bewertet**, etwa durch Stichproben, Self-Assessments, KPI-Überwachung oder interne Qualitätsreviews.
   - **Erkannte Schwachstellen werden dokumentiert**, analysiert und durch definierte Maßnahmen behoben; deren Umsetzung wird nachverfolgt.
   - **Unabhängige Prüfungen**, (z. B. durch Interne Revision oder externe Auditoren) ergänzen die Eigenüberwachung und liefern eine objektive Beurteilung.

- In reifen Organisationen ist Monitoring ein **kontinuierlicher Bestandteil der Leistungserbringung**, nicht nur ein punktuelles Prüfungsereignis.

6. **Dokumentation**

   „Nicht dokumentiert" gilt im IKS als „nicht existent".

   Für Dienstleister bedeutet das:

   - Jede Kontrolle benötigt eine **nachvollziehbare Beschreibung, Verantwortlichkeit und Nachweisführung.**
   - Die Dokumentation dient als **Grundlage** für Schulungen, Selbstprüfungen und externe Audits.
   - Eine aktuelle, strukturierte IKS-Dokumentation ist der **zentrale Nachweis der Systemreife** gegenüber Auftraggebern und Prüfern.

Ein funktionierendes dienstleistungsbezogenes IKS entsteht nicht durch Einzelkontrollen, sondern durch das **Zusammenspiel dieser sechs Elemente**.

3.3 Kontrolltypen und -kategorien

Das Kontrollsystem eines Dienstleisters besteht aus unterschiedlichen Ebenen und Ausprägungen von Kontrollen. Diese lassen sich nach Art der Durchführung (manuell oder automatisiert) sowie nach Wirkungsweise (präventiv oder detektiv) unterscheiden. Darüber hinaus ergänzen Managementkontrollen als übergeordnete Steuerungsebene die operativen Maßnahmen.

3.3.1. Managementkontrollen

Managementkontrollen bilden die oberste Ebene des Kontrollsystems. Sie dienen der Überwachung und Steuerung der Dienstleistungsprozesse auf aggregierter Ebene und liefern Hinweise, ob das IKS im Ganzen funktioniert.

Typische Beispiele sind:

- regelmäßige Risiko- und Performanceberichte,
- Budget- und Soll-Ist-Vergleiche,
- Management-Reviews über Kontrollergebnisse und KPI-Entwicklungen,
- Risikoberichterstattung an Geschäftsleitung oder Aufsichtsorgane.

Diese Kontrollen sind häufig detektiv und kompensierend: Sie erkennen Schwachstellen, wenn operative Kontrollen versagen und ermöglichen eine Reaktion auf höherer Ebene.

3.3.2. Operative Kontrollen

Die operative Ebene umfasst die eigentlichen Prozesskontrollen, die direkt in den Abläufen des Dienstleisters wirken.

Sie werden in zwei Dimensionen unterschieden:

Charakteristik	Präventiv	Detektiv
Manuelle Kontrollen	Funktionstrennung, Kompetenzregelungen, Zugriffs- und physische Schutzvorkehrungen	Abstimmkontrollen, manuelle Prüfungen, physische Kontrollen
Automatische Kontrollen	Funktionstrennung in Systemen, Passwort- und Zugriffsvorschriften	Zugriffsüberwachung, Datenabgleiche und Protokollauswertungen

Präventive Kontrollen verhindern Fehler bereits bei der Entstehung, während detektive Kontrollen Abweichungen oder Verstöße im Nachhinein erkennen. Automatisierte Kontrollen sind wiederholbar und effizient, manuelle Kontrollen bleiben dort erforderlich, wo fachliche Beurteilung oder situatives Ermessen gefragt ist.

Ein **effektives Kontrollsystem kombiniert** diese Formen.

3.3.3. Zusammenspiel der Kontrollarten

Managementkontrollen, manuelle und automatisierte Prozesskontrollen wirken im Idealfall **aufeinander abgestimmt wie ein Schichtsystem**:

- Automatische Kontrollen verhindern und erkennen operative Fehler.
- Manuelle Kontrollen ergänzen dort, wo menschliches Urteil erforderlich ist.
- Managementkontrollen schaffen Transparenz über die Gesamtsituation und ermöglichen Korrekturen auf Führungsebene.

Dieses mehrschichtige Zusammenspiel erhöht die Widerstandsfähigkeit des IKS. Ein Fehler, der eine Ebene passiert, wird mit hoher Wahrscheinlichkeit auf der nächsten erkannt.

3.4 Schlüsselkontrollen

In der Praxis ist nicht jede Kontrolle gleich bedeutsam. **Schlüsselkontrollen** sind jene Maßnahmen, die für die Erreichung der Kontrollziele entscheidend sind und daher im Fokus jeder IKS-Prüfung stehen.

Typische Merkmale einer Schlüsselkontrolle:

- sie wirkt direkt auf ein wesentliches Risiko,
- ihr **Ausfall** hätte **erhebliche Auswirkungen**,
- sie ist **klar dokumentiert und prüfbar**.

Beispiele:

- Freigabe von Änderungen an IT-Systemen,
- Berechtigungsfreigaben durch Systemverantwortliche,
- Abstimmung von Schnittstellen in Datenprozessen.

Die Fokussierung auf Schlüsselkontrollen ist **zentraler Erfolgsfaktor** einer effizienten IKS-Implementierung und -Prüfung. Sie reduziert Komplexität und stellt sicher, dass Prüfungsaufwand und Risikorelevanz im Gleichgewicht bleiben.

4. Aufbau eines dienstleistungsbezogenen IKS

Die beste Kontrolle ist wertlos, wenn ihr Zweck nicht verstanden wird.

Ein IKS ist kein statisches Regelwerk, sondern das Ergebnis eines klar definierten Aufbaus. Nur wenn Prozesse, Risiken und Kontrollen aufeinander abgestimmt sind entsteht ein System, das im Alltag funktioniert und prüfbar bleibt.

Für Zwecke einer externen Prüfung – etwa nach **IDW PS 951 n.F.** oder **ISAE 3402** – muss dieser Aufbau in einer **IKS-Beschreibung** nachvollziehbar dokumentiert sein. Sie bildet die Grundlage für die Beurteilung durch den Prüfer und zeigt, wie der Dienstleister sein Kontrollsystem strukturiert, betreibt und überwacht.

Der IDW PS 951 n.F. nennt hierfür Mindestinhalte, die in jeder IKS-Beschreibung enthalten sein müssen:

Für den Aufbau des dienstleistungsbezogenen IKS haben sich in der Praxis folgende **sechs Phasen** bewährt:

4.1 Erfassung der Dienstleistung

Am Anfang steht die präzise Erfassung der angebotenen Dienstleistungen. Dieser Schritt ist oft anspruchsvoller, als er scheint:

- Vertragsunterlagen sind nicht immer eindeutig formuliert oder veraltet.
- Der tatsächliche Leistungsumfang weicht häufig von der ursprünglichen Vereinbarung ab.
- Standardisierte Vertragsmuster decken individuelle Besonderheiten nicht vollständig ab.

Ziel dieser Phase ist eine **vollständige, aktuelle und abgestimmte Leistungsbeschreibung**, die als Bezugsrahmen für alle weiteren IKS-Aktivitäten dient.

In der Praxis ist es hilfreich eine Übersicht zu erstellen, welche Dienstleistungen für welche Kunden erbracht werden und welche Prozesse, Systeme und Subdienstleister jeweils beteiligt sind.

4.2 Zerlegung in Prozessschritte

Sind die Dienstleistungen definiert, müssen sie in **Einzelprozesse und Prozessschritte** zerlegt werden.
Dadurch entsteht Transparenz, wie die Dienstleistung tatsächlich erbracht wird. Wichtige Punkte:

- Dokumentation von Abläufen, Verantwortlichkeiten und IT-Systemen.
- Zuordnung der Prozessschritte zu den beteiligten Organisationseinheiten.
- Identifikation von Schnittstellen zwischen Prozessen und Systemen.

Zur Visualisierung eignen sich **Ablaufdiagramme, Swimlane-Darstellungen oder RACI-Matrizen**, um Verantwortlichkeiten und Informationsflüsse eindeutig festzuhalten. Diese Prozesssicht ist die Grundlage für die spätere Risikoanalyse und die Definition von Kontrollen.

4.3 Festlegung von Qualitätskriterien

Auf Basis der Prozessanalyse werden **Kriterien** definiert, die festlegen, wann eine Dienstleistung als ordnungsgemäß erbracht gilt. Diese Kriterien dienen sowohl dem internen Qualitätsmanagement als auch der späteren IKS-Prüfung.
In der Praxis werden drei Ebenen unterschieden:

1. **Gesetzliche und regulatorische Kriterien** – z. B. DSGVO, GoBD, HGB, MaRisk.
2. **Branchen- oder standardspezifische Kriterien** – z. B. ISO 27001, COBIT®, ITIL, BSI-Grundschutz.
3. **Selbst entwickelte bzw. vertragliche Kriterien** – z. B. Service-Level-Agreements, interne Richtlinien.

Damit ein Prüfer die Kriterien verwenden kann, müssen sie **relevant, vollständig, verlässlich, neutral und verständlich** formuliert sein. Für Dienstleister sind diese Kriterien der Ausgangspunkt für die Definition der Kontrollziele.

4.4 Definition von Kontrollzielen

Aus den Kriterien werden Kontrollziele abgeleitet. Sie beschreiben, welchen Zweck eine Kontrolle verfolgt.

Beispiel:

- **Kriterium**: „Alle Datenverarbeitungen sind vollständig und richtig durchzuführen."
- **Kontrollziel**: „Unvollständige oder fehlerhafte Transaktionen werden verhindert oder erkannt."
- **Kontrolle:** „Automatischer Datenabgleich zwischen Eingangssystem und Hauptbuch."

Kontrollziele ergeben sich insbesondere aus den gesetzlichen bzw. aufsichtsrechtlichen Anforderungen sowie aus den Erfordernissen der jeweiligen Geschäftstätigkeit

4.5 Risikoerfassung und -bewertung

Die Risikoanalyse ist das Bindeglied zwischen den Kontrollzielen und den zu implementierenden Kontrollen. Ziel ist es diejenigen Risiken zu identifizieren, die die Erreichung der Kriterien und Kontrollziele gefährden, um darauf dann mit geeigneten Kontrollen reagieren zu können.

Vorgehensweise:

- Risiken werden **prozessbezogen** identifiziert (Fehlerquellen, Systemausfälle, Compliance-Risiken, Reputationsrisiken).
- Anschließend erfolgt eine **Bewertung nach Eintrittswahrscheinlichkeit und Schadenshöhe**, häufig auf Basis einer einfachen Skala (z. B. niedrig/mittel/hoch).
- Die Ergebnisse werden dokumentiert und regelmäßig aktualisiert, insbesondere bei Prozessänderungen oder neuen regulatorischen Anforderungen.

Diese Risikoübersicht bildet die Grundlage für die Festlegung von **Schlüsselkontrollen** und für die Bewertung der Wirksamkeit des IKS.

4.6 Festlegung von IKS-Maßnahmen

Zur Erreichung der Kontrollziele sind anschließend geeignete IKS-Maßnahmen festzulegen. Einzelne Kontrollen können dabei mehrere Kontrollziele adressieren. Ebenso kann die Erreichung von Kontrollzielen die Kombination mehrerer Kontrollen erfordern.

Eine **Risiko-Kontroll-Matrix** dient als zentrales Arbeitsinstrument. Sie dokumentiert:

- das adressierte Risiko oder Kontrollziel,

- die jeweilige Kontrollbeschreibung (Art, Automatisierungsgrad, Verantwortlicher),
- die Frequenz und den Kontrollanlass,
- Nachweise und Maßnahmen bei Abweichungen.

Damit wird das IKS prüfbar und operationalisiert.

4.7 Berichterstattung und kontinuierliche Überwachung

Ein strukturiertes Berichtswesen bildet den Abschluss der Implementierung – und zugleich den Beginn des laufenden IKS-Zyklus. Ziel ist es Transparenz über die Wirksamkeit der implementierten Kontrollen zu schaffen und eine Grundlage für Entscheidungen des Managements und für externe Prüfungen zu bieten.

Ein wirksames Reporting:

- fasst Ergebnisse aus Kontrollen und Monitoring zusammen,
- zeigt Auffälligkeiten, Ausnahmen und Trends,
- dokumentiert Maßnahmen und deren Umsetzung,
- dient Auftraggebern als Nachweis für die Angemessenheit und Funktionsfähigkeit des IKS.

In reifen Organisationen ist das Berichtswesen Teil eines **kontinuierlichen Verbesserungsprozesses.** Erkenntnisse aus Prüfungen und Monitoring fließen regelmäßig in die Weiterentwicklung des IKS ein.

5. Prüfung und Nachweis des IKS in der Praxis

Ein Prüfungsbericht ist kein Pflichtdokument – er ist eine Visitenkarte für Zuverlässigkeit.

Ein dokumentiertes IKS entfaltet seinen Wert erst wenn nachvollziehbar ist, dass es auch in der Praxis gelebt wird. Eine Prüfung nach IDW PS 951 n.F. oder ISAE 3402 **bestätigt unabhängig**, dass das Kontrollsystem des Dienstleisters angemessen ausgestaltet und wirksam betrieben wird.

5.1 Prüfungsgegenstand und Ablauf

Gegenstand der Prüfung ist die IKS-Beschreibung des Dienstleisters mit den dargestellten Prozessen, Risiken, Kontrollzielen und Kontrollen. Der Prüfer beurteilt zunächst, ob das System sachgerecht beschrieben und konzipiert wurde („Design“ = Typ 1), und ggf., ob es im Prüfungszeitraum tatsächlich wirksam funktioniert hat („Operating Effectiveness“ = Typ 2).

Der typische Prüfungsablauf gliedert sich in:

- Vorbereitungsphase: Abstimmung des Prüfungsumfangs, Festlegung des Berichtsformats (Typ 1 oder Typ 2).
- Systemanalyse: Prüfung der IKS-Beschreibung, der Risiko-Kontroll-Matrix und der Prozessdokumentationen.
- Kontrolltests: (Stichprobenweise) Prüfung der Schlüsselkontrollen auf Wirksamkeit.
- Beurteilung und Berichtserstellung: Zusammenfassung der Ergebnisse, Darstellung der Feststellungen und Gesamtbeurteilung des Systems.

5.2 Erforderliche Unterlagen

Für eine effiziente Prüfung sollten Dienstleister eine strukturierte Dokumentation bereithalten, insbesondere:

- Beschreibung des dienstleistungsbezogenen internen Kontrollsystems,
- Organigramme und Prozessdiagramme,
- Verfahrensbeschreibungen und Richtlinien (z. B. Berechtigungsmanagement, Änderungsmanagement),
- Risiko-Kontroll-Matrix mit Zuständigkeiten, Häufigkeit und Nachweisen,

- Nachweisdokumente zu den Kontrollen (z. B. Reports, Freigabeprotokolle, Tickets, Logs),
- Bridge Letters oder Prüfberichte von Subdienstleistern (bei Nutzung von Outsourcing-Ketten).

Eine gute Vorbereitung dieser Unterlagen reduziert Rückfragen erheblich und verkürzt die Prüfungsdauer.

5.3 Erklärungen des Dienstleisters

Neben der Dokumentation ist auch eine Erklärung der gesetzlichen Vertreter des Dienstleisters erforderlich.

Der Dienstleister bestätigt darin gegenüber dem Prüfer u. a.:

- dass die IKS-Beschreibung vollständig und zutreffend ist,
- dass alle wesentlichen Risiken und Kontrollen enthalten sind,
- und dass bekannte Schwachstellen offengelegt wurden.

Diese Erklärung ist Bestandteil jedes Prüfungsauftrags nach ISAE 3402 oder IDW PS 951 n.F. und dient als formale Grundlage für das Prüfungsurteil. Entsprechende Muster finden sich in Anlage 3 zum IDW PS 951 n.F.

Zudem wird durch die Prüfer i.d.R. zu Beginn und am Ende eine Vollständigkeitserklärung eingeholt, in der der Dienstleister

- die Angaben der gesetzlichen Vertreter bestätigt.
- zusichert, dass alle relevanten Informationen zur Verfügung gestellt wurden.
- zusichert, dass alle Informationen mitgeteilt wurden, zu
    - Gesetzesverstößen, dolose Handlungen, etc.,
    - Mängel in Bezug auf die Angemessenheit von Kontrollen,
    - Fälle, in denen Kontrollen nicht wie in der IKS-Beschreibung dargestellt durchgeführt werden,
    - Ereignisse, die eine erhebliche Auswirkung auf die Bescheinigung haben können.

5.4 Qualität von Prüfungsberichten erkennen

Ein Prüfungsbericht ist mehr als ein formales Testat – er ist der **zentrale Nachweis über die Verlässlichkeit des Kontrollsystems**. Seine Qualität zeigt sich daran, wie klar, **nachvollziehbar und aussagekräftig** die Darstellung des IKS und der Prüfungsergebnisse erfolgt:

- **Nachvollziehbare Systembeschreibung**:

  Die Prozesse, Kontrollziele und Kontrollen des Dienstleisters werden vollständig, verständlich und mit erkennbarem Bezug zur tatsächlichen Leistungserbringung dargestellt.

- **Klare Struktur der Kontrollziele und -maßnahmen**:

  Ein qualitativ hochwertiger Bericht verknüpft jedes Kontrollziel mit den dazugehörigen Kontrollen. Leser erkennen auf Anhieb, welche Risiken adressiert werden und wie die Kontrolle wirkt.

- **Transparente Darstellung der Prüfungshandlungen**:

  Der Bericht erläutert, wie der Prüfer vorgegangen ist – etwa durch Interviews, Systemtests, Stichproben oder Dokumentenprüfungen. Hierdurch ist die Nachvollziehbarkeit der Schlussfolgerungen sichergestellt.

- **Eindeutige Prüfungsbeurteilung**:

  Das Prüfungsurteil („Opinion“) ist klar formuliert und entspricht den Vorgaben des Standards. Falls der Prüfer Einschränkungen äußert, sollten diese sachlich begründet und auf konkrete Kontrollen bezogen sein.

- **Angemessenes Detailniveau:**

  Gute Berichte verzichten auf übermäßige Standardformulierungen oder Textblöcke ohne Aussagewert. Sie bieten ausreichend Details, um die Wirksamkeit der Kontrollen zu verstehen, ohne den Leser mit Prüfmethodik zu überfrachten.

Ein hochwertiger Prüfungsbericht dient nicht nur als **Nachweis für Kunden und Prüfer**, sondern auch als **Vertrauens- und Kommunikationsinstrument**. Er zeigt, dass der

Dienstleister sein IKS beherrscht, aktiv weiterentwickelt und externe Prüfung als Bestandteil seiner Governance versteht.

6. Erfolgsfaktoren und typische Stolpersteine

Transparenz ist die neue Währung im Dienstleistungsmarkt.

Ein dienstleistungsbezogenes IKS lebt nicht von Umfang oder Formalität, sondern von Klarheit, Risikoorientierung und Konsistenz. In der Praxis zeigen sich dabei wiederkehrende Erfolgsfaktoren – und typische Fehler, die vermieden werden sollten.

6.1 Erfolgsfaktoren

- Frühzeitige Integration: IKS-Anforderungen sollten von Beginn an in Prozesse, IT-Systeme und Verantwortlichkeiten integriert werden – nicht erst kurz vor der Prüfung.
- Risikoorientierung statt Vollständigkeit: Wichtiger als flächendeckende Kontrollen ist der Fokus auf wesentliche Risiken und Schlüsselkontrollen.
- Verantwortung und Ownership: Für jede Kontrolle muss klar sein, wer sie durchführt, wer sie überwacht und wer bei Abweichungen entscheidet.
- Dokumentation mit Mehrwert: Eine gut strukturierte IKS-Dokumentation ist nicht nur Prüfungsgrundlage, sondern internes Steuerungsinstrument.
- Kontinuierliche Verbesserung: Erkenntnisse aus Monitoring, interner Revision und externen Prüfungen sollten regelmäßig in die IKS-Weiterentwicklung einfließen.

6.2 Typische Stolpersteine

- Unklare Leistungsabgrenzung: Fehlende Transparenz darüber, welche Services tatsächlich geprüft werden sollen.
- Unvollständige oder veraltete Prozessdokumentation: erschwert die Nachvollziehbarkeit und führt zu Rückfragen im Prüfungsprozess.
- Kontrollen ohne Risikoanbindung: Kontrollen werden implementiert, ohne dass das zugrunde liegende Risiko klar beschrieben ist.
- Fehlende Nachweise: Nicht dokumentierte Kontrollen gelten als nicht existent – auch wenn sie tatsächlich durchgeführt werden.

- Unklare Subdienstleister-Grenzen: Fehlende Bridge Letters oder Schnittstellenregelungen führen zu Lücken im Prüfungsumfang.

Ein IKS ist dann erfolgreich, wenn es nicht als zusätzliche Pflicht, sondern als integrierter Bestandteil des operativen Geschäfts verstanden wird.

So wird es vom Prüfungsgegenstand zum Steuerungsinstrument – und zum echten Qualitätsmerkmal gegenüber Kunden.

Hinweis:

Das Whitepaper wurde von den Geschäftsführern der R3 Audit & Assurance GmbH Wirtschaftsprüfungsgesellschaft erstellt. Es dient der allgemeinen Information und ersetzt keine individuelle rechtliche oder prüferische Beratung.

Die R3 Audit & Assurance GmbH Wirtschaftsprüfungsgesellschaft unterstützt Dienstleistungsunternehmen bei der Konzeption, Implementierung und unabhängigen Prüfung dienstleistungsbezogener interner Kontrollsysteme (IKS) nach IDW PS 951 n.F. und ISAE 3402.

www.r3audit.de