Präsenzschulung Prüfer:innen

Prüfung allgemeiner IT-Kontrollen

WP Claudia Buchta, GdW
CISA Enrico Großer, Bavaria Treu AG
02.11.2026

GdW Die Wohnungswirtschaft Deutschland

Agenda

I. Einleitung

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

III. III. Prüfung genereller IT-Kontrollen nach ISA [DE] 315 (Revied 2019) – Überblick

IV. Bestimmung der Komplexität (531.KPL)

V. Anforderungsliste IT

VI. Dokumentation: Allgemeine IT-Kontrollen (531.ORD.MIN)

VII. Dokumentation: Allgemeine IT-Kontrollen (531. und ORD.PP)

Agenda

VIII. Risikoidentifizierung aus dem Einsatz von IT und Erfassung

IX. Erfassung von IT-Kontrollen

X. Risiko-Kontroll-Matrix 540

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

XII. Vorgehen bei ausgelagerter rechnungslegungsrelevanter IT-Systeme

XIII. Wichtige Prüfungsfeststellungen (320)

XIV. Arbeitspapiere und Berichterstattung

I. Einleitung

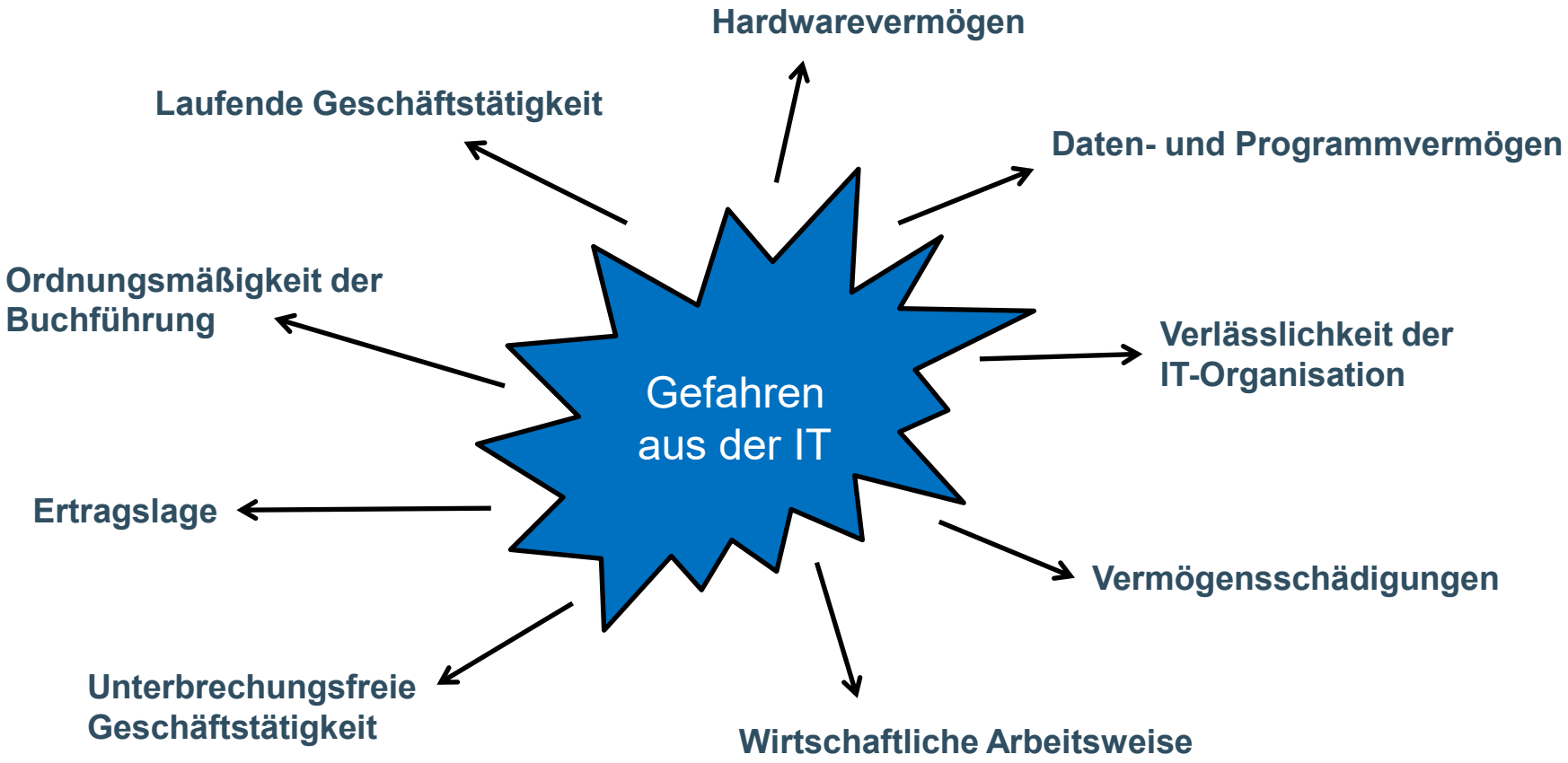
I. Einleitung

Warum beschäftigen wir Prüfer uns mit der IT beim geprüften Unternehmen?

- Identifizierung der Risiken, die aus dem Einsatz von IT resultieren
- alle Geschäftsprozesse erfolgen IT-gestützt
- hohe Komplexität der Systeme
- starke Abhängigkeit von der IT
- Buchungsgenerierung durch automatische Prozesse
- starker Auswirkungsgrad von fehlerhaften Parametern/Einstellungen
- Risiken aufgrund schlechter Wartung, Pflege und Customizing der Systeme
- Die rechnungslegungsrelevanten Daten aus der IT bilden die Grundlage/Basis für den Jahresabschluss
- Einsatz von KI

I. Einleitung

Auswirkungen der Gefahren aus dem Einsatz von IT



I. Einleitung

Welche Prüfungsstandards gelten?

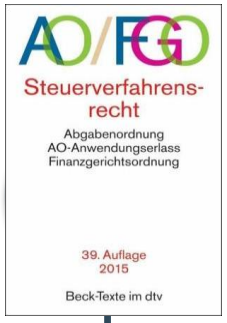
- GoA unter Einbeziehung der ISA
- Anwendung des ISA [DE] 315 (Revised 2019)
  "Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen"
- Keine separaten IT-Prüfungsstandards mehr
- die Prüfung der Risiken aus dem Einsatz von IT ist integraler Bestandteil der Jahresabschlussprüfung
- ISA [DE] 402 "Überlegungen bei der Abschlussprüfung von Einheiten, die Dienstleister in Anspruch nehmen"

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

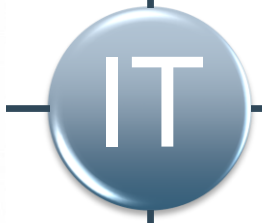
II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

§ 238 HGB:
Buchführungspflicht
§ 239 HGB:
Führung der Handels-bücher
§ 257 HGB:
Aufbewahrung von Unterlagen, Aufbewahrungsfristen
§ 261 HGB:
Vorlegung von Unterlagen auf Bild- oder Datenträgern





§ 146 AO:
Ordnungsvorschriften für die Buchführung und für Aufzeichnungen
§ 147 AO:
Ordnungsvorschriften für die Aufbewahrung von Unterlagen







ISA [DE] 315 (Revised 2019)
Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen

F & A zu ISA [DE] 315 (Revised 2019)
Zur Risikoidentifizierung und -beurteilung nach ISA [DE] 315 (Revised 2019)

ISA [DE] 402
Überlegungen bei der Abschlussprüfung von Einheiten, die Dienstleister in Anspruch nehmen

IDW RS FAIT 1:
Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie

IDW PS 880:
Die Prüfung von Softwareprodukten
(IDW PS 880 n.F. (01.2022))

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

F & Q zu ISA [DE] 315 (Revised 2019) Frage 4.12

Was sind Risiken, die aus dem Einsatz von IT resultieren?

ISA [DE] 315 (Revised 2019), Tz. 12(i), definiert Risiken aus dem Einsatz von IT als:

"Anfälligkeit der Kontrollen der Informationsverarbeitung für unwirksame Ausgestaltung oder Funktion oder Risiken für die Integrität von Informationen (d.h. die Vollständigkeit, Richtigkeit und Gültigkeit von Transaktionen und anderen Informationen) im Informationssystem der Einheit aufgrund unwirksamer Ausgestaltung oder Funktion von Kontrollen in den IT-Prozessen der Einheit (siehe IT-Umgebung)".

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

F & Q zu ISA [DE] 315 (Revised 2019) Frage 4.12
Beispiele:

- das Risiko, dass automatisierte oder IT-gestützte Kontrollen, die als relevant für die Abschlussprüfung identifiziert wurden, nicht in der Lage sind, eine wesentliche falsche Darstellung zu verhindern, z.B. im System hinterlegte automatische Kontenfindung, Kalkulationstabellen oder Bewertungsschemata (d.h., dass Daten falsch verarbeitet werden)

  IT-gestützte Kontrollen in den Prozessen (Kontrollen der Informationsverarbeitung)

- das Risiko, dass relevante Informationen (bspw. Daten oder Reports) manipuliert oder verändert werden bzw. in anderer Hinsicht nicht verlässlich sind, z.B. weil veraltete oder manipulierte Daten verwendet werden (d.h., dass falsche Daten verarbeitet werden).

  Generelle IT-Kontrollen / Report-Kontrollen

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Definitionen

Generelle IT-Kontrollen werden von ISA [DE] 315 (Revised 2019), Tz. 12(d), wie folgt definiert:

"Kontrollen über die IT-Prozesse der Einheit, die den kontinuierlichen ordnungsgemäßen Betrieb der IT-Umgebung unterstützen, einschließlich der kontinuierlich wirksamen Funktion der Kontrollen der Informationsverarbeitung und der Integrität von Informationen (d.h. Vollständigkeit, Richtigkeit und Gültigkeit von Informationen) im Informationssystem der Einheit"

(vgl. zu weiteren konkreten Beispielen zu generellen IT-Kontrollen Anlage 6 des ISA [DE] 315 (Revised 2019) und Frage 4.17 zur Definition von IT-Umgebung).

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

- Kontrollen sind in die **Komponenten des IKS** der Einheit eingebettet.
- **Regelungen** werden durch Handlungen des Personals der Einheit implementiert oder dadurch, dass das Personal daran gehindert wird, Handlungen vorzunehmen, die in Konflikt zu solchen Regelungen stehen würden.
- Maßnahmen können durch formale Dokumentation oder andere Kommunikation des Managements oder der für die Überwachung Verantwortlichen angeordnet werden oder können aus Verhaltensweisen resultieren, die nicht angeordnet, sondern eher durch die Unternehmenskultur der Einheit konditioniert sind. Maßnahmen können durch die von den in der Einheit eingesetzten IT-Anwendungen zugelassenen Handlungen oder andere Aspekte der IT-Umgebung der Einheit durchgesetzt werden.
- Kontrollen können direkt oder indirekt sein. **Direkte Kontrollen** sind Kontrollen, die präzise genug sind, um Risiken wesentlicher falscher Darstellungen auf Aussageebene zu behandeln. **Indirekte Kontrollen** sind Kontrollen, die direkte Kontrollen unterstützen.

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Definitionen

Kontrollen der Informationsverarbeitung werden von ISA [DE] 315 (Revised 2019), Tz. 12(e), wie folgt definiert:

"Kontrollen in Bezug auf die Verarbeitung von Informationen in IT-Anwendungen oder manuelle Informationsprozesse im Informationssystem der Einheit, die Risiken für die Integrität von Informationen (d.h. die Vollständigkeit, Richtigkeit und Gültigkeit von Transaktionen und anderen Informationen) direkt behandeln."

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Warum sind Risiken, die aus dem Einsatz von IT resultieren, zu identifizieren?

Das Verständnis von und eine Identifizierung der **aus dem IT-Einsatz resultierenden Risiken** und von den von der Einheit zur Behandlung dieser Risiken implementierten **generellen IT-Kontrollen** sich in mehrfacher Hinsicht auf die Abschlussprüfung auswirken:

- auf die Entscheidung, ob die Funktion von automatisierten bzw. IT-gestützten Kontrollen geprüft wird, um Risiken wesentlicher falscher Darstellungen auf Aussageebene zu adressieren
  - Geht nicht ohne verlässliche generelle IT-Kontrollen als "Basis"

- auf die Beurteilung des Kontrollrisikos auf Aussageebene durch den Abschlussprüfer
  - Die wirksame Ausgestaltung einer IT-gestützten Kontrolle kann von bestimmten generellen IT-Kontrollen abhängen, Kontrollrisiko ist höher, wenn generelle IT-Kontrollen unwirksam sind oder gar nicht erst geprüft werden

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Warum sind Risiken, die aus dem Einsatz von IT resultieren, zu identifizieren?

- auf die Strategie des Abschlussprüfers für die Prüfung von Informationen, die vom Unternehmen unter Nutzung von IT-Anwendungen des Unternehmens erstellt werden oder derartige Informationen einbeziehen
  - betrifft Funktion der Kontrollen über systemgenerierte Berichte, einschließlich der Identifizierung und Prüfung der Funktion der generellen IT-Kontrollen, die Programmänderungen oder das Berichtswesen betreffen
- auf die Beurteilung des inhärenten Risikos durch den Abschlussprüfer
  - Änderungen in der IT können Auswirkungen auf die Risikofaktoren der inhärenten Risiken haben
- auf die Planung weiterer Prüfungshandlungen
  - Bestehen Zweifel an der Ausgestaltung/Funktion genereller IT-Kontrollen, sind mehr aussagebezogenen PH durchzuführen

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Finden sich in ISA [DE] 315 (Revised 2019) konkret genannte Beispiele für Risiken, die aus dem Einsatz von IT resultieren können?

- unautorisierter Datenzugriff, der zur Vernichtung von Daten oder zu unsachgemäßen Änderungen an Daten führen kann. Dies kann einerseits die Aufzeichnung unautorisierter oder nicht vorhandener Geschäftsvorfälle und andererseits die fehlerhafte Aufzeichnung von Geschäftsvorfällen einschließen. Derartige Risiken können bspw. dort auftreten, wo mehrere Nutzer auf eine gemeinsame Datenbank zugreifen
- die Möglichkeit, dass IT-Personal Zugriffsberechtigungen erhält, die über die für die Erfüllung der ihm zugeteilten Aufgaben notwendigen hinausgehen, wodurch die Funktionstrennung aufgehoben wird
- unautorisierte Änderungen an Daten in den Stammdateien

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Finden sich in ISA [DE] 315 (Revised 2019) konkret genannte Beispiele für Risiken, die aus dem Einsatz von IT resultieren können?

- unautorisierte Änderungen an IT-Anwendungen und anderen Aspekten der IT-Umgebung
- Versäumnis, notwendige Änderungen an IT-Anwendungen oder anderen Aspekten der IT-Umgebung vorzunehmen
- unangemessene manuelle Eingriffe
- möglicher Datenverlust oder fehlende Möglichkeit, erforderlichenfalls auf Daten zuzugreifen.

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Wer ist verantwortlich für die Überwachung der Risiken, die aus dem Einsatz von IT resultieren?

Es ist **Aufgabe und Verantwortlichkeit des Managements** der Einheit, durch Einrichtung sog. genereller IT-Kontrollen die Risiken aus dem Einsatz von IT zu adressieren.

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Was versteht man unter der IT-Umgebung der Einheit?

ISA [DE] 315 (Revised 2019), Tz. 12(g), definiert die **IT-Umgebung** als IT-Anwendungen und unterstützende IT-Infrastruktur sowie IT-Prozesse und Personal, die in diejenigen Prozesse eingebunden sind, die eine Einheit zur Unterstützung des Geschäftsbetriebs und zur Erreichung von Geschäftsstrategien einsetzt.

- Eine **IT-Anwendung** ist ein Programm oder eine Reihe von Programmen, die für die Initiierung, Verarbeitung, Aufzeichnung und Berichterstattung von Geschäftsvorfällen oder Informationen eingesetzt werden. IT-Anwendungen schließen Data Warehouses und Report-Writer ein.
- Die **IT-Infrastruktur** besteht aus dem Netzwerk, Betriebssystemen und Datenbanken sowie der zugehörigen Hardware und Software.
- Die **IT-Prozesse** sind die Prozesse der Einheit zur Verwaltung des Zugriffs auf die IT-Umgebung, der Programmänderungen oder der Änderungen der IT-Umgebung und des IT-Betriebs.

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Ist der IDW RS FAIT 1 überhaupt noch anzuwenden?

- Dazu gibt es keine konkrete Aussage.
- Jedoch müssen zusätzlich zur Identifizierung Risiken wesentlicher falscher Darstellungen auch die Grundsätze ordnungsmäßiger Buchführung (GoB) eingehalten werden.
- ISA [DE] 200.D3.1:
  In die Prüfung des Jahresabschlusses ist nach § 317 Abs. 1 Satz 1 HGB die **Buchführung einzubeziehen**. Im Prüfungsbericht ist dazu nach § 321 HGB Abs. 2 Satz 1 HGB festzustellen, ob die Buchführung den gesetzlichen Vorschriften entspricht. Im Prüfungsbericht ist gemäß § 321 Abs. 2 Satz 2 HGB auch über Beanstandungen zur Buchführung zu berichten, die nicht zur Einschränkung oder Versagung des Bestätigungsvermerks geführt haben, soweit dies für die Beaufsichtigung der Geschäftsführung und des geprüften Unternehmens von Bedeutung ist.

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

IDW RS FAIT 1

Die **Ordnungsmäßigkeit der Buchführung** basiert regelmäßig auf dem Einsatz von IT.

Der Jahresabschluss ist nach § 243 Abs. 1 HGB nach den Grundsätzen ordnungsmäßiger Buchführung aufzustellen.

Somit hat der Abschlussprüfer im Rahmen der Abschlussprüfung zu beurteilen, ob das eingesetzte IT-gestützte Rechnungslegungssystem den gesetzlichen Anforderungen an die GoB entspricht.

Die Ordnungsmäßigkeit der Buchführung ist dann gegeben, wenn Geschäftsvorfälle vollständig, richtig, zeitnah, geordnet, nachvollziehbar und unveränderlich verarbeitet werden. Auf ein Rechnungslegungssystem und deren rechnungslegungsrelevanten Daten angewandt bedeutet dies, dass es Funktionen aufweisen muss, die den Anforderungen der Ordnungsmäßigkeit der Buchführung gerecht werden. Diese Funktionen sind **Belegfunktion, Journalfunktion, Kontenfunktion, Dokumentationsfunktion und Aufbewahrungsfunktion**.

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

IDW RS FAIT 1 (Tz 25 ff.)

Die **GoB** bei IT-gestützter Rechnungslegung sind nur erfüllt, wenn das Rechnungslegungs-system die Einhaltung der folgenden allgemeinen **Ordnungsmäßigkeitskriterien** bei der Erfassung, Verarbeitung, Ausgabe und Aufbewahrung der rechnungslegungsrelevanten Daten über die Geschäftsvorfälle sicherstellt:

- Vollständigkeit (§ 239 Abs. 2 HGB)
- Richtigkeit (§ 239 Abs. 2 HGB)
- Zeitgerechtigkeit (§ 239 Abs. 2 HGB)
- Ordnung (§ 239 Abs. 2 HGB)
- Nachvollziehbarkeit (§ 238 Abs. 1 Satz 2 HGB)
- Unveränderlichkeit (§ 239 Abs. 3 HGB)

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

IDW RS FAIT 1 (Tz 23)

Die gesetzlichen Vertreter sind verantwortlich für:

- Erfüllung der gesetzlichen Ordnungsmäßigkeitsanforderungen
- Einhaltung der Sicherheit der zugrundeliegenden IT-Systeme und der rechnungslegungsrelevanten Daten

Notwendige **Sicherheitsanforderungen**

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Autorisierung
- Authentizität
- Verbindlichkeit

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Übungsaufgabe

Sind die gesetzlichen Ordnungsmäßigkeitskriterien bei folgenden Softwareprodukten erfüllt?

- Reporting-Tool in Excel
- Projektplanungs-Tool in Excel
- Baubuch in Excel
- Bewertungs-Tool in Excel
- Anlagenverzeichnis in Excel
- Anlagenbuchhaltung in Excel

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Übersicht



Quelle:

WP-Praxis Nr. 7 vom 30.06.2021

WP/StB Prof. Dr. Jonas Tritschler

"Die IT-Prüfung im Kontext des ISA 315 (Revised 2019)"

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Belegfunktion (IDW RS FAIT 1 Tz 33 ff.)

- Jede Buchung muss durch einen Beleg vollständig nachgewiesen werden können (Grundsatz der Belegbarkeit)
- Grundsatzvoraussetzung für die Beweiskraft der Buchführung
- Nachweise über
  - Konventionelle Belege
  - Nachweis durch das Verfahren (automatische Buchungen)
- Mindestbestandteile
  - Buchungstext, Betrag, Belegdatum, Autorisierung, Kontierung, Ordnungskriterium, Buchungsdatum

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Journalfunktion (IDW RS FAIT 1 Tz 41 ff.)

- Nachweis der tatsächlichen und zeitgerechten Verarbeitung der Geschäftsvorfälle (zeitliche Ordnung)
- Erfüllung nur bei Schutz der gespeicherten Aufzeichnungen vor Veränderung oder Löschung
- Nachweis der Geschäftsvorfälle mit allen für die Erfüllung der Belegfunktion erforderlichen Angaben im Journal

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Kontenfunktion (IDW RS FAIT 1 Tz 46 ff.)

- Abbildung der im Journal in zeitlicher Reihenfolge aufgezeichneten Geschäftsvorfälle in sachlicher Ordnung auf Konten (Sach- und Personenkonten)
- I. d. R. werden die Journal- und Kontenfunktion gemeinsam wahrgenommen
- Notwendige Angaben:
  - Kontenbezeichnung
  - Kennzeichnung der Buchungen
  - Summen und Salden nach Soll und Haben
  - Buchungsdatum
  - Belegdatum
  - Gegenkonto
  - Belegverweis
  - Buchungstext

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

(Verfahrens)Dokumentation (IDW RS FAIT 1 Tz 52 ff.)

- Voraussetzung für die Nachvollziehbarkeit des Buchführungs- und Rechnungslegungsverfahrens ist eine ordnungsgemäße Verfahrensdokumentation
- Bestandteile
  - Anwenderdokumentation
  - Technische Systemdokumentation
  - Betriebsdokumentation

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Aufbewahrung (IDW RS FAIT 1 Tz 60 ff.)

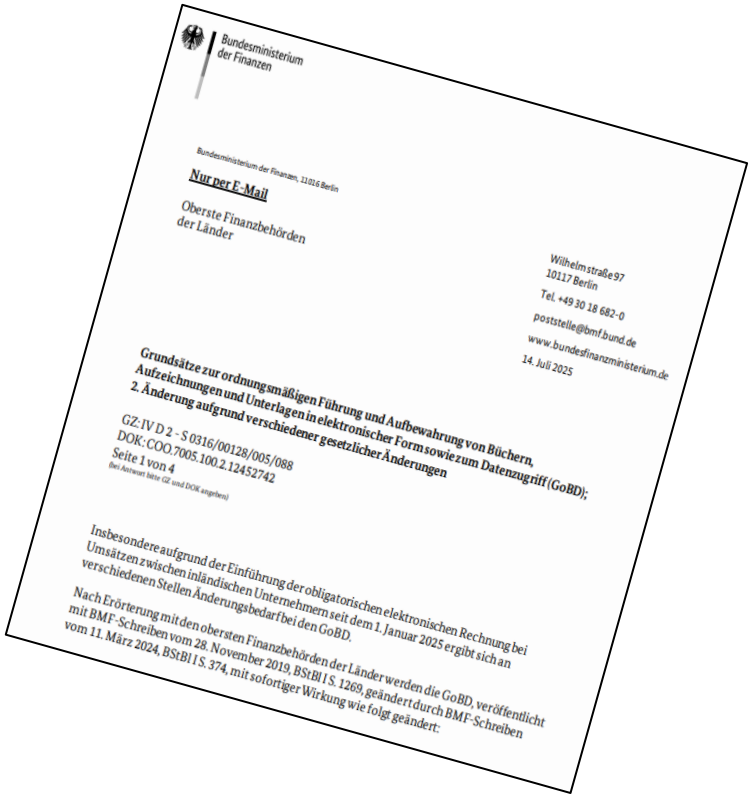
- Aufbewahrung der Buchführungsunterlagen über die gesetzlich vorgesehenen Zeiträume
  - Beachtung der Anforderungen an die Art der Aufbewahrungsmedien (Original, Datenträger)
  - Gewährleistung der technischen Voraussetzungen für die jederzeitigen Lesbarmachung (§§ 257, 261 i.V.m. § 239 Abs. 4 Satz 2 HGB).
  - Einhaltung der Aufbewahrungsfristen nach § 257 HGB, § 247 AO
  - ggf. Einsatz von Archivierungssystemen

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

Steuerliche Grundlagen

GoBD: Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form zum Datenzugriff

BMF-Schreiben vom 14.11.2014/28.11.20219
Neufassung der GoBD am 28.11.2019
geändert durch BMF-Schreiben vom 11.03.2024
angepasst durch BMF-Schreiben vom 14.07.2025



Bundesministerium der Finanzen

Bundesministerium der Finanzen, 11016 Berlin

Nur per E-Mail

Oberste Finanzbehörden
der Länder

Wilhelmstraße 97
10117 Berlin
Tel. +49 30 18 682-0
poststelle@bmf.bund.de
www.bundesfinanzministerium.de

14. Juli 2025

Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD); 2. Änderung aufgrund verschiedener gesetzlicher Änderungen

GZ: IV D 2 - S 0316/00128/005/088
DOK: COO.7005.100.2.12452742
Seite 1 von 4
Bei Antwort bitte GZ und DOK angeben

Insbesondere aufgrund der Einführung der obligatorischen elektronischen Rechnung bei Umsätzen zwischen inländischen Unternehmern seit dem 1. Januar 2025 ergibt sich an verschiedenen Stellen Änderungsbedarf bei den GoBD.

Nach Erörterung mit den obersten Finanzbehörden der Länder werden die GoBD, veröffentlicht mit BMF-Schreiben vom 28. November 2019, BStBl I S. 1269, geändert durch BMF-Schreiben vom 11. März 2024, BStBl I S. 374, mit sofortiger Wirkung wie folgt geändert:

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

GoBD - Grundlagen

- Präzisierung die Anforderungen an die Steuerpflichtigen bei elektronischer Datenverarbeitung in Bezug auf die Buchführung, Aufbewahrung und den Datenzugriff
- Für die Ordnungsmäßigkeit elektronischer Bücher und Verfahren ist der **Steuerpflichtige verantwortlich**; dies gilt ebenso bei teilweiser oder vollständiger organisatorischer und technischer Auslagerung von Buchführungs- und Aufzeichnungspflichten auf Dritte (Tz 21)
- Sicherstellung, für elektronische Bücher die gleichen Ordnungsmäßigkeitsprinzipien eingehalten werden, wie bei manuell erstellten Büchern oder Aufzeichnungen (Buchungen sollen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden) (Tz 22)

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

GoBD – Ordnungsmäßigkeitsprinzipien (Tz 26)

Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit

- Belegfunktion
- progressiven (Ausgangspunkt Beleg) und retrograden Prüfbarkeit (Ausgangspunkt JA) der Buchführung
- Lückenlose Nachverfolgung

Grundsatz der Wahrheit, Klarheit und fortlaufenden Aufzeichnung

- Vollständigkeit
- Einzelaufzeichnungspflicht
- Richtigkeit
- Zeitgerechtigkeit
- Ordnung
- Unveränderbarkeit

II. Rechtliche Grundlagen / ISA [DE] 315 (Revised 2019)

GoBD – Internes Kontrollsystem (IKS) (Tz 102)

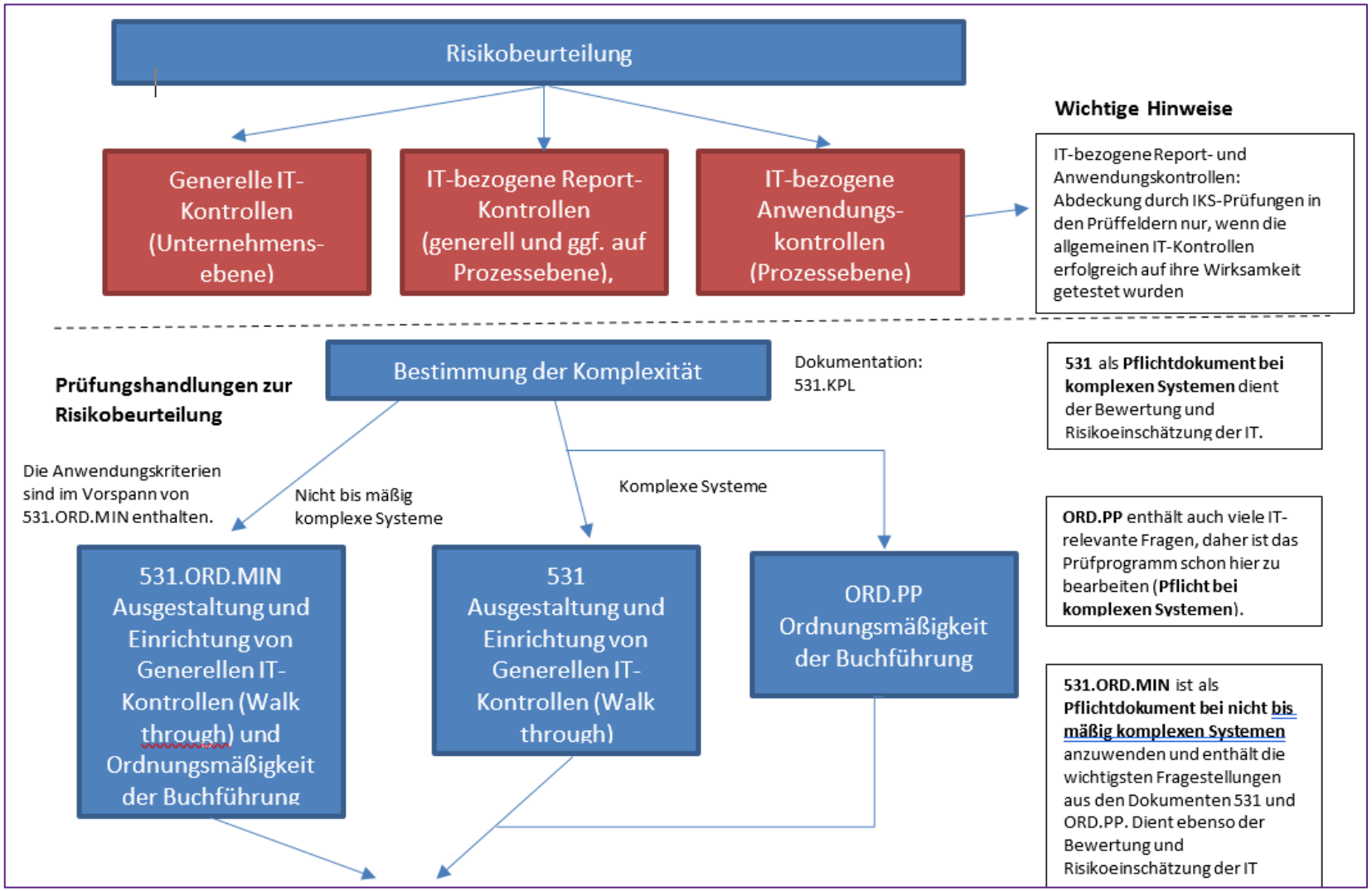
Sicherstellung, dass alle Buchungen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden (§ 146 Abs. 1 AO)! Die Beschreibung des IKS ist Bestandteil der Verfahrensdokumentation. Um dies zu gewährleisten sind Kontrollen einzurichten, auszuüben und zu protokollieren:

- Zugangs- und Zugriffsberechtigungskontrollen
- Funktionstrennungen
- Erfassungskontrollen (Fehlerhinweise, Plausibilitätsprüfungen)
- Abstimmungskontrollen bei der Dateneingabe
- Verarbeitungskontrollen
- Schutzmaßnahmen gegen Verfälschung

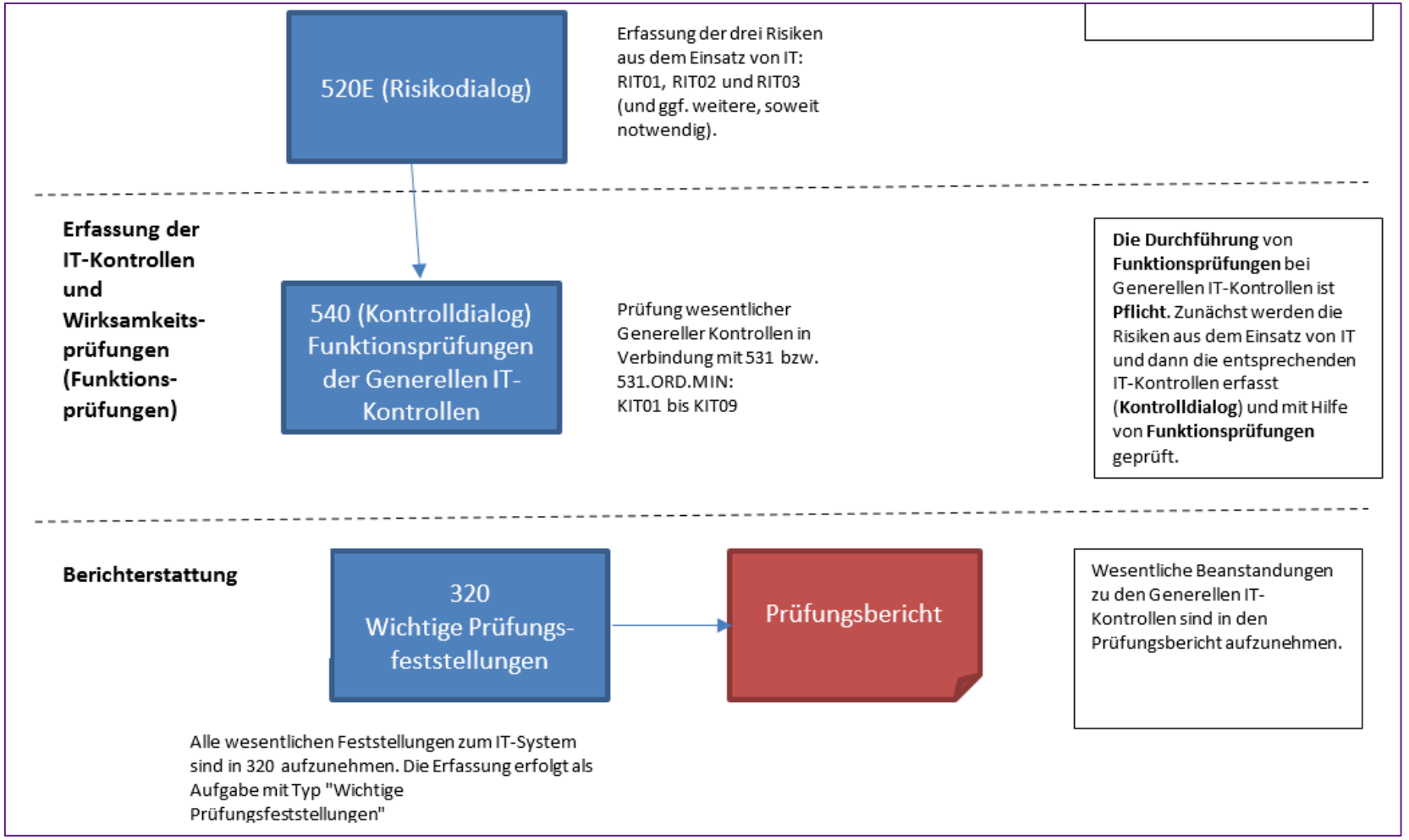
Die Beschreibung des IKS ist Bestandteil der Verfahrensdokumentation (Tz 102)!

III. Prüfung genereller IT-Kontrollen nach ISA [DE] 315 (Revised 2019) - Überblick

III. Prüfung genereller IT-Kontrollen nach ISA [DE] 315 (Revised 2019) - Überblick

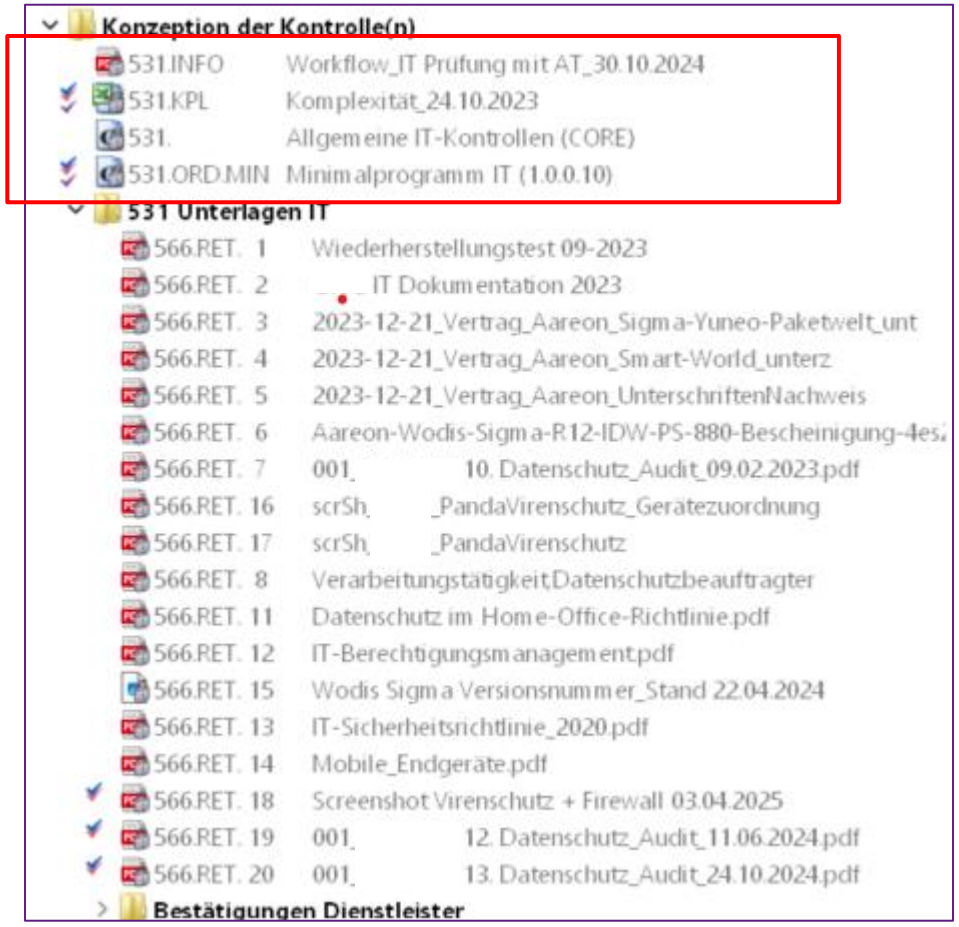


III. Prüfung genereller IT-Kontrollen nach ISA [DE] 315 (Revised 2019) - Überblick



III. Prüfung genereller IT-Kontrollen nach ISA [DE] 315 (Revised 2019) - Überblick

Wo sind diese Checklisten zu finden? Im Ordner "Risikobeurteilung".



III. Prüfung genereller IT-Kontrollen nach ISA [DE] 315 (Revised 2019) - Überblick

Und …
Im Ordner "Prüfungshandlungen - Sonstige".



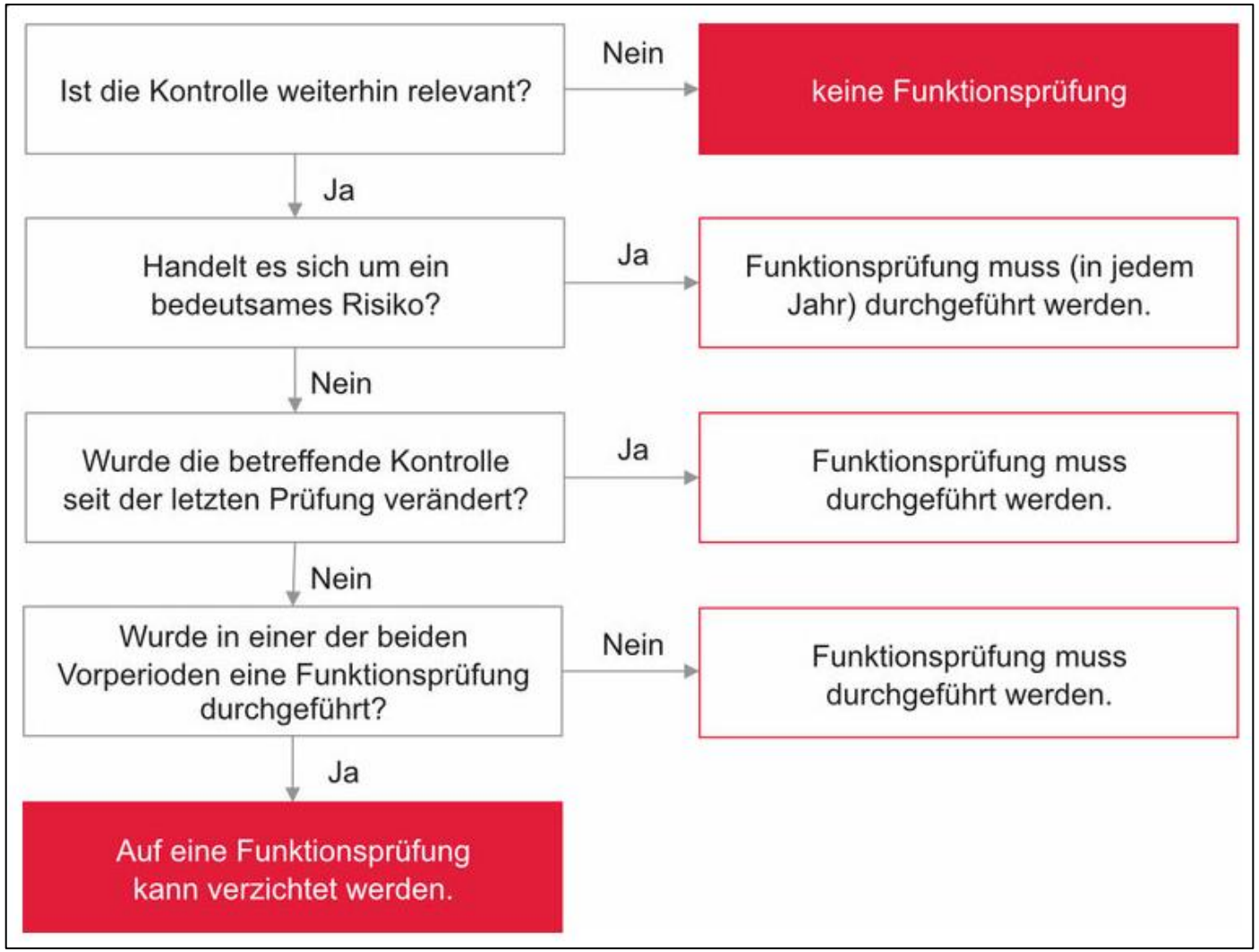
III. Prüfung genereller IT-Kontrollen nach ISA [DE] 315 (Revised 2019) - Überblick

Bearbeitung

- Jährliche Bearbeitung/Aktualisierung von 531. und ORD.PP bzw. 531.ORD.MIN
- Jährliche Aktualisierung von 531.KPL
- Jährliche Neubewertung der im Vorjahr identifizierten Risiken aus dem Einsatz von IT
- die Durchführung von Funktionsprüfungen bestimmt sich nach den Vorgaben des ISA [DE] 330.8 ff. Dies betrifft:
  - IT-gestützte Kontrollen in den Prozessen (Kontrollen der Informationsverarbeitung)
  - Report-Kontrollen
  - Generelle IT-Kontrollen

III. Prüfung genereller IT-Kontrollen nach ISA [DE] 315 (Revised 2019) - Überblick

Vorgaben in
ISA [DE] 330
Tz 13 und 14



III. Prüfung genereller IT-Kontrollen nach ISA [DE] 315 (Revised 2019) - Überblick

Exkurs: Funktionsprüfungen (ISA [DE] 330)

- Art (A5)
  - Inaugenschein-/ Einsichtnahme
  - Beobachtung
  - **Befragung (reicht alleine nicht aus, muss kombiniert werden, A26)**
  - Bestätigung
  - Nachrechnen
  - Nachvollzug
- Umfang (A28) => höherer Umfang bedeutet mehr Sicherheit
  bei automatischen Kontrollen reicht ein Test-of-One
- Funktionsprüfung und Einzelfallprüfung für denselben Geschäftsvorfall kann gleichzeitig erreicht werden (sog. „Dual-Purpose-Test“) (A23)

IV. Bestimmung der Komplexität – 531.KPL

IV. Bestimmung der Komplexität – 531.KPL

Abschlussprüfer muss ein Verständnis der Struktur und der **Komplexität der IT-Umgebung** des Unternehmens gewinnen. ➔ ISA [DE] 315 (Revised 2019).A56

- Eine Übersicht über Bestimmung der Komplexität enthält die Anlage 5 zum ISA
- In Anlage 5 werden verschiedene Skalierungsmöglichkeiten in Abhängigkeit der Komplexität beschrieben
- Die Checkliste 531.KPL basiert auf der Tabelle aus Anlage 5

IV. Bestimmung der Komplexität – 531.KPL

Die Checkliste 531.KPL wird wie folgt angewendet:

- Bei jedem Merkmal ist eine **individuelle Einschätzung** abzugeben, ob es nicht komplex, mäßig komplex oder komplex ausgeprägt ist
- Entsprechende Informationen können dokumentiert und mit einer **Referenz** versehen werden
- Beim **Gesamturteil** zählt nicht etwa die höchste Summe der einzelnen Urteile, sondern es ist individuell abzuwägen. Somit sind einzelne Urteile mit "komplex" unschädlich. Wird jedoch ein deutlich überwiegender Anteil der Merkmale mit "komplex" eingestuft, so ist eine Gesamtbeurteilung als komplex zu erwägen.
- Im Zweifel muss eine **Abstimmung** mit dem auftragsverantwortlichen Wirtschaftsprüfer erfolgen

IV. Bestimmung der Komplexität – 531.KPL

Kategorien	Nr.	Merkmale	Nicht-komplexer Standard Software	Mittelgrosser und mäßig komplexer Standard Software oder IT Anwendungen	Großen oder komplexen IT Anwendungen (z.B. ERP Systeme)	Bewertung	Bemerkungen/Erläuterungen
Ausmaß der Automatisierung und Nutzung von Daten	1.1	Ausmaß der automatisierten Verarbeitungsverfahren und die Komplexität dieser Verfahren, einschließlich, ob es eine hochautomatisierte papierlose Verarbeitung gibt	nicht zutreffend	nicht zutreffend	Umfangreich und häufig komplexe automatisierte Verfahren mit hochtechnischer papierloser Verarbeitung (Dokumenten-archivierungssystem)	**mäßig komplex**	keine automatisierte Verarbeitung, ersetzendes Scannen ist seit 1.1.2023 eingerichtet, digitale Rechnungsprüfung seit 1.4.2023; tlw. X-Rechnung (Versorger) und Rechnungserkennung über Aareon Rechnungsportal
	1.2	Ausmaß, in dem sich die Einheit auf systemgenerierte Berichte bei der Verarbeitung von Informationen verlässt	Einfache automatisierte Berichtslogik	Einfache relevante automatisierte Berichtslogik	Komplexe automatisierte Berichtslogik, Report-Writer Software	**mäßig komplex**	div. Auswertungen (bspw. Anbu, Mieten etc.), nicht hoch komplex
	1.3	Wie die Daten eingegeben werden (d.h. manuelle Eingabe, Eingabe durch Mieter oder Lieferanten oder Laden aus Datei)	Manuelle Dateneingaben	Geringe Anzahl von Dateneingaben oder einfache Schnittstellen	Große Anzahl von Dateneingaben oder komplexe Schnittstellen	**mäßig komplex**	Dateneingaben sind tlw. manuell, zunehmend digital
	1.4	Wie die IT die Kommunikation zwischen Anwendungen, Datenbanken oder anderen Aspekten der IT-Umgebung intern und extern, sofern angemessen, durch Systemschnittstellen erleichtert	Keine automatisierten Schnittstellen (ausschließlich manuelle Eingaben)	Geringe Anzahl von Dateneingaben oder einfache Schnittstellen	Große Anzahl von Dateneingaben oder komplexe Schnittstellen	**mäßig komplex**	vgl. 1.3
	1.5	Volumen und Komplexität von Daten in digitaler Form, die vom Informationssystem verarbeitet werden, einschließlich ob Unterlagen des Rechnungswesens oder andere Informationen in digitaler Form gespeichert werden sowie der Speicherort	Geringes Volumen von Daten oder einfache Daten, die manuell verifiziert werden können; Daten lokal verfügbar	Geringes Volumen von Daten oder einfache Daten	Großes Volumen von Daten oder komplexe Daten; Data Warehouses; Nutzung von internen oder externen IT-Dienstleistern (z.B. externe Speicherung oder Hosting von Daten)	**mäßig komplex**	Datenvolumen überschaubar, Auslagerung Infrastruktur (IaaS); Software wird selbst administriert, aber nichts programmiert, nur einfache Updates

IV. Bestimmung der Komplexität – 531.KPL

Kategorien	Nr.	Merkmale	Nicht-komplexer Standard Software	Mittelgrosser und mäßig komplexer Standard Software oder IT Anwendungen	Großen oder komplexen IT Anwendungen (z.B. ERP Systeme)	Bewertung	Bemerkungen/Erläuterungen
Mit den IT-Anwendungen und der IT-Infrastruktur verbundene Sachverhalte	2.1	Art der Anwendung (z.B. eine Standard-Anwendung mit geringen oder keinen Anpassungen oder eine hochgradig angepasste oder hochintegrierte Anwendung, die gekauft und angepasst oder intern entwickelt sein kann)	Gekaufte Anwendung mit geringen oder keinen Anpassungen	Gekaufte Anwendung, einfaches Altsystem oder Low-End-ERP Anwendungen mit geringen oder keinen Anpassungen	Kundenspezifisch entwickelte Anwendungen oder komplexere ERP mit bedeutsamen Anpassungen	**mäßig komplex**	Standardsystem Wodis Yuneo und Maareon
	2.2	Komplexität der Art der IT- Anwendungen und die zugrunde liegende IT-Infrastruktur	Kleine einfache Laptop- oder Client-Server-basierte Lösung	Ausgereifter und stabiler Großrechner, kleiner oder einfacher Client-Server, Software-as-a-Service Cloud	Komplexer Großrechner, großer oder komplexer ClientServer, webbasiert, Infrastructure-as-a-Service Cloud	**komplex**	Systeme sind an Dienstleister ausgelagert (IaaS)
	2.3	Ob es externes Hosting oder IT-Auslagerung gibt	Wenn ausgelagert, kompetenter, ausgereifter und erprobter Anbieter (z.B. Cloud-Anbieter, Rechenzentrum)	Wenn ausgelagert, kompetenter, ausgereifter und erprobter Anbieter (z.B. Cloud-Anbieter, Rechenzentrum)	Kompetenter, ausgereifter, erprobter Anbieter für bestimmte Anwendungen und neuer oder Start-Up Anbieter für andere	**nicht komplex**	erfahrene Dienstleister
	2.4	Ob die Einheit neu entstehende Technologien nutzt, die ihre Rechnungslegung beeinflussen	Keine Nutzung von neu entstehenden Technologien	Beschränkte Nutzung von neu entstehenden Technologien in einigen Anwendungen	Gemischte Nutzung von neu entstehenden Technologien über Plattformen hinweg	**nicht komplex**	nicht wirklich

IV. Bestimmung der Komplexität – 531.KPL

Kategorien	Nr.	Merkmale	Nicht-komplexer Standard Software	Mittelgrosser und mäßig komplexer Standard Software oder IT Anwendungen	Großen oder komplexen IT Anwendungen (z.B. ERP Systeme)	Bewertung	Bemerkungen/Erläuterungen
Mit IT-Prozessen verbundene Sachverhalt	3.1	Das in die Wartung der IT-Umgebung eingebundene Personal (Anzahl und Fähigkeitsniveau der IT-Support Ressourcen, die die Sicherheit und Änderungen in der IT-Umgebung verwalten)	Wenig Personal mit beschränkten IT-Kenntnissen zur Durchführung von Anbieter-Upgrades und zur Verwaltung des Zugriffs	Begrenztes Personal mit IT-Kenntnissen / begrenztes für IT zweckbestimmtes Personal	Zweckbestimmte IT-Abteilungen mit sachkundigem Personal, einschließlich Programmierungskenntnissen	**nicht komplex**	nur die Administration der Zugänge wird selbst verwaltet, ansonsten alles ausgelagert
	3.2	Komplexität der Prozesse zur Verwaltung von Zugriffsrechten	Einzelne natürliche Person mit Administratorenrechten verwaltet Zugriffsrechte	Wenige natürliche Personen mit Administratorenrechten verwalten Zugriffsrechte	Komplexe von der IT-Abteilung verwaltete Prozesse für Zugriffsrechte	**nicht komplex**	ein Admin, Rest machen Dienstleister
	3.3	Komplexität der Sicherheit über die IT-Umgebung, einschließlich Anfälligkeit der IT-Anwendungen, Datenbanken und anderer Aspekte der IT-Umgebung für Cyberrisiken, insbesondere wenn es webbasierte Geschäftsvorfälle oder Geschäftsvorfälle gibt, die in externe Schnittstellen eingebunden sind	Einfacher lokaler Zugriff ohne externe webbasierte Elemente	Einige webbasierte Anwendungen mit hauptsächlich einfacher, rollenbasierter Sicherheit	Mehrere Plattformen mit webbasiertem Zugriff und komplexen Sicherheitsmodellen	**mäßig komplex**	Yuneo ist webbassiert, Hosting Server RZ IBH
	3.4	Ob Programmänderungen an der Weise, wie Informationen verarbeitet werden, vorgenommen wurden, und das Ausmaß solcher Änderungen während des Zeitraums	Standard-Software ohne installierten Quellcode	Einige kommerzielle Anwendungen ohne Quellcode und andere ausgereifte Anwendungen mit einer geringen Anzahl an einfachen Änderungen, traditioneller Lebenszyklus der Systementwicklung	Neue oder große Anzahl an komplexen Änderungen, mehrere Entwicklungszyklen jedes Jahr	**nicht komplex**	Standardsystem Wodis Yuneo und Maareon
	3.5	Ausmaß der Änderung innerhalb der IT Umgebung (z.B. neue Aspekte der IT Umgebung oder bedeutsame Änderungen in den IT Anwendungen oder der zugrunde liegenden IT Infrastruktur)	Änderungen beschränkt auf Versionen-Upgrade von Standard-Software	Änderungen bestehen aus Upgrades von Standard-Software, ERP Versionen Upgrades oder Altsystemerweiterungen	Neue oder große Anzahl an komplexen Änderungen, mehrere Entwicklungszyklen jedes Jahr, erhebliche ERP Anpassungen	**nicht komplex**	einfache Udpadetes werden selbst vorgenommen, bzw. von Dienstleistern eingespielt ([redacted]für Windows etc., Aareon für Wodis)
	3.6	Ob es während des Zeitraums wichtige Datenkonvertierungen gab und, wenn dies zutrifft, die Art und Bedeutsamkeit der vorgenommenen Änderungen sowie wie die Konvertierung vorgenommen wurde.	Vom Anbieter zur Verfügung gestellte Software-Upgrades; keine Datenkonvertierungs-funktionen für Upgrades	Kleinere Versions Upgrades für Standard Softwareanwendungen, bei denen nur ein begrenzter Teil der Daten konvertiert wird	Größere Versions-Upgrade, neues Release, Plattformwechsel	**nicht komplex**	nur kleinere Updates bzw. Updrade welche durch Dienstleister Aareon bereitgestellt werden

IV. Bestimmung der Komplexität – 531.KPL

Kategorien	Nr.	Merkmale	Nicht-komplexer Standard Software	Mittelgrosser und mäßig komplexer Standard Software oder IT Anwendungen	Großen oder komplexen IT Anwendungen (z.B. ERP Systeme)	Bewertung	Bemerkungen/Erläuterungen
Ergebnis der Komplexitäts beurteilung	Hinweis zur Bearbeitung: Bei jedem Merkmal ist eine individuelle Einschätzung abzugeben, ob es nicht komplex, mäßig komplex oder komplex ausgeprägt ist. Entsprechende Informationen können dokumentiert und mit einer Referenz versehen werden. Beim Gesamturteil zählt nicht etwa die höchste Summe der einzelnen Urteile, sondern es ist individuell abzuwägen. Somit sind einzelne Urteile mit "komplex" unschädlich. Wird jedoch ein deutlich überwiegender Anteil der Merkmale mit "komplex" eingestuft, so ist eine Gesamtbeurteilung als komplex zu erwägen. Im Zweifel muss eine Abstimmung mit dem auftragsverantwortlichen Wirtschaftsprüfer erfolgen. Hinweis zum Ergebnis: Bei nicht komplex, nicht komplex bis mäßig komplex und bei mäßig komplexen Systemen ist 531.ORD.MIN als Pflichtdokument zu bearbeiten. Bei komplexen Systemen sind 531. und ORD.PP als Pflichtdokumente zu bearbeiten. Der Risiko- (520E) und Kontrolldialog (540) sind im Rahmen der IT-Prüfung immer zu bearbeiten.				**nicht bis mäßig komplex**	Systeme sind an Dienstleister ausgelagert (IaaS), als Software wird ein Standardsystem verwendet

IV. Bestimmung der Komplexität – 531.KPL

Die Checkliste 531.KPL wird wie folgt angewendet:

- Bei nicht komplex bis mäßig komplex und bei mäßig komplexen Systemen ist 531.ORD.MIN als Pflichtdokument zu bearbeiten
- Bei komplexen Systemen sind 531. und ORD.PP als Pflichtdokumente zu bearbeiten
- Der Risiko- (520E) und Kontrolldialog (540) sind im Rahmen der IT-Prüfung immer zu bearbeiten

Ausnahmen:

Im Berichtsjahr erfolgte eine Systemumstellung (mit Datenmigration) - dann ist nicht nur die Migration zu prüfen, sondern auch die Dokumente 531. und ORD.PP als Pflichtdokumente zu bearbeiten ➔ Siehe Einleitung zu 531.ORD.MIN

IV. Bestimmung der Komplexität – 531.KPL

Exkurs Migration von ERP-Systemen Wodis Sigma/Wodis Yuneo:

- Bei der Umstellung von Wodis Sigma auf Wodis Yuneo handelt es sich nicht um eine klassische Migration, sondern eher um ein Upgrade (keine Änderungen an der Datenbank)
- Aber: Berechtigungskonzept und digitale Prozesse (bspw. Rechnungsworkflow etc.) müssen neu aufgesetzt werden. => hier liegt das Risiko
- Aareon führt „Readyness Check“ hinsichtlich inkonsistenter Datensätze durch, sollte angefordert werden.

Hinweis:

Bei einer Umstellung von Wodis Sigma auf Wodis Yueno muss nicht grundsätzlich von einem hohen Risiko ausgegangen werden und 531. ausgefüllt werden. Mit einer entsprechenden Begründung kann auch 531.ORD.MIN hinreichend sein. (mit WP besprechen)

IV. Bestimmung der Komplexität – 531.KPL

Skalierungsmöglichkeiten gemäß Anlage 5 (Tz 15) – nicht bis mäßig komplexe IT-Systeme

- Weniger aus dem IT-Einsatz resultierende Risiken, daher Bearbeitung der vorgeschlagen IT-Risken
- Weniger Stützung auf IT-gestützte Kontrollen
- Mehr aussagebezogene Prüfungshandlung
- Weniger Stützung auf Report-Kontrollen, da das Management, obwohl es bei seinen Kontrollen systemgenerierte Berichte nutzt, sich nicht auf diese Berichte verlässt. Stattdessen stimmt es die Berichte mit der Dokumentation in Papierform/Excel ab und verifiziert die Berechnungen in den Berichten

IV. Bestimmung der Komplexität – 531.KPL

Skalierungsmöglichkeiten gemäß Anlage 5 (Tz 15) – komplexe IT-Systeme

- Mehr aus dem IT-Einsatz resultierende Risiken, daher ggf. mehr Risiken identifizieren
- Eher Stützung auf IT-gestützte Kontrollen und generelle IT-Kontrollen
- Schwierig Vollständigkeit und Genauigkeit der Daten mit Hilfe aussagebezogener Prüfungshandlung zu prüfen

V. Anforderungsliste

V. Anforderungsliste

A – Allgemeine IT-Risiken		
Anforderung	**Dokumentation/Beispiel(e)**	**Erledigt**
1. Überblick über das IT-System	Liste der eingesetzten Software (i.W. mit Bezug zum ERP-System, Archivsystem), aktuelle Netzwerkübersicht	
2. IT-Richtlinien	Sicherheitsrichtlinien, IT-Strategie, Arbeits- und Dienstanweisungen mit IT-Bezug	
3. Schulungen	Nachweise über Datenschutz- und IT-Sicherheitsschulungen	
4.	Aktuelles Softwaretestat (vollständiger Bericht)	
5.	Verträge über Softwareauslagerungen, SaaS etc. (Neuverträge, Vertragsänderungen)	
6.	Aktuelle Liste der IT-Verantwortlichkeiten (Name, Aufgabe, E-Mail-Adresse und Telefonnummer)	

B – Risiken des Datenverlustes (RIT01)	
Anforderung	**Dokumentation/Beispiel(e)**
1. Datensicherung und Datenwiederherstellung (KIT01)	***Wie ist die Datensicherung konzipiert und wie wird sie umgesetzt?*** Backupkonzept, Protokolle, Screenshots oder E-Mails, die erfolgreiche Datensicherungen belegen; Nachweise über die Auslagerung von Backups, z. B. Verträge mit Cloud-Anbietern oder Dokumentation über physische Sicherungsmedien
2. Sicherheitsmaßnahmen IT-Infrastruktur (KIT06)	***Wie werden die Server vor Schäden und unbefugtem Zugriff geschützt?*** Fotos von Serverräumen (Zutrittsschutz Serverräume und -schränke, Klimaanlagen, Rauchmelder)

C – Risiken der Datenmanipulation (RIT02)	
Anforderung	**Dokumentation/Beispiel(e)**
1. Zugriffsschutz (KIT02)	***Besteht eine dokumentierte Passwortrichtlinie und wie ist diese in Windows/im ERP-System umgesetzt?*** Passwortrichtlinien (dokumentierte Vorgaben und systemseitige Einstellungen – Screenshot Passwortrestriktionen Windows Domäne und ERP-System)
2. Berechtigungskonzept (KIT03)	***Welche Berechtigungen sind eingerichtet und wie sind die Verantwortlichkeiten zur Anlage/Änderung/Löschung verteilt?*** Übersicht der Benutzerrollen und zugehörigen Berechtigungen (z. B. Screenshots aus dem ERP-System), Berechtigungen für elektronische Prozesse im Bereich Auftragsvergabe und Rechnungsprüfungs- und -freigabeverfahren (Zuordnung Mitarbeiter zu Prozessschritten) sowie Zahlungsverkehr; Dokumentation zur Vergabe, Änderung und Entzug von Zugriffsrechten (z. B. bei Mitarbeiterwechsel), Nachweis einer durchgeführten Berechtigungsinventur
3. Einschaltung der systemseitigen Stammdatenänderungs-protokollierung (KIT04)	***Welche Protokollierungen werden mit dem ERP-System durchgeführt?*** Systemseitige Protokollierung von Veränderungen bspw. bei Geschäftspartnern wie Kreditoren, Mietern, oder Anlage von FIBU- Konten. Screenshots eines Stammdatenänderungsprotokolls (Änderungshistorie eines Stammdatensatzes wie z.B. Mietvertrag im ERP-System).

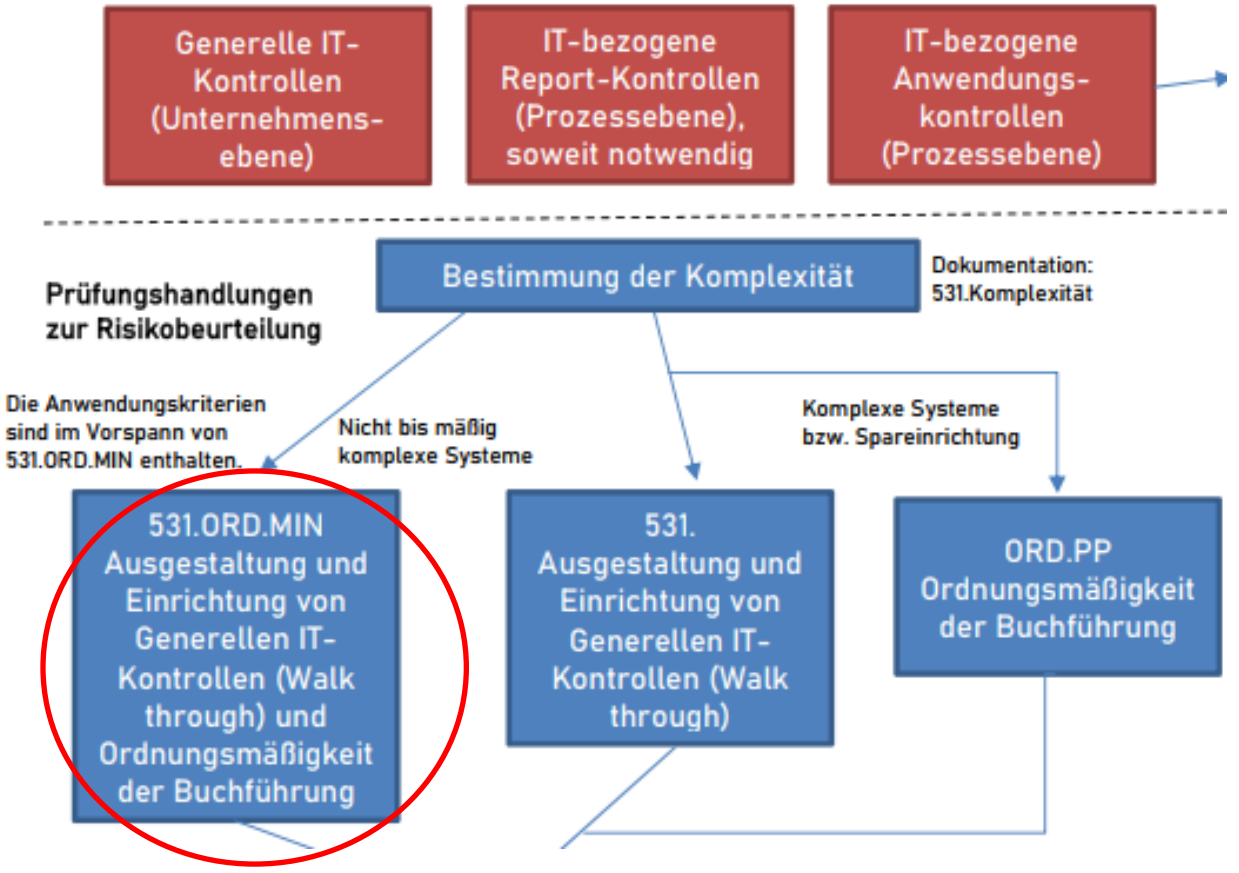
V. Anforderungsliste

D – Risiken falscher Datenverarbeitung (RIT03)	
Anforderung	**Dokumentation/Beispiel(e)**
1. Update-Prozess (KIT05)	***Welche wesentlichen Updates/Änderungen der eingesetzten Software wurden vorgenommen?*** Änderungsprotokolle oder Dokumentation wesentlicher Updates im Berichtsjahr, z.B. Screenshots der eingesetzten Versionsstände des ERP-Systems (vor allem bei In-house-Software), elektr. Archiv, Windows
2. Sicherheitsmaßnahme Netzwerk (KIT07)	***Welche Maßnahmen zur Netzwerksicherheit sind konzipiert und angewendet?*** Screenshots der aktuellen Version von Firewall und Virenschutz, Art der Verschlüsselung der VPN-Verbindung bei externem Zugriff durch Dienstleister, Art der Verschlüsselung von mobilen Endgeräten, Verwendung eines Mobile Device Managements (MDM), Screenshots vom Monitoring der IT-Systeme
3. Überprüfung Datenverarbeitung und Datenübernahme (KIT08)	***Welche Schnittstellen bestehen zum ERP-System und wie wird die korrekte Übernahme der Daten kontrolliert? Welche automatisierten Prüfungen des ERP-Systems bestehen und werden verwendet?*** Nachweis über integrierte Kontrollsysteme wie Plausibilitätsprüfungen oder Fehlerprotokolle (bspw. Sollstellung, Lastschriftlauf, Erstellung Beko-Abrechnung, Mussfeld-Vorgaben im Anlagevermögen) und Dokumentation dieser. Vier-Augen-Prüfung bei Stammdatenänderungen (bspw. Kreditoren), Screenshots einer Freigabemaske Verarbeitungsprotokolle und Schnittstellenprotokolle, vor allem bei Einsatz von weiteren Drittsystemen in Verbindung mit ERP-System (bspw. Handwerkerkopplung, vorgelagerten Systemen zur Rechnungsprüfung oder Warenwirtschaftssystemen)
4. Notfallplan (KIT09)	***Welches Vorgehen ist bei IT-Notfällen dokumentiert?*** Dokumentation der durchzuführenden Maßnahmen und Ansprechpartner im Falle eines IT-Notfalls, Protokolle über Tests des Notfallplans, z.B. Datenwiederherstellungen

E – Mit (IT-) Prozessen verbundene Risiken	
Anforderung	**Dokumentation/Beispiel(e)**
Dokumentation/Beschreibung von elektronischen Workflows	***Welche elektronischen Workflows sind eingerichtet und dokumentiert?*** - Elektronische Archivierung - Elektronische Auftragsvergabe - Elektronisches Rechnungsprüfungs- und Freigabeverfahren inkl. Zahlungsfreigabe, Beispieldokumentation in Form von Screenshots

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

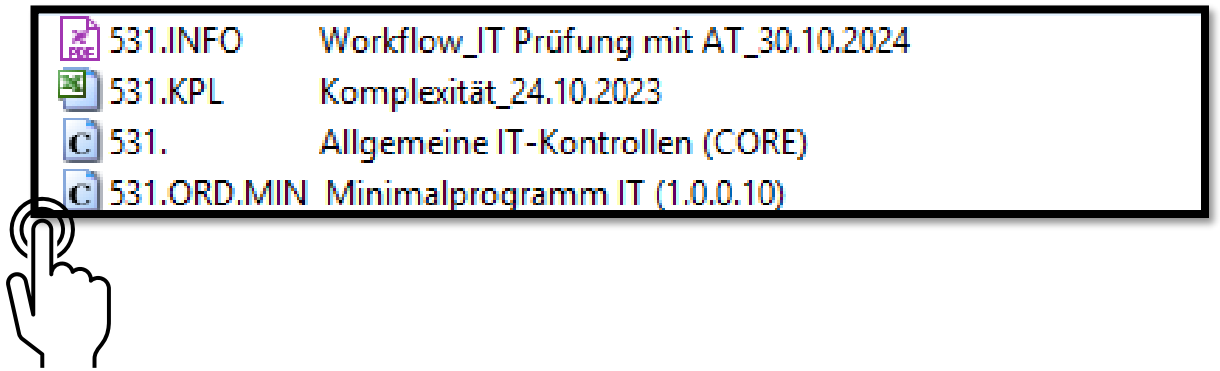


VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

Was ist die 531.ORD.MIN eigentlich?

- 531.ORD.MIN ist eine Zusammenstellung der wichtigsten Fragen aus 531. und ORD.PP

  ➔ Die Bearbeitung von 531. entfällt damit ersatzlos
- Es ist nur ein Teil des RET-Ansatzes



VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Kriterien für die Anwendung von 531.ORD.MIN

Diese Checkliste ist bei nicht bis mäßig komplexen IT-Systemen (gemäß Komplexitätseinschätzung in 531.KPL) anzuwenden und **ersetzt die Checklisten 531 sowie das Prüfprogramm ORD.PP** unter den folgenden Voraussetzungen:

- Risikobewusstsein und Risikokultur in Bezug auf die IT sind im Unternehmen ausgeprägt (bisherige Erfahrungen)
- Einsatz einer wohnungswirtschaftlichen Standardsoftware (ggf. Testat vorhanden)
- System ist als verlässlich bekannt und wurde bei Einführung im üblichen Maße konfiguriert
- der Quellcode kann vom Unternehmen nicht verändert werden
- die Software bearbeitet ein für Wohnungsunternehmen übliches Datenvolumen
- die Standardsoftware läuft in einem Rechenzentrum oder als Inhouse-System mit "externer" Systembetreuung

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Kriterien für die Anwendung von 531.ORD.MIN

- keine bis wenige Schnittstellen (d.h. zu externen Systemen, die rechnungslegungsrelevante Daten in das Buchhaltungssystem übertragen)
- keine Spareinrichtung
- keine oder unwesentliche Beanstandungen aus der Vorjahresprüfung (IT/Buchführung)

Hinweis: Die Kriterien gelten nicht kumulativ

➔ Soweit einzelne Kriterien nicht erfüllt werden, ist abzuwägen, ob dieses Dokument noch angewendet werden kann (Eine solche Entscheidung ist zu begründen)

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Grundlagen

Prüfung der vom Unternehmen eingerichteten Maßnahmen zur Sicherung der Vollständigkeit und Verfügbarkeit der Daten und Programme

➔ Weitere Hinweise und Informationen in **IDW RS FAIT 1 Tz 85 f**

Exkurs:

IDW RS FAIT 1: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Grundlagen

Bspw. Gefahren bei fehlenden oder ungenügenden Datensicherungs- und Auslagerungsverfahren:

- Betriebsstörungen
- Betriebsausfall
- Ungenügende Datenrekonstruktion
- Überschreiben von Daten
- Datenverlust
- Buchungsstau



Die Ordnungsmäßigkeit der Buchführung ist gefährdet

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

1.	**Beschreibung** Wurden die allgemeinen Informationen zur IT-Umgebung der Einheit (einschließlich Hardware und Software) zusammengefasst?	Dokumentiert in	DAK 01.07.2025	531.ORD.MIN-

Exkurs ISA 315.12g

4.17. Was versteht man unter der IT-Umgebung der Einheit?

ISA [DE] 315 (Revised 2019), Tz. 12(g), definiert die **IT-Umgebung** als IT-Anwendungen und unterstützende IT-Infrastruktur sowie IT-Prozesse und Personal, die in diejenigen Prozesse eingebunden sind, die eine Einheit zur Unterstützung des Geschäftsbetriebs und zur Erreichung von Geschäftsstrategien einsetzt.

(i) Eine **IT-Anwendung** ist ein Programm oder eine Reihe von Programmen, die für die Initiierung, Verarbeitung, Aufzeichnung und Berichterstattung von Geschäftsvorfällen oder Informationen eingesetzt werden. IT-Anwendungen schließen Data Warehouses und Report-Writer ein.

(ii) Die **IT-Infrastruktur** besteht aus dem Netzwerk, Betriebssystemen und Datenbanken sowie der zugehörigen Hardware und Software.

(iii) Die **IT-Prozesse** sind die Prozesse der Einheit zur Verwaltung des Zugriffs auf die IT-Umgebung, der Programmänderungen oder der Änderungen der IT-Umgebung und des IT-Betriebs.

Zur weiteren Konkretisierung von Kontrollen der IT-Umgebung wird auf Anlage 6 des ISA [DE] 315 (Revised 2019) verwiesen.

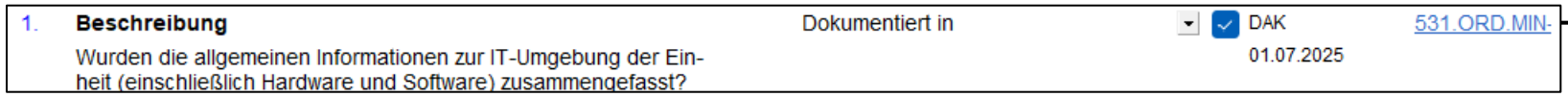
4.2.1. Verständnis von der Einheit, ihrem Umfeld und den maßgebenden Rechnungslegungsgrundsätzen (Vgl. Tz. A50–A55)

Der Abschlussprüfer hat Prüfungshandlungen zur Risikobeurteilung durchzuführen, um ein Verständnis zu erlangen

(a) von den folgenden Aspekten der Einheit und ihres Umfelds:

(i) der Organisationsstruktur, Eigentümerschaft sowie Führung und Überwachung der Einheit sowie deren Geschäftsmodell, einschließlich des Umfangs, in dem das Geschäftsmodell den IT-Einsatz integriert; (Vgl. Tz. A56–A67)

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)



Verlinkung mit den zu Grunde liegenden Unterlagen und Dokumenten!

1. Beschreibung

Die Gesellschaft betreibt ein eigenes IT-System [Windows Server 2025; Clients Win 11] mit ca. 20 IT-Arbeitsplätzen)

Als ERP-System wird Wodis Yuneo (Version xx.xx) der Fa. Aareon als SaaS eingesetzt und im Rechenzentrum der Fa. Aareon in Mainz gehostet.

die IT-Betreuung erfolgt intern durch einen Mitarbeiter; des Weiteren werden ext. Dienstleister herangezogen; Aareon - Software; Fa. XY (Hardware/Software)
=> entsprechende Verträge liegen vor.

Laufende Updates werden durch die Dienstleister zur Verfügung gestellt und eingespielt.

Die Lohnbuchhaltung wird inhouse vorbereitet und durch ein Steuerbüro durchgeführt (Datenaustausch per PDF). Entsprechende Verträge liegen vor.

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

2.	**Anwendbarkeit** Liegen die in der Einführung beschriebenen Voraussetzungen für die Anwednung des Minimalprüfprogramms vor?	Dokumentiert in	☑ DAK 01.07.2025	531.KPL 531.ORD.MIN- 531.ORD.MIN-	

→ Verlinkung mit den zu Grunde liegenden Unterlagen und Dokumenten!

2. Anwendbarkeit

ja, liegen vor, Standardsoftware, Testat liegt vor, EDV-Betreuung i.W. durch ext. Dienstleister

Vertrag mit IT-Systembetreuuer liegt vor, ebenso liegen für alle wesentlichen Softwareprodukte (bspw. auch für das ERP-System Wodis Yuneo) entsprechende Supportverträge mit den Anbietern vor.

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

3.	**IT-Rollen und -Verantwortlichkeiten** Gibt es Richtlinien und Verfahren, mit denen IT-Rollen und -Zuständigkeiten, -Berichterstellung, -Richtlinien, -Standards und -Verfahren definiert werden?	Dokumentiert in	DAK 01.07.2025	KIT03 KIT02-KIT03_ KIT03_2	! (RIT02) Datenmanipulation (KIT03) Berechtigungskonzept

Verknüpfung mit Risiko

3. IT-Rollen und -Verantwortlichkeiten

Die Gesellschaft hat Benutzerrichtlinien erlassen und eine Funktionstrennung eingerichtet. Bzgl. der Verantwortlichkeit für den IT-Bereich im Unternehmen vgl. Ref. (Organigramm)

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT03	Einrichtung eines Berechtigungskonzeptes	RIT02	540.	gesonderte Dokumentation mit Referenz

➔ **Übersicht von Risiken aus dem Einsatz von IT – vgl. VII. Zuordnung**

➔ **Vgl. XI. Funktionsprüfungen der 9 allg. IT-Kontrollen KIT03**

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)



4. Backup

Datensicherung erfolgt täglich, Auslagerung über NAS (netzwerkgebundenes Speichersystem) in Nebengebäude (andere Brandschutzzone). Des Weiteren liegt ein Datensicherungskonzept vor, dieses ist jedoch in Teilen veraltet und sollte aktualisiert werden.

oder

An Dienstleister ausgelagert (Cloud) vgl. Rahmenvertrag Cloud Dienste. !Cloud Sicherung sollte verschlüsselt sein!

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT01	Kontrolle der ordnungsmäßigen Datensicherung und Datenwiederherstellung	RIT01	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

4. Backup

a.	Sind angemessene Richtlinien und Verfahren für das Sichern von Systemen, Anwendungen, Daten und Dokumentationsunterlagen vorhanden?	Dokumentiert in	DAK 01.07.2025	! (RIT01) Datenverlust (KIT01) Datensicherung und Datenwiederherstellung

Ja, vgl. KIT01_1

b.	Werden die Richtlinien regelmäßig geprüft und sind sie ordnungsgemäß dokumentiert?	Dokumentiert in	DAK 01.07.2025

Ja, aber nur teilweise, die Doku ist veraltet und müsste mal wieder aktualisiert werden.

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

4. Backup

Exkurs Datensicherung (1) – Fragestellungen

- Werden die Datensicherungen automatisiert durchgeführt oder muss ein Mitarbeiter die Datensicherung manuell vornehmen?
- Wird die erfolgreiche Durchführung der Datensicherung geprüft?
- Wird die Wiederherstellung einer Datensicherung regelmäßig geprüft?
- Werden Datensicherungen ausgelagert?

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

4. Backup

Exkurs Datensicherung (1) – Fragestellungen

Wie oft werden die Sicherungen durchgeführt, welche Art von Sicherung wird verwendet?

- Vollsicherung? (Regelfall)
- Snapshot? (Sicherung zu einem Zeitpunkt, nur Änderungen)
- Generationenprinzip? (Backup-Strategie um unterschiedliche Zeiträume wieder herzustellen)

Datensicherungen sollten in einen anderen Brandabschnitt ausgelagert werden!

NICHT bei Mitarbeitern zu Hause!

Datensicherungen und ein geregeltes Wiederanlaufverfahren (Notfallkonzept) sind die **Lebensversicherung** eines jeden Unternehmens!

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

4. Backup

Exkurs Datensicherung (2)

Kann mich eine Datensicherung allein immer „retten“?

➔ NEIN – Hacker können sich bei Cyberangriffen lange im Netzwerk verstecken und Schadsoftware auch in Datensicherungen einschleusen

Folge: Auch Datensicherungen können kompromittiert sein und durch einen Verschlüsselungstrojaner (Ransomware) unbrauchbar werden

Wichtig: regelmäßiger Rücksicherungstest

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

4. Backup

Exkurs Datensicherung (3)

Auslagerung (von Datensicherungen) in die Cloud – Was ist zu beachten?:

- Verschlüsselung der Übertragung und der Speicherung (Datei)
- Immutable/unveränderbare Backups (Lösch- und Überschreibungsschutz – Schutz gegen Ransomware)
- Backup vom Produktivsystem trennen
- Cloud-Anbieter prüfen (Zertifizierung, Datenschutz – keine Lagerung von Daten außerhalb der EU)
- Exit-Strategie (vertraglich klären, wie Backups bei Anbieterwechsel übertragen bzw. sicher gelöscht werden können)
- Auch bei Auslagerung sind Wiederherstellungstests wichtig!

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)



5. Fortführung des Geschäftsbetriebs

Es liegt ein Notfallkonzept vor, welches die Zuständigkeiten (Ansprechpartner bei den Dienstleistern) beschreibt. Aufgrund der geringen Komplexität des IT-Systems sind gesonderte Pläne nicht erforderlich.

Für die Datenbank sowie die Handwerkerkopplung liegen Dienstleistungsverträge vor.
Diese sehen auch angemessene Reaktionszeiten der Dienstleister vor.

Eine Beschreibung des Wideranlaufverfahrens der eigenen Server wird derzeit durch den IT-Dienstleister erstellt.

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT09	Einrichung eines IT-Notfallplans	RIT03	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

5. Fortführung des Geschäftsbetriebs

a.	Sind Pläne vorhanden, mit denen sichergestellt wird, dass kritische Geschäftsprozesse bei Unterbrechungen des normalen Geschäftsbetriebs nahtlos fortgeführt oder sofort wieder aufgenommen werden?	Dokumentiert in	DAK 01.07.2025	! (RIT03) Falsche Datenverarbeitung (KIT09) Notfallplan

Durch die vertraglichen Vereinbarungen mit den Dienstleistern geht die Geschäftsführung davon aus, das innerhalb der maximal tolerierbaren Ausfallzeit von 3-4 Werktagen die Systeme auch bei größeren Störungen wieder lauffähig zur Verfügung stehen.
Vgl. KIT09_1

b.	Werden die Richtlinien regelmäßig geprüft und sind sie ordnungsgemäß dokumentiert?	Dokumentiert in	DAK 01.07.2025

Ja, Hauptansprechpartner sind definiert, falls diese sich ändern wird dies im Notfallplan dokumentiert und den Mitarbeitern mitgeteilt, für Unternehmensgröße i.O.

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Notfallpläne (1)

- Wurden die zeitkritischen Geschäftsprozesse bzw. Anwendungen bestimmt?
- Wurden die maximalen Ausfallzeiten für die zeitkritischen GP oder Anwendungen festgelegt?
- Kann der Dienstleister diese maximalen Zeiten einhalten? – Vertraglich mit Dienstleister vereinbaren!

Achtung: Die Reaktionszeit bedeutet nicht, dass in dieser Zeit das System wieder funktionsfähig ist!

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Notfallpläne (2)

IT-Notfall-Handbuch → Stand-Mai-2022¶
¶
Bei Störungen mit Gefährdungspotential 1 "Notfall", die einen Ausfall von wichtigen Komponenten des IT-Systems zur Folge haben, leitet der EDV-Administrator bzw. sein Stellvertreter unverzüglich notwendige Maßnahmen ein.¶
¶
Mögliche Szenarien von IT-Sicherheitsvorfällen:¶
- Ausfall von IT-Systemen – komplett oder teilweise - durch:¶
  - Elementarschäden¶
  - Malware, Ransomware, Kompromittierungen (z.B. Active Directory)¶
  - Hardwareausfall¶
  - Konfigurationsfehler (z.B. fehlerhafte Patches)¶
  - Stromausfall, USV-Schaden¶
  - Ausfall Klimatisierung¶
- Ausfall internes Netzwerk¶
  - Switches, Firewalls, VPN-Verbindungen, Telefonanlage¶

Information an Geschäftsleitung:¶
- Nur Kurzinfo, ohne Anspruch auf Details¶
- Erst-Info an Mitarbeiter organisieren¶

¶
Erst-Analyse – Überblick verschaffen – Ruhe bewahren – Notizen machen¶
- Was ist vorgefallen – Wann und Wo?¶
- Welche Systeme sind betroffen (Monitoring nutzen)?¶
- Welche aktuellen Auswirkungen gibt es?¶
- Welche möglichen Ursachen kann es geben?¶
  Erste Maßnahmen zur Gefahrenabwendung abschätzen¶
- Herunterfahren der Systeme notwendig und sinnvoll?¶
  Trennung zum Internet vornehmen?¶

¶
Krisenstab bilden, Verantwortlichkeiten bestimmen, Meldekette festlegen¶
Der Krisenstab sollte sich mindestens zusammensetzen aus:¶

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Notfallpläne (3)

Regelbetrieb:

Der geordnete Regelbetrieb von IT-Anwendungen setzt dokumentierte Verfahrensabläufe für alle Bereiche des IT-Betriebes voraus.

Die zu treffenden Maßnahmen sind von der Komplexität der eingesetzten Hardware und der Netzkomponenten abhängig. Bei kleinen IT-Systemen, die aus kleinen Netzwerken bestehen, kann der Regelungsbedarf geringer sein. Die jederzeitige Verfügbarkeit des IT-Systems ist eine wesentliche Voraussetzung für die Aufrechterhaltung des Geschäftsbetriebs.

(IDW RS FAIT 1 Kapitel 4.2)

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Notfallpläne (4)

Notfallbetrieb:

Die Maßnahmen für den Notfallbetrieb ergänzen die Maßnahmen für den Regelbetrieb um organisatorische Regelungen und technische Verfahren zur Wiederherstellung der IT nach teilweisem oder vollständigem Ausfall der IT-Infrastruktur.

Es ist zwischen dem kurzfristigen Ersatz einzelner Systemkomponenten und sogenannten Katastrophen-Szenarien zu unterscheiden.

(IDW RS FAIT 1 Kapitel 4.2)

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Notfallpläne (5)

Wichtig:

- Das Wiederanlaufverfahren (Server) sollte beschrieben sein, damit auch ein fachkundiger Dritter im Notfall die Systeme neu starten kann
- Die Einrichtung eines Notfallusers ist dabei unerlässlich!
- Auf die Nutzerdaten des Notfallusers muss man auch zugreifen können – Passwörter müssen hinterlegt sein!

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

6.	**Physischer Zugriff** Ist der physische Zugang zu den Computersystemen auf autorisier-tes Personal beschränkt?	Dokumentiert in	DAK 01.07.2025	KIT06	! (RIT01) Datenverlust (KIT06) Sicherheitsmaßnahmen IT-Infrastruktur

6. Physischer Zugriff

Nur autorisiertes Personal kann auf die IT-Systeme zugreifen, Ausstattung Serverraum entsprechend der Größe des Unternehmens angemessen, vgl. Ref.

alternativ

ja, Server etc. sind komplett an Dienstleister XY ausgelagert. Bei der WBG selbst stehen nur Clients die über das Web mit dem Server beim Dienstleister verbunden sind. Für die Sicherheit der IT-Anlagen ist lt. Vertrag die Fa. XY zuständig. XY ist ISO/IEC 27001 und ISO 9001 zertifiziert. Vgl. Ref.

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT06	Sicherheitsmaßnahmen IT-Infrastruktur	RIT01, RIT02	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Physischer Zugriff

a) Es entstehen Risiken bei fehlenden oder ungenügenden physischen Sicherungsmaßnahmen:

- ➔ Diebstahl von Hardware
- ➔ Diebstahl von Daten

b) Verlust von Daten durch:

- ➔ Feuer, Wasser
- ➔ Stromausfall
- ➔ Sabotage

c) Datenmanipulation durch unautorisierte Zugriffe

! Infrastruktur wird verstärkt an Dienstleister ausgelagert! – Verantwortung trägt Unternehmen weiterhin!

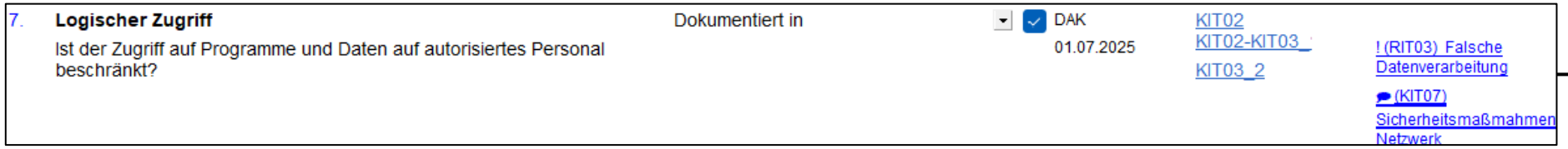
VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Physischer Zugriff

Anforderungen an einen Serverraum – normaler Schutzbedarf (gem. BSI):

- Geschlossener Sicherheitsbereich
- Unterbrechungsfreie Stromversorgung (USV)
- Notausschalter
- Überwachung Lufttemperatur und –Feuchtigkeit
- Zutrittskontrolle
- selbstschließende Tür
- Brandmeldeanlage
- Lösch- und Brandvermeidungsanlage
- Automatische Überwachung der Infrastruktur (Klima-, Strom-, USV-Anlagen, Brandmelder etc.)
- Klimatisierung
- regelmäßige Funktionstests

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)



7.	**Logischer Zugriff** Ist der Zugriff auf Programme und Daten auf autorisiertes Personal beschränkt?	Dokumentiert in	DAK 01.07.2025	KIT02 KIT02-KIT03_ KIT03_2	! (RIT03) Falsche Datenverarbeitung (KIT07) Sicherheitsmaßmahmen Netzwerk

7. Logischer Zugriff

Jeder Nutzer hat einen eigenen Zugang mit eigenem Login-Daten (auf Netzwerk- und Anwendungsebene). Keine MFA (Multi-Faktor-Authentifizierung) im Einsatz.

Keine direkte Nutzung der Server durch Benutzer, nur Admin und administrative User Aareon.

Den jeweiligen Usern sind entsprechende Berechtigungen zugeordnet (i.d.R. Gruppenrechte)

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT02	Kontrolle durch Zugriffschutz	RIT02	540.	gesonderte Dokumentation mit Referenz

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT07	Sicherheitsmaßmahmen Netzwerk	RIT03	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Logischer Zugriffskontrollen (1)

Zwei Konzepte:

1) **Minimalprinzip** (Benutzer bekommt nur die Rechte, die er benötigt)
2) **Maximalprinzip** (Benutzer bekommt die Rechte „weggenommen“, die er nicht benötigt)

Minimalprinzip ist besser, Maximalprinzip (jeder kann erst einmal ALLES ist bei kleinen Unternehmen die Regel)

Wichtig bei kleinen Unternehmen ohne umfangreiches IKS: High Level Kontrollen
Bspw. im Bereich Rechnungs- und Zahlungsfreigabe mit 4-Augen-Prinzip

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Logische Zugriffskontrollen (2)

Sicherheitsmaßnahmen Netzwerk:

- Passwortschutz
- Firewall
- Virenschutz
- regelmäßige Schulung der Mitarbeiter zu Cyberrisiken
- Verschlüsselte Kommunikation nach außen (VPN-Verbindung)
- Multi-Faktor-Authentifizierung (MFA)
- Monitoring/Überwachung der IT-Systeme
- Verschlüsselung von mobilen Endgeräten
- Mobile Device Management (MDM)
- Berechtigungssysteme
- geregeltes Updateverfahren

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Logische Zugriffskontrollen (3)

Multi-Faktor-Authentifizierung (MFA)

Merkmale

- Wissen (z. B. Passwort, PIN)
- Besitz (z. B. Token, Smartphone)
- inhärente Merkmale (z. B. biometrische Daten wie Fingerabdrücke, Gesichtserkennung)

Vorteile/Umsetzung/Empfehlung

- „Angreifer muss gleichzeitig Zugriff auf zwei Systeme haben, um erfolgreich zu sein - schwierig
- Praktische Umsetzung: Passwort und zusätzlich einen Einmalcode aus einer Authenticator-App oder per SMS
- Empfehlung: „Pflicht“ bei externem Zugriff auf die IT-Systeme (bspw. Homeoffice, Cloud-Anwendungen etc.) oder Zugriff auf sensible Firmendaten, bspw. über Microsoft etc. einfach umsetzbar

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

8.	**Kennwortverwaltung** Werden Kennwörter angemessen verwaltet, u. a. in Bezug auf folgende Aspekte: • Implementierte Kennwörter • Erzwungene regelmäßige Änderung von Kennwörtern • Kennwortänderung bei einer tatsächlichen oder mutmaßlichen Sicherheitsverletzung • Entfernen von Benutzern/Ändern von Kennwörtern bei Ausscheiden von Personen aus der Organisation	Dokumentiert in	☑ DAK 01.07.2025	KIT02 KIT02-KIT03_ KIT02_2	! (RIT02) Datenmanipulation (KIT02) Zugriffschutz

8. Kennwortverwaltung

Jeder User hat ein eigenes Kennwort (Netzwerk- und Anwendungsebene), Restriktionen sind hinterlegt und entsprechen den Empfehlungen des BSI.

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT02	Kontrolle durch Zugriffschutz	RIT02	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Kennwortverwaltung (1)

- Werden im Unternehmen Passwörter verwendet?
- Ist der Umgang mit den Passwörtern schriftlich geregelt?
- Dürfen Mitarbeiter ihr eigenes Passwort an ihre Vertretung weitergeben?
- Sind die Passwörter jedem Mitarbeiter bekannt?
- Müssen die Kennwörter Sonderzeichen enthalten?
- Beträgt die Passwortlänge mindestens 8, bei Administratoren mind. 10-12 Zeichen (Empfehlung BSI)?
- Werden für das Netzwerk und die Anwendung unterschiedliche Passwörter verwendet?
- Benutzt die Anwendung das Passwort für das Netzwerk-Login (Single Sign On)?

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Kennwortverwaltung (2)

IT-Dienstleister verwenden oft einen Benutzer (z.B. Name „Service“) für mehrere Personen. So lässt sich nicht mehr nachvollziehen, wer welche administrativen Arbeiten vorgenommen hat.

Eine Kennwortrichtlinie alleine reicht nicht aus, die Inhalte der Passwortrichtlinie sollten auch durch technische Parameter abgesichert werden.

Es sollten die Parameter von Windows und des ERP-Systems dokumentiert werden (Kennwortrichtlinie).

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Kennwortverwaltung (3)

- Müssen die Benutzer regelmäßig ihr Kennwort ändern?

  ➔ wird nicht mehr empfohlen, wichtiger sind **komplexe Kennwörter**)
- Wird eine Kennworthistorie geführt, z.B. die letzten 5 Kennwörter?
- Muss der Benutzer sein Kennwort ändern, wenn er es an seine Kollegen weitergegeben hat?
- Muss der Benutzer sein Kennwort ändern, wenn der Verdacht besteht, dass das Kennwort „gehackt“ wurde?

  ➔ **SOFORT**
- Werden nicht mehr benötigte Benutzerkonten gesperrt?

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Kennwortverwaltung (4)

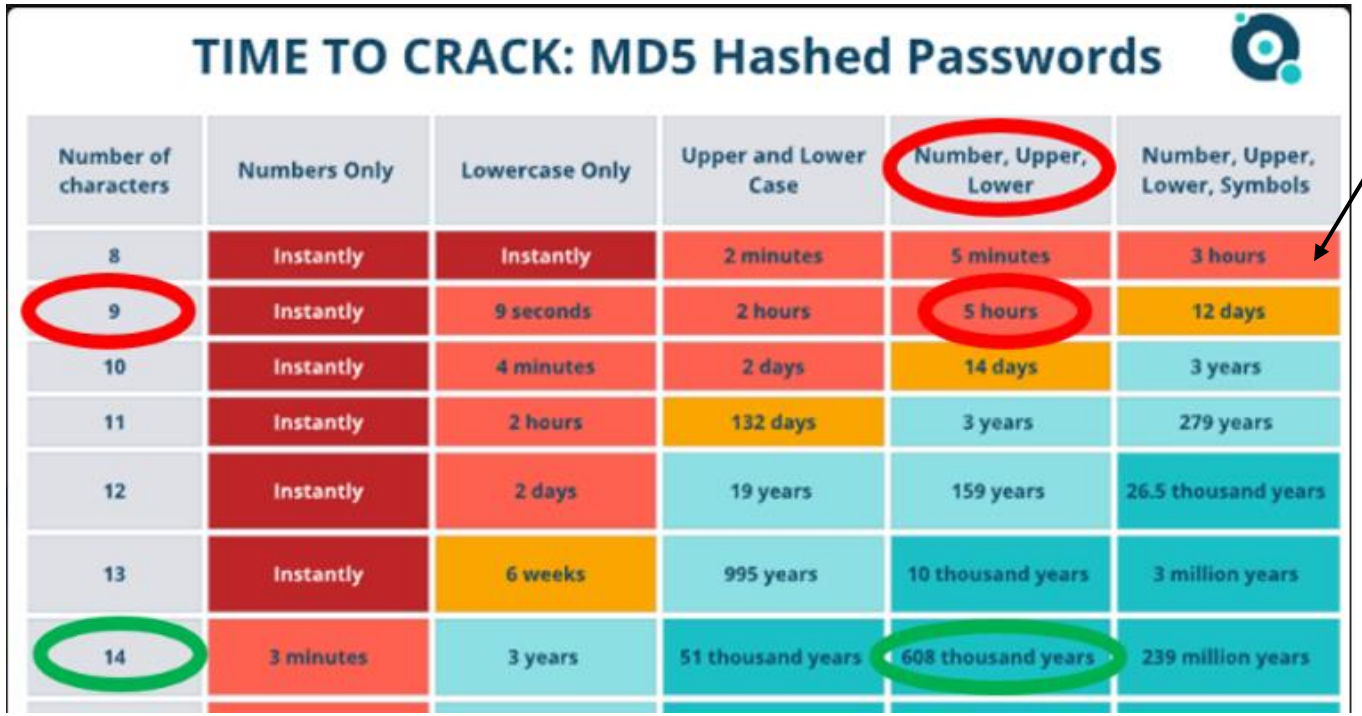
- Wenn die **Passwortlängen zu groß** sind und ein komplexes Passwort gefordert wird, sind die Mitarbeiter schneller bereit, das Passwort aufzuschreiben => Alternative: Passwortmanager



- Ist die **Passwortlänge zu kurz** (7 Zeichen oder weniger), stimmt das Passwort mit dem Benutzernamen oder Unternehmensnamen überein ist das Risiko hoch, dass das Passwort entschlüsselt wird.

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Kennwortverwaltung (4)



TIME TO CRACK: MD5 Hashed Passwords

Number of characters	Numbers Only	Lowercase Only	Upper and Lower Case	Number, Upper, Lower	Number, Upper, Lower, Symbols
8	Instantly	Instantly	2 minutes	5 minutes	3 hours
9	Instantly	9 seconds	2 hours	5 hours	12 days
10	Instantly	4 minutes	2 days	14 days	3 years
11	Instantly	2 hours	132 days	3 years	279 years
12	Instantly	2 days	19 years	159 years	26.5 thousand years
13	Instantly	6 weeks	995 years	10 thousand years	3 million years
14	3 minutes	3 years	51 thousand years	608 thousand years	239 million years

https://specopssoft.com

MFA für sicheren Schutz erforderlich!

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Kennwortverwaltung (5) - Beispiel Kennwortrichtlinie Netzwerk/Windows

Kontorichtlinien/Kennwortrichtlinien

Richtlinie	Einstellung
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwortchronik erzwingen\ngespeicherte Kennwörter	2 gespeicherte Kennwörter
Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert
Maximales Kennwortalter	0 Tage
Minimale Kennwortlänge	8 Zeichen
Minimales Kennwortalter	0 Tage

Kontorichtlinien/Kontosperrungsrichtlinien

Richtlinie	Einstellung
Kontensperrungsschwelle	5 ungültige Anmeldeversuche
Kontosperrdauer	30 Minuten
Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

9. Cybersicherheit

9.	**Cybersicherheit** Sind angemessene Kontrollen für die Ermittlung und Bewältigung von Cyberrisiken eingerichtet? Berücksichtigen Sie Folgendes: • Anti-Virus-Software • Anti-Spam-Software • Vom Management überwachte Benachrichtigungen	Dokumentiert in	DAK 01.07.2025	KIT07 KIT03 KIT05 KIT05_1	! (RIT03) Falsche Datenverarbeitung (KIT05) Update-Prozess (KIT03) Berechtigungskonzept (KIT07) Sicherheitsmaßmahmen Netzwerk	

Das Unternehmen hat ein Mehrstufiges Schutzsystem im Einsatz (Hardware-Firewall; Anti-Virenschutz-Software, Mail/SAPM-Schutz etc.) Updates erfolgen laufend automatisiert. Hinsichtlich der Cyber-Gefahren werden die Mitarbeiter auskunftsgemäß jährlich im Rahmen der Datenschutzschulung geschult. Ein Monitoring der IT-Systeme darüber hinaus erfolgt nicht. Hierzu finden nach Rücksprache mit dem GF derzeit Abstimmungen mit dem IT-Dienstleister hinsichtlich der Einrichtung eines Monitorings der Systeme statt

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT07	Sicherheitsmaßmahmen Netzwerk	RIT03	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs: Was ist Cybersicherheit?

> Als Cybersicherheit werden alle Technologien, Verfahren und Richtlinien zur Verhinderung von Cyberangriffen oder zur Minderung ihrer Auswirkungen bezeichnet. Die Cybersicherheit zielt darauf ab, Computersysteme, Anwendungen, Geräte, Daten, finanzielle Assets und Menschen vor Ransomware und anderer Malware, Phishing-Betrug, Datendiebstahl und anderen Cyberbedrohungen zu schützen.
>
> (www.ibm.com)

- **Cyberangriffe** können zu Datenverlust, Datenmanipulation und falscher Datenverarbeitung führen und somit alle IT-Risiken adressieren.
- **Cyberrisiken** können insbesondere durch KIT03 Berechtigungskonzept, KIT05 Update-Prozess und KIT07 Sicherheitsmaßnahmen Netzwerk sowie Sensibilisierung der User gemindert werden.
- Wichtig: **Monitoring der Systeme** (ggf. Auslagerung auf Dienstleister) – vgl. 531. Frage Nr. 11

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

10.	**Änderungsprozess** Ist ein formal genehmigtes und überwachtes Verfahren für die Verwaltung von Änderungen an Hardware, Programmen, Datenbanken und Betriebssystemen vorhanden?	Dokumentiert in	☑ DAK 01.07.2025	KIT05 KIT05_1	! (RIT03) Falsche Datenverarbeitung (KIT05) Update-Prozess

10. Änderungsprozess

Änderungen an der Software nimmt nur der Dienstleister in Form von Updates vor (Fa. XY) vor, Änderungen Hardware nur in Abstimmung mit dem Geschäftsführer.

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT05	Kontrolle durch festgelegten Updateprozess	RIT03	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

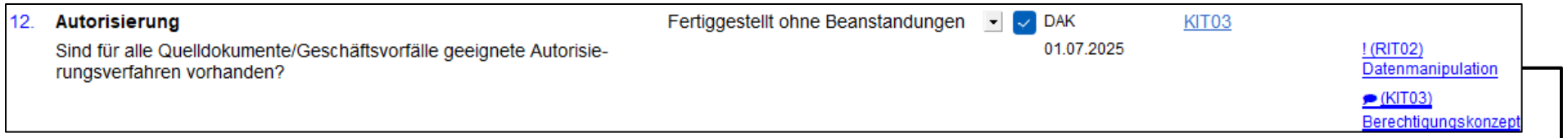
11.	**Datengenauigkeit** Sind Kontrollen eingerichtet, mit denen sichergestellt wird, dass Informationen gültig, genau und vollständig sind?	Fertiggestellt ohne Beanstandungen	DAK 01.07.2025	KIT08	! (RIT03) Falsche Datenverarbeitung (KIT08) Überprüfung Datenverarbeitung und Datenübernahme

11. Datengenauigkeit

Im ERP-Systems selbst sind Verarbeitungs- und Plausibilitätskontrollen hinsichtlich der Datenkonsistenz programmtechnisch abgebildet. Weitere Prüfungen werden durch Mitarbeiter des Unternehmens durchgeführt. Bspw. Sollstellungs- und Lastschriftlauf bei Wohnungsunternehmen.

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT08	Überprüfung Datenverarbeitung und Datenübernahme	RIT03	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)



KRL03; KRL04; KRL05

12. Autorisierung

Die Autorisierung wird durch Berechtigungen gesteuert. Diese liegen insbesondere im Bereich der Rechnungsprüfung (Workflow) und Zahlungsfreigabe vor. Des Weiteren ist im ERP-System ein rollenbasiertes Berechtigungskonzept implementiert. Vgl. Ref.

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT03	Einrichtung eines Berechtigungskonzeptes	RIT02	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs: Kontrollen in Bezug auf Journalbuchungen (1)

Bereich Rechnungslegung:

KRL01 - Regelmäßige Durchsicht der Berechtigungsliste auf Aktualität der vergebenen Berechtigungen und Einhaltung der Funktionstrennung zwischen Fachabteilungen und/oder IT-Abteilung (Berechtigungskonzept)

➔ bspw. Funktionstrennung elektr. Rechnungsprüfung/-freigabe und bei Stammdaten

KRL02 - Protokollierung und systemseitige Freigabe von Stammdatenänderungen (einschließlich Neuanlagen und Löschungen) durch Fachvorgesetzten bzw. Durchsicht von Stammdatenänderungsprotokollen auf Richtigkeit etc., Gegenzeichnung

➔ bspw. elektr. 4-Augenprinzip bei Stammdatenänderungen im Bereich Bankverbindungen

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs: Kontrollen in Bezug auf Journalbuchungen (2)

KRL03 - Regelmäßige Abstimmung manueller bzw. automatischer Schnittstellen von den Nebenbüchern (z.B. Anlagenbuchhaltung, Mietenbuchhaltung, Personalabrechnung, Debitoren, Kreditoren) in das Hauptbuch, regelmäßige Kontrolle und Bearbeitung fehlerhafter Übertragungen

➔ bspw. Ausgleich Verrechnungskonten (Schnittstellen)

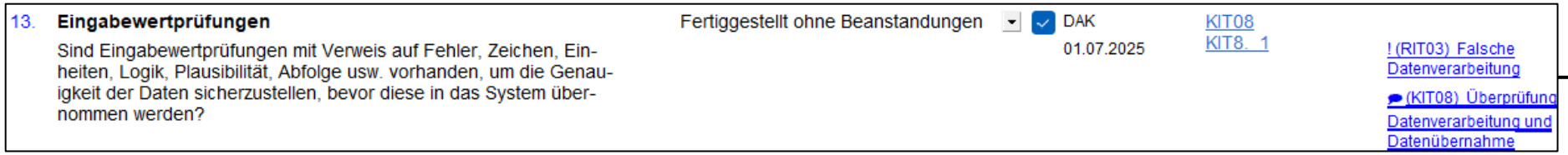
KRL04 - Rechnungsprüfung sachlich und rechnerisch ➔ bspw. elektr. Workflow

KRL05 - Durchsicht der Zahlungsvorschlagsliste hinsichtlich Sperrvermerke/Reklamationen bzw. bereits erfolgter Zahlung (z.B. wegen fehlenden Auszifferns)

➔ bei Sperrvermerk im System sollte eine Aufnahme des Kreditors in die Zahlungsliste nicht möglich sein (systemseitig unterbunden)

! Kontrollen Rechnungslegung haben je nach Ausgestaltung auch Wirkung auf IT-Kontrollen!

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)



13.	**Eingabewertprüfungen** Sind Eingabewertprüfungen mit Verweis auf Fehler, Zeichen, Einheiten, Logik, Plausibilität, Abfolge usw. vorhanden, um die Genauigkeit der Daten sicherzustellen, bevor diese in das System übernommen werden?	Fertiggestellt ohne Beanstandungen	DAK 01.07.2025	KIT08 KIT8. 1	! (RIT03) Falsche Datenverarbeitung (KIT08) Überprüfung Datenverarbeitung und Datenübernahme

13. Eingabewertprüfungen

Durch programminterne Kontrollen werden Fehleingaben weitestgehend vermieden. Die notwendigen Eingaben werden in der Softwaredokumentation beschrieben und die Mitarbeiter wurden/werden entsprechend geschult.

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT08	Überprüfung Datenverarbeitung und Datenübernahme	RIT03	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Eingabewertprüfungen

- Werden durch das Programm Belegnummern vergeben?
- Sind diese Belegnummern lückenlos? (Hinweise evtl. im Software-Testat)
- Kontrolliert das Unternehmen regelmäßig die lückenlose Vergabe von Belegnummern?
- Wenn Belegnummernlücken vorhanden sind, wurde die Ursache dokumentiert?

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Prüfungspfad Eingabevalidierungen - Rechnungen

Rechnungen sind nur dann ordnungsgemäß, wenn die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit der Rechnung gewährleistet ist.

Nach Abschn. 14.4 Abs. 4 UStAE muss das Unternehmen durch ein innerbetriebliches Verfahren sicherstellen, dass diese Voraussetzungen erfüllt sind. Das ist der Fall, wenn er ein internes Kontrollverfahren einführt, das einen "verlässlichen Prüfungspfad zwischen Rechnung und Leistung" schafft.

Dieser verlässliche Prüfungspfad zwischen Rechnung und Leistung wird zum Beispiel geschaffen, wenn die vorliegende Rechnung mit der Zahlungsverpflichtung abgeglichen wird. Das bedeutet, das Unternehmen muss sicherstellen, dass er nur Rechnungen bezahlt, zu deren Begleichung er verpflichtet ist.

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Prüfungspfad, 14.4 Abs. 4 UStAE

(4) Die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit der Rechnung müssen, sofern keine qualifizierte elektronische Signatur verwendet oder die Rechnung per elektronischen Datenaus-tausch (EDI) übermittelt wird (vgl. Absätze 7 bis 10), durch ein innerbetriebliches Kontrollverfahren, das einen verlässlichen Prüfungspfad zwischen Rechnung und Leistung schaffen kann, gewährleistet werden.
§ 14 Abs. 1 Satz 5 und 6 UStG

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Prüfungspfad, 14.4 Abs. 4 UStAE

Checkliste Rechnungsprüfung
(Mindestumfang an Prüfschritten)

Prüfschritte	**Ja**	**Nein**
Anforderungen an Authentizität (Echtheit der Herkunft)		
a) Ist der **Aussteller der Rechnung** (Erbringer der Leistung) bekannt?		
b) Wurden von diesem Rechnungsaussteller Lieferungen oder Leistungen **bestellt** und **bezogen**, und wird somit eine Rechnung erwartet?		
c) Sind **sämtliche Angaben auf der Rechnung** (insbesondere USt-ID-Nummer/ Steuernummer, Anschriften, Firmierung und Bankverbindung) **korrekt**? Können diese Daten fehlerfrei gegen die eigene Stammdatenbank abgeglichen werden?		
Anforderungen an Integrität (Unversehrtheit des Inhalts)		
d) Wurde die ausgewiesene Lieferung/ Leistung in korrekter **Art, Menge und Preis** ausgeführt? Lässt sich das mit Lieferschein, Wareneingangsbescheinigungen bzw. –daten abgleichen?		
e) Sind alle gesetzlich geforderten **Pflichtangaben** auf der Rechnung enthalten?		
f) Ist die Rechnung **rechnerisch korrekt**?		

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

14.	**Elektronische Trennung von Funktionen** Wurde eine elektronische Trennung von Funktionen implementiert, um sicherzustellen, dass die Initiierung und Autorisierung eines Geschäftsvorfalls von dessen Ausführung und Verifizierung getrennt ist?	Fertiggestellt ohne Beanstandungen	☑	DAK 01.07.2025	540. P KRL04; KRL05

14. Elektronische Trennung von Funktionen

Die Funktionstrennung wird durch das in Wodis Yuneo eingerichtete Berechtigungskonzept sicher gestellt. Weiterhin gibt es elektr. Funktionstrennungen im Bereich des Zahlungsverkehrs (elektr. Unterschrift). Hier erfolgt eine Hinterlegung bei den Banken (vgl. Bankbestätigung) sowie im Bereich der Rechnungsprüfung/-freigabe, welche als elektr. Workflow im Unternehmen eingerichtet ist.

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

15.	SOFTWAREBESCHEINIGUNG Holen Sie für eingesetzte rechnungslegungsrelevante Programme eine Softwarebescheinigung ein (falls verfügbar). Prüfen Sie die Versionsnummer der Software und auf der Softwarebescheinigung! Beurteilen Sie, ob die in der Softwarebescheinigung genannten Bedingungen zu Installation und Einsatz der Software von der Einheit erfüllt werden.	Dokumentiert in	☑ DAK 01.07.2025	KIT08 KIT08_1

15. Softwarebescheinigung

Für das eingesetzte ERP-Programm Wodis Sigma liegt eine Softwarebescheinigung vor. Es handelt sich um einen vollständigen Bericht und die Versionen stimmen überein. Der Bericht enthält keine Einschränkungen in Bezug auf die Software.

ODER

Für die rechnungslegungsrelevanten Programme liegt keine (verwertbare) Softwarebescheinigung vor.

aktuelle Version Yuneo: 25.106.0; Testat: 23.77.0

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT08	Überprüfung Datenverarbeitung und Datenübernahme	RIT03	540.	gesonderte Dokumentation mit Referenz

Dies ist die einzige Frage in Bezug auf eine vorliegende Softwarebescheinigung

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Softwaretestat (1)

Inhaltsverzeichnis **Seite**

Abkürzungsverzeichnis 5

A. Auftrag und Auftragsdurchführung 7

B. Zusammenfassung der Prüfungsergebnisse und Bescheinigung 10

C. Prüfungsfeststellungen im Einzelnen 11

I. Verarbeitungsfunktionen 11

1. Einhaltung der GoB 11

a) Belegfunktion 11

b) Journalfunktion 12

c) Kontenfunktion 13

d) Transfers 13

e) Kontrollen bei der Erfassung von Daten und Protokollierungsfunktionen 15

2. GoB-relevante Wodis Yuneo-Module 17

a) Finanzbuchhaltung 17

b) Mietenbuchhaltung 18

c) Betriebskostenabrechnung 18

d) Mitgliederverwaltung 20

e) Eigentümerbuchhaltung (Fremdverwaltung) 20

f) Eigentümerabrechnung (Fremdverwaltung) 21

g) Sparverkehr 22

h) Anlagenbuchhaltung 23

i) Darlehen & Hypotheken 24

j) Kautionsverwaltung 25

k) Konfiguration 25

3. Prüfung der programmierten Verarbeitungsregeln 26

4. Abgleich der Reports in Wodis Sigma und Wodis Yuneo 26

II. Softwaresicherheit 27

1. Zugriffsberechtigung (Rechteverwaltung) 27

2. Datensicherungs- und Wiederanlaufverfahren 29

3. Programmentwicklung, -wartung und -freigabe 29

III. Dokumentation 31

1. Anwenderdokumentation 31

2. Technische Systemdokumentation und Betriebsdokumentation 31

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Softwaretestat (2)

14. Zusammengefasst kommen wir zu dem Ergebnis, dass das Anwendungssystem

Wodis Yuneo Release 23.77.0

der

Aareon Deutschland GmbH, Mainz,

bei sachgerechter Anwendung unter Verwendung der empfohlenen, automatischen Belegnummernvergabe eine den Grundsätzen ordnungsmäßiger Buchführung entsprechende Rechnungslegung ermöglicht. Unserer Prüfung haben wir auftragsgemäß die unter Text 8 aufgeführten Kriterien zugrunde gelegt.

Aufgrund unserer Untersuchungen erteilen wir folgende Prüfungsbescheinigung:

"Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse ermöglicht das von uns geprüfte Softwareprodukt Wodis Yuneo Release 23.77.0 bei sachgerechter Anwendung eine den Grundsätzen ordnungsmäßiger Buchführung entsprechende Rechnungslegung und entspricht den vorstehend aufgeführten Kriterien."

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

16.	STAMMDATENPLEGE Prüfen Sie, ob die Verfahren zur Anlage, Änderung und Löschung von Stammdaten den Grundsätzen ordnungsgemäßer Buchführung entsprechen (z.B. Vier-Augen-Prinzip, Genehmigung, Dokumentation).	Dokumentiert in	DAK 01.07.2025	KIT04	! (RIT02) Datenmanipulation (KIT04) Einschaltung der systemseitgen Stammdatenänderungsprotokollierung

KRL02

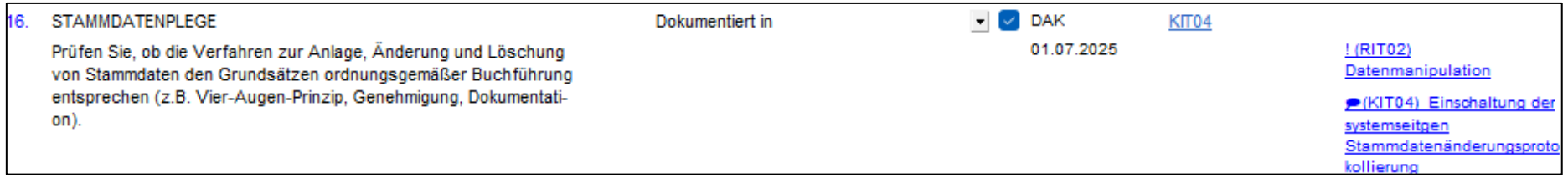
16. Stammdatenpflege

Änderungsprotokollierung ist im Yuneo standardmäßig aktiv und kann auch nicht ausgeschalten werden. Bei den Geschäftspartnern ist ein 4-Augen-Prinzip bei der Änderung von Bankverbindungen hinterlegt, ohne Freigabe kann nicht auf diese bezahlt werden (vgl. KRL02).

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT04	Einschaltung der systemseitgen Stammdatenänderungs-protokollierung	RIT02	540.	gesonderte Dokumentation mit Referenz

Wenn möglich, lassen Sie sich die entsprechenden Einstellungen zu einem Beispiel zeigen!

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)



16.	STAMMDATENPLEGE Prüfen Sie, ob die Verfahren zur Anlage, Änderung und Löschung von Stammdaten den Grundsätzen ordnungsgemäßer Buchführung entsprechen (z.B. Vier-Augen-Prinzip, Genehmigung, Dokumentation).	Dokumentiert in	DAK 01.07.2025	KIT04	! (RIT02) Datenmanipulation (KIT04) Einschaltung der systemseitgen Stammdatenänderungsprotokollierung

16. Stammdatenpflege

Dies ist eine wichtige Frage in Bezug auf die Ordnungsmäßigkeit der Buchführung:

- Führen Sie ein Gespräch mit dem IT-Verantwortlichen
- Besprechen Sie insbesondere, ob bei dem vorliegenden Buchhaltungsprogramm die Protokollierung von Stammdatenänderungen eingerichtet ist
- Wenn möglich, lassen Sie sich die entsprechenden Einstellungen zu einem Beispiel zeigen

Bspw. im SAP lässt sich die Protokollierung ausschalten - Argument ist meistens die Performance

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

17.	BELEGFUNKTION Prüfen Sie, ob sichergestellt ist, dass keine Buchung ohne einen entsprechenden Nachweis vorgenommen wird und dieser alle notwendigen Angaben enthält (u.a. Erläuterung/Begründung Geschäftsvorfall, Werte, Zeitpunkt des Geschäftsvorfalls, Kontierung, Belegnummer, Buchungsdatum).	Dokumentiert in	☑ DAK 01.07.2025	KIT8. 1 KRL04	

17. Belegfunktion

Der Grundsatz der Belegunktion wird eingehalten (vgl. auch Softwaretestat). Zu jedem Geschäftsvorfall gibt es entweder einen physischen oder technischen Beleg.

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT08	Überprüfung Datenverarbeitung und Datenübernahme	RIT03	540.	gesonderte Dokumentation mit Referenz

Anhaltspunkt: Softwarebescheinigung

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

17.	BELEGFUNKTION Prüfen Sie, ob sichergestellt ist, dass keine Buchung ohne einen entsprechenden Nachweis vorgenommen wird und dieser alle notwendigen Angaben enthält (u.a. Erläuterung/Begründung Geschäftsvorfall, Werte, Zeitpunkt des Geschäftsvorfalls, Kontierung, Belegnummer, Buchungsdatum).	Dokumentiert in	DAK 01.07.2025	KIT8. 1

17. Belegfunktion

Keine Buchung ohne Beleg

- Nehmen Sie Einsicht ins Buchungsjournal (sind alle notwendigen Angaben enthalten?)
- Vollziehen Sie dies für einen manuellen Beleg (Rechnung) und einen automatischen Beleg nach (z. B. automatische AfA-Buchungen oder monatlichen Sollmietenstellung

IDW RS FAIT 1 Tz 33 ff.:
Konventioneller Beleg oder maschineller Beleg!
Hinweis: Auch digitale Belege können bspw. im elektr. Archivsystem einer Buchung zugeordnet werden.
Dies geht auch bspw. für Jahresabschlussbuchungen.

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

18.	JOURNALFUNKTION Prüfen Sie, ob die vollständige, zeitgerechte, chronologische und formal richtige Erfassung und Verarbeitung der Geschäftsvorfälle gewährleistet ist (z.B. durch systemseitige Protokollierung, lückenlose Belegnummernvergabe, keine doppelte Belegnummernvergabe). Prüfen Sie, dass Buchungen nur von autorisierten Personen ausgelöst werden können (z. B. Berechtigungen).	Dokumentiert in	DAK 01.07.2025	KIT8. 1

18. Journalfunktion

Ja, dass Buchungsjournal enthält alle notwendigen Informationen (vgl. auch Softwaretestat). Das Berechtigungskonzept gibt keinen Hinweis darauf, dass nicht autorisierte Personen Buchungen durchführen.

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

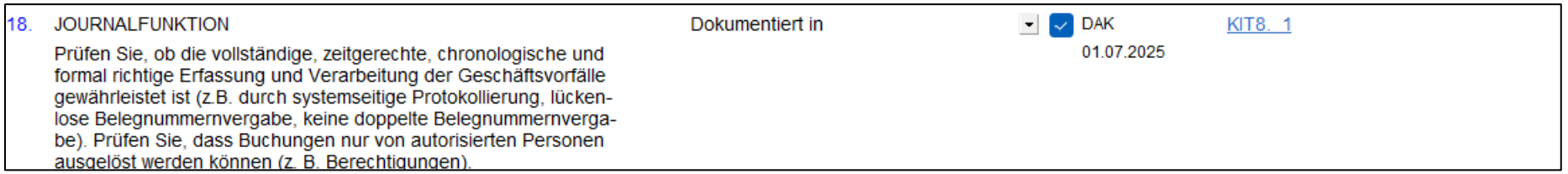
18.	JOURNALFUNKTION Prüfen Sie, ob die vollständige, zeitgerechte, chronologische und formal richtige Erfassung und Verarbeitung der Geschäftsvorfälle gewährleistet ist (z.B. durch systemseitige Protokollierung, lückenlose Belegnummernvergabe, keine doppelte Belegnummernvergabe). Prüfen Sie, dass Buchungen nur von autorisierten Personen ausgelöst werden können (z. B. Berechtigungen).	Dokumentiert in	DAK 01.07.2025	KIT8. 1

18. Journalfunktion

Nehmen Sie Einsicht ins Berechtigungskonzept:

- Wer darf alles buchen?
- Wie ist sichergestellt, dass keine Belegnummern doppelt vergeben werden?
- Wie wird nachgewiesen, dass es keine Lücken in den Belegnummern gibt?

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)



18.	JOURNALFUNKTION Prüfen Sie, ob die vollständige, zeitgerechte, chronologische und formal richtige Erfassung und Verarbeitung der Geschäftsvorfälle gewährleistet ist (z.B. durch systemseitige Protokollierung, lückenlose Belegnummernvergabe, keine doppelte Belegnummernvergabe). Prüfen Sie, dass Buchungen nur von autorisierten Personen ausgelöst werden können (z. B. Berechtigungen).	Dokumentiert in	DAK 01.07.2025	KIT8. 1

18. Journalfunktion

Sicherstellung der zeitlichen Ordnung

IDW RS FAIT 1 Tz 41 ff.

- Besprechen Sie dies mit dem Leiter Rechnungswesen
- Nehmen Sie ggf. Screenshots zu den Arbeitspapieren
- Ggf. prüfen Sie dies in Zusammenhang mit den IKS-Prüfungen

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

19.	KONTENFUNKTION Prüfen Sie, ob die einzelnen Konten in sachlich richtiger, übersichtlicher und verständlicher Form dargestellt werden (u. a., Angabe der Kontenbezeichnung, Kennzeichnung der Buchungen, Summen nach Soll und Haben, Gegenkonto, Buchungsdatum, Belegverweis, Buchungstext).	Dokumentiert in	DAK 01.07.2025	KIT8. 1

19. Kontenfunktion

Die Kontenfunktion wird eingehalten (vgl. Softwaretestat).

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT08	Überprüfung Datenverarbeitung und Datenübernahme	RIT03	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

19.	KONTENFUNKTION Prüfen Sie, ob die einzelnen Konten in sachlich richtiger, übersichtlicher und verständlicher Form dargestellt werden (u. a., Angabe der Kontenbezeichnung, Kennzeichnung der Buchungen, Summen nach Soll und Haben, Gegenkonto, Buchungsdatum, Belegverweis, Buchungstext).	Dokumentiert in	DAK 01.07.2025	KIT8. 1

19. Kontenfunktion

Überprüfen Sie, ob für jede Buchung die notwendigen Informationen vorhanden sind:

- Kontenbezeichnung
- Kennzeichnung der Buchungen
- Soll und Haben
- Buchungs- und Belegdatum
- Gegenkonto
- Buchungstext

IDW RS FAIT 1 Tz 41 ff.
Sicherstellung der sachlichen Ordnung!

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

20.	UNVERÄNDERBARKEIT DER DATEN Prüfen Sie, ob Änderungen der ursprünglichen Daten feststellbar sind, indem sie beurteilen, ob sowohl der ursprüngliche Inhalt als auch Veränderungen erkennbar bleiben (z.B. durch systemseitige Protokollierungen von Änderungen).	Dokumentiert in	DAK 01.07.2025	KIT08 KIT8. 1 KIT8. 2	! (RIT02) Datenmanipulation (KIT04) Einschaltung der systemseitgen Stammdatenänderungsprotokollierung	KRL02

20. Unveränderbarkeit der Daten

Die eingesetzte Standardsoftware enthält eine Protokollierung von Änderungen in den Stammdaten. Eine Auswertung erfolgt anlassbezogen.

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT04	Einschaltung der systemseitgen Stammdatenänderungs-protokollierung	RIT02	540.	gesonderte Dokumentation mit Referenz

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

20.	UNVERÄNDERBARKEIT DER DATEN Prüfen Sie, ob Änderungen der ursprünglichen Daten feststellbar sind, indem sie beurteilen, ob sowohl der ursprüngliche Inhalt als auch Veränderungen erkennbar bleiben (z.B. durch systemseitige Protokollierungen von Änderungen).	Dokumentiert in	DAK 01.07.2025	KIT08 KIT8. 1 KIT8. 2	! (RIT02) Datenmanipulation (KIT04) Einschaltung der systemseitgen Stammdatenänderungsprotokollierung

20. Unveränderbarkeit der Daten

- Stellen Sie fest, ob eine Protokollierung von Stammdatenänderungen eingeschaltet ist
- Ferner ist heraufzufinden, ob vorhandene Buchungen nicht geändert werden, sondern nur storniert werden können
- Jede Buchung muss sich zu seinem Verursacher rückverfolgen lassen

Grundsatz der Unveränderlichkeit (§ 239 Abs. 3 HGB)

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

21.	KONTENZUORDNUNG Prüfen Sie, ob die Konten den Posten der Bilanz sowie der Gewinn und Verlustrechnung richtig zugeordnet worden sind.	Dokumentiert in	☑	DAK 01.07.2025	5. 3

21. Kontenzuordnung

Ja, alle Konten sind vollständig zugeordnet, vgl. Ref. 5.3

- Überprüfung erfolgt schon beim Einlesen der SuSaLi in Audicon
- Hier ist die lückenlose Kontenzuordnung zu bestätigen

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

22.	SALDOVORTRAG Prüfen Sie, ob sichergestellt ist, dass sämtliche Salden zutreffend auf das Berichtsjahr vorgetragen wur- den.	Dokumentiert in	AIR 29.06.2026	IMPORV

22. Saldenvortrag – Frage neu ab 2026, analog Frage 17 ORD.PP

Saldenvorträge wurden vollständig abgestimmt, keine Beanstandungen, vgl. Ref.

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

23. ABSTIMMUNG HAUPT- UND NEBENBUCH Prüfen Sie, ob die Daten von Haupt- und Nebenbuch (Personalbuchhaltung, Anlagen-, Debitoren-, Kreditorenbuch, etc.) regelmäßig abgestimmt werden und die Abstimmungen dokumentiert und nachvollziehbar sind.	Fertiggestellt ohne Beanstandungen	DAK 01.07.2025	540. P 1050. PP 1400. PP 3500. PP 5050. PP	KRL03

23. Abstimmung Haupt- und Nebenbuch

Ja, die Haupt- und Nebenbücher werden überwacht. Vgl. Investitionen, Mietenbuchhaltung, Debitoren/Kreditoren, Darlehensbuchhaltung etc. Eine Dokumentation erfolgt nicht.

- Besprechung mit dem Leiter Rechnungswesen, wie er dies sicherstellt
- Werden die Überprüfungen dokumentiert?

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

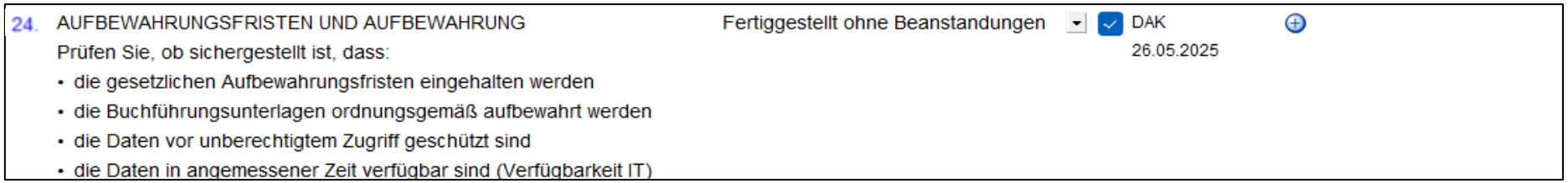
24.	AUFBEWAHRUNGSFRISTEN UND AUFBEWAHRUNG Prüfen Sie, ob sichergestellt ist, dass: • die gesetzlichen Aufbewahrungsfristen eingehalten werden • die Buchführungsunterlagen ordnungsgemäß aufbewahrt werden • die Daten vor unberechtigtem Zugriff geschützt sind • die Daten in angemessener Zeit verfügbar sind (Verfügbarkeit IT)	Fertiggestellt ohne Beanstandungen	DAK 26.05.2025

24. Aufbewahrungsfristen und Aufbewahrung

Bei der Prüfung ergaben sich keine Hinweise, dass die gesetzlichen Aufbewahrungsfristen nicht eingehalten werden. Auskunftsgemäß wird aus dem ERP-System und dem elektr. Archiv nichts gelöscht (nur entsprechend dem Datenlöschkonzept anonymisiert). Papierunterlagen werden im Archiv entsprechend den Aufbewahrungsfristen gelagert.

Aufbewahrungsvorschriften: § 257 HGB und § 146 AO

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)



24. AUFBEWAHRUNGSFRISTEN UND AUFBEWAHRUNG — Fertiggestellt ohne Beanstandungen — DAK — 26.05.2025

Prüfen Sie, ob sichergestellt ist, dass:

- die gesetzlichen Aufbewahrungsfristen eingehalten werden
- die Buchführungsunterlagen ordnungsgemäß aufbewahrt werden
- die Daten vor unberechtigtem Zugriff geschützt sind
- die Daten in angemessener Zeit verfügbar sind (Verfügbarkeit IT)

24. Aufbewahrungsfristen und Aufbewahrung

- Finden Sie heraus, ob die gesetzlichen Aufbewahrungsvorschriften eingehalten werden
- Nehmen Sie Einsicht in eine bestehende Datenschutzrichtlinie/ führen Sie ein Gespräch mit dem Leiter IT
- Ist die Datenschutzrichtlinie mit den gesetzlichen Vorgaben vereinbar?
- Seit 2025 Pflicht zum Empfang von E-Rechnungen, diese müssen auch elektr. archiviert werden

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

Exkurs Verfahrensdokumentation ersetzendes Scannen

Verfahrensdokumentation zum ersetzenden Scannen
(Version 1.0; Stand: 20.11.2023)

Erarbeitet von der

Inhaltsverzeichnis

1 Vorbemerkungen zur Verfahrensdokumentation ... 3
2 Zielsetzung und Überblick ... 3
2.1 Zielsetzung und Anwendungsbereich ... 3
2.2 Unternehmen und organisatorisches Umfeld ... 4
2.2.1 Unternehmensportrait ... 4
2.2.2 Einsatzorte ... 4
2.3 Rechtliche Grundlagen und Ordnungsmäßigkeitskriterien ... 6
2.4 Relevante Dokumente ... 8
2.5 Einweisung in die Digitalisierungsverfahren ... 8
2.6 Abgrenzung der Bearbeitungsbereiche ... 9
3 Organisation und Sicherheit des IT-gestützten Verfahrens ... 9
3.1 Eingesetzte Hard- und Software ... 9
3.2 Zuständigkeiten ... 10
3.3 Organisation und Internes Kontrollsystem (IKS) ... 12
3.4 Datenschutz und Datensicherheit ... 13
4 Verfahren und Maßnahmen zum zentralen Scannen ... 13
4.1 Posteingang und Vorsortierung mit Prüfung auf Echtheit ... 13
4.2 Identifikation der zu scannenden Belege (rechtliche bzw. faktische Prüfung) ... 13
4.3 Vorbereitung der zu digitalisierenden Dokumente (technische Prüfung) ... 14
4.4 Digitalisierung ... 14
4.5 Vollständigkeits-/Lesbarkeits- und Plausibilitätskontrolle ... 15
4.6 Nachverarbeitung und Archivierung mit Integritätssicherung ... 15
4.7 Vernichtung der digitalisierten Papierbelege ... 17
4.8 Löschung der digitalen Archivbestände nicht vor Ablauf der Aufbewahrungsfrist ... 17
5 Mitgeltende Unterlagen ... 17
6 Änderungshistorie ... 18
7 Glossar ... 19

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)


25. ORDNUNGSMÄSSIGKEIT DER BUCHFÜHRUNG BEI AUSLAGERUNG DER IT

Stellen Sie aufgrund der durchgeführten IT-Systemprüfung fest, ob im Fall der Auslagerung der IT die Sicherheit und Ordnungsmäßigkeit der Buchführung in Frage steht (Hinweis auf IDW RS FAIT 5 Tz. 19-21). In diesem Fall prüfen Sie, ob

25. Ordnungsmäßigkeit der Buchführung bei Auslagerung der IT

Datenauslagerung erfolgt in ein Rechenzentrum (SaaS – Software as a Service) bei xy, dazu liegen vertragliche Vereinbarungen vor. xy ist ISO 9001 und ISO/IEC 27001 zertifiziert, dies bestätigt, dass ein entsprechendes IKS eingerichtet ist.

<u>Alternativ</u>

Der Dienstleister ist nach IDW PS 951 Typ 2 (oder vergleichbaren Standard wie ISAE 3402 Typ II) testiert. Vgl. Ref.

Weiterhin erfolgt die Lohnbuchhaltung durch einen ext. Dienstleister. Hier werden die Daten aber manuell im Wodis eingegeben, keine Schnittstelle

Hier Angabe der bestehenden Auslagerung

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)



25. ORDNUNGSMÄSSIGKEIT DER BUCHFÜHRUNG BEI AUSLAGERUNG DER IT

Stellen Sie aufgrund der durchgeführten IT-Systemprüfung fest, ob im Fall der Auslagerung der IT die Sicherheit und Ordnungsmäßigkeit der Buchführung in Frage steht (Hinweis auf IDW RS FAIT 5 Tz. 19-21). In diesem Fall prüfen Sie, ob

25. Ordnungsmäßigkeit der Buchführung bei Auslagerung der IT

a. die gesetzlichen Vertreter des auslagernden Unternehmens ein internes Kontrollsystem im Hinblick auf die ausgelagerten Funktionen angemessen ausgestaltet haben, um Unrichtigkeiten sowie Verstöße gegen rechtliche Normen und darüber hinausgehende Ordnungsmäßigkeitskriterien zu verhindern bzw. aufzudecken und festgestellte Schwächen abzustellen (Hinweis auf IDW RS FAIT Tz. 45-61).

Hier ist das IKS an der Schnittstelle zu untersuchen

Wie ist es eingerichtet?
Ggf. Bezug auf eine IKS-Prüfung nehmen (z. B. im Bereich Personal)

Ja, ein IKS bzgl. der Nutzung des ausgelagerten ERP-Systems ist bei der WBG eingerichtet. Die Kontrollmaßnahmen sind angemessen ausgestaltet (vgl. IKS-Prüfungen Ref.)

=> Bei einer Geschäftsbesorgung kann hier ggf. auch auf der IKS der Muttergesellschaft etc. verwiesen werden.

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

25. ORDNUNGSMÄSSIGKEIT DER BUCHFÜHRUNG BEI AUSLAGERUNG DER IT

Stellen Sie aufgrund der durchgeführten IT-Systemprüfung fest, ob im Fall der Auslagerung der IT die Sicherheit und Ordnungsmäßigkeit der Buchführung in Frage steht (Hinweis auf IDW RS FAIT 5 Tz. 19-21). In diesem Fall prüfen Sie, ob

25. Aufbewahrungsfristen und Aufbewahrung

b. die vorgesehenen Maßnahmen (einschließlich solcher zur Überwachung) vom Unternehmen eingerichtet wurden, um die Risiken für die Ordnungsmäßigkeit der Buchführung zu minimieren bzw. zu beseitigen. Berücksichtigen Sie dabei die Wirksamkeit der Maßnahmen im Hinblick auf

- Kontrollumfeld/Organisation
- IT-Infrastruktur
- IT-Anwendungen
- IT-gestützte Geschäftsprozesse.

Hinweis auf IDW RS FAIT Tz. 62ff.

Hier Wirksamkeit der eingerichteten Kontrollen

Hier als Bsp. Rechenzentrum und Personal.
Ist das eingerichtete IKS wirksam?
Ggf. Bezug auf eine IKS-Prüfung nehmen z. B. im Bereich Personal.

Ja, für die Rechenzentrumsnutzung gibt es einen umfassenden Vertrag, die Einhaltung der Vorgaben erfolgt durch Performancemessungen (mtl. Reporting durch Dienstleister) und ein internes Überwachungssystem (vgl. Testat nach IDW PS 951 Typ 2 oder bspw. ISAE 3402 Typ II).

VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN)

26. Kommunikation

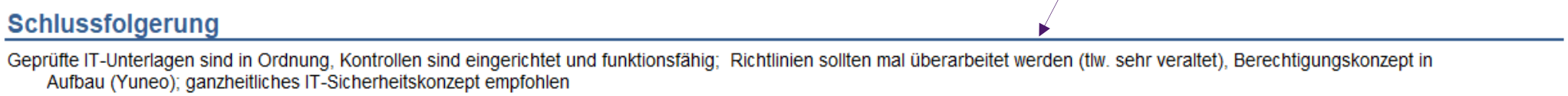
26.	Stellen Sie sicher, dass bedeutsame Schwächen des rechnungslegungsbezogenen Internen Kontrollsystems dem Aufsichtsorgan sowie den gesetzlichen Vertretern und ggf. anderen Führungskräften in angemessener Zeit schriftlich mitgeteilt werden (IDW PS 261 Tz. 89). Darüber hinaus ist im Prüfungsbericht im Abschnitt „Buchführung und weitere geprüfte Unterlagen" auf bestehende Mängel in der Buchführung und auf ihre Auswirkung auf die Rechnungslegung sowie ihren Einfluss auf das Prüfungsergebnis hinzuweisen (IDW PS 450 Tz. 65).	Fertiggestellt ohne Beanstandungen	DAK 01.07.2025	509.

Keine bedeutsamen Mängel, Richtlinien sollten mal überarbeitet werden (tlw. veraltet), Berechtigungskonzept in Aufbau (ERP-System XY); ganzheitliches IT-Sicherheitskonzept empfohlen.

VI. Dokumentation Allgemeine IT-Kontrollen (531.ORD.MIN)

Schlussfolgerung

- Am Ende der Prüfungshandlungen wird noch eine abschließende Beurteilung abgegeben
- Um diese einzufügen, muss dort mit der rechten Maustaste hin geklickt werden
- Es erscheint "Schlussfolgerung bearbeiten„
- Danach wird das Dokument abgezeichnet



VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN) - Exkurs

Zu 4. Backup

Exkurs Datensicherung (1) – Wesentliche Arten der Sicherung

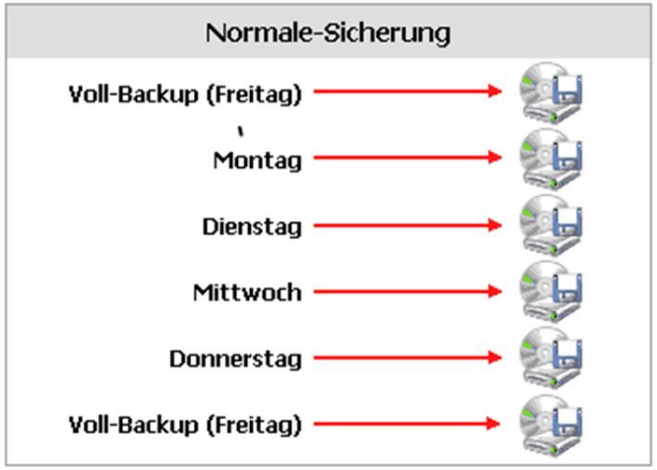
- Differentielle Sicherung
  - ➔ Sicherung der seit dem letzten kompletten Backup geänderten Daten
- Generationenprinzip
  - ➔ Sicherung nur der seit der letzten Datensicherung geänderten Daten
- Komplettsicherungen
  - ➔ Sicherung aller Daten unabhängig von der letzten Sicherung
    (heute Standard – Speicherplatz genügend vorhanden)

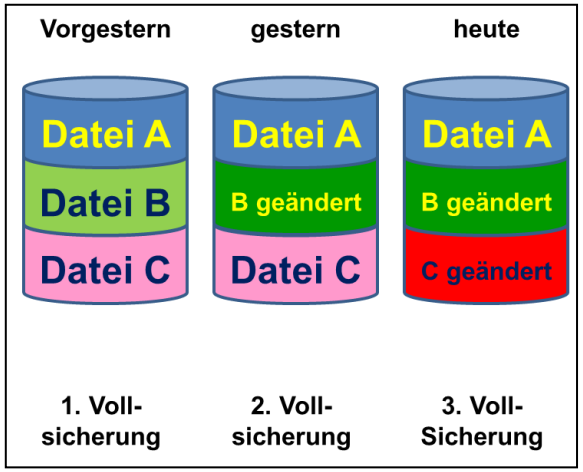
VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN) - Exkurs

Zu 4. Backup

Exkurs Datensicherung (2)

Bei der normalen Sicherung (**Vollsicherung**) werden alle ausgewählten Dateien kopiert und als gesichert markiert. Im Rücksicherungsfall braucht man lediglich die aktuellste Kopie der Sicherungsdatei oder des Bandes, um sämtliche Dateien wiederherzustellen.



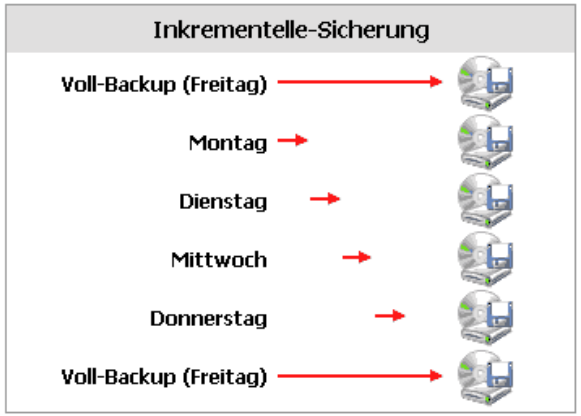


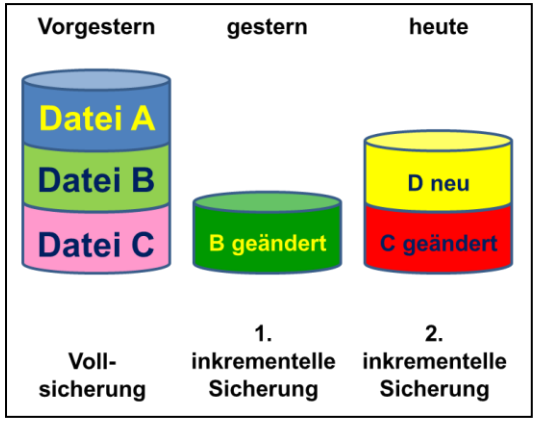
VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN) - Exkurs

Zu 4. Backup

Exkurs Datensicherung (3)

Bei einer **inkrementellen Sicherung** werden nur die Dateien gesichert, die seit der letzten Sicherung des Typs "Normal" oder Inkrementell erstellt bzw. geändert wurden. Dabei werden die gesicherten Dateien als solche markiert. Wird eine Kombination aus normalen und inkrementellen Sicherungen verwendet, werden im Wiederherstellungsfall die letzte volle Datensicherung und zum anderen alle seitdem durchgeführten inkrementellen Sicherungen benötigt.



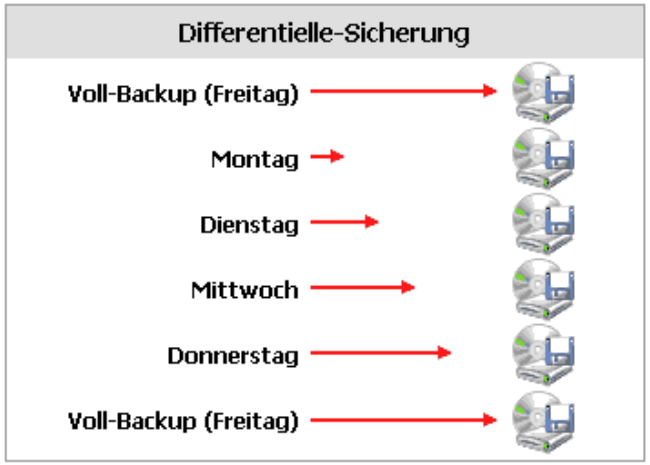


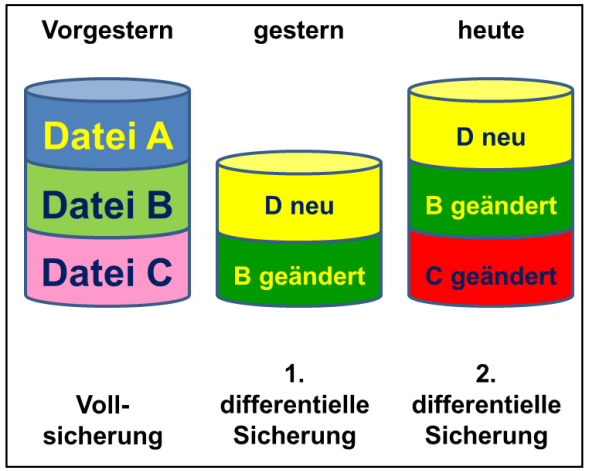
VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN) - Exkurs

Zu 4. Backup

Exkurs Datensicherung (4)

Bei der **differentiellen Sicherung** werden Dateien gesichert, die seit der ersten Sicherung des Typs Differenziell erstellt bzw. geändert wurden. Dateien werden nicht als gesichert gekennzeichnet. Im Datensicherungsfall müssen die letzte Vollsicherung und die letzte differentielle Sicherung eingespielt werden.



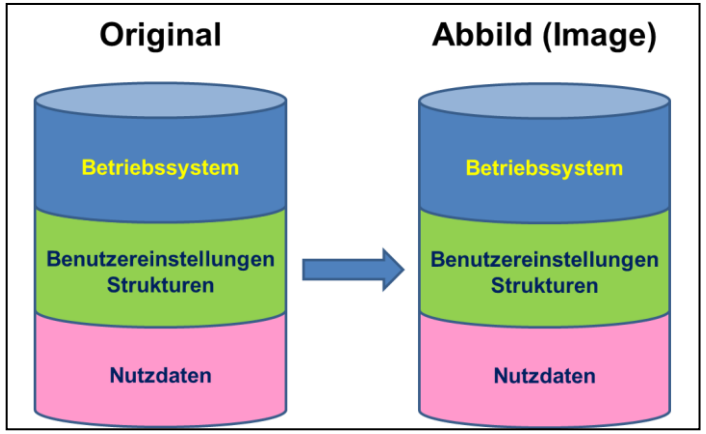


VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN) - Exkurs

Zu 4. Backup

Exkurs Datensicherung (5)

Bei einer Speicherabbildsicherung (SnapShot) wird der komplette Datenträger durch ein 1-zu-1-Abbild gesichert (Image Backup). Der Vorteil ist, dass bei einem Totalausfall des Systems die Daten (Nutzdaten, Betriebssystem und Benutzereinstellungen) vollständig auf ein neues System wieder hergestellt werden können, auf dem neuen System wird die Originalstruktur wieder hergestellt.



VI. Dokumentation
Allgemeine IT-Kontrollen (531.ORD.MIN) - Exkurs

Zu 4. Backup

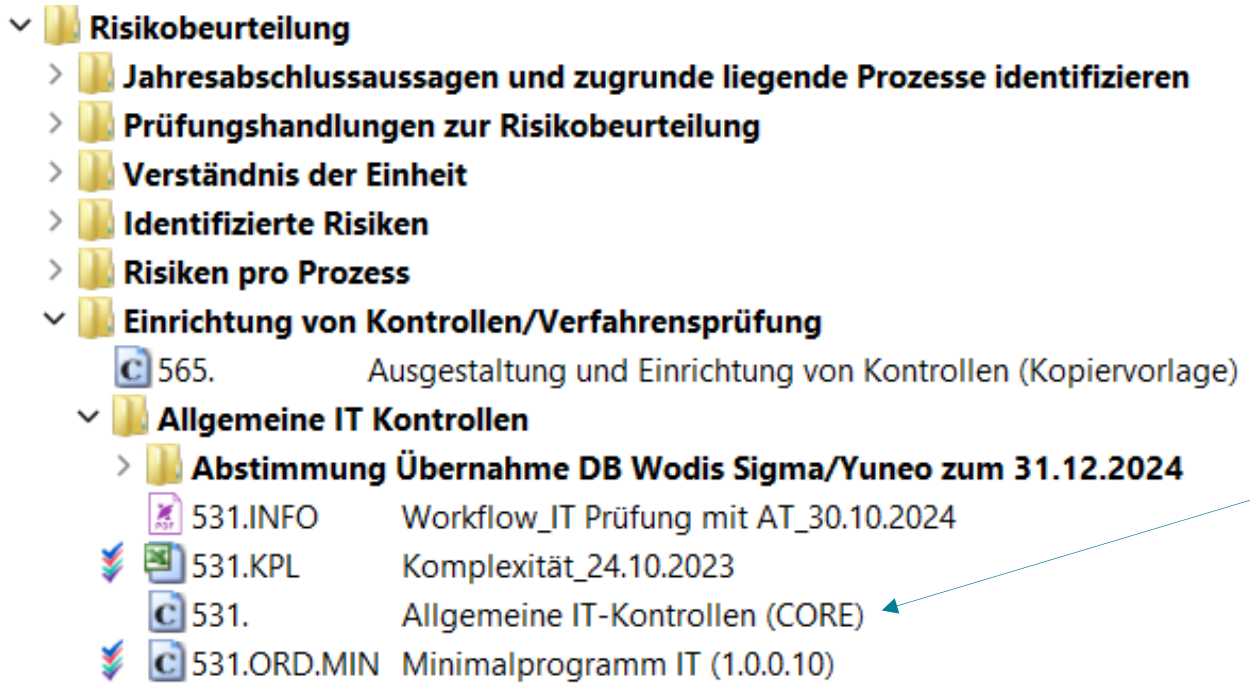
Exkurs Datensicherung (6)

Wie lange kann ich auf eine Datensicherung zurückgreifen (Generationen-Prinzip)?
➔ Heute in der Regel Tages-, Wochen-, Monats- und Jahressicherungen

Werden die gesetzlichen Aufbewahrungsfristen durch die Datensicherung sichergestellt?
➔ 6 Jahre/10 Jahre, Achtung: kann DSGVO (Datenschutz-Grundverordnung) widersprechen

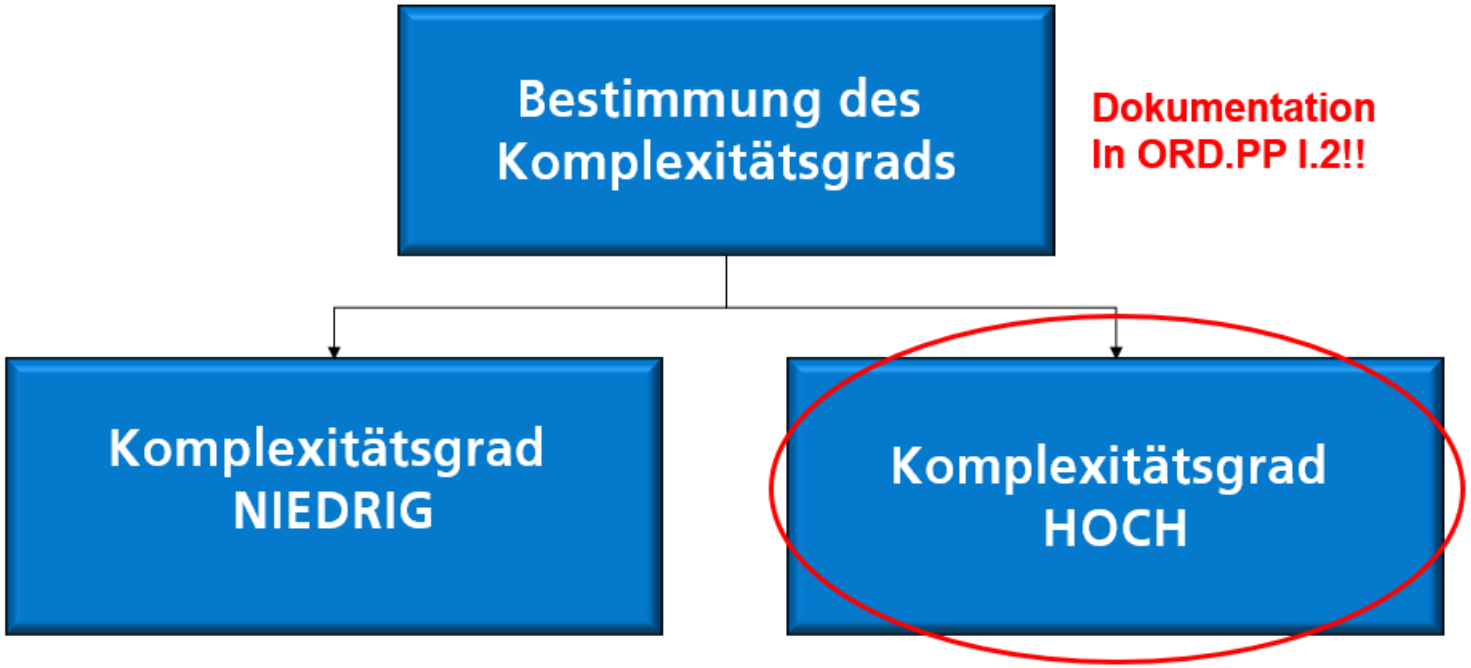
VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)



Die Checkliste 531. ist bei der Prüfung zu bearbeiten, soweit nicht 531.ORD.MIN verwendet wird!

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)



VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Übersicht über das IT-System

1. **Beschreibung**

   Wurden die allgemeinen Informationen zur IT-Umgebung der Einheit (einschließlich Hardware und Software) zusammengefasst? (Dokument 510-1 und Dokument 510-2 oder gleichwertige Dokumente)

2. **Externe Unterstützung**

   Wurde das IT-System in Bezug auf Komplexität geprüft, und wurde die Notwendigkeit angesprochen, einen IT-Experten hinzuzuziehen?

   Berücksichtigen Sie bei der Beurteilung der Komplexität die folgenden Faktoren:
   - Umfang der Anpassung - Handelt es sich bei der Anwendung um eine kommerzielle Standardanwendung mit geringer Anpassung oder um eine kundenspezifisch entwickelte Anwendung oder ein komplexes ERP-System mit Zugang zur Codierung?
   - Ausmaß der Integration - Ist die Anwendung mit anderen Anwendungen oder Komponenten der IT-Umgebung verbunden? Sind die Finanzsysteme webfähig?
   - Automatisierungsgrad - Gibt es eine hochautomatisierte papierlose Verarbeitung oder komplexe automatisierte Verfahren?

Es handelt sich um ein komplexes System mittler Größe (ca. 110 Clients). Neben der Standardsoftware XYZ werden Eigenentwicklungen und ein Warenwirtschaftssystem genutzt. IT-Betrieb läuft auf 11 physischen und 35 virtuellen Servern. Weiterhin werden weitere Gesellschaften „geschäftsbesorgt“. IT-Betreuung erfolgt durch drei Mitarbeiter, sowie externe Dienstleister. Ein IT-Prüfer wurde zur Unterstützung hinzugezogen.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Übersicht über das IT-System

3. **Vorläufige Risikobeurteilung**

Während der Berichtsperiode hat die Einheit:

- die IT-Umgebung geändert
- bedeutsame neue Betriebssysteme installiert
- eine wichtige Anwendung implementiert oder geändert
- Umfassende Datenkonvertierung

Falls ja, wurden etwaige Auswirkungen auf die Prüfungsplanung dokumentiert?

Hier Aussage zur vorläufigen Risikobeurteilung!

Im Berichtsjahr wurden zwei Server ausgetauscht und Microsoft 365 eingeführt; daraus ergeben sich keine besonderen Risiken mit Auswirkungen auf die Prüfung. Das vorläufige Risiko kann, auch unter Berücksichtigung der Prüfungsfeststellungen des Vorjahres, als gering eingeschätzt werden.

- Hinweis: In der Schlussfolgerung von 531. sollte das zuvor eingeschätzte Risiko bestätigt werden oder anderes eingeschätzt
- Achtung: korrespondiert mit MEMO.PA4 1i. (ISA 315.26b/ISA 315.26c)!

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Übersicht über das IT-System

4. **Verletzungen der IT-Sicherheit**

   Gab es während des Berichtszeitraums Verstöße oder Cybervorfälle (z. B. Ransomware-Angriffe)?

   Falls ja, wurden etwaige Auswirkungen auf die Prüfungsplanung dokumentiert?

Befragung des IT-Leiters Herrn X am 12.5.2026, Verstöße sind im Berichtszeitraum nicht bekannt, Cyberangriffe erfolgen laufend, waren aber nicht erfolgreich. Diese wurden im Rahmen des Monitorings des Systems bzw. durch die Firewall/Virenschutz verhindert.

Auswirkungen auf dem Geschäftsbetrieb sind nicht bekannt.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

5. **Strategie**

Übernimmt das Management Verantwortung für den IT-Plan und die IT-Strategie?

Eine ausformulierte IT-Strategie gibt es im Unternehmen nicht. Durch den zuständigen IT-Mitarbeiter wird jährlich ein IT-Investitionsplan erstellt (Bestandteil des Wirtschaftsplans). Weiterhin berichtet dieser regelmäßig in Geschäftsleiterrunden über Probleme/Störungen etc. Die Verantwortung trägt somit immer die Geschäftsführung.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

5. **Strategie**

   Übernimmt das Management Verantwortung für den IT-Plan und die IT-Strategie?

oft Bestandteil des RMS – bei Großunternehmen

Mindestinhalte der IT-Strategie sind:

1. Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation sowie IT-Dienstleistungen und sonstige wichtige Abhängigkeiten von Dritten
2. Strategische Entwicklung der IT-Architektur
3. Zuordnung der gängigen Standards
4. Ziele, Zuständigkeiten und Einbindung der Informationssicherheit
5. Aussagen zum IT-Notfallmanagement
6. Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hardware- und Software-Komponenten)

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

6. **IT-Plan**

Sind die laufenden IT-Aktivitäten konsistent mit dem IT-Plan?

Es liegt für den IT-Bereich ein langfristiger Investitions- und ein kurzfristiger Umsetzungsplan (Bestandteil des Wirtschaftsplans) vor. Inkonsistenzen haben wir nicht festgestellt

Folgende IT-Kosten sollten in der Planung berücksichtigt werden:

- Kosten für Hardware, Software, Lizenzen
- Kosten für den Betrieb (Strom, Wartungskosten)
- Kosten für Personal und für externe Unterstützung
- Kosten für Projekte und Innovationen

IT-Planung ist der erste Schritt zur Umsetzung der IT-Strategie

Planung sollte jährlich erfolgen (Bestandteil des Wirtschaftsplanes)

Eine Begrenzung des IT-Budgets ohne wirksame Kostensenkungsmaßnahmen führt auf Dauer zur Veralterung der IT eines Unternehmens.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

7. **IT-Rollen und -Verantwortlichkeiten**

Gibt es Richtlinien und Verfahren, mit denen IT-Rollen und -Zuständigkeiten, -Berichterstellung, -Richtlinien, -Standards und -Verfahren definiert werden?

Rollen und Verantwortlichkeiten sind im Unternehmen festgelegt.

Regelungen dazu finden sich bspw. im Sicherheitskonzept (beinhaltet u.a. Datensicherungskonzept, Notfallkonzept, Regelungen zu den Passwörtern) Anweisung zur Internetnutzung als Anlage zum Arbeitsvertrag Schulungsunterlagen zum Verhalten am Arbeitsplatz, Datenschutz, Stellenbeschreibung IT-Mitarbeiter etc.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

8. IT-Sicherheitsrichtlinie

a. Ist eine formale IT-Sicherheitsrichtlinie vorhanden, die von der entsprechenden Managementebene genehmigt und an die Mitarbeiter kommuniziert wurde?

Die Gesellschaft hat eine formale, von der Geschäftsführung freigegebene IT-Sicherheitsrichtlinie im Einsatz. Diese ist im Intranet der Gesellschaft für alle Mitarbeiter zugänglich.

b. Ist die IT-Sicherheitsrichtlinie für Größe und Komplexität der Einheit angemessen?

Ja, diese entspricht den Anforderungen der Gesellschaft und orientiert sich am IT-Grundschutzkatalog des BSI.
Jährlich erfolgt eine IT-Analyse durch den IT-Mitarbeiter, er berichtet bei Bedarf in Dienstberatungen, für Unternehmensgröße angemessen.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

Exkurs – Aufbau einer IT-Sicherheitslinie (1)

1	Gefährdungsanalyse
2	Allgemeine Festlegungen
3	Maßnahmenkatalog
4	Havarie-Szenarien und Handlungsanweisungen
5	Notfallplan

Anlage 1:	Datensicherung
Anlage 2:	Berechtigungskonzept
Anlage 3:	Passwort-Richtlinien
Anlage 4:	Aareon-Hotline

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

Exkurs – Aufbau einer IT-Sicherheitslinie (2) - Gefährdungsanalyse

	Gefährdungspotential
1.1 Höhere Gewalt	
1.1.1 Personalausfall im EDV-Bereich	2
1.1.2 Feuer	1
1.1.3 Unzulässige Temperaturen	2
1.1.4 Gebäudeschäden durch äußere Einflüsse	1
1.3 Menschliche Fehlhandlungen	
1.3.1 Gefährdung durch Reinigungs- und Fremdpersonal	3
1.3.2 Unbeabsichtigte Datenmanipulation	2
1.3.3 Beschädigungen an PC-Technik und Datenverkabelung	2
1.4 Technisches Versagen	
1.4.1 Ausfall der Stromversorgung, Spannungsschwankungen	2
1.4.2 Defekte Datenträger	2
1.4.3 Verlust gespeicherter Daten	2
1.4.4 Ausfall zentraler Serverkomponenten des Produktivsystems	1

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

9. **Dokumentationsrichtlinien**

Sind in der Einheit angemessene IT-Dokumentationsrichtlinien in Kraft, mit denen sichergestellt wird, dass die Dokumentation umfassend, auf dem aktuellen Stand und für die relevanten Mitarbeiter zugänglich ist?

Ja, angemessene Richtlinien liegen vor und sind im Intranet der "Unternehmensgruppe" für alle Mitarbeiter einsehbar. Über Änderungen werden die Mitarbeiter laufend durch die IT-Abteilung informiert

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

10. **Monitoring von Kontrollen**

Gibt es eine regelmäßige Überwachung und Berichterstattung hinsichtlich der Wirksamkeit der IT-Kontrollen an das Management?

Das Management oder die interne Revision führen in regelmäßigen Abständen Kontrollen durch. Monatlich erfolgt im Rahmen von Leitungssitzungen eine Berichterstattung des IT-Leiters an das Management.

Das Unternehmen führt IT-Kontrollen durch, wie z. B.

- die Überprüfung der Datensicherungen
- die Einrichtung der Zutritts- und Zugriffskontrollen und Berechtigungen
- Aktualität und Einhaltung der Richtlinien

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management - Monitoring von IT-Systemen

Was wird überwacht:

- IT-Systeme (von Servern und Clients bis hin zu einzelnen Druckern)

Wie erfolgt die Überwachung?:

- Systemüberwachung (z. B. Verfügbarkeit, CPU, Speicher)
- Sicherheitsüberwachung (z. B. Log-Analyse, Angriffsversuche)
- Backup-/Job-Monitoring (z. B. Erfolg von Sicherungen)

Reaktion/Auswertung:

- Visuelle Auswertungen (z. B. Dashboards)
- Automatische Warnmeldungen per E-Mail oder SMS
- Monitoring-Reports

! Einsatz von ganzheitlichen Tools!

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

11. Kompetenzen der IT-Mitarbeiter

Gibt es Prüfungshandlungen, um sicherzustellen, dass IT-Mitarbeiter die entsprechenden Schulungen durchlaufen und die erforderlichen Fähigkeiten erworben haben?

Das IT-Personal ist langjährig erfahren und nimmt auskunftsgemäß auch regelmäßig an Schulungen und Veranstaltungen der Softwareanbieter teil. Für alle Bereiche, wo spezielles Wissen erforderlich ist, werden Dienstleister herangezogen.

12. Dokumentation von Anwendungen

Sind dokumentierte Prüfungshandlungen vorhanden, in denen die Methoden für die ordnungsgemäße Verarbeitung von Geschäftsvorfällen in jeder Anwendungen erläutert werden?

Vgl. Softwaretestat ERP-System, Handwerkerkopplung und Archiv, es liegt eine entsprechende Anwenderdokumentation sowie eine Betriebsdokumentation vor.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

13. **Automatisierte Prozesse**

a. Sofern die Einheit auf automatisierte Prozesse vertraut, werden diese überwacht, um deren vollständige Ausführung sicherzustellen?

b. Wie werden Berichte über Ausnahmen generiert und verarbeitet?

Automatisierte Prozesse wie die Sollstellung, Abschreibungen, Beko-Abrechnung, Aktivierung unfertige Leistungen etc. laufen nicht vollständig automatisch und unterliegen einer Kontrolle/ Freigabe. Voll automatisierte Prozesse sind nicht im Einsatz

➔ In diesem Fall bei a) und b) die Antwort „N/A“ wählen

Beispiele für automatisierte Prozesse

- Verbuchung der Bestandserhöhung/ unfertige Leistungen bei den Betriebskosten
- Darlehenssollstellung
- mtl. Sollstellung der Mieten/ Mieterhöhungen

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Corporate Governance, IT-Governance und Management

14. **Lizenzierung**

Sind geeignete Verfahren implementiert, um die Einhaltung von Gesetzen und Vorschriften in Bezug auf Lizenzierungsanforderungen und den Umgang mit urheberrechtlich geschütztem Material oder Rechten am geistigen Eigentum sicherzustellen?

Die Überwachung der ordnungsgemäßen Lizenzierung erfolgt durch den Leiter der EDV. Er führt entsprechende Listen und gleicht diese regelmäßig ab.

Exkurs Überwachung von Lizenzen

- Sehr wichtig und kann für die Unternehmen sehr teuer werden
- Eine große Rolle spielen vor allem Microsoft Lizenzen (Server, Datenbank, Clients, Office etc.)
  - Microsoft gleicht diese automatisiert ab
  - Falls Unternehmen nicht genug Lizenzen haben kann Microsoft Strafzahlungen erheben
- Im Bereich ERP-System ist das Risiko eher gering, da i.d.R. nur so viele Mitarbeiter auf das System zugreifen können wie Lizenzen vorhanden sind (insbesondere bei SaaS-Lösungen)

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Datenverwaltung

15. Klassifizierung und Vertraulichkeit von Daten

Sind Richtlinien vorhanden und dokumentiert, anhand derer die Informationen sowie die zugrunde liegenden ergänzenden Daten klassifiziert werden, um sicherzustellen, dass sie ausschließlich in dem nötigen Umfang zugänglich sind und dass sie entsprechend den maßgeblichen Gesetzen und Vorschriften gehandhabt werden?

Über das implementierte Berechtigungskonzept wird sichergestellt, dass nur berechtigte Personen auf Daten und Informationen zugreifen können. Eine Datenklassifizierung, die die Daten in entsprechende Schutzklassen einteilt wird im ERP-System nicht verwendet. Die Zugriffsteuerung erfolgt modulbezogen. Eine Datenklassifizierung gem. DSGVO ist in eingerichtet (Thema: Löschkonzept)

Exkurs Datenklassifizierung

- In der Wohnungswirtschaft wird durch die verwendeten ERP-Systeme im Rahmen des Berechtigungsmanagements bereits eine einfache Datenklassifizierung der rechnungsrelevanten Daten vorgenommen.
- Die DSGVO fordert eine Datenklassifizierung (auch wegen des Löschkonzepts) für personenbezogene Daten (Vertraulichkeit), das Gesetz zum Schutz von Geschäftsgeheimnissen auch für die anderen Daten.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Datenverwaltung

16. Datenspeicherung

a. Werden in den Richtlinien für die Datenspeicherung geltende Gesetze und Vorschriften, einschließlich Datenschutzgesetzen, Steuergesetzen und sonstigen gesetzlichen Bestimmungen eingehalten?

Die Gesellschaft hat eine Datenschutzrichtlinie implementiert sowie Festlegungen zur Aufbewahrung und Verfügbarkeit in einer IT-Sicherheitsrichtlinie getroffen. Die Überwachung erfolgt durch den Datenschutzbeauftragten. Dieser führt jährlich ein Audit durch.

b. Werden die Richtlinien regelmäßig geprüft und sind sie ordnungsgemäß dokumentiert?

nichts gegenteiliges festgestellt

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Fortführung des Geschäftsbetriebs

19. **Wiederherstellung im Notfall**

a. Wurden angemessene Sicherheitsvorkehrungen getroffen, um sicherzustellen, dass zentrale IT-Systeme bei Unterbrechung des Betriebs wiederhergestellt werden können?

entsprechende Sicherheitsvorkehrungen liegen vor, vgl. IT-Sicherheitskonzept

b. Werden die Richtlinien regelmäßig geprüft und sind sie ordnungsgemäß dokumentiert?

eine laufende Aktualisierung liegt in Verantwortung der IT/EDV-Abteilung

20. **Tests**

Werden Pläne für die Fortführung des Geschäftsbetriebs regelmäßig dokumentiert, aktualisiert und getestet?

Regelmäßige Tests der Notfallpläne werden durchgeführt und entsprechend dokumentiert. Dokumentation siehe Referenz.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Fortführung des Geschäftsbetriebs

21. Externe Speicherung

a. Werden alle kritischen Sicherungsmedien, Dokumentationsunterlagen, Daten und sonstigen erforderlichen Ressourcen für die IT-Wiederherstellung an einem externen Standort aufbewahrt?

Die Sicherungsmedien werden in einer anderen Brandschutzzone und zusätzlich am Außenstandort der Gesellschaft sowie als Cloudsicherung in einem externen Rechenzentrum aufbewahrt.
Die Vorgehensweise ist in der IT-Sicherheitsrichtlinie (vgl. Ref.) dokumentiert.

b. Ist die Sicherungsrichtlinie dokumentiert und wird ein Sicherungsprotokoll gepflegt?

Ja, vgl. Referenz.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Informationssicherheit

23. Sicherheitsverwaltung

Sind Administratorkonten auf autorisiertes Personal beschränkt und wird der Zugriff auf die betreffenden Konten überwacht?

Die Administratorenkonten sind durch entsprechende Passwörter gesichert. Alle Admin-Konten sind personalisiert. Eine Passwortrichtlinie liegt vor, diese sieht für diese Konten eine Mindestpasswortlänge von 18 Zeichen vor. Die Admin-Zugänge für die Administratoren der Dienstleister (Fa. XY) müssen neu freigegeben werden. Dies gilt besonders für das Konto „WFW“, dass als Mehrfachuser durch den Dienstleister genutzt wurde. Eine Überwachung der Konten erfolgt durch den IT-Leiter und ggf. im Rahmen von Prüfungen durch die interne Revision.

- Es sollten ausschließlich personalisierte Administratorkonten verwendet werden.
- Für die Absicherung der Administratorenkonten sollte eine 2-Faktor-Authentisierung oder eine Multifaktor-Authentisierung implementiert sein.
- Die Verwendung eines Administratorkontos sollte protokolliert werden, auch wer das Konto genutzt hat (falls kein personalisierter Admin im Einsatz war) – bspw. bei Notfallusern

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Informationssicherheit

26. **Zugriffsverletzungen**

Werden Sicherheitsverletzungen überwacht und nachbereitet?

Bei mehr als 5 fehlerhaften Anmeldungen wird das Konto automatisch für 30 Minuten gesperrt (Netzwerk).

Kennung	Beschreibung	Risiken	FT	Bemerkungen
KIT02	Kontrolle durch Zugriffschutz	RIT02	540.	gesonderte Dokumentation mit Referenz

Wie werden Falschanmeldungen behandelt?

Risiko hacking!

- Dauerhafte Sperre
- Sperre für eine gewisse Zeit, abhängig von der Anzahl der Fehlversuche
- Keine Reaktion auf Fehlversuche (hohes Risiko für „erfolgreiche“ Cyberangriffe)

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Informationssicherheit

Exkurs - Zugriffsverletzungen

- Ein Virenscanner und eine Firewall ist ein absolutes Muss in einem IT-System, ohne darf kein Zugriff auf das Internet erfolgen
- Der Virenscanner sollte zentral verwaltet werden, um unterschiedliche Versionen und Konfigurationen zu vermeiden

Exkurs - Logische Zugriffskontrollen

IDW RS FAIT 1 Tz 84 ff

- Logische Zugriffskontrollen sind wesentliche Elemente der Datensicherheit und des Datenschutzes und Voraussetzung zur Gewährleistung von Vertraulichkeit
- Die Sicherheitsanforderungen Autorisierung und Authentizität bedingen logische Zugriffskontrollen.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Informationssicherheit

Exkurs - Logische Zugriffskontrollen - Begriffe

(IDW RS FAIT 1 Kapitel 2.1, 2.2 und 2.3)

Integrität:

liegt vor, wenn Daten, Anwendungen und IT-Infrastruktur vollständig und richtig zur Verfügung stehen. Sie müssen vor Manipulation und fehlerhaften/ungewollten Änderungen bzw. Löschen geschützt sein.

Vertraulichkeit:

verlangt, dass von Dritten erlangte Daten nicht unberechtigt weitergegeben oder veröffentlicht werden.

Verfügbarkeit:

bedeutet, dass die Daten dann zur Verfügung stehen, wenn sie zur Durchführung des Geschäftsbetriebs notwendig sind. Zudem müssen die Daten und IT-Infrastruktur bei einer Störung in angemessener Zeit wieder zur Verfügung stehen.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531 und ORD.PP)

Informationssicherheit

27. **Mobile Computernutzung**

Sind angemessene Kontrollen für alle Computer (inkl. Mobilgeräten) eingerichtet?

Variante 1) => auskunftsgemäß derzeit noch nicht im Einsatz, nur Smartphones (Outlook) => Steuerung/Administration über Exchange (Kommunikationsserver) => ist angemessen

Variante 2) => Ein Mobile-Device-Managmentsystem (MDM) von XX ist seit Juni 202x und ein Application Management System (MAM) von der Fa. YY Mobile im Einsatz. => ist angemessen

Exkurs – Mobile Computing

- Wird eine Software zur Verwaltung von mobilen Endgeräten eingesetzt, z.B. mobile device management (MDM)?
- Werden sogenannte Containersysteme verwendet, die private Daten von dienstlichen Daten trennen?
- Werden mobile Geräte verschlüsselt und durch Kennwort oder Fingerabdruck gesichert (Multifaktorauthentifizierung – sollte bei externen Geräten mit ERP-System-Zugriff Standard sein)?

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Informationssicherheit

28. **Remote-Zugriff**

Sind angemessene Kontrollen für die Autorisierung und Steuerung des Remote-Zugriffs eingerichtet?

Berücksichtigen Sie Folgendes:

- VPN
- Remote-Desktop
- Software für Remote-Zugriff

Der Remote Zugriff wird über das Programm XY realisiert. Der Zugang ist nur mit Genehmigung des Admins zulässig. Der ERP-System-Anbieter setzt das Programm XY ein, der Zugriff muss von dem betroffenen Mitarbeiter aktiv zugelassen werden.

Exkurs – Remote Zugriff (1)

- Setzt das Unternehmen VPN Verbindungen ein, um Mitarbeiter, die bspw. im Home Office arbeiten anzubinden?
- Können Mitarbeiter über einen Remote-Desktop Zugriff auf das Netzwerk zugreifen?
- Wird für den Remote-Desktop Zugriffe ein spezielles Programm verwendet?
- Können Support-Dienstleister auf das System zugreifen?
- Werden die Remote-Aktivitäten protokolliert?

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Informationssicherheit

Exkurs – Remote Zugriff (2)

Über eine Fernwartung kann der Dienstleister möglicherweise Daten verändern, ohne dass das Unternehmen davon Kenntnis erhält.

Die Mindestanforderung ist deshalb, dass das Unternehmen den Zugriff erlauben muss.

➔ **ODER** Personalisierter Zugang mit Zwei-Faktor-Authentifizierung!

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Informationssicherheit

29. **Verschlüsselung**

Wird die Vertraulichkeit sensibler Informationen durch Verschlüsselung geschützt?

- Nach außen VPN-Tunnel => Verschlüsselung: AES256 und Krypto Hash: SHA2 256
- Handys mit PIN
- Laptops ohne Verschlüsselung
- Ansonsten erfolgt der Zugriff auf Daten über die Steuerung durch Berechtigungen (Verzeichnisse im Netzwerk)

Fragestellungen:

- Werden vertrauliche Informationen verschlüsselt?
- Welches Programm wird zur Verschlüsselung eingesetzt?
- Ist das Programm zertifiziert?
- Wer kann die Verschlüsselung aufheben?
- Was passiert, wenn das Passwort vergessen wird?

Es wird empfohlen, alle mobilen Geräte, die Daten enthalten können, zu verschlüsseln (Tablet, Notebook, Laptop, Smartphone)

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Änderungsmanagement

31. **Hardware**

Ist ein formal genehmigter und überwachter Prozess zum Verwalten von Änderungen an Hardware vorhanden?

Hardwareänderungen sind im IT-Invest/Maßnahmeplan aufgenommen und werden im Rahmen des Wirtschaftsplans durch die GF genehmigt.

Fragen:

- Gibt es eine zentrale Einkaufsabteilung?
- Gibt ein Verfahren, das sicherstellt, dass die Beschaffung von Hardware den gesetzlichen Vorschriften entspricht?
- Nach welchen Kriterien werden Hardwareänderungen eingeleitet, beispielsweise Kapazitätsengpässe oder „vorrausschauend“?

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Änderungsmanagement

32. **Zugelassene Systeme**

Verfügt die Einheit über eine Liste formal genehmigter Programme, Datenbanken und Betriebssysteme?

Die Gesellschaft führt eine Inventarliste, Mitarbeiter können und dürfen keine Software selbständig installieren (vgl. IT-Sicherheitsrichtlinie). Es werden nur lizenzierte Programme installiert.

Fragen:

- Dürfen im Unternehmen nur genehmigte Programme eingesetzt werden?
- Dürfen die Anwender selbständig Software installieren?

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Änderungsmanagement

34. **Dokumentation**

Werden Änderungen an Hardware, Programmen, Datenbanken und Betriebssystemen angemessen dokumentiert?

Alle Änderungen an Hardware und Software werden in einer Inventarliste aufgeführt.

Fragen:

- Gibt es ein geregeltes Testverfahren für neue Hardware oder Software?
- Gibt es ein geregeltes Dokumentations-verfahren mit Hilfe von standardisierten Testfällen?

Änderungen an Software, Hardware oder Konfigurationen sollten vollständig dokumentiert werden.

Dokumentation sollte von den Anforderungen über die Umsetzung, Test bis zur Produktivsetzung in einem zentralen System (Ticketsystem) erfolgen ➔ Idealfall bei Großunternehmen.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Änderungsmanagement

35. **Testumgebung**

Werden alle wesentlichen Änderungen an Hardware, Programmen, Datenbanken und Betriebssystemen vor der Implementierung getestet?

Es handelt sich um eine ERP-Software im SaaS-Model. Im RZ existiert eine isolierte Testumgebung.

Für die lokalen System gibt es wegen der Größe der Gesellschaft keine isolierte Testumgebung. Bei Update der Betriebssysteme (Windows) werden die Änderungen durch den Administrator getestet bevor die Änderungen an alle Mitarbeiter verteilt werden. Außer bei kritischen Zero Day Updates.
Hier erfolgt die Verteilung ohne Tests. Größere rechnungslegungsrelevante Eigenentwicklungen gibt es nicht

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Dienstleister

36. **Dienstleister**

Ist ein eindeutig definierter Vertrag mit einer Beschreibung der Schlüsselaspekte der Vereinbarung vorhanden?

Die Gesellschaft hat einen Support- und Wartungsvertrag mit der XY abgeschlossen. Die ERP-Software wird in einem Rechenzentrum (kurz: RZ) der XY in XY betrieben. Zum RZ-Betrieb liegt ein Datenverarbeitungsvertrag mit AVB (Allgemeinen Vertrags-bedingen) sowie eine aktuelle Testierung nach IDW PS 951 Typ 2 vor.

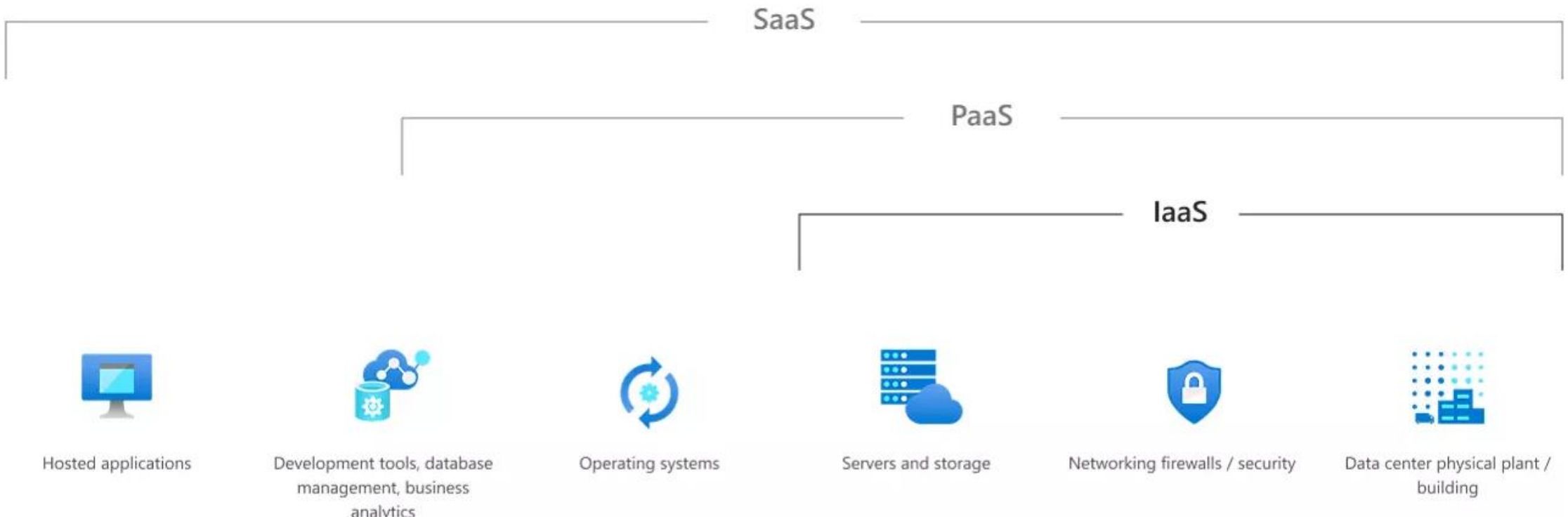
Exkurs

- Große Rechenzentren werden regelmäßig geprüft, maßgeblich ist der IDW PS 951 Typ 1 oder Typ 2
- Bei international agierenden Dienstleistern (Cloud) gibt es auch den ISAE 3402
- Weitere gängige Standards sind auch ISO 27001 Zertifizierungen

➔ Testate/Zertifizierungen als **Grundlage zur Risikobeurteilung** der Auslagerung an einen Dienstleister heranziehen!

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Exkurs – Verträge mit Dienstleistern (Überblick) => weitere Informationen siehe Exkurs (Anlage)



VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Dienstleister

37. **Einhaltung der IT-Richtlinien**

Werden Verträge mit Dienstleistern in Übereinstimmung mit vorhandenen IT-Richtlinien und -Standards der Einheit bewertet und überwacht?

Die Dienstleister arbeiten nur nach Anweisung auf den Systemen der Gesellschaft. Entsprechende Vereinbarungen wurden getroffen. Eine Überwachung erfolgt durch die Mitarbeiter der IT-Abteilung.

Servicelevel Agreement (SLA) ist eine Vereinbarung zwischen einem Servicegeber und Servicenehmer über Quantität und Qualität von Service-leistungen.

Bestandteile eines SLA

- Vertragspartner
- Übergabepunkte / Schnittstellen
- Serviceumfang
- Qualitätsmerkmale
- Messkriterien
- Berichtswesen
- Rechte und Pflichten
- Ziel und Umfang der Vereinbarung
- Dienstleistungen im Detail
- Antwortzeitverhalten / Performance
- Organisatorische Regelungen

Problem: In der Praxis ist oft keine Dokumentation bzw. Kontrolle vorhanden – es wird sich auf Dienstleister verlassen!

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Genauigkeit, Vollständigkeit und Echtheit

40. **Fehlervermeidung**

Sind Programme konfiguriert, mit denen sichergestellt wird, dass im Bedarfsfall Fehlervermeidungs-, Fehlererkennungs- und Fehlerbehebungsroutinen ausgeführt werden?

Die Mitarbeiter werden regelmäßig, vor allem bei neuen Anwendungen, geschult.
Programminterne Kontrollen sorgen dafür, dass Fehlereingaben rechtzeitig schon bei der Eingabe erkannt werden (vgl. Softwaretestat).
Bei Fehlern werden diese über das Ticketsystem der Fa. XY gemeldet und von dieser je nach Dringlichkeit beseitigt.

Sind bei der Anwendungssoftware Fehler bekannt?

Hinweise sind möglicherweise im Softwaretestat (IDW PS 880) zu finden!

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Genauigkeit, Vollständigkeit und Echtheit

41. **Fehlerbehandlung**

Sind schriftlich fixierte Verfahren zum Beheben von Fehlern vorhanden?

Ein schriftlich dokumentiertes Verfahren zur Fehlerbehandlung ist nicht eingerichtet. Fehler werden zentral über das Ticketsystem der Fa. XY gemeldet und vom Dienstleister beseitigt.
Die Dokumentation dazu erfolgt im Ticketsystem.

Bei einer ERP-Software, die in einem Rechenzentrum nach dem Modell SaaS betrieben wird, führt der Softwarehersteller notwendige Programmanpassungen durch und dokumentiert die Änderungen.

Bei einem Inhouse-System muss das Unternehmen die vom Softwarehersteller durchgeführten Programmanpassungen in Form von Updates selbst einspielen. (siehe auch Änderungsmanagement)

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Genauigkeit, Vollständigkeit und Echtheit

43. **Überschreiben von Daten**

Besteht die Möglichkeit, eingegebene Daten zu überschreiben, ist dieser Vorgang auf entsprechende Mitarbeiter und genehmigte Situationen beschränkt und wird hierfür ein Protokoll gepflegt und geprüft?

Buchungen können so lange diese vorläufig erfasst sind noch geändert werden. Nach der Verbuchung von Geschäftsvorfällen sind nur Stornierungen möglich.
Änderungen bei den Stammdaten sind möglich und werden protokolliert.
Die Verbuchung von Geschäftsvorfällen wird ebenfalls protokolliert.

44. **Prüfpfad**

Stellt das System Protokolle für einen Prüfpfad für ausgeführte Programme und alle verarbeiteten Geschäftsvorfälle bereit?

Entsprechende Protokolle werden durch das System automatisiert erstellt (bspw. bei Sollstellungen, Lastschriftlauf, Wertberichtigungen auf Forderungen etc.).

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Genauigkeit, Vollständigkeit und Echtheit

45. **Dokumente außerhalb von Rechnungslegungsanwendungen**

Sind Kontrollen in Fällen implementiert, in denen bedeutsame Dokumente außerhalb des Systems für Rechnungslegungsanwendungen ausgearbeitet wurden (z. B. Kalkulationstabellen oder Word-Dokumente)?

Außerhalb des ERP-Systems werden insbesondere Kalkulationen (bspw. für Mieten oder Angebote) in den Abteilungen auf den jeweiligen Serverlaufwerken abgelegt.
Für die Serverlaufwerke liegen entsprechende Berechtigungskonzepte vor, so dass die Dateien nur Befugte lesen und ggf. ändern können. Perspektivisch sollen Kalkulationen in elektronischen Archivsystem abgelegt werden.

Trennung von Funktionen

47. **IT-Mitarbeiter**

Sind IT-Mitarbeiter von der Initiierung und Autorisierung von Geschäftsvorfällen ausgeschlossen?

IT-Mitarbeiter sind insbesondere vom Zahlungsverkehr und der Verbuchung von Geschäftsvorfällen ausgeschlossen (vgl. auch Organigramm - eDA und Stellenbeschreibung)

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Sonstiges

48. Elektronischer Handel

Gibt es geeignete Kontrollen in Bezug auf folgende Sachverhalte:

a. Dolose Handlungen?

b. Datenschutz?

c. Verarbeitung von Geschäftsvorfällen, einschließlich von Maßnahmen, mit denen verhindert werden soll, dass Geschäftsvorfälle ausgelassen oder dupliziert werden?

Es wird kein E-Commerce (elektronischer Handel) betrieben.

49. Datenaustausch

Sind geeignete Verträge und Protokolle für den elektronischen Datenaustausch (EDI) vorhanden?

EDI-Verfahren werden nicht genutzt. (kann bspw. auch eine Schnittstelle zur Warenwirtschaft sein)

EDI (Electronic Data Interchange):

EDI ist ein Verfahren, mit dem Daten in strukturierter Form (ein Bild ist nicht strukturiert) nach standardisierten Verfahren und in standardisierter Form übertragen werden. Der Übermittlungsprozess geschieht automatisch. Das Format EDIFACT ist am weitesten verbreitet, auch Elster gehört zu den EDI- Verfahren.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Warum gibt es ORD.PP?

- ORD.PP dient der Prüfung, ob die Buchführung den gesetzlichen Vorschriften und den ergänzenden Bestimmungen des Gesellschaftsvertrags oder der Satzung entspricht (§ 321 Abs. 2 Satz 1 HGB)
- Ferner wird abgeprüft, ob das IT-gestützte Buchführungssystem die im IDW RS FAIT 1 konkretisierten gesetzlichen Anforderungen (Sicherheit der rechnungslegungsrelevanten Daten und IT-Systeme) erfüllt
- Dies ist ein Pflichtdokument!
  ➔ **Ausnahme:** Voraussetzungen für 531.ORD.MIN liegen vor

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Systemüberblick

Dies ist die einzige Frage in Bezug auf eine vorliegende Softwarebescheinigung.

1. SOFTWAREBESCHEINIGUNG

Holen Sie für eingesetzte rechnungslegungsrelevante Programme eine Softwarebescheinigung ein (falls verfügbar). Prüfen Sie die Versionsnummer der Software und auf der Softwarebescheinigung! Beurteilen Sie, ob die in der Softwarebescheinigung genannten Bedingungen zu Installation und Einsatz der Software von der Einheit erfüllt werden.

Fertiggestellt ohne Beanstandungen ☐

Für das eingesetzte ERP-Programm Wodis Sigma liegt eine Softwarebescheinigung vor.
Es handelt sich um einen vollständigen Bericht und die Versionen stimmen überein.
Der Bericht enthält keine Einschränkungen in Bezug auf die Software.

ODER

Für die rechnungslegungsrelevanten Programme liegt keine (verwertbare) Softwarebescheinigung vor.

Hinweis: Keine Berücksichtigung bei der Verwertung von Prüfungsergebnissen Dritter (MEMO.PA7, Frage 6ff.) notwendig

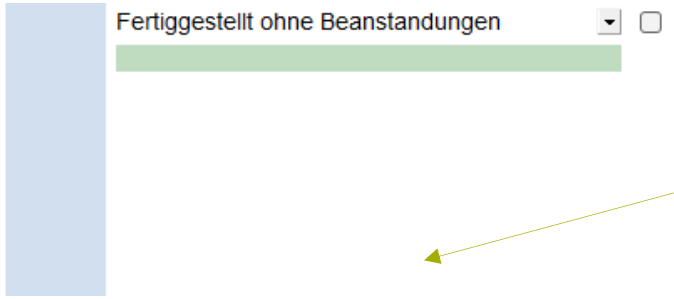
VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Systemüberblick

2. FINANZBUCHHALTUNGSSYSTEM

Beurteilen Sie die Komplexität des Buchhaltungssystems (z.B. ERP-System) und verschaffen sich einen Überblick über die einzelnen Nebenbücher und Schnittstellen zum Hauptbuch. Handelt es sich um manuelle oder automatische Schnittstellen? Nebenbücher können z.B. sein:

- Anlagenbuch,
- Debitoren-, Kreditorenbuch,
- Personal-, Zeiterfassungssysteme
- Materialwirtschaft



Hier Abfrage der Komplexität des IT-Systems

Als ERP-System wird ein Standardsystem (XY) mit den typischen Nebenbüchern (Anbu, Darlehen, Miete, BK, Debitoren/Kreditoren etc.) eingesetzt. Weiterhin gibt es eine Warenwirtschaft zur Tochter-gesellschaft, die Personalbuchhaltung wird intern über Sage abgewickelt. Es liegt eine umfangreiche Serverinfrastruktur vor und es sind ca. 150 IT-Arbeitsplätze (Clients) angebunden. Das System kann als komplex eingestuft werden.

Es ist zu entscheiden, ob bei einem komplexen System die Prüfungshandlungen ausgeweitet werden müssen (ggf. ist ein IT-Spezialist hinzuzuziehen)

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Organisation und allgemeine Funktionen

3. ÜBERBLICK

Verschaffen Sie sich einen Überblick über die Organisation der Buchführung (z.B. durch Einholung Organigramm, Organisationsanweisungen, Richtlinien) und prüfen Sie, ob im Geschäftsjahr wesentliche Änderungen erfolgt sind.

Fertiggestellt ohne Beanstandungen ☐

Dauerakte

Es liegen umfangreiche Dokumentationen vor. Bzgl. Organigramm, Organisations-anweisungen und Richtlinien vgl. eDA. Im Geschäftsjahr ergaben sich keine wesentlichen Änderungen.

Fragen nach wesentlichen Software- oder Hardwareänderungen, geplanten Auslagerungen etc.

Hier alle Unterlagen zur Organisation der Buchhaltung einsammeln (Unterlagen für eDauerakte)

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Organisation und allgemeine Funktionen

4. AUFGABENVERTEILUNG UND KOMPETENZEN

Prüfen Sie, ob hinsichtlich der Buchführung die Aufgaben und Kompetenzen eindeutig geregelt wurden und angemessene Stellvertreterregelungen vorliegen.

Fertiggestellt ohne Beanstandungen ☐

! (RRL03) Hinweise auf dolose Handlungen

(KRL01) Berechtigungskonzept Finanzbuchhaltung

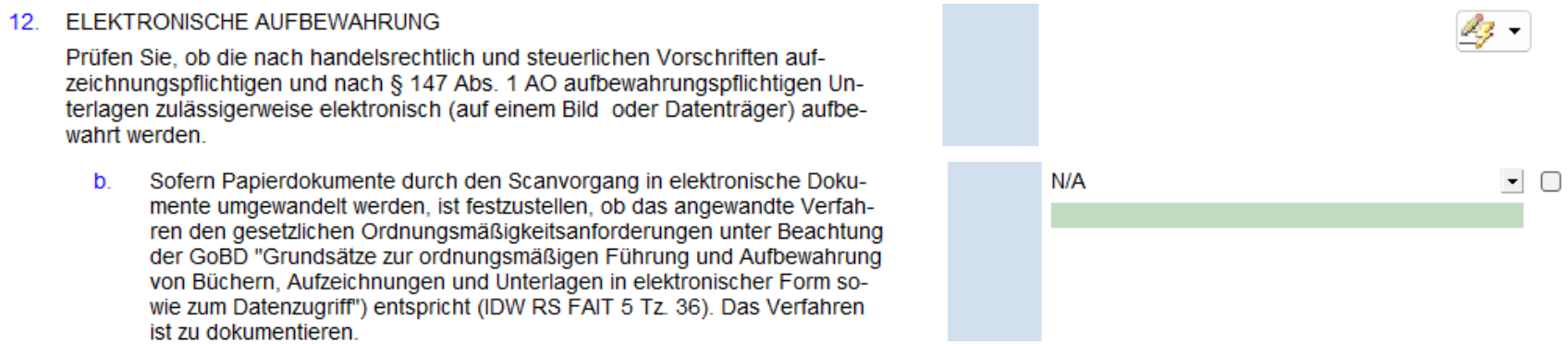
Gespräch mit dem Leiter ReWe geführt und Einsicht in Berechtigungskonzept genommen (vgl. Gesprächsnotiz in Ref.).

Diese Frage zielt auf das eingerichtete Berechtigungskonzept ab:

- Wer darf was und gibt es Vertretungsregeln?
- Sind die im Unternehmen handelnden Personen kompetent?
- Bekommen die Mitarbeiter ausreichende Schulungen?
- Insbesondere in Bezug auf die Softwarebenutzung?

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Organisation und allgemeine Funktionen



Ersetzendes Scannen ist im Unternehmen im Einsatz. Als Archivsystem wird Archiv kompakt genutzt. Eine Verfahrensdokumentation zum ersetzenden Scannen liegt vor.

Siehe 531.ORD.MIN => hier wird tiefer nachgefragt als bei ORD.MIN

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Kontenzuordnung und Schnittstellen

16. AUSGLEICH DER HAUPTABSCHLUSSÜBERSICHT
Prüfen Sie, ob die Hauptabschlussübersicht (HÜ) auf „Null“ aufgeht.

Fertiggestellt ohne Beanstandungen ☐

Ja, die Hauptabschlussübersicht geht auf, vgl. Referenz.

Referenz bspw. auf CaseWare 5.2.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Periodenabschluss



Der Saldenvortrag ist ordnungsgemäß erfolgt, vgl. Abstimmung in Ref.

Vorträge aus der vorliegenden Saldenliste vom Mandaten mit den eigenen Vorträgen gemäß Vorjahresprüfungsbericht (CaseWare) abstimmen und Referenzieren

- Besprechung mit dem Leiter Rechnungswesen, wie er dies sicherstellt
- Dies erfolgt in der Regel automatisiert im Rahmen der Eröffnung eines neuen Wirtschaftsjahres im ERP-System
- Da nach der Eröffnung eines Wirtschaftsjahres noch Buchungen im Vorjahr erfolgen, müssen die Vorträge nach Erstellung des Jahresabschlusses aktualisiert werden

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Steuerliche Vorschriften

18. STEUERLICHE AUSSENPRÜFUNG

Stellen Sie fest, ob im Rahmen einer steuerlichen Betriebsprüfung (oder vergleichbarer Prüfungen) Feststellungen zur Ordnungsmäßigkeit der Buchführung gemacht wurden und beurteilen Sie sich daraus ergebene Konsequenzen.

N/A

Die letzte Betriebsprüfung in 2024 ergab keine Feststellungen hinsichtlich der Ordnungsmäßigkeit der Buchführung. Vgl. eDA Steuerliche Verhältnisse.

- Besprechung mit dem Leiter Rechnungswesen und Durchsicht der vorliegenden Berichte über steuerlichen Betriebsprüfungen
- Soweit Beanstandungen der Steuerbehörden zur Ordnungsmäßigkeit der Buchführung vorliegen, ist nachzuvollziehen, wie die Schwächen vom Unternehmen beseitigt worden sind

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Steuerliche Vorschriften

19. GOBD

Prüfen Sie, ob die Anforderungen der § 147 Abs. 5 und 6 AO sowie der GOBD („Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff") durch die Einheit erfüllt werden. Stellen Sie sicher, dass die Einheit

- die Aufbewahrungsvorschriften erfüllt und
- die gesetzlichen Zugriffsmöglichkeiten auf die Aufzeichnungen erlaubt.

Fertiggestellt ohne Beanstandungen ☐

Ja, die gesetzlichen Aufbewahrungsfristen werden eingehalten. Die notwendigen Zugriffsmöglichkeiten (Schnittstellen) sind gegeben, bzw. können über den Softwarehersteller die Datenabzüge angefordert werden.

- Besprechung mit dem Leiter Rechnungswesen, ob der GOBD Zugriff eingerichtet ist
- Zu den Aufbewahrungsfristen wurde bereits in Fragen 11 und 12 beantwortet.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Steuerliche Vorschriften

20. ANFORDERUNGEN AN KASSEN/ KASSENSYSTEME

Prüfen Sie das Vorhandensein der nach GoB/GoBD erforderlichen Unterlagen für manuelle Kassen bzw. elektronische Kassensysteme.

§ 146 Abs. 1 AO

Es werden keine derartigen Kassensysteme eingesetzt.

Solche Systeme werden bei Wohnungsunternehmen i.d.R. nicht eingesetzt.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Kommunikation mit dem Management und dem Aufsichtsorgan, Berichterstattung

21. Stellen Sie sicher, dass bedeutsame Schwächen des rechnungslegungsbezogenen Internen Kontrollsystems dem Aufsichtsorgan sowie den gesetzlichen Vertretern und ggf. anderen Führungskräften in angemessener Zeit schriftlich mitgeteilt werden (IDW PS 261 Tz. 89).

Darüber hinaus ist im Prüfungsbericht im Abschnitt „Buchführung und weitere geprüfte Unterlagen“ auf bestehende Mängel in der Buchführung und auf ihre Auswirkung auf die Rechnungslegung sowie ihren Einfluss auf das Prüfungsergebnis hinzuweisen (IDW PS 450 Tz. 65).



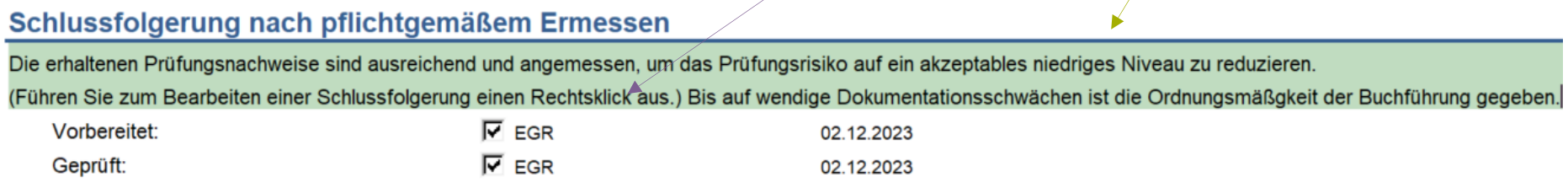
Es haben sich keine bedeutsamen berichtspflichtigen Beanstandungen ergeben.

- Soweit nicht bedeutsame Beanstandungen vorliegen sind dies als "Wichtige Prüfungsfeststellungen" im Dokument 320 (als Aufgaben) zu erfassen
- Ein berichtspflichtiges Element wird im Dokument 360. gezeigt
- Die Erfassung erfolgt entweder direkt dort oder über die Erfassung eines bedeutsamen Risikos oder einer damit zusammenhängenden Kontrolle (siehe auch Dokument 540.)

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Schlussfolgerung

- Am Ende der Prüfungshandlungen wird noch eine abschließende Beurteilung abgegeben
- Um diese einzufügen, muss dort mit der rechten Maustaste hin geklickt werden
- Es erscheint "Schlussfolgerung bearbeiten„
- Danach wird das Dokument abgezeichnet



VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP) - Exkurs

Corporate Governance, IT-Governance und Management 531.

zu 531. Frage 13 Dokumentation von Anwendungen (1)

13. **Dokumentation von Anwendungen**

Sind dokumentierte Prüfungshandlungen vorhanden, in denen die Methoden für die ordnungsgemäße Verarbeitung von Geschäftsvorfällen in jeder Anwendungen erläutert werden?

Die Dokumentation der Anwendung sollte mindestens folgende Inhalte umfassen (Exkurs):

a) Allgemeine Beschreibung
b) Anwenderdokumentation

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP) - Exkurs

Corporate Governance, IT-Governance und Management

zu 531. Frage 13 Dokumentation von Anwendungen (2)

Anwenderdokumentation:

- Die Anwenderdokumentation muss alle Informationen beinhalten, die für eine sachgerechte Bedienung einer IT-Anwendung erforderlich sind
- Gegenstand der Anwenderdokumentation sind eine Beschreibung der fachlichen Prozesse, insbesondere der Datenerfassung, Prüfung, Abstimmung und Ausgabe der Daten sowie eine Liste der Daten- und Dokumentenbestände einschließlich der Aufbewahrungsregeln und Aufbewahrungsfristen.
- Weitere Inhalte bilden Schnittstellenbeschreibungen, Regeln für den Datenaustausch sowie Organisationsanweisungen und Benutzerhandbücher

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP) - Exkurs

Zu Corporate Governance, IT-Governance und Management

zu 531. Frage 13 Dokumentation von Anwendungen (3)

Die Dokumentation der Anwendung sollte mindestens folgende Inhalte umfassen (Exkurs):

Betriebsdokumentation

- Die Betriebsdokumentation muss alle Informationen beinhalten, die für eine sachgerechte Betrieb einer IT-Anwendung erforderlich sind
- Gegenstand der Betriebsdokumentation sind eine Beschreibung der Funktion einer Anwendung, die Systemarchitektur und die Darstellung der Schnittstellen zu anderen Systemen (extern und intern), die Systemvoraussetzungen, die Installation sowie das Starten und Stoppen der Anwendung, das Berechtigungsmanagement in der Anwendung und die regelmäßig mit der Anwendung verbundenen Tätigkeiten

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP) - Exkurs

Zu Corporate Governance, IT-Governance und Management

zu 531. Frage 13 Dokumentation von Anwendungen (4)

Die Dokumentation der Anwendung umfasst mindestens folgende Inhalte:

Technische Systemdokumentation

- Die technische Systemdokumentation enthält alle erforderlichen Informationen zur im Verfahren eingesetzten Hard- und Software
- Soweit keine intern entwickelten Lösungen zum Einsatz kommen, sollte bezüglich der Spezifikationen der einzelnen Komponenten auf Handbücher und technische Beschreibungen der Hersteller verwiesen werden

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP) - Exkurs

Zu 531. Informationssicherheit

Exkurs – Schadsoftware (1)

Computerviren

Viren sind die ältesten Schadprogramme. Sie können sich nur in einem Computer verbreiten. Um auf andere PCs zu gelangen, brauchen sie die „Hilfe“ des Computerbenutzers: Der muss eine vireninfizierte Datei weitergeben.

Würmer

Technisch gesehen sind Würmer Nachfolger der Viren. Sie können sich selbständig über Netzwerk- und Internetverbindungen von einem Computer zum anderen verbreiten (zum Beispiel per E-Mail). Deshalb treten sie inzwischen deutlich häufiger auf und richten mehr Schaden an als Viren.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP) - Exkurs

Zu 531. Informationssicherheit

Exkurs – Schadsoftware (2)

Trojaner

Diese Schädlinge tarnen sich als nützliche Hilfsprogramme. In ihnen stecken aber gut getarnte Schadprogramme. Trojaner werden in der Regel vom Computerbesitzer selbst auf den PC überspielt, oft in dem Glauben, eine gute Software im Internet kostenlos ergattert zu haben.

Spionage-Programme („Spyware“)

Sie gelangen oft über Trojaner in den Computer. Ihr Auftrag: Daten sammeln und weiterleiten, mit denen andere Zeitgenossen Geld machen können. Sei es, dass Sie auf Grund der von Ihnen besuchten Internetseiten massenhaft Werbung erhalten oder dass Betrüger mit Ihrer Kreditkartennummer einkaufen.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP) - Exkurs

Zu 531. Informationssicherheit

Exkurs – Schadsoftware (3)

Hintertür-Programme („Backdoor“)

Sie erlauben Computergaunern direkten Zugriff auf den Computer bis hin zur Fernsteuerung. So wurde schon mancher unvorsichtige PC-Benutzer zum Massenversender von Werbe-E-Mails.

Erpressungsprogramme („Ransomware“)

Verhindern oder schränken den Zugriff auf Daten und Systeme ein oder verhindern. Eine Freigabe dieser Ressourcen erfolgt nur gegen Zahlung eines Lösegeldes (engl. ransom). Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form von digitaler Erpressung.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP) - Exkurs

Zu 531. Informationssicherheit

Exkurs – Schadsoftware (4)

Betrügerische E-Mails („Phishing“)

Dies sind keine Schadprogramme, aber höchst gefährlich. Sie gaukeln als Absender etwa Ihre Bank vor und wollen Sie auf fingierte Internetseiten locken. Dort sollen Sie Ihre Konto-Zugangsdaten angeben. Mit den Daten wird dann Ihr Bankkonto geplündert.

Falschmeldungen

Die vorsätzlichen Falschmeldungen „informieren“ Sie über angebliche Sicherheitslücken des PCs. Bestenfalls fordern sie Sie nur zur Weiterleitung der Nachricht auf und müllen damit E-Mail-Postfächer zu. schlimmstenfalls empfehlen sie die Installation eines „Schutzprogramms“ aus dem Internet, das dann einen der oben genannten Schädlinge bekämpft.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP) - Exkurs

Zu 531. Frage 37 Dienstleister (1)

Verträge und Vereinbarungen (AGBs) müssen immer vorliegen. Besonders bei der Dienstleistung der **Systemadministration** wird oft auf eine vertragliche Regelung verzichtet, da die Dienstleistung nur bei Bedarf abgerufen wird. Dies stellt auch unter Datenschutzgesichtspunkten einen Mangel dar.

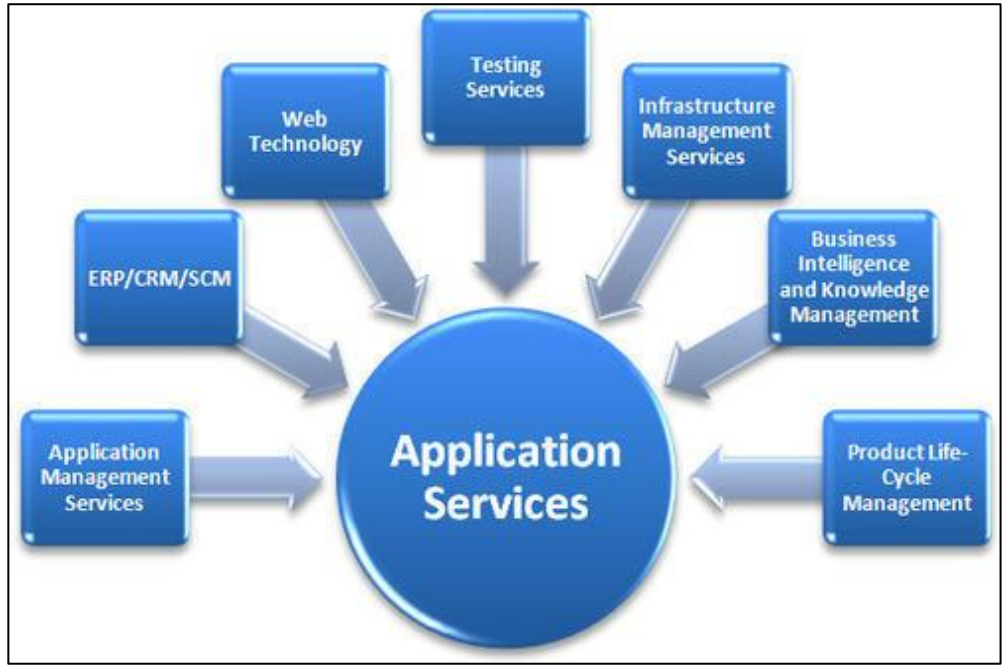
➔ Ist auch bei Mutter-/Tochter-Geschäftsbesorgungen ein Thema!

Der Buchführende ist **immer für die Daten verantwortlich**, deshalb muss er sich durch geeignete Kontrollmaßnahmen von der Richtigkeit der Dienstleistung überzeugen. Lassen Sie sich die Kontrollmaßnahmen beschreiben.

➔ In der Praxis ein schweres Thema, da kaum ein Reporting von Dienstleistern an den Auftraggeber erfolgt (Nachweis der Erbringung von Dienstleistungen).

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Zu 531. Frage 37 Dienstleister (2)



Exkurs – Verträge mit Dienstleistern (ASP)

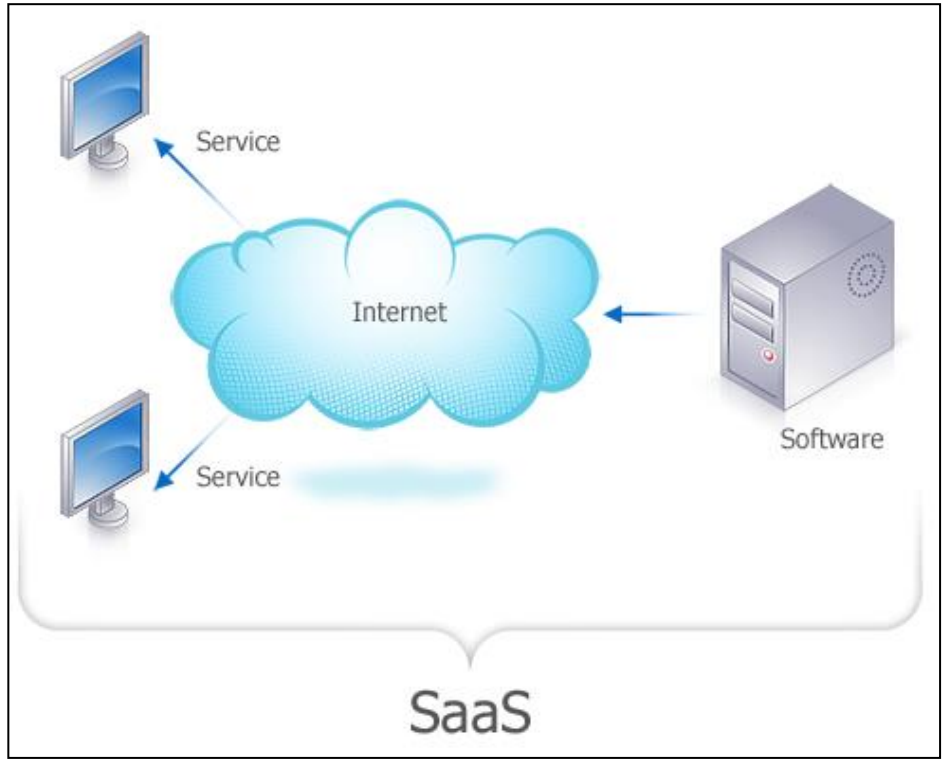
Bei einer ASP (Applikation Service Providing) Lösung laufen die Anwendungen in einem Rechenzentrum, die Anwendungen werden über eine spezielle Verbindung (Terminalserver-Technologie) zur Verfügung gestellt.

Jedem Betreiber wird eine individuelle Anwendung bereitgestellt

Die Software wird im Regelfall gemietet.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Zu 531. Frage 37 Dienstleister (3)



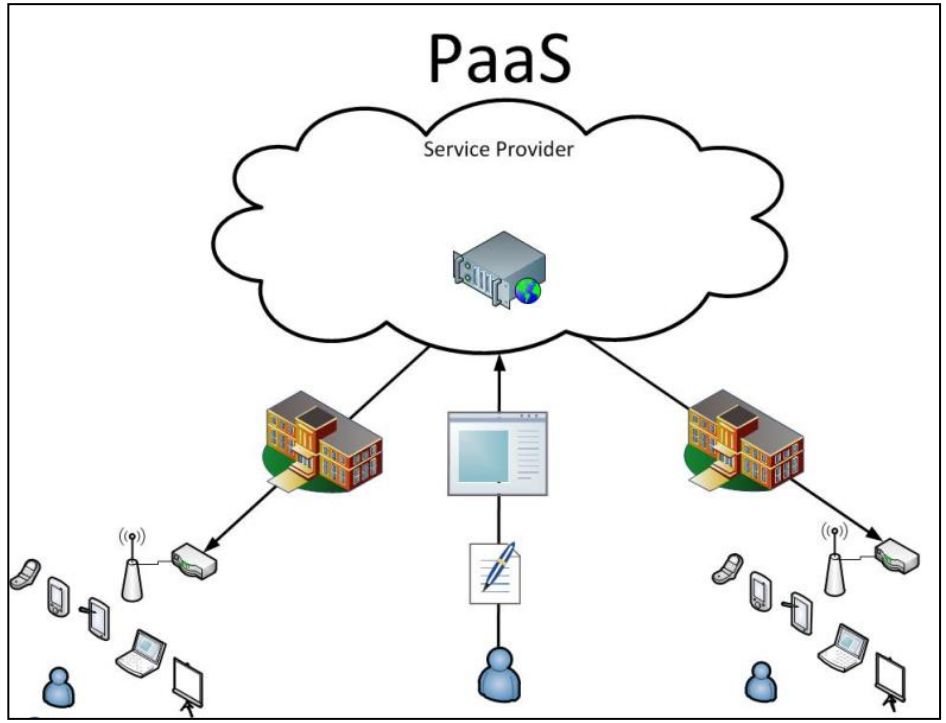
Exkurs – Verträge mit Dienstleistern (SaaS)

Bei einer SaaS (Software as a Service)
Lösung erfolgt der Zugriff auf die zentral (für eine Vielzahl von Kunden) bereitgestellten Anwendungen über das Internet und einen Browser.

Die Software wird im Regelfall gemietet.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Zu 531. Frage 37 Dienstleister (4)



Exkurs – Verträge mit Dienstleistern (PaaS)

Bei einer PaaS (Plattform as a Service) stellt der Dienstleister nur die Server, Speicher, Firewall etc. zur Verfügung, der Kunde nutzt im Regelfall eigene Anwendungen, für die er auch eine Lizenz erworben hat oder die er selbst erstellt hat.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Zu 531. Frage 37 Dienstleister (5)



Exkurs – Verträge mit Dienstleistern (IaaS)

Bei einer IaaS (Infrastructur as a Service) stellt der Dienstleister umfangreiche Infrastruktur (virtuelle Hardware, Serverleistung, verteilte Systeme zur Optimierung der Zugriffsgeschwindigkeit etc.) zur Verfügung.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Zu 531. Frage 37 Dienstleister (6)



Exkurs – Verträge mit Dienstleistern (Server-Hosting)

Beim Server-Hosting stellt der Dienstleister gemietete Server in einer Rechenzentrumsumgebung zur Verfügung

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP)

Zu 531. Frage 37 Dienstleister (7)



Exkurs – Verträge mit Dienstleistern (Serverhousing)

Beim Serverhousing beherbergt der Dienstleister Server des Kunden, die zusammen mit der genutzten Software auch Eigentum des Kunden sind.

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP) - Exkurs

Zu ORD.PP Frage 20 - Steuerliche Vorschriften

Exkurs – Elektronische Kassensysteme (1)

20. ANFORDERUNGEN AN KASSEN/ KASSENSYSTEME

Prüfen Sie das Vorhandensein der nach GoB/GoBD erforderlichen Unterlagen für manuelle Kassen bzw. elektronische Kassensysteme.

§ 146 Abs. 1 AO

es gibt entpsrechende Kassenrichtlinie, folgende Kassen werden betrieben:

1) Arena => elektr. Kassensystem
2) Campingplatz => elektr. Kassensystem
3) Hauptkasse => manuelle Handkasse mit Kassenbuch (laufen nur geringe Umsätze drüber)

a.	Stellen Sie fest, ob es sich bei der Kasse um eine offene Ladenkasse handelt. Beantworten Sie diese Frage mit "Ja" oder "Nein". es sind keine offenen Ladenkassen im Einsatz	Nein
b.	Prüfen Sie, ob für jede Verkaufsstelle Kassenaufzeichnungen entsprechend den gesetzlichen Vorgaben geführt werden und vorhanden sind. bei 1) und 2) elektr. Kasse und 3) händisches Kassenbuch (Kassenbesandsprotokoll vgl. IKS Finanzdispo) => des Weiteren gelten entsprechende DO	Ja

VII. Ausgestaltung und Einrichtung von allgemeinen IT-Kontrollen (531. und ORD.PP) - Exkurs

Zu ORD.PP Frage 20 - Steuerliche Vorschriften

Exkurs – Elektronische Kassensysteme (2)

c.	Prüfen Sie bei Einsatz von elektronischen Registrierkassen, ob	
	entsprechende Schreiben des EB liegen vor	
i.	die Speicherung der Einzelaufzeichnungen Folgendes beachtet: • Vollständigkeit der Daten (Bonierungen, Stornierungen, Zahlungsvorgänge) • Unveränderbarkeit der gespeicherten Daten • Datenexportmöglichkeit für das Finanzamt (Hinweis auf die besonderen Anforderungen und Aufbewahrungsmodalitäten nach dem BMF-Schreiben vom 26.10.2010, BStBl. I 2010, S. 1342).	Ja
	Exportmöglichkeit gegeben, durch zuständige Mitarbeiterin bei Frau XY am PC auch die entsprechenden Protokolle zeigen lassen, des weiteren gilt die entsprechende DA	
ii.	die Speicherung der Einzelaufzeichnungen Folgendes beachtet: • Vollständigkeit der Daten (Bonierungen, Stornierungen, Zahlungsvorgänge) • Unveränderbarkeit der gespeicherten Daten • Datenexportmöglichkeit für das Finanzamt (Hinweis auf die besonderen Anforderungen und Aufbewahrungsmodalitäten nach dem BMF-Schreiben vom 26.10.2010, BStBl. I 2010, S. 1342).	Ja
	Exportmöglichkeit gegeben, durch zuständige Mitarbeiterin bei Frau XY am PC auch die entsprechenden Protokolle zeigen lassen, des weiteren gilt die entsprechende DA	
iii.	Prüfen Sie, ob alle Einzeldaten von der Einheit, die durch die Nutzung der Kasse entstehen, während der Aufbewahrungsfrist von 10 Jahren aufbewahrt werden (vgl. § 147 Abs. 3 S. 1 AO und § 257 Abs. 4 HGB).	N/A
	im Rahmen der Prüfung nichts gegenteiliges festgestellt, da die Kassen insgesamt von untergeordneter Natur sind auch keine Tiefenprüfung durchgeführt	
iv.	Prüfen Sie, ob nicht aufrüstbare Kassensysteme längstens bis zum 31.12.2016 eingesetzt werden (Härtefallregelung des BMF-Schreibens vom 26.10.2010, BStBl. I 2010, S. 1342).	N/A
	vgl. ORD.4, alle eingesetzten Kassen entsprechen gem. vorliegenden Unterlagen den Anforderungen der GoBD	

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Wiederholung: Vom IT-Einsatz ist ein Verständnis zu erlangen. Gemäß A56 umfasst dies die Struktur (531.ORD.MIN / 531. und ORD.PP) und die Komplexität (531.KPL) der IT-Umgebung der Einheit.

4.2.1 Verständnis von der Einheit, ihrem Umfeld und den maßgebenden Rechnungslegungsgrundsätzen (Vgl. Tz. A50–A55)

19 Der Abschlussprüfer hat Prüfungshandlungen zur Risikobeurteilung durchzuführen, um ein Verständnis zu erlangen

(a) von den folgenden Aspekten der Einheit und ihres Umfelds:

(i) der Organisationsstruktur, Eigentümerschaft sowie Führung und Überwachung der Einheit sowie deren Geschäftsmodell, einschließlich des Umfangs, in dem das Geschäftsmodell den IT-Einsatz integriert; (Vgl. Tz. A56–A67)

(ii) branchenbezogene, regulatorische und andere externe Faktoren (Vgl. Tz. A68–A73) und

(iii) den zur Beurteilung des wirtschaftlichen Erfolgs der Einheit intern und extern genutzten Kennzahlen; (Vgl. Tz. A74–A81)

(b) von den maßgebenden Rechnungslegungsgrundsätzen sowie den Rechnungslegungsmethoden der Einheit und den Gründen für etwaige diesbezügliche Änderungen (Vgl. Tz. A82–A84) und

(c) wie sich inhärente Risikofaktoren auf die Anfälligkeit von Aussagen für falsche Darstellung auswirken und in welchem Maß sie dies bei der Aufstellung des Abschlusses in Übereinstimmung mit den maßgebenden Rechnungslegungsgrundsätzen tun, basierend auf dem nach (a) und (b) erlangten Verständnis. (Vgl. Tz. A85–A89)

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Wiederholung: Dokumentiert wird dies in MEMO.PA3/6j

j.	Geschäftsmodell (einschließlich des Umfangs, in dem das Geschäftsmodell den IT-Einsatz integriert)

Hier am besten einen Verweis auf das Dokument 531. oder 531.ORD.MIN einfügen, da dort neben der Erfassung der generellen IT-Kontrollen auch die IT-Umgebung zu beschrieben ist.
Hinweis: **Die Dokumente 531. und 531.ORD.MIN sind um Beschreibungen zu den einzelnen Fragen zu ergänzen. "Fertiggestellt ohne Beanstandungen" ohne Beschreibungen bzw. nur Referenzen reichen nicht aus.**

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Wiederholung:

Verständnis von den Komponenten des IKS der Einheit (Tz 25)

Teilbereich: Informationssystem und Kommunikation

Dies betrifft Tranksaktions-flüsse und die Informations-verarbeitung

25

Der Abschlussprüfer hat ein Verständnis von dem Informationssystem und der Kommunikation der Einheit, die für die Aufstellung des Abschlusses relevant sind, zu erlangen durch die Durchführung von Prüfungshandlungen zur Risikobeurteilung mittels: (Vgl. Tz. A131)

(a) Verstehen der Informationsverarbeitungstätigkeiten der Einheit, einschließlich ihrer Daten und Informationen, der bei solchen Tätigkeiten genutzten Ressourcen und der Regelungen, die für bedeutsame Arten von Geschäftsvorfällen, Kontensalden und Abschlussangaben Folgendes definieren: (Vgl. Tz. A132–A143)

(i) wie die Informationen durch das Informationssystem der Einheit fließen, einschließlich:

a. wie Geschäftsvorfälle ausgelöst und die Informationen darüber aufgezeichnet, verarbeitet, erforderlichenfalls korrigiert, in das Hauptbuch übertragen und im Abschluss abgebildet werden; und

b. wie Informationen über Ereignisse und Umstände, die keine Geschäftsvorfälle sind, erfasst, verarbeitet und im Abschluss angegeben werden.

(ii) die Unterlagen des Rechnungswesens, spezifische Konten im Abschluss und weitere unterstützende Unterlagen in Bezug auf die Informationsflüsse im Informationssystem.

(iii) den angewandten Rechnungslegungsprozess zur Aufstellung des Abschlusses der Einheit, einschließlich Abschlussangaben; und

(iv) die für (a)(i) bis (a)(iii) oben relevanten Ressourcen der Einheit, einschließlich der IT-Umgebung;

und

(c) die Beurteilung, ob das Informationssystem und die Kommunikation der Einheit die Aufstellung des Abschlusses der Einheit in Übereinstimmung mit den maßgebenden Rechnungslegungsgrundsätzen angemessen unterstützen. (Vgl. Tz. A146)

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Wiederholung:

5.3.5.6.5 IT-Einsatz der Einheit im Informationssystem

Warum der Abschlussprüfer die für das Informationssystem relevante IT-Umgebung versteht

A140 Das Verständnis des Abschlussprüfers vom Informationssystem schließt die für die Transaktionsflüsse und Verarbeitung von Informationen im Informationssystem der Einheit relevante IT-Umgebung ein, da der Einsatz von IT-Anwendungen durch die Einheit oder andere Aspekte in der IT-Umgebung zu aus dem IT-Einsatz resultierenden Risiken führen können.

A141 Das Verständnis vom Geschäftsmodell der Einheit und wie es den IT-Einsatz integriert, können ebenfalls nützlichen Kontext für Art und Umfang der im Informationssystem erwarteten IT geben.

Verständnis vom IT-Einsatz der Einheit

A142 Das Verständnis des Abschlussprüfers von der IT-Umgebung kann sich auf die Identifizierung und das Verstehen von Art und Anzahl der spezifischen IT-Anwendungen und andere, für die Transaktionsflüsse und Verarbeitung von Informationen im Informationssystem relevante Aspekte der IT-Umgebung fokussieren. Änderungen im Transaktionsflusse oder Informationen innerhalb des Informationssystems können aus Programmänderungen an IT-Anwendungen oder unmittelbaren Änderungen von Daten in den bei der Verarbeitung oder Speicherung solcher Geschäftsvorfälle oder Informationen eingebundenen Datenbanken resultieren.

A143 Der Abschlussprüfer kann die IT-Anwendungen und die unterstützende IT-Infrastruktur gleichzeitig mit seinem Verständnis darüber, wie Informationen bzgl. bedeutsamer Arten von Geschäftsvorfällen, Kontensalden und Abschlussangaben in das IT-System der Einheit hinein-, durch dieses hindurch- und aus diesem herausfließen, identifizieren.

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Wiederholung: Dokumentiert wird dies in MEMO.PA4/1e

Hier ist auch auf das Dokument 531. bzw. 531.ORD.MIN zu verweisen, da dem Informationssystem auch die IT zu Grunde liegt.

e. **Rechnungslegungsrelevante Informationssysteme (ISA 315.25a)**. Erfassen Sie den Prozess der Einheit und das Verständnis bezüglich der bedeutsamen Arten von Geschäftsvorfällen, Kontensalden und Abschlussangaben, des Informationsflusses, der damit zusammenhängenden Regelungen, der Unterlagen des Rechnungswesens, der Art der Erfassung von Geschäftsvorfällen sowie des Rechnungslegungsprozesses und der hierfür relevanten Ressourcen.

ISA 315.25a
Hinweis: Zur Reichweite des zu erlangenden Verständnisses des rechnungslegungsbezogenen Informationssystems gibt ISA 315.D.A92.1 weitere Hinweise:
Das nach Tz. 18 dieses ISA [DE] erforderliche Verständnis vom rechnungslegungsrelevanten Informationssystem (einschließlich des Verständnisses von relevanten Aspekten dieses Systems im Zusammenhang mit im Abschluss angegebenen Informationen, die inner- oder außerhalb des Hauptbuchs und der Nebenbücher erlangt wurden) ist eine Frage des pflichtgemäßen Ermessens des Abschlussprüfers. Zum Beispiel können bestimmte Beträge oder Angaben im Abschluss der Einheit (wie bspw. Angaben zum Kredit-, Liquiditäts- und Marktrisiko) auf aus dem Risikomanagementsystem der Einheit erlangten Informationen basieren. Der Abschlussprüfer ist jedoch nicht verpflichtet, sämtliche Aspekte des Risikomanagementsystems zu verstehen, und wendet bei der Festlegung des notwendigen Verständnisses pflichtgemäßes Ermessen an.

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Wiederholung: Das Informationssystem ist in MEMO.PA4/1g abschließend zu beurteilen

g.	Beurteilung des Informationssystems und der Kommunikation der Einheit (ISA 315.25c)

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Wiederholung:

4.2.2.2.2 Kontrollaktivitäten

26

Der Abschlussprüfer hat ein Verständnis von der Komponente Kontrollaktivitäten zu erlangen durch die Durchführung von Prüfungshandlungen zur Risikobeurteilung mittels: (Vgl. Tz. A147–A157)

Es ist ein Verständnis über die Kontrollaktivitäten der Einheit zu erlangen.
Dies schließt manuelle und IT-Kontrollen ein.

Hinweis: Der Prüfer ist nicht verpflichtet sämtliche Kontrollen der Informationsverarbeitungstätigkeiten zu identifizieren und zu beurteilen (A148)

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Wiederholung: Die Kontrollaktivitäten sind in MEMO.PA4/1h zu dokumentieren.

h. **Kontrollaktivitäten (ISA 315.26a).** Nehmen Sie weitere Bereiche des rechnungslegungsrelevanten IKS auf und identifizieren Sie die eingerichteten Kontrollen, die die Risiken wesentlicher falscher Darstellungen auf Aussageebene im IKS behandeln.



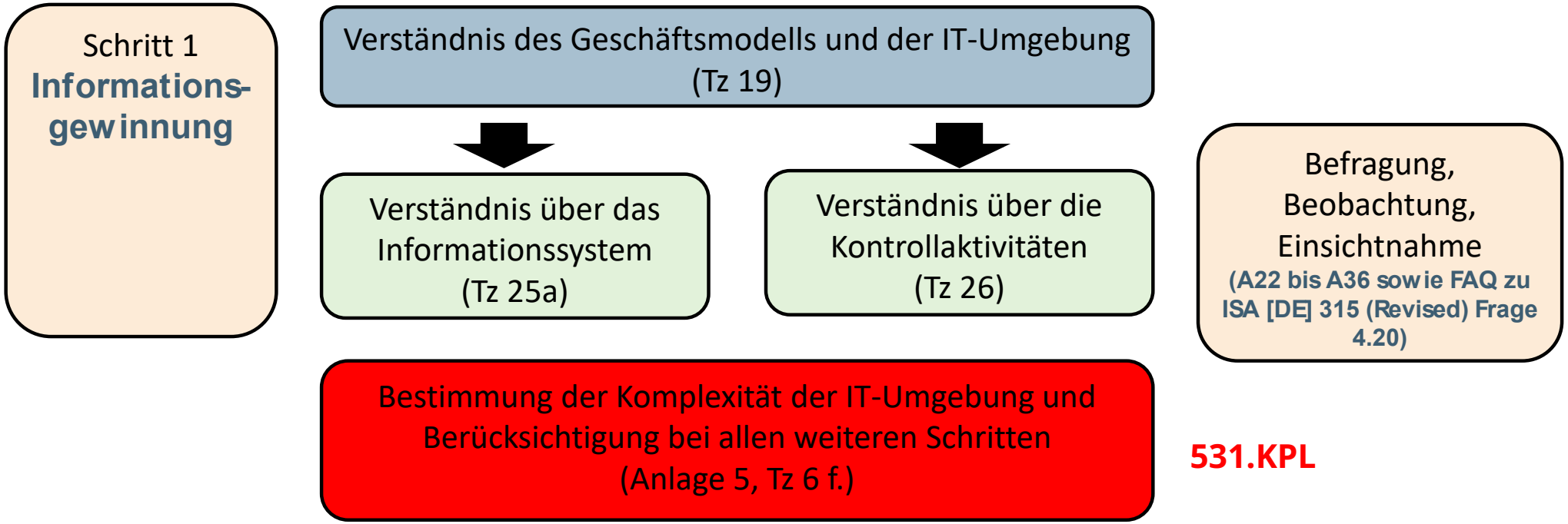
ISA 315.26a

Hier bieten sich Verweise auf die prozessbezogenen Aufbauprüfungen an. Dort sind die Abläufe sowie die Kontrollen identifiziert (von dort erfolgt dann ja auch Verweis auf Kontrolldialog).

Für die generellen IT-Kontrollen ist auf das **Dokument 531 bzw. 531.ORD.MIN** zu verweisen.

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Wiederholung: Zusammenfassung



531.KPL

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

In Tz 26a werden die folgenden Kontrollen identifiziert, die den Risiken wesentlicher falscher Darstellungen auf Aussageebene entgegenwirken:

- Kontrollen, die ein bedeutsames Risiko betreffen
- Kontrollen über Journalbuchungen (=> KJA01 bis KJA03 und KRL01 bis KRL05)
- Kontrollen,
  - für die der Prüfer plant, die Wirksamkeit deren Funktion zu prüfen
  - die Risken behandeln für die aussagebezogene Prüfungshandlungen alleine keine ausreichend geeigneten Prüfungsnachweise liefern
- andere Kontrollen nach Ermessen

Darauf basierend: Identifikation der relevanten IT-Anwendungen und anderer Aspekte der IT-Umgebung (Tz 26b). Damit verbunden:

- Identifizierung von sich aus dem IT-Einsatz ergebenden **Risiken (RIT01 bis RIT03)**
- Identifizierung **genereller IT-Kontrollen (KIT01 bis KIT09)**, die diese Risiken behandeln

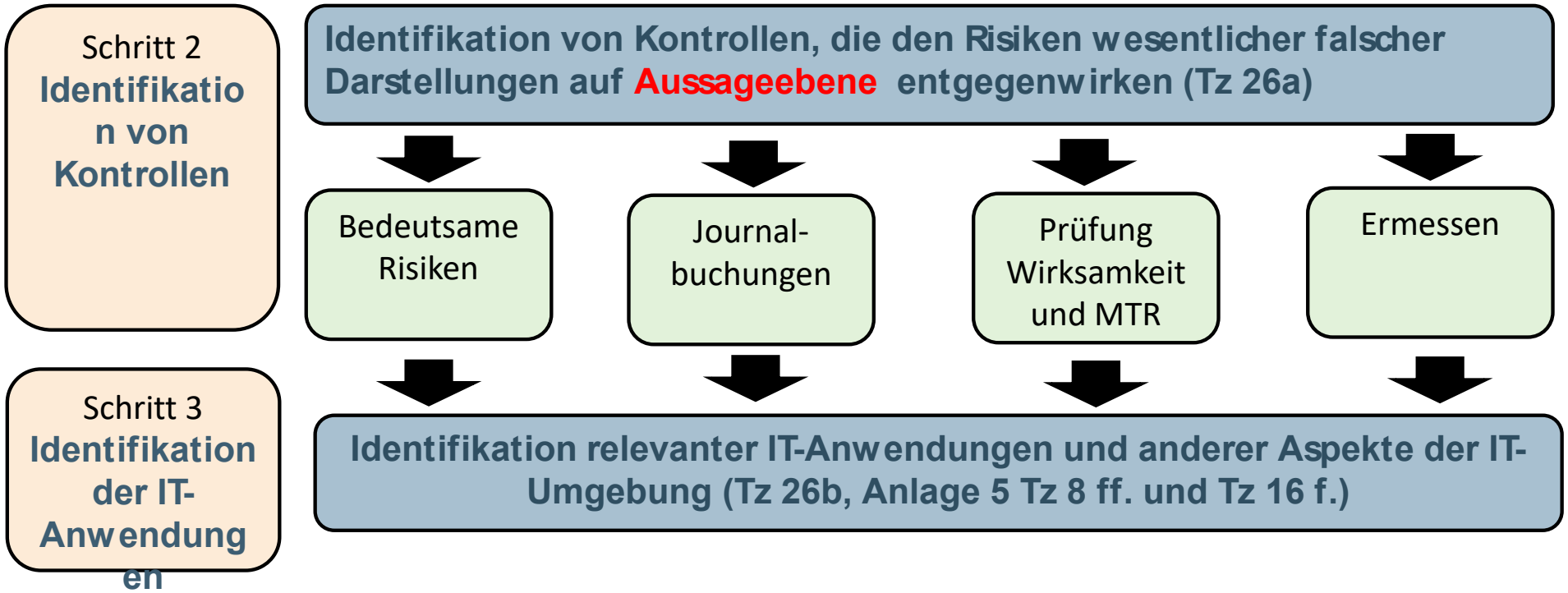
VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Definition **genereller IT-Kontrollen** (Tz. 12d):

Kontrollen über die IT-Prozesse der Einheit, die den kontinuierlichen ordnungsgemäßen Betrieb der IT-Umgebung unterstützen, einschließlich der kontinuierlich wirksamen Funktion der Kontrollen der Informationsverarbeitung und der Integrität von Informationen (d.h. Vollständigkeit, Richtigkeit und Gültigkeit von Informationen) im Informationssystem der Einheit.

(vgl. zu weiteren konkreten Beispielen zu generellen IT-Kontrollen Anlage 6 des ISA [DE] 315 (Revised 2019))

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung



VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Schritt 3 **Identifikation der IT-Anwendungen**	**Identifikation relevanter IT-Anwendungen und anderer Aspekte der IT-Umgebung (Tz 26b, Anlage 5 Tz 8 ff. und Tz 16 f.)**
Schritt 4 **Identifikation von IT-Risiken**	**Identifikation von sich aus dem IT-Einsatz ergebenden Risiken (IT-Risiken) (Tz 26c, Anlage 5 Tz 18 ff.)**
Schritt 5 **Identifikation genereller IT-Kontrollen**	**Identifikation genereller IT-Kontrollen, die diesen Risiken begegnen (Tz 26c, Anlage 5 Tz 18 ff.) aber auch die anwendungsbezogenen IT-Kontrollen**

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Schritt 5
Identifikation genereller IT-Kontrollen

Identifikation genereller IT-Kontrollen, die diesen Risiken begegnen (Tz 26c, Anlage 5 Tz 18 ff.)
aber auch die anwendungsbezogenen IT-Kontrollen

Schritt 6
Aufbauprüfung der identifizierten Kontrollen

Aufbauprüfung der identifizierten Kontrollen Wirksam ausgestaltet? (Tz 26d (i))

Aufbauprüfung der identifizierten Kontrollen Kontrolle implementiert?
(Tz 26d (ii))
Befragung des Personals und eigene PH

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Durchführung der Aufbauprüfung / Prüfungshandlungen bei Kontrollen:

Prüfungshandlungen zur Risikobeurteilung, um Prüfungsnachweise über die Ausgestaltung und Implementierung von identifizierten Kontrollen in der Komponente Kontrollaktivitäten zu erlangen, können einschließen (vgl. ISA [DE] 315 (Revised 2019), Tz. A177):

- Befragung des Personals der Einheit
- Beobachtung der Anwendung bestimmter Kontrollen
- Einsichtnahme in Dokumente und Berichte.

Eine Befragung allein reicht jedoch für diese Zwecke nicht aus.

(vgl. FAQ zu ISA [DE] 315 (Revised 2019) Frage 4.20)

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Durchführung der Aufbauprüfung / Walk-Through:

Der Abschlussprüfer kann für Zwecke der Aufbauprüfung auch die Erkenntnisse nutzen, die er aus einem **"Walk-Through"** erlangt hat. Hierbei handelt es sich um das Nachvollziehen eines Geschäftsvorfalls von seiner Entstehung bis zur Abbildung im Abschluss (vgl. ISA [DE] 315 (Revised 2019), Tz. A136). Er gibt grundsätzlich Aufschluss darüber, ob der Prozess tatsächlich so abläuft und ob identifizierte Kontrollen tatsächlich so gehandhabt werden, wie vom Mandanten beschrieben bzw. erläutert.

Ein Walk-Through ist daher vom Ansatz her primär darauf ausgerichtet, ein Verständnis über das für die Aufstellung des Abschlusses relevante Informationssystem zu erlangen (vgl. ISA [DE] 315 (Revised 2019), Tz. A136); er kann **zugleich** in Bezug auf die identifizierten Kontrollen auch als **Nachweis für deren Einrichtung (Implementierung)** als Bestanteil der Erlangung eines Verständnisses genutzt werden.

(vgl. FAQ zu ISA [DE] 315 (Revised 2019) Frage 4.20)

=> die Aufbauprüfung erfolgt in 531. und ORD.PP oder in 531.ORD.MIN

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Dokumentation der Aufbauprüfungen in 531 und ORD.PP bzw. 531.ORD.MIN

IT-Kontrollen und Kontrollen im Bezug auf Journalbuchungen		Risken	Aufbauprüfung in … (Referenz Funktionstest)		
			531.	ORD.PP	531.ORD.MIN
KIT01	Kontrolle der ordnungsmäßigen Datensicherung und Datenwiederherstellung	RIT01	17		4
KIT02	Kontrolle durch Zugriffschutz	RIT02	24, 25		7, 8
KIT03	Einrichtung eines Berechtigungskonzeptes	RIT02	7		3
KIT04	Einschaltung der systemseitgen Stammdatenänderungsprotokollierung	RIT02		6, 10	16, 20
KIT05	Kontrolle durch festgelegten Updateprozess	RIT03	33		10
KIT06	Sicherheitsmaßnahmen IT-Infrastruktur	RIT01, RIT02	22, 23		6
KIT07	Sicherheitsmaßmahmen Netzwerk	RIT03	24, 30		7, 9
KIT08	Überprüfung Datenverarbeitung und Datenübernahme	RIT03	38, 42		11, 13
KIT09	Einrichung eines IT-Notfallplans	RIT03	18, 19, 20		5

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Von der Aufbauprüfung ist die **Funktionsprüfung** abzugrenzen:

Hiervon abzugrenzen ist die Beurteilung der Funktion einer Kontrolle, die auch als Funktionsprüfung bezeichnet wird. Die **Funktionsprüfung ist Teil der Reaktionen** eines Abschlussprüfers auf erkannte Fehlerrisiken und ist daher nicht Teil der Risikobeurteilung. Dessen ungeachtet steht es dem Abschlussprüfer frei, soweit möglich, aus Effizienzgründen diese zugleich mit der Aufbauprüfung durchzuführen.

(vgl. FAQ zu ISA [DE] 315 (Revised 2019) Frage 4.19)

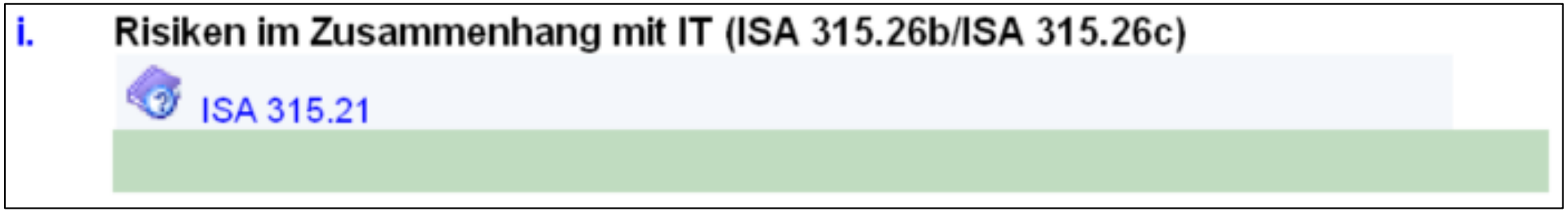
VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Verständnis und Identifizierung der aus dem Einsatz von IT resultierenden Risiken und die dementsprechend implementierten generellen IT-Kontrollen haben Auswirkungen auf … (FAQ zu ISA [DE] 315 (Revised 2019) Frage 4.13

- Entscheidung, ob die Funktion IT-gestützter Kontrollen geprüft wird, um Risiken wesentlicher falscher Darstellungen auf Aussageebene zu adressieren
- die Beurteilung des Kontrollrisikos auf Aussageebene
- die Strategie für die Prüfung von Informationen, die unter Nutzung der IT erstellt werden
- die Beurteilung des inhärenten Risikos
- die Planung weitere Prüfungs-handlungen

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Die Risiken aus dem Einsatz der IT sind in MEMO.PA4/1i zu dokumentieren.

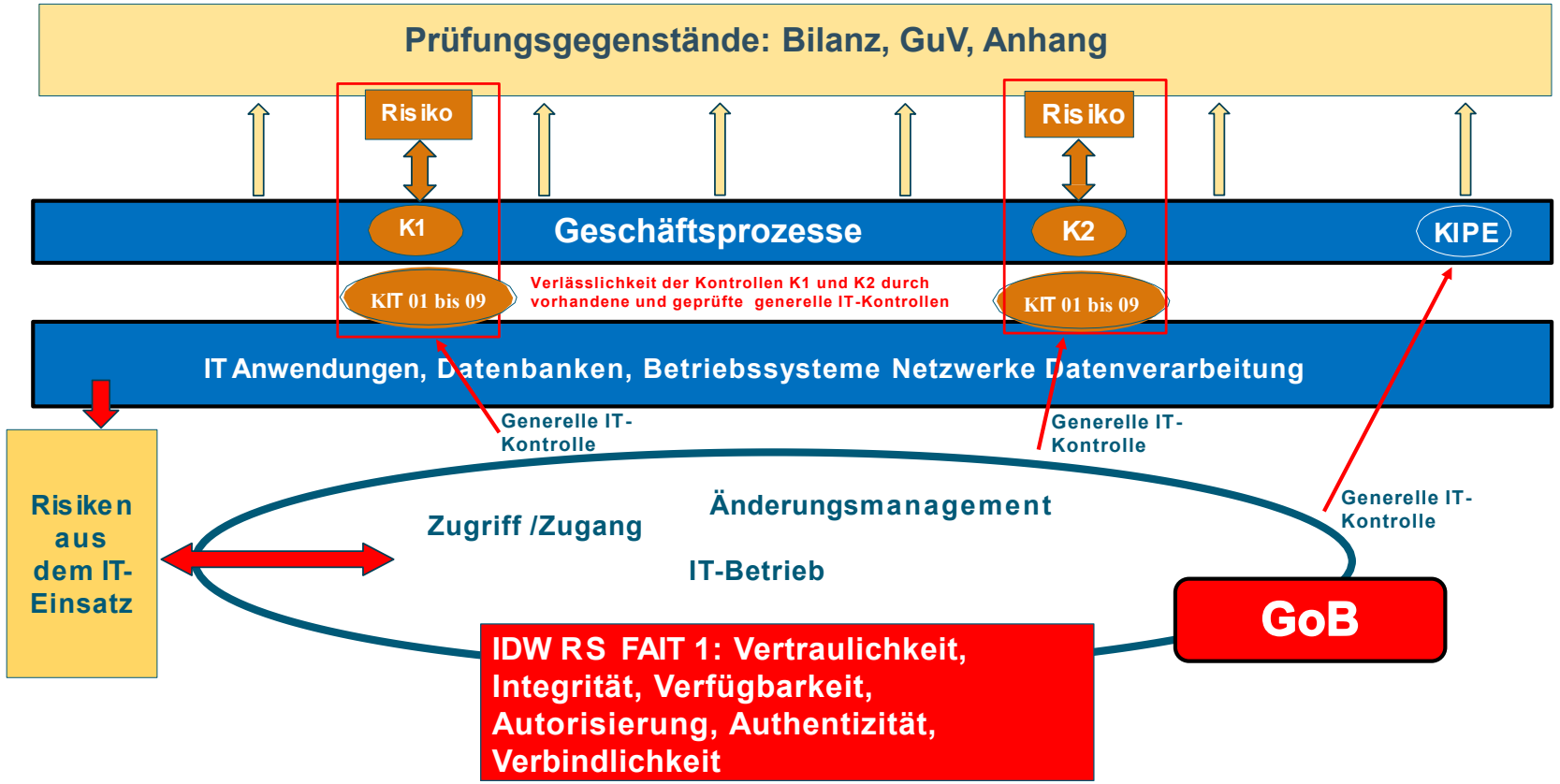


Verweis auf folgende Dokumentationen:

- 531. oder 531.ORD.MIN
- 520E. (IT-Risiken)
- 540. (Kontrolldialog)

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

(In Anlehnung an Vortrag Herr Teipel vom 20.01.2023)



ISA [DE] 315 (Revised 2019)

Anlage

5 und 6

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

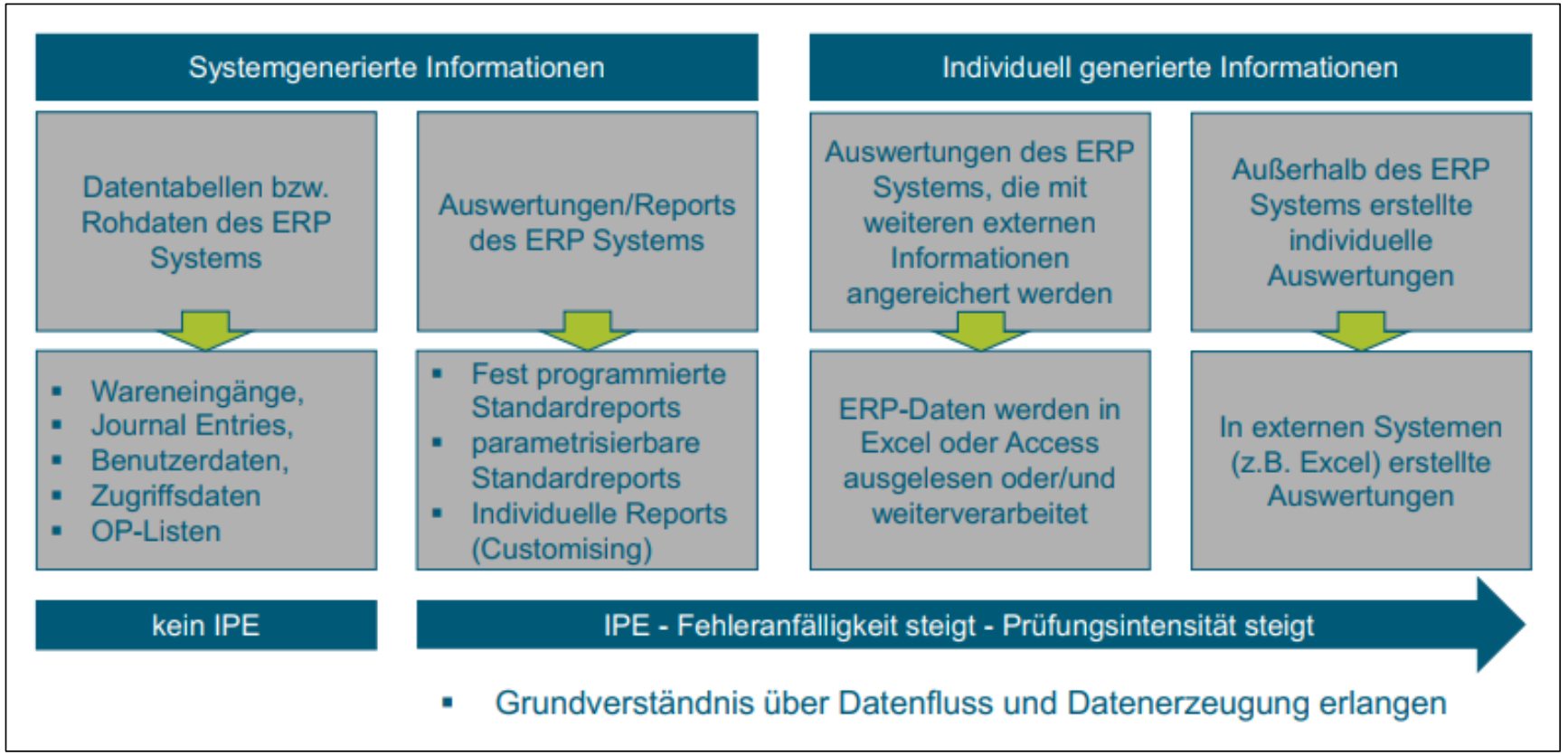
(Quelle: Vortrag Herr Teipel vom 20.01.2023 / Exkurs : IPE (Information produced by the entity)

Auswertungen (systemgenerierte oder andere Berichte) des Unternehmens, die vom Management für die Aufstellung und von Abschlussprüfer zur Durchführung von Prüfungshandlungen genutzt werden. Die Informationen der Auswertungen sind nicht direkter Prüfungsgegenstand.

Altersstrukturliste	Informationen zur Überfälligkeit werden für die Prüfung der EWB genutzt
Planungsrechnungen	Informationen zu künftigen CFs werden für die Prüfung von Beteiligungsbewertungen genutzt
Nicht finanzielle Daten (Mengen, QM, MA)	Mengeninformationen werden für analytischen Prüfungshandlungen genutzt
Reichweitenanalysen Vorräte	Informationen über Bestand und Abverkäufe werden für die Prüfung der Abwertung genutzt
Umsatz-/Kostenstellenreports	Aufbereitete Informationen der FiBu werden zur Beurteilung von Mgt.-Kontrollen genutzt
Einzelaufstellungen zu Gewährleistungen	Aufbereitete Informationen werden für die Prüfung von Rückstellungen genutzt
Fehlerreports (3-Way-Match)	Im ERP System vorhandener Fehlerreport wird zur Prüfung der Kontrolle zur Umsatzrealisation genutzt
Systemdaten (MA-Kennungen und Transaktionsschlüssel)	Systeminformationen werden für die Prüfung der Funktionstrennung genutzt
.....	

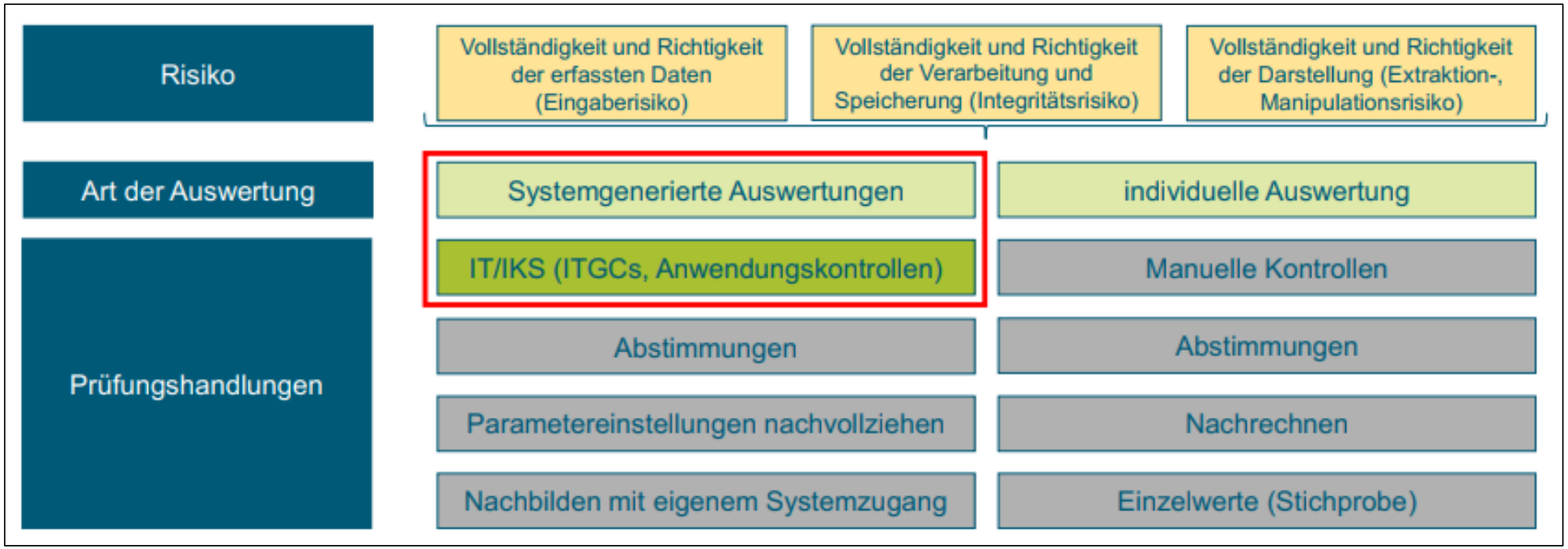
VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

(Quelle: Vortrag Herr Teipel vom 20.01.2023 / Exkurs : IPE (Information produced by the entity)



VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

(Quelle: Vortrag Herr Teipel vom 20.01.2023 / Exkurs : IPE (Information produced by the entity)



VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Mit welchen Kontrollen muss man sich im Rahmen der Prüfung nun befassen?

Generelle IT-Kontrollen KIT01 bis KIT09 (=> bei jeder Prüfung!)

- Selbst anlegen
- Risiko-Import

Kontrollen, die Reports betreffen

- Nach eigenem prüferischen Ermessen unter Berücksichtigung der Komplexität selbst anlegen

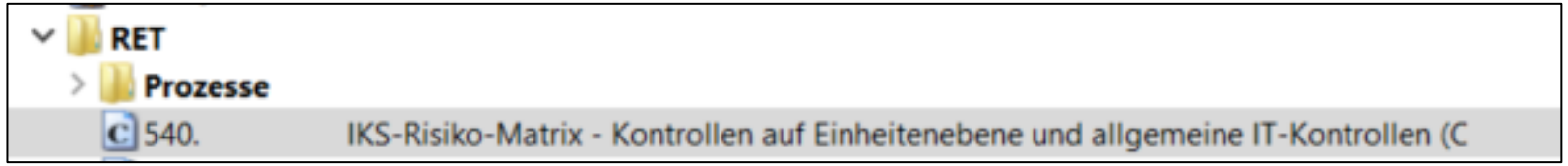
in Prozessen integrierte IT- gestützte Kontrollen

- Nach eigenem prüferischen Ermessen unter Berücksichtigung der Komplexität selbst anlegen

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Generelle IT-Kontrollen (KIT01 bis KIT09):

- Hierzu werden Risiken im Risikodialog erfasst (520E.)
- Dann werden entsprechende IT-Kontrollen im Kontrolldialog erfasst und zugeordnet (540)
- Es handelt sich hierbei um allgemeine Geschäftsrisiken auf Abschlussebene.



- Funktionsprüfungen sind durchzuführen und die Ergebnisse im Kontrolldialog einzutragen.
- Daraus resultierende wichtige Prüfungsfeststellungen sind im Dokument 320 zu erfassen.

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Es gibt folgende zwei Möglichkeiten Risiken aus dem Einsatz von IT zu erfassen:

- Manuelle Erfassung
- Risikoimport aus der Importvorlage

Die drei Risiken aus dem Einsatz von IT "Datenverlust" (TIR01), "Datenmanipulation" (RIT02) und "Falsche Datenverarbeitung" (RIT03) gehören zu den Dirty 8-Risiken auf Abschlussebene!!

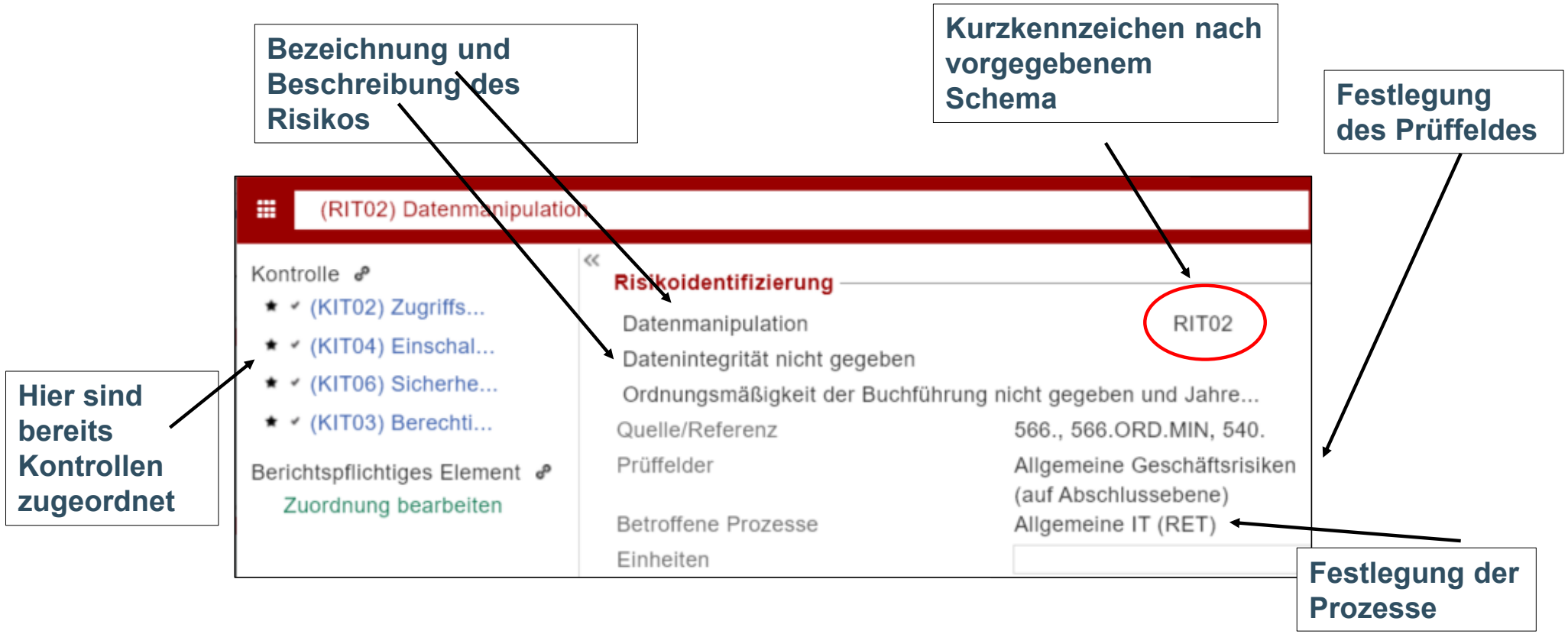
Sie sind bei jeder Prüfung zu erfassen und jährlich zu pflegen!

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Wann und wie werden im Rahmen der IT-Prüfung Risiken erfasst?

- Soweit sich bei der Bearbeitung der Dokumente 531. und ORD.PP bzw. 531.ORD.MIN Risken aus dem Einsatz von IT gezeigt haben 
- Die Erfassung erfolgt z. B. über die Dokumente 531. und ORD.PP bzw. 531.ORD.MIN
- In der IKS-Risiko-Matrix 540 für Kontrollen auf Einheitenebene und allgemeine IT-Kontrollen werden später alle Risiken mit den entsprechenden Kontrollen verknüpft.
- Dazu wird zunächst das Risiko erfasst und dann um die entsprechende Kontrolle ergänzt.
- Erst danach werden die Funktionsprüfungen durchgeführt.

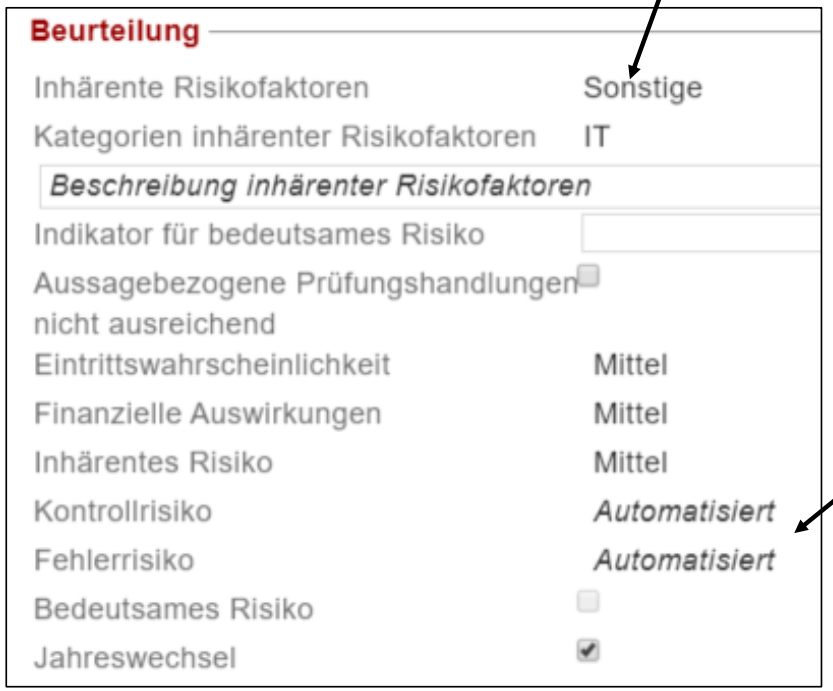
VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung



VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Für IT immer diesen Indikator auswählen

Falls es sich um ein bedeutsames Risiko handelt, sind diese beiden Felder auszufüllen.



Kontroll- und Fehlerrisiko bleibt noch "automatisiert", da eine Kontrollprüfung zu diesem Zeitpunkt noch nicht stattgefunden hat.

VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Reaktion des Managements eintragen.

Unsere Reaktion auf das Risiko eintragen.



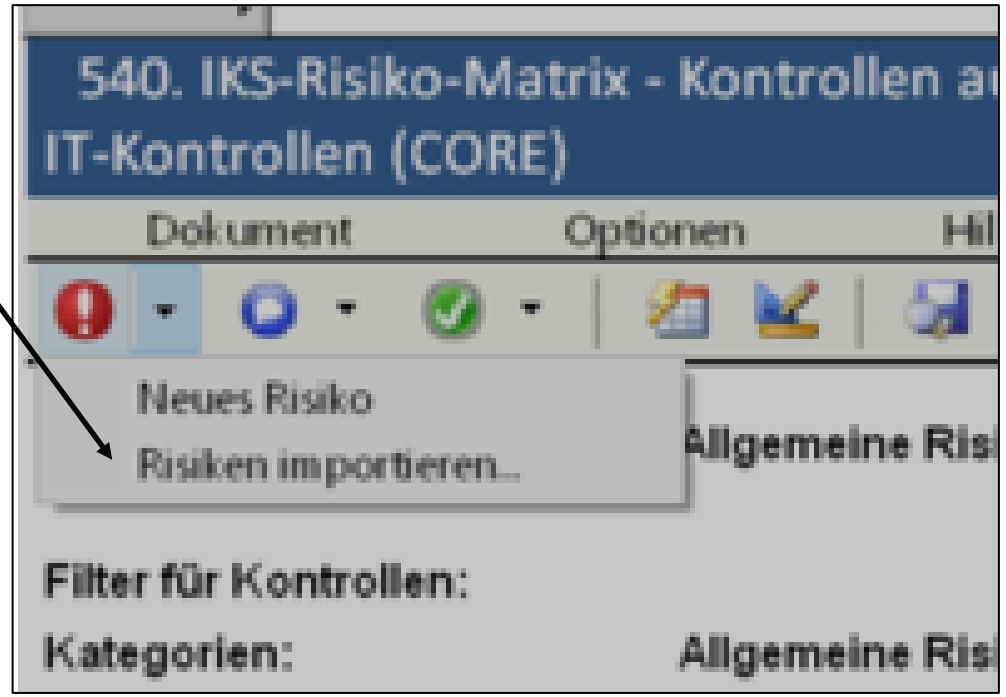
~~Oder~~
531
531.ORD.MIN

Jedes Risiko muss adressiert werden.

Jedem Risiko wird/werden die entsprechende/n Kontrolle/n zugeordnet.

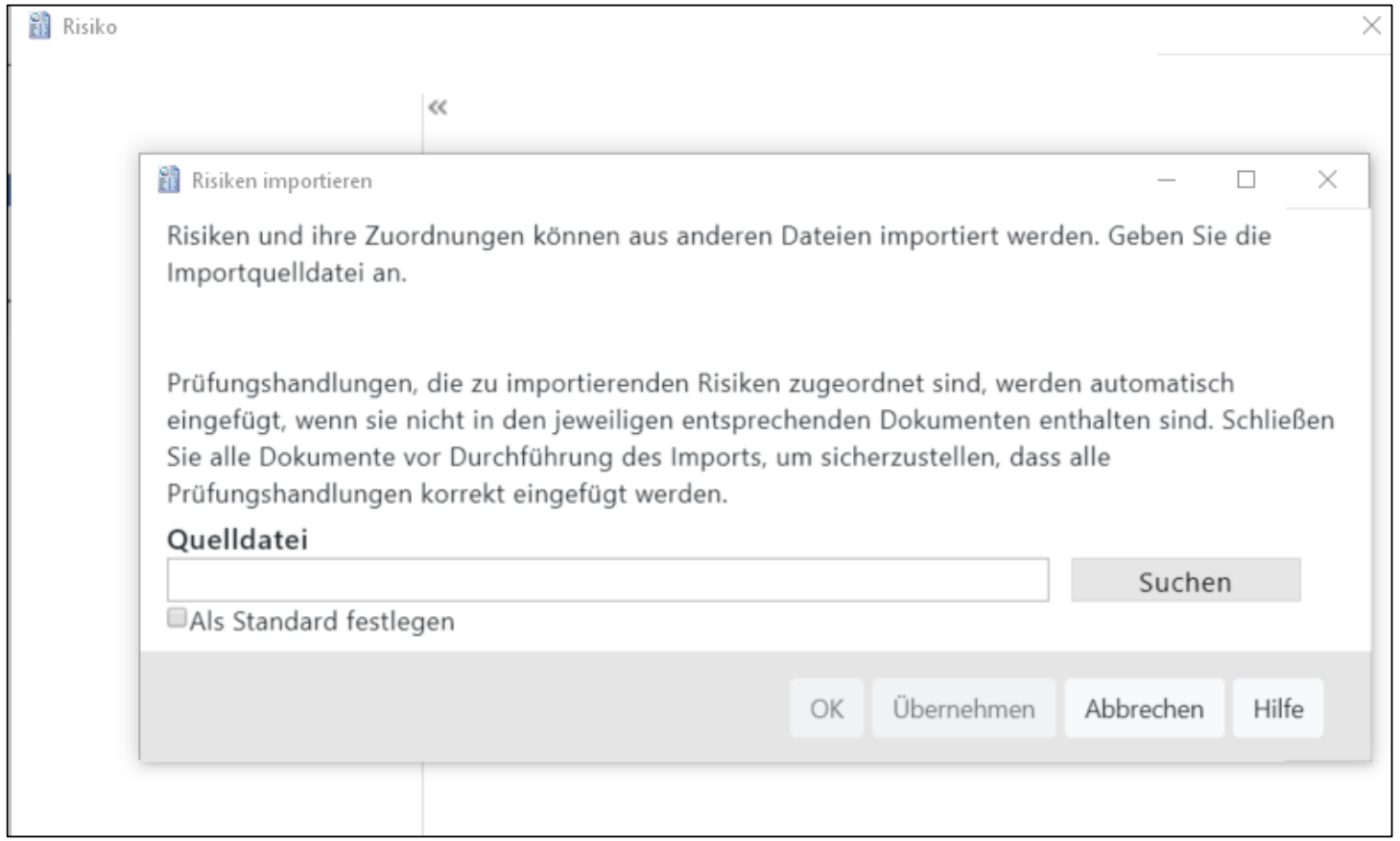
VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Import von IT-Risiken aus der Importvorlage



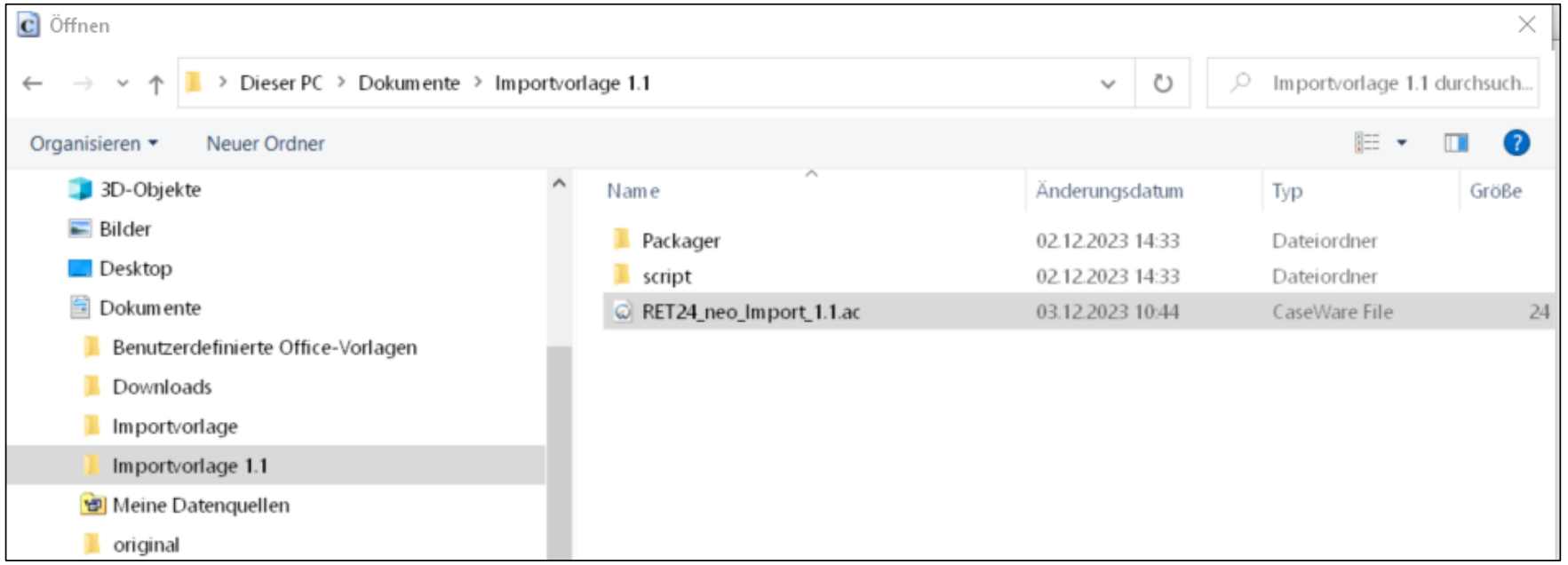
VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Auswahl der Quelldatei



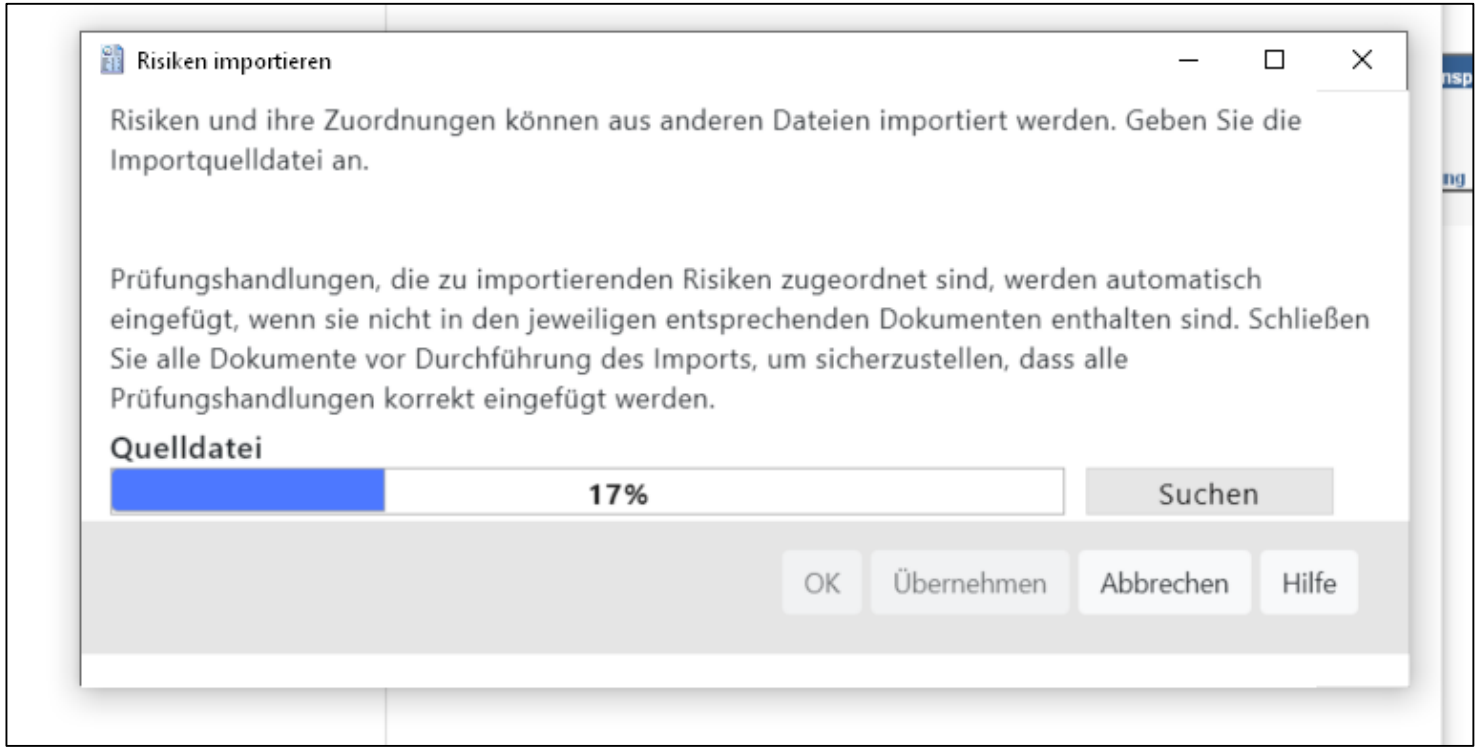
VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Auswahl der Quelldatei



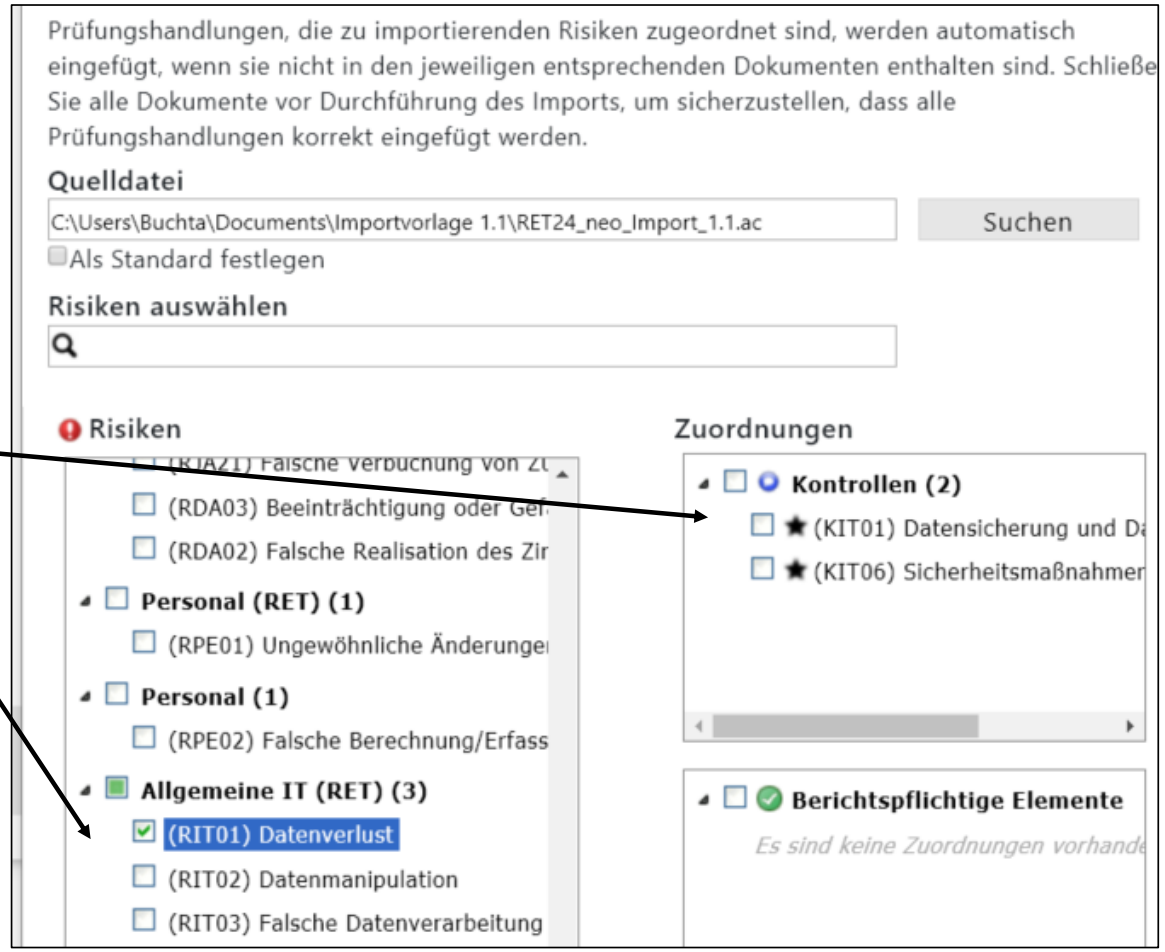
VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Auswahl der Quelldatei



VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Auswahl der Risiken und gleichzeitig der Kontrollen

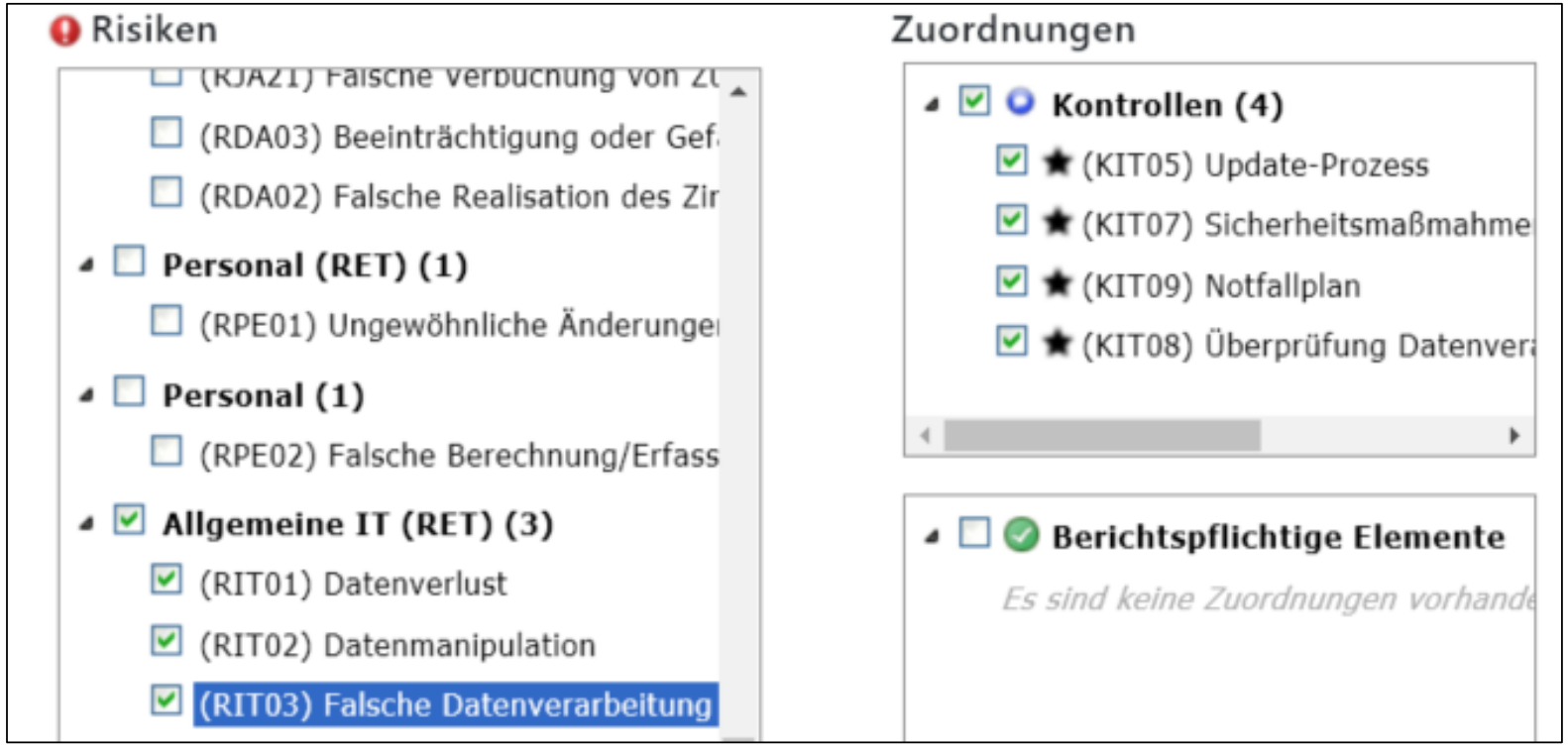


VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Im Beispiel wurden alle IT-Risiken und Kontrollen importiert

Es handelt sich um die generellen IT-Kontrollen!

Nach der Auswahl "Übernehmen" und "OK" anklicken für jedes Risiko.



VIII. Risikoidentifizierung aus dem Einsatz von IT und deren Erfassung

Bereits in der Importvorlage enthaltene IT-Risiken und IT-Kontrollen

Risiken aus dem Einsatz von IT	IT-Kontrolle
Datenverlust (RIT01)	Datensicherung und Datenwiderherstellung (KIT01)
	Sicherheitsmaßnahmen IT-Infrastruktur (KIT06)
Datenmanipulation (RIT02)	Zugriffsschutz (KIT02)
	Einschaltung der systemseitgen Stammdatenänderungsprotokollierung (KIT04)
	Sicherheitsmaßnahmen IT-Infrastruktur (KIT06)
	Berechtigungskonzept (KIT03)
Falsche Datenverarbeitung (RIT03)	Update-Prozess (KIT05)
	Sicherheitsmaßmahmen Netzwerk (KIT07)
	Überprüfung Datenverarbeitung und Datenübernahme (KIT08)
	Notfallplan (KIT09)

IX. Erfassung von IT-Kontrollen

IX. Erfassung von IT-Kontrollen

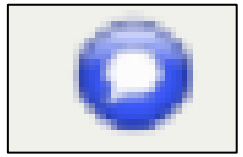
Es gibt folgende zwei Möglichkeiten IT-Kontrollen zu erfassen:

- Manuelle Erfassung
- Risikoimport aus der Importvorlage (erfolgt i.d.R. gleichzeitig mit dem Import der IT-Risiken)

IX. Erfassung von IT-Kontrollen

Wann und wie werden IT-Kontrollen erfasst?

- Erfassung genereller IT-Kontrollen im Zusammenhang mit den Risiken aus dem Einsatz von IT i.d.R. in den Dokumenten 531. und ORD.PP bzw. 531.ORD.MIN
- Erfassung IT-gestützter Kontrollen in Bezug auf bestimmte Prüffelder bzw. Prozesse
- Erfassung von Report-Kontrollen in Bezug auf bestimmte Prüffelder bzw. Prozesse
- Zu sehen in der IKS-Risiko-Matrix 540 für Kontrollen auf Einheitenebene und allgemeine IT-Kontrollen sowie in den IKS-Risiko-Matrizen einzelner Prüffelder/Prozesse.
- Zu jeder Kontrolle ist auch ein Risiko erfasst.
- Erst danach werden die Funktionsprüfungen durchgeführt.

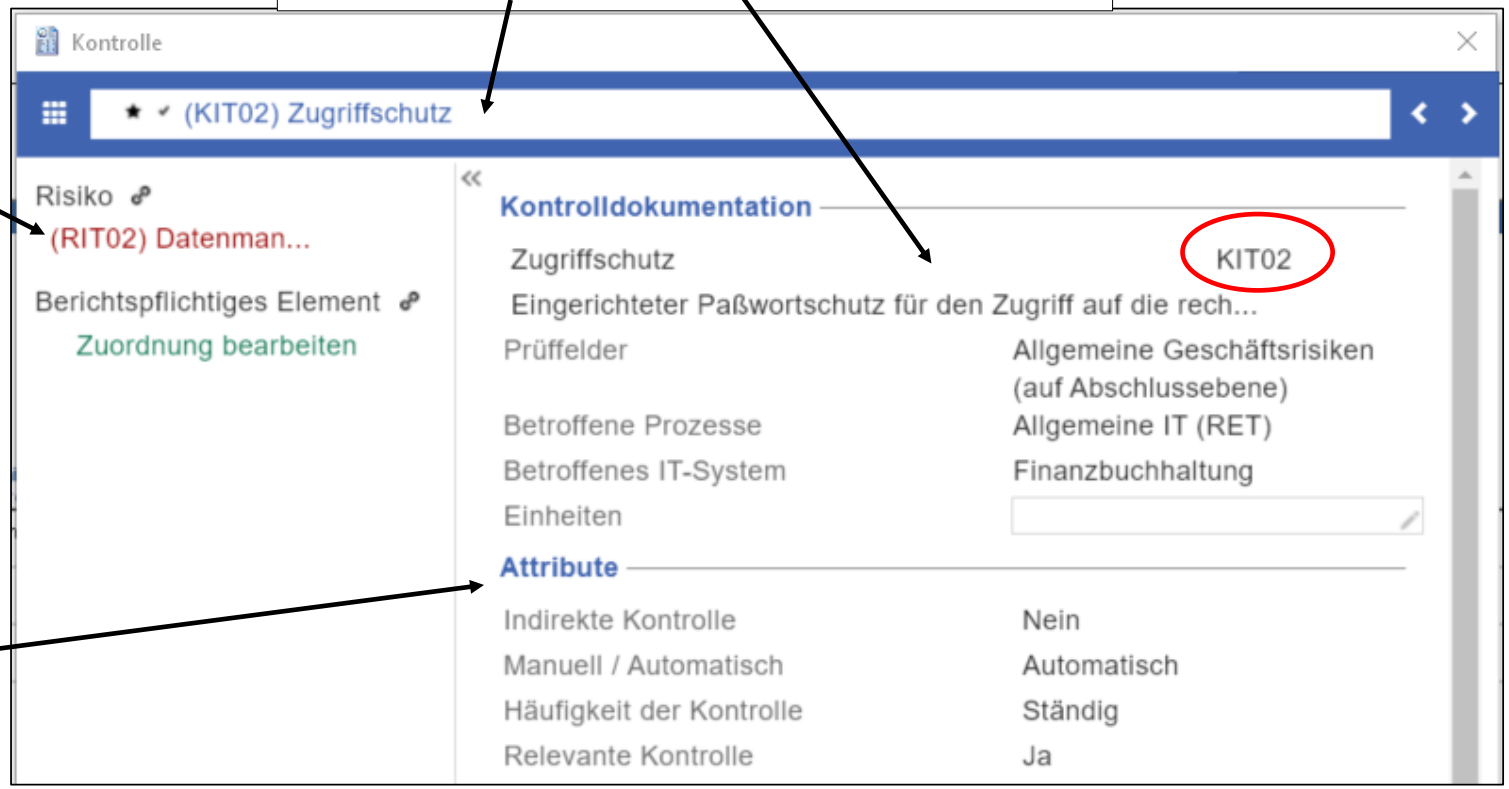


IX. Erfassung von IT-Kontrollen

Bezeichnung und Beschreibung der Kontrolle

Ver-knüpftes Risiko.

Eigenschaften der Kontrolle



IX. Erfassung von IT-Kontrollen

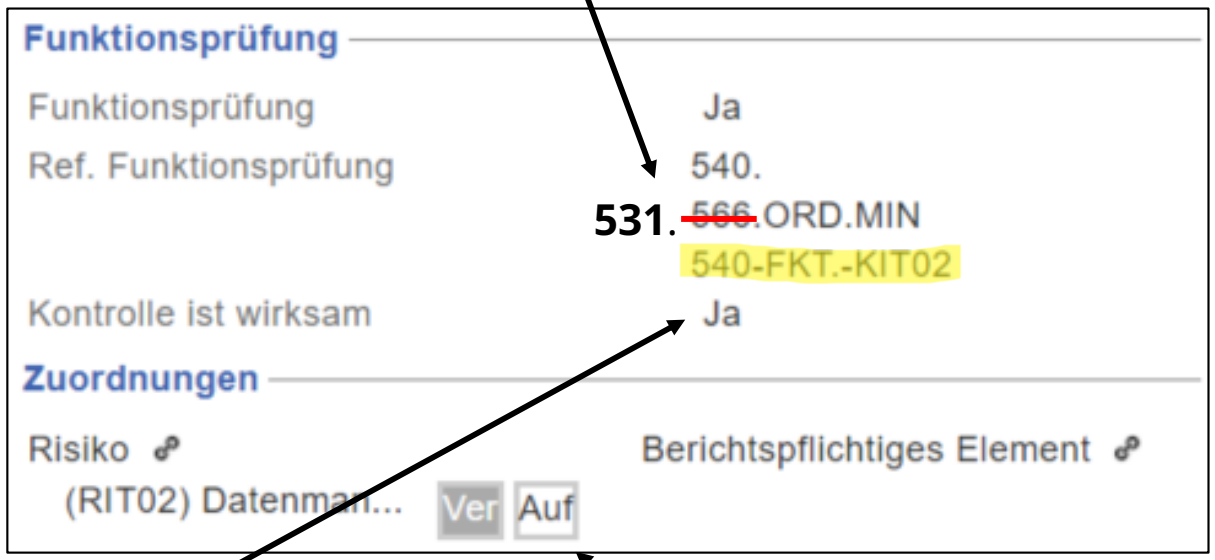
Verknüpfung der Kontrolle mit der Aufbauprüfung



"zufriedenstellend" oder "nicht zufriedenstellend"

IX. Erfassung von IT-Kontrollen

Verknüpfung der dokumentierten Funktionsprüfung

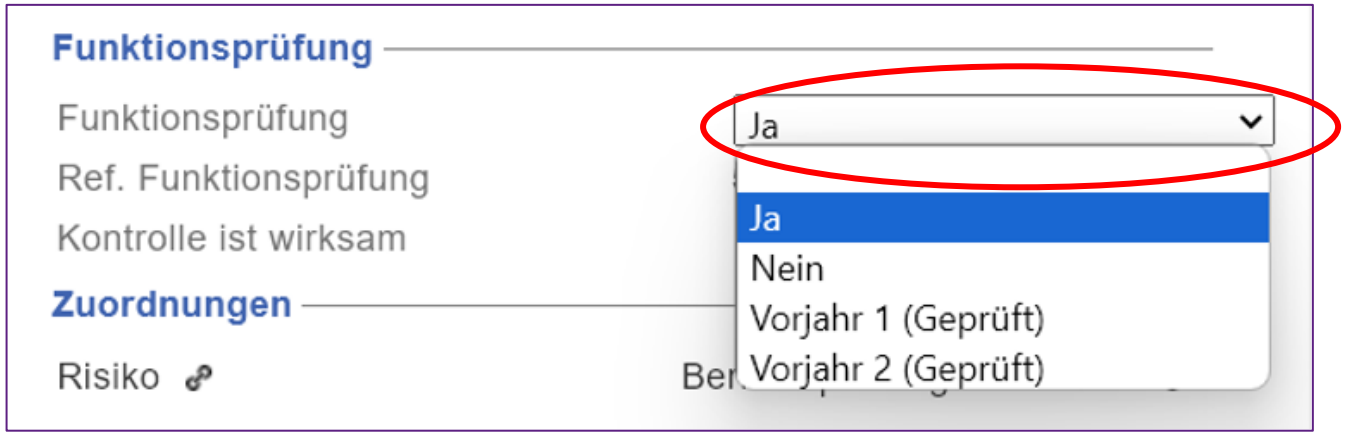


Ergebnis der Wirksamkeit der Kontrolle (ja, nein, nicht geprüft)

Angabe, ob es sich um einer verhindernde (Ver) oder eine aufdeckende (Auf) Kontrolle handelt.

IX. Erfassung von IT-Kontrollen

Dies ist der **"Zähler"**! Hier wird angezeigt, wie "alt" die Kontrollprüfung ist.

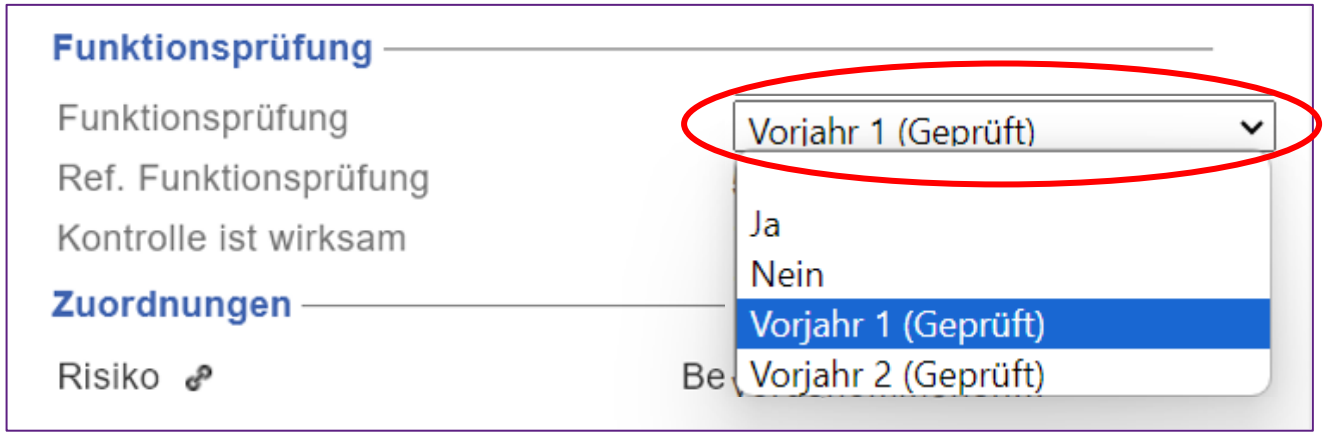


- Nein = Kontrolle wird nicht geprüft.
- Ja = Kontrolle wurde im aktuellen Berichtsjahr geprüft.
- Vorjahr 1 (Geprüft) = Kontrolle wurde im vorherigen Jahr geprüft
- Vorjahr 2 (Geprüft) = Kontrolle wurde vor 2 Jahren geprüft

Weitere gibt es nicht, denn alle drei Jahre muss die Kontrolle spätestens aktuell geprüft werden!!

IX. Erfassung von IT-Kontrollen

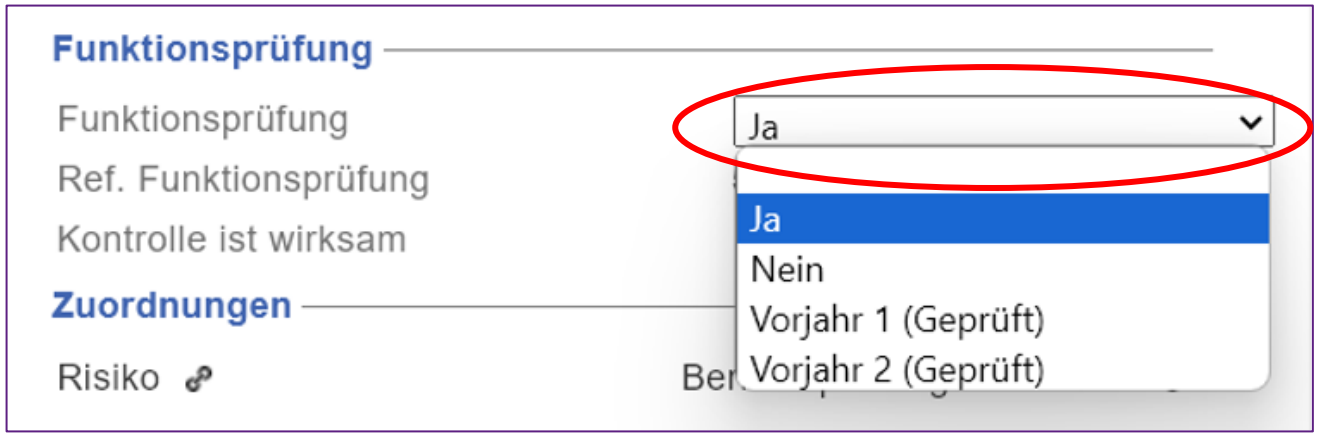
Der **"Zähler"** verändert sich mit dem **Jahreswechsel**.



- Aus "Ja" wird "Vorjahr 1 (Geprüft)"
- Aus "Vorjahr 1 (Geprüft)" wird "Vorjahr 2 (Geprüft)"
- Aus "Vorjahr 2 (Geprüft)" wird " "

IX. Erfassung von IT-Kontrollen

Was ist zu tun, wenn eine Kontrolle im aktuellen Berichtsjahr erneut geprüft werden muss, z.B. weil sie ein bedeutsames Risiko betrifft?

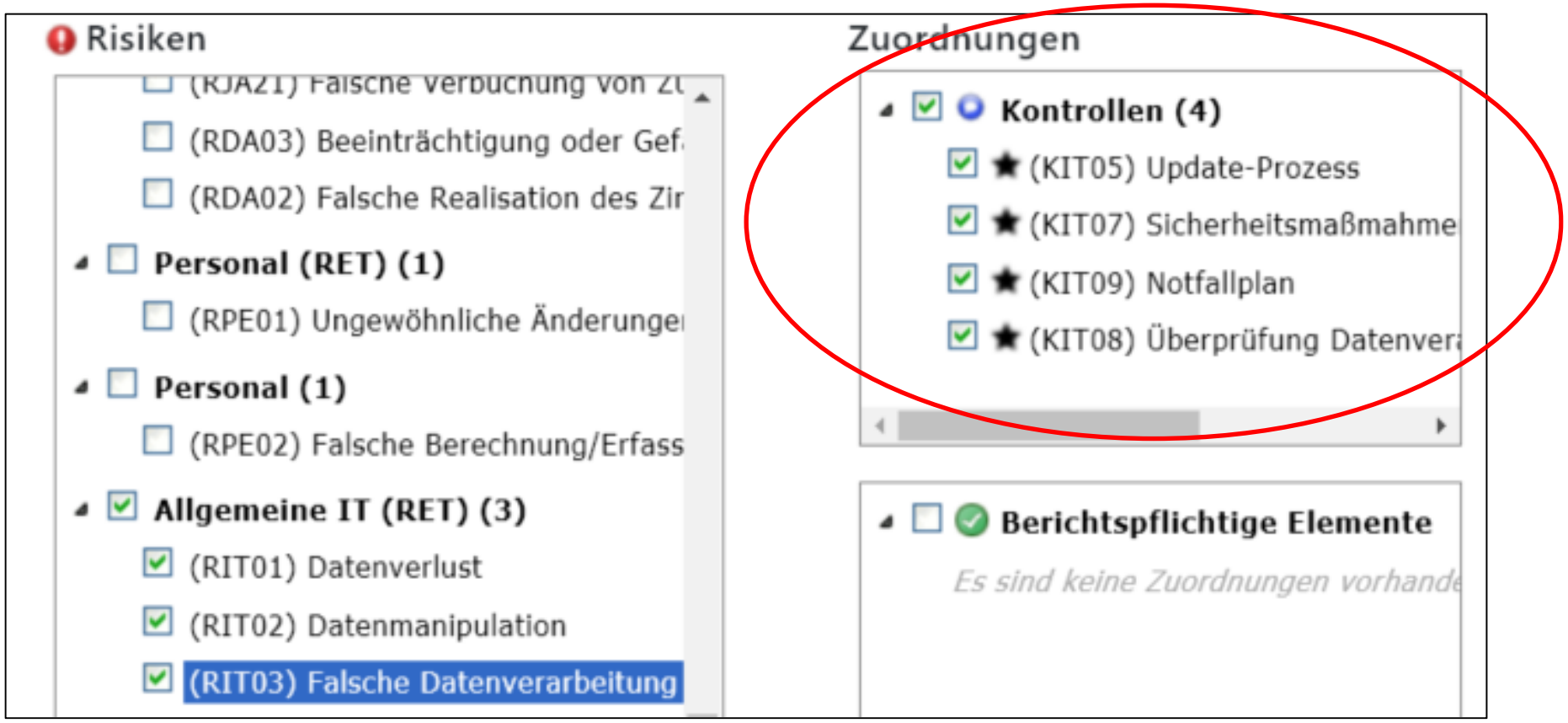


Lösung: Dann ist der "Zähler" der entsprechenden Kontrolle (nach dem Jahreswechsel nun als "Vorjahr 1 (Geprüft)" ausgewiesen) manuell auf "Ja" gesetzt.

Somit weist 540 dann immer den richtigen zeitlichen Stand der Kontrollen aus!!

IX. Erfassung von IT-Kontrollen

Bereits in der Importvorlage enthaltene IT-Risiken und IT-Kontrollen

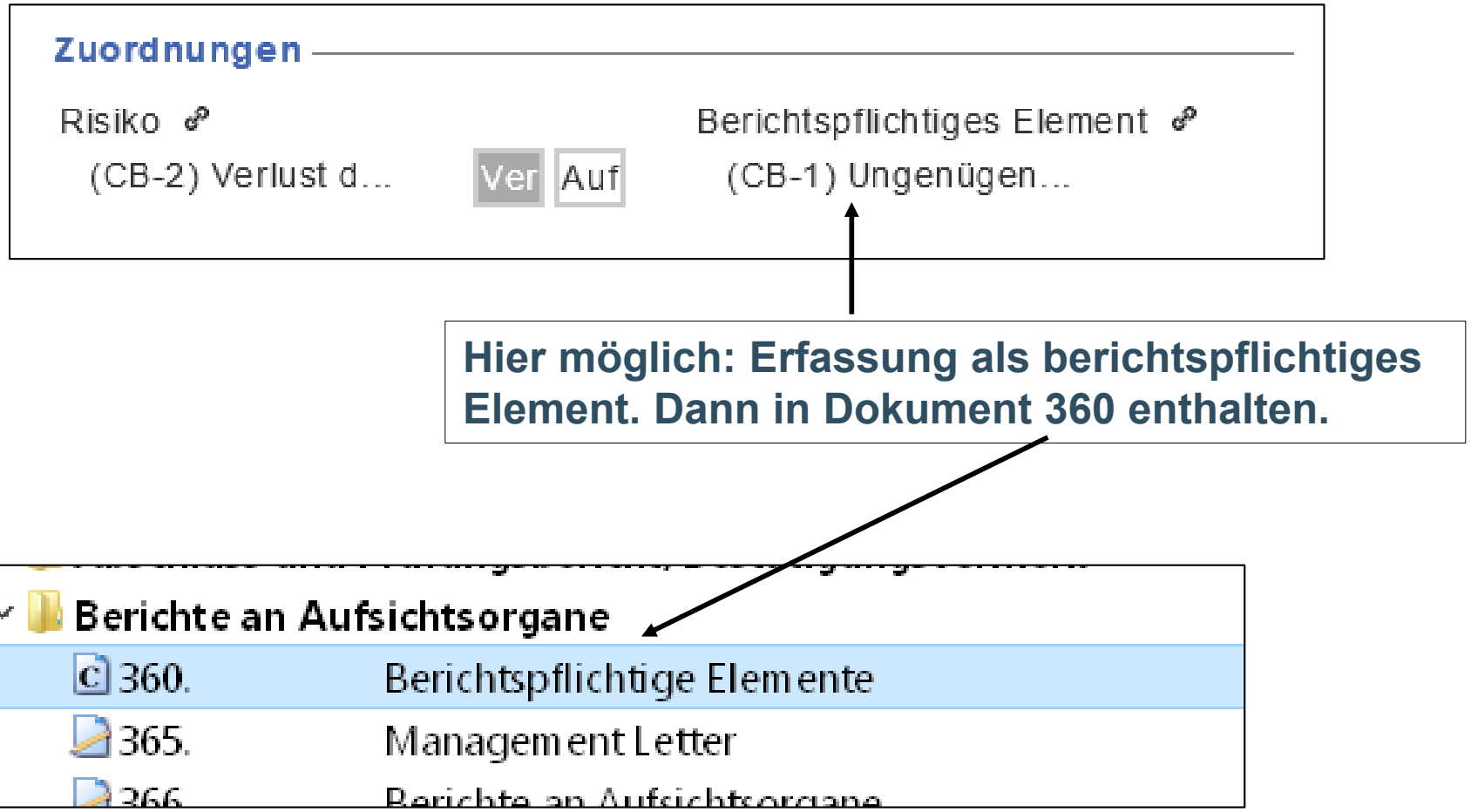


IX. Erfassung von IT-Kontrollen

Bereits in der Importvorlage enthaltene IT-Risiken und IT-Kontrollen

Risiken aus dem Einsatz von IT	IT-Kontrolle
Datenverlust (RIT01)	Datensicherung und Datenwiderherstellung (KIT01)
	Sicherheitsmaßnahmen IT-Infrastruktur (KIT06)
Datenmanipulation (RIT02)	Zugriffsschutz (KIT02)
	Einschaltung der systemseitgen Stammdatenänderungsprotokollierung (KIT04)
	Sicherheitsmaßnahmen IT-Infrastruktur (KIT06)
	Berechtigungskonzept (KIT03)
Falsche Datenverarbeitung (RIT03)	Update-Prozess (KIT05)
	Sicherheitsmaßmahmen Netzwerk (KIT07)
	Überprüfung Datenverarbeitung und Datenübernahme (KIT08)
	Notfallplan (KIT09)

IX. Erfassung von IT-Kontrollen



IX. Erfassung von IT-Kontrollen

Dokument 360 – Berichterstattung an den Aufsichtsrat

Berichtspflichtige Elemente	Einheiten	Feststellungsdatum	Identifiziert von	Eingeschlossen in: Management Let...	Eingeschlossen in: Bericht für die f...	Begründung	Bewertung	Gruppier
31.12.2017								
Wesentliche Schwächen im internen Kontrollsystem								
(CB-1) Ungenügende Datensicherung		26.11.2018	Claudia Buchta	Ja	Ja	Es läuft doch	Bedeutsam	

IX. Erfassung von IT-Kontrollen

Überblick:

IT-Kontrollen und Kontrollen im Bezug auf Journalbuchungen		Risken	Aufbauprüfung in … (Referenz Funktionstest)		
			531.	ORD.PP	531.ORD.MIN
KIT01	Kontrolle der ordnungsmäßigen Datensicherung und Datenwiederherstellung	RIT01	17		4
KIT02	Kontrolle durch Zugriffschutz	RIT02	24, 25		7, 8
KIT03	Einrichtung eines Berechtigungskonzeptes	RIT02	7		3
KIT04	Einschaltung der systemseitgen Stammdatenänderungsprotokollierung	RIT02		6, 10	16, 20
KIT05	Kontrolle durch festgelegten Updateprozess	RIT03	33		10
KIT06	Sicherheitsmaßnahmen IT-Infrastruktur	RIT01, RIT02	22, 23		6
KIT07	Sicherheitsmaßmahmen Netzwerk	RIT03	24, 30		7, 9
KIT08	Überprüfung Datenverarbeitung und Datenübernahme	RIT03	38, 42		11, 13
KIT09	Einrichung eines IT-Notfallplans	RIT03	18, 19, 20		5

Erinnerung: In 531. und ORD.PP sowie 531.ORD.MIN sind immer die IT-Risiken und IT-Kontrollen zu verknüpfen!!

X. Risiko-Kontroll-Matrix 540

X. Risiko-Kontroll-Matrix 540

Zusammengefasste Darstellung in Dokument 540

	Kontrollen	Einheiten	Betroffenes IT-System	Feststellungsdatum	Aufbauprüfung		
					Ref. Walkthrough	Konzeption der Kontrolle(n)	Kontrolle eingerichtet
1	(KIT01) Datensicherung und Datenwiederherstellung		Finanzbuchhaltung	02.07.2024	KIT01 KIT01_1 KIT01_3	Zufriedenstellend	Ja
2	(KIT02) Zugriffschutz		Finanzbuchhaltung	02.07.2024	KIT02 KIT02_KIT07_2	Zufriedenstellend	Ja

X. Risiko-Kontroll-Matrix 540

Zusammengefasste Darstellung in Dokument 540

Aufbauprüfung				
Ref. Walkthrough	Konzeption der Kontrolle(n)	Kontrolle eingerichtet	Ergebnisse Walkthrough	Seit der vorherigen Bewertung geändert
KIT01 KIT01_1 KIT01_3	Zufriedenstellend	Ja	Zufriedenstellend	Nein
KIT02 KIT02_KIT07_2	Zufriedenstellend	Ja	Zufriedenstellend	Nein

X. Risiko-Kontroll-Matrix 540

Zusammengefasste Darstellung in Dokument 540

Kontrollattribute				Funktionsprüfung				
Relevante Kontrolle	Indirekte Kontrolle	Manuell / Automatisch	Häufigkeit der Kontrolle	Funktionsprüfung	Ref. Funktionsprüfung	Kontrolle ist wirksam	Berichtspflichtiges Element	Risikofaktoren
Ja	Ja	Manuell	Täglich	Ja	KIT01 KIT01_1 KIT01_3 540. 531.ORD.MIN - 4. Backup	Ja		
Ja	Nein	Automatisch	Ständig	Ja	KIT02 KIT02_KIT07_2 540. 531.ORD.MIN - 8. Kennwortverwaltung - Dokumentiert in 531.ORD.MIN - 12. Autorisierung - Dokumentiert in	Ja		

"Zähler"

X. Risiko-Kontroll-Matrix 540

Zusammengefasste Darstellung in Dokument 540

Risikofaktoren	(RRL03) Hinweise auf ...	(RRL04) Management Ov...	(RJA28) Genauigkeit a...	(RIT02) Datenmanipula...	(RDA03) Beeinträchtig...	(RIT01) Datenverlust	(RJA27) Existenz auf ...	(RIT03) Falsche Daten...	(RJA26) Vollständigke...
	RAE	RAE	RAE	RAE	RAE	RAE	RAE	RAE	RAE
						Ver			
				Ver					

X. Risiko-Kontroll-Matrix 540

Alle Risiko-Kontroll-Matrizen in der RET Vorlage



XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

Überblick - Kontrollen

- KIT01 – Datensicherung und Datenwiederherstellung
- KIT02 – Zugriffschutz
- KIT03 – Berechtigungskonzept
- KIT04 – Einschaltung der systemseitigen Stammdatenänderungsprotokollierung
- KIT05 – Updateprozess
- KIT06 – Sicherheitsmaßnahmen IT-Infrastruktur
- KIT07 – Sicherheitsmaßnahmen Netzwerk
- KIT08 – Überprüfung der Datenverarbeitung und Datenübernahme
- KIT09 – Notfallplan

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

Überblick Zuordnung Risiken und Kontrollen

Risiken aus dem Einsatz von IT	IT-Kontrolle	531.	ORD.PP	531.ORD.MIN
Datenverlust (RIT01)	Datensicherung und Datenwiederherstellung (KIT01)	17		4
	Sicherheitsmaßnahmen IT-Infrastruktur (KIT06)	22		6
Datenmanipulation (RIT02)	Zugriffsschutz (KIT02)	24, 25		8, 7
	Einschaltung der systemseitgen Stammdatenänderungsprotokollierung (KIT04)		6, 10	16, 20
	Sicherheitsmaßnahmen IT-Infrastruktur (KIT06)	22, 23		6
	Berechtigungskonzept (KIT03)	7, 23		3
Falsche Datenverarbeitung (RIT03)	Update-Prozess (KIT05)	33		10
	Sicherheitsmaßmahmen Netzwerk (KIT07)	24, 30		7, 9
	Überprüfung Datenverarbeitung und Datenübernahme (KIT08)	38, 42		11, 13
	Notfallplan (KIT09)	18, 19, 20		5

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

Dokumentation der Kontrollen

- Aufbauprüfung
- Funktionstest
- Ergebnis
- Beurteilung Kontrollrisiko
- Prüfungsnachweise

- **Musterdokumente zur Unterstützung bei der Dokumentation der Kontrollen**

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT01 – Datensicherung und Datenwiederherstellung

Muster

Identifizierte Kontrolle
KIT01 - Datensicherung und Datenwiederherstellung
Zugeordnete Risiken
RIT01 - Daten sind nicht verfügbar bzw. vollständiger Datenverlust
Aufnahme des Prozesses/Aufbauprüfung
Im Zuge einer **Befragung** des IT-Verantwortlichen - Hrn. X - wurde die Einrichtung und Funktion der Datensicherung und Wiederherstellung hinterfragt. Nach Auskunft von Hrn. X erfolgt die Datensicherung täglich als Vollsicherung auf Festplatte, weiterhin wird eine Kopie auf ein Backupsystem gespiegelt. Einmal wöchentlich erfolgt eine Auslagerung der Wochensicherungen (5 Tagessicherungen auf einer Festplatte) in einen Tresor in einem gesicherten Raum in einer anderen Brandschutzzone. Regelmäßige Datenrücksicherungstests finden statt und werden im Excel dokumentiert. **Einsichtnahme** in entsprechende Unterlagen. (optional: Eine Überprüfung der Wiederherstellbarkeit der Datensicherungen erfolgt auskunftsgemäß in unregelmäßigen Abständen (bei Bedarf), dies wird nicht dokumentiert.) (optional: Regelungen zur Datensicherung und Wiederherstellung finden sich im IT-Sicherheitskonzept des Unternehmens wieder und entsprechen den Beschreibungen des Administrators.)
Ergebnis Aufbauprüfung und Einschätzung Kontrollrisiko
Eingerichtete Kontrollen sind angemessen. Das **Kontrollrisiko** kann als "gering" eingeschätzt werden. (optional - wenn keine Wiederherstellungstests vorgenommen werden "mittel")

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT01 – Datensicherung und Datenwiederherstellung

Muster

Funktionsprüfung/aussagebezogene Prüfungshandlungen: Prüfung der Umsetzung im System

Einsichtnahme letztes Sicherungsprotokoll und Überblick letzte Sicherungen (Auszug s.u.), Einsichtnahme Datenauslagerung - Tresor im Nachbargebäude (andere Brandschutzzone)
Letzter Datenrücksicherungstest erfolgte am 21.11.2023, Einsichtnahme Doku Administrator s.u.

Ergebnis

Ein hinreichendes Datensicherungsverfahren ist eingerichtet und funktionsfähig. Ebenfalls finden regelmäßige Datenrücksicherungstets statt.
(optional: Datenrücksicherungstests finden auskunftsgemäß nicht statt, Administrator und Geschäftsführer darauf hingewiesen das Datenrücksicherungstests essentienl für das Unternehmen sein können - Stichwort: Verschlüsselungstrojaner)

Prüfungsnachweise

Auszug letztes Sicherungsprotokoll (detail)

Zeit : Letzte 24 Stunden	Knotenname : All	Generiert von : Alle	Job-ID : Alle	Jobtyp : Siche	SiteName : Al	Meldungs-ID :	Meldung : Alle
Zeit	Knotenname	Generiert von	Job-ID	Jobtyp	SiteName	Meldungs-ID	Meldung
29.11.2023 22:54	xa-master1.inter	srvbackup.intern.wl	216556	Sichern	Lokale Site	30607	Die VMDK-Dateien des virtuellen Rechners wurden geschlossen.
29.11.2023 22:54	xa-master1.inter	srvbackup.intern.wl	216556	Sichern	Lokale Site	30157	Sicherungsjob wurde erfolgreich abgeschlossen.
29.11.2023 22:54	xa-master1.inter	srvbackup.intern.wl	216556	Sichern	Lokale Site	30630	Insgesamt 378,45 MB ins Ziel geschrieben nach einer Ersparnis v

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT01 – Datensicherung und Datenwiederherstellung

Muster

Uberblick letzte Sicherungsprotokolle

Name	Server	Speicher	Auftragstyp	Auftragsstatus	Verarbeitet %	Startzeit	Endzeitpunkt	Verstrichen...	Byte (Anzahl)	Auftragsrate	Fehlercode	Deduplizierungsrate	Auswahl	Backup-Methode
BackupServer-Inkremen...	BackupServer...	B2D	Sichern	Erfolgreich	100%	17.01.2024 0...	17.01.2024 0...	00:08:12	3,41 GB	882,72 MB/min			\\BackupServer[redacted]	Inkrementell
[redacted]Cluster-Inkrementell	[redacted]Cluster...	B2D	Sichern	Erfolgreich...	100%	16.01.2024 2...	16.01.2024 2...	00:51:38	34,0 GB	1.776,10 MB/...			\\[redacted]Cluster[redacted]	Inkrementell
BackupServer-Inkremen...	BackupServer...	B2D	Sichern	Erfolgreich	100%	16.01.2024 0...	16.01.2024 0...	00:08:25	3,50 GB	888,13 MB/min			\\BackupServer[redacted]	Inkrementell
[redacted]Cluster-Inkrementell	[redacted]Cluster...	B2D	Sichern	Erfolgreich...	100%	15.01.2024 2...	15.01.2024 2...	01:05:43	55,9 GB	2.036,68 MB/...			\\[redacted]luster[redacted]	Inkrementell
BackupServer-Inkremen...	BackupServer...	B2D	Sichern	Erfolgreich...	100%	15.01.2024 0...	15.01.2024 0...	00:08:37	3,25 GB	723,36 MB/min			\\BackupServe[redacted]	Inkrementell
Hyper-V-Server-Kopie	ServerHyp03...	RDX1	Kopie	Erfolgreich	100%	13.01.2024 1...	13.01.2024 1...	00:38:38	75,4 GB	2.995,51 MB/...				

Doku letzte Datenwiederherstellung - Auszug Doku Servertests Administrator

Durchführung von Tests an Serversystemen 2024

Datum	Administrator	Art des Test	Ergebnis	Bemerkungen
21.11.2023	Admin	Datensicherung/Wiederherstellung UDP	i.O.	Netapp und Bandsicherung XIFS+XUN getestet

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT02 – Zugriffschutz

Muster

Identifizierte Kontrolle
KIT02 - Kontrolle durch Zugriffschutz
Zugeordnete Risiken
RIT02 - Datenintegrität nicht gegeben (Datenmanipulation)
Aufnahme des Prozesses/Aufbauprüfung
Im Zuge einer **Befragung** des IT-Verantwortlichen - Hrn. X - wurde auch die Einrichtung und Funktion des Zugriffsschutzes auf das Unternehmensnetzwerk und ERP-System hinterfragt. Nach Auskunft von Hrn. X hat jeder User sowohl auf Netzerk- als auch auch ERP-Systemebene eine eigene Nutzerkennung (Benutzername und Passwort). Die Parameter sind fest im System hinterlegt, d.h. die Mitarbeiter werden gezwungen, ihren Zugriffsschutz aktuell zu halten, um arbeitsfähig zu bleiben. Die Einstellungen können nur durch den IT-Admin geändert werden. **Einsichtnahme** der Einstellungen im System.
Ergebnis Aufbauprüfung und Einschätzung Kontrollrisiko
Eingerichtete Kontrollen sind angemessen. Das **Kontrollrisiko** kann als "gering" eingeschätzt werden.
Funktionsprüfung/aussagebezogene Prüfungshandlungen: Prüfung der Umsetzung im System
Passwortrestriktionen sind insbesondere auf Netzwerkebene und ERP-System-Ebene (Citrix/Rechenzentrum) eingerichtet, vgl. Screenshots (s.u.)
Ergebnis
Die (systemintegrierte) Kontrolle "Zugriffsschutz" ist aktiv und wirksam.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT02 – Zugriffschutz

Beispiel

Prüfungsnachweise

Kennwortrichtlinie Netzwerk Windows (Domäne)

Kennwortrichtlinie Domäne intern[redacted]

Kontorichtlinien/Kennwortrichtlinien

Richtlinie	Einstellung
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwortchronik erzwingen\ngespeicherte Kennwörter	2 gespeicherte Kennwörter
Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert
Maximales Kennwortalter	0 Tage
Minimale Kennwortlänge	8 Zeichen
Minimales Kennwortalter	0 Tage

Kontorichtlinien/Kontosperrungsrichtlinien

Richtlinie	Einstellung
Kontensperrungsschwelle	5 ungültige Anmeldeversuche
Kontosperrdauer	30 Minuten
Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT02 – Zugriffschutz

Beispiel

Kennwortrichtlinie Wodis/Citrix (Rechenzentrum)



XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT03 – Berechtigungskonzept

Muster

Identifizierte Kontrolle
KIT03 - Berechtigungskonzept
Zugeordnete Risiken
RIT02 - Datenintegrität nicht gegeben (Datenmanipulation)
Aufnahme des Prozesses/Aufbauprüfung
Im Zuge einer **Befragung** des IT-Verantwortlichen - Hrn. X - wurde auch die Einrichtung eines Berechtigungskonzeptes hinterfragt und **nachvollzogen**. Nach Auskunft von Hrn. X sind Berechtigungen insbesondere wie folgt vergeben: - Netzwerkebene => Die Mitarbeiter sind im Netztwerk je nach Aufgabengebiet verschiedenen Netzlaufwerken und Ordnern zugeordnet - Wodis Sigma => ein rollenbasiertes Berechtigungskonzept ist eingerichtet, den Rollen sind aufgabenbezogen Mitarbeiter des Unternehmens zugeordnet, weiterhin ist ein 4-Augen-Prinzip im Bereich Stammdatenänderungen Geschäftspartner (Bankverbindungen) im System eingerichtet - Auftragsvergabe/Rechnungsprüfung => erfolgt über in Wodis eingerichtete Workflows - elektr. Archivsystem => Mitarbeiter können nur auf die Ordner zugreifen welche sie für ihren Tätigkeitsbereich benötigen - elektronischer Zahlungsverkehr => Berechtigungen bei der Bank hinterlegt Ein fomal dokumentiertes und von der Unternehmensleitung freigegebenes "Soll-Konzept" gibt es weder für das Netzwerk, noch für das ERP-System. (optional: Ein von der Unternehmensleitung freigegebenes "Soll-Konzept" liegt für das ERP-System und das Archivsystem vor.) Die Einrichtung der Berechtigungen (bis auf den elektr. Zahlungsverkehr) erfolgt durch den Administrator auf Basis eines "Arbeitsauftrages" (i.d.R. per Mail) durch den Abteilungsleiter oder Geschäftsführers. Dies erfolgt in der Regel bei neuen Mitarbeitern oder bei Änderung/Erweiterung von Arbeitsaufgaben. Bei Austritt eines Mitarbeiters aus dem Unternehmen wird der User im System gesperrt und kann nicht mehr verwendet werden. Eine Sichtung der eingerichteten Berechtigungen erfolgt durch das Unternehmen auskunftsgemäß nur bei Bedarf.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT03 – Berechtigungskonzept

Muster

Aufnahme des Prozesses/Aufbauprüfung
Bei der **elektronischen Rechnungsprüfung** wurden nach Rechnungsarten entsprechende Workflows mit Prüfschritten im System angelegt und den Schritten Mitarbeiter zugeordnet (vgl. KRL04 "Rechnungsprüfung") Die **Änderung von Stammdaten** (hier: Bankverbindungen) im ERP-System erfolgt im 4-Augen-Prinzip, entsprechende Berechtigungen sind hinterlegt, erst nach Freigabe durch einen zweiten Mitarbeiter können Rechnungen in der Zahlungsliste verarbeitet werden.) Vgl. KRL02.)
Berechtigungen im Bereich elektronischer Zahlungsverkehr sind im Wodis über das BK01-Verfahren bei der Aareal-Bank hinterlegt. Weiterhin sind ebenfalls Berechtigungen bei der Sparkasse eingerichtet. => die bei der Bank hinterlegten Berechtigungen wurden eingesehen (KRL04) und stimmen mit der Unterschriftenrichtlinie des Unternehmens überein. Vgl. auch Bankbestätigung 500.RET => Die Änderung von Zeichnungsberechtigungen bei der Bank ist formalisiert. Es muss eine Meldung gem. Formblatt an die Bank erfolgen, anschließend richtet die Bank entsprechend die Berechtigung ein. Im Unternehmen selbst kann kein Mitarbeiter selbständig die elektr. Berechtigungen bei der Bank ändern. Berechtigungskonzept Wodis Sigma und Archiv kompakt wurde vor Ort zusammen mit dem Administrator **eingesehen** und ist vom Aufbau her nicht zu beanstanden.
Ergebnis Aufbauprüfung und Einschätzung Kontrollrisiko
Eingerichtete Kontrollen sind teilweise angemessen, es liegt kein dokumentiertes Soll-Konzept für das ERP-System, das Netzwerk und den Rechnungsworkflow vor. Das **Kontrollrisiko** kann als "mittel" eingeschätzt werden.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT03 – Berechtigungskonzept

Muster

Funktionsprüfung/aussagebezogene Prüfungshandlungen: Prüfung der Umsetzung im System
Verschiedene Berechtigungen im Berechtigungskonzept wurden nachvollzogen, insbesondere im Bereich der Rechnungsprüfung und Zahlungsfreigabe (vgl. KRL04 "Rechnungsprüfung")
Ergebnis
Beim Unternehmen sind elektr. Berechtigungskonzepte auf mehreren Ebenen eingerichtet und funktionsfähig. Ein durch die Unternehmensleitung freigegebenes "Soll-Konzept" gibt es nicht. Eine Prüfung/Sichtung der Berechtigungen auf Netzwerk- und ERP-System-Ebene erfolgt nicht. In Bezug auf die Auftragsvergabe- und Rechnungsprüfungsworkflows sowie die elektr. Zahlungsfreigabe werden die Berechtigungen auskunftsgemäß durch die kfm. Prokuristin und die Geschäftsführung überwacht. Dies erfolgt insbesondere bei Ein- und Austritt von Mitarbeitern.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT03 – Berechtigungskonzept

Beispiel

Prüfungsnachweise

Arbeitsauftrag Einrichtung Berechtigung

Einrichtung Arbeitsplatz Frau [redacted] ab 01.02.2024 [redacted]

Antworten | Allen antworten | Weiterleiten

An [redacted]

Fr 17.11.2023

Zur Nachverfolgung. Beginn am Montag, 20. November 2023. Fällig am Montag, 20. November 2023.

Hallo [redacted],

ab 01.02.2024 nimmt Frau [redacted] ihre Arbeit in unserem Bereich auf.

Zimmer [redacted] Durchwahl [redacted] (ehem. Arbeitsplatz Frau [redacted])

Sie benötigt folgende Zugriffe bzw. Berechtigungen:

Berechtigungen in Wodis analog Frau [redacted]
Freischaltung: Bibo K, OHB
Outlook alle allgemeinen Kalender/Fahrtenbücher W-Bereich
Server W, WV, TIM
[redacted]

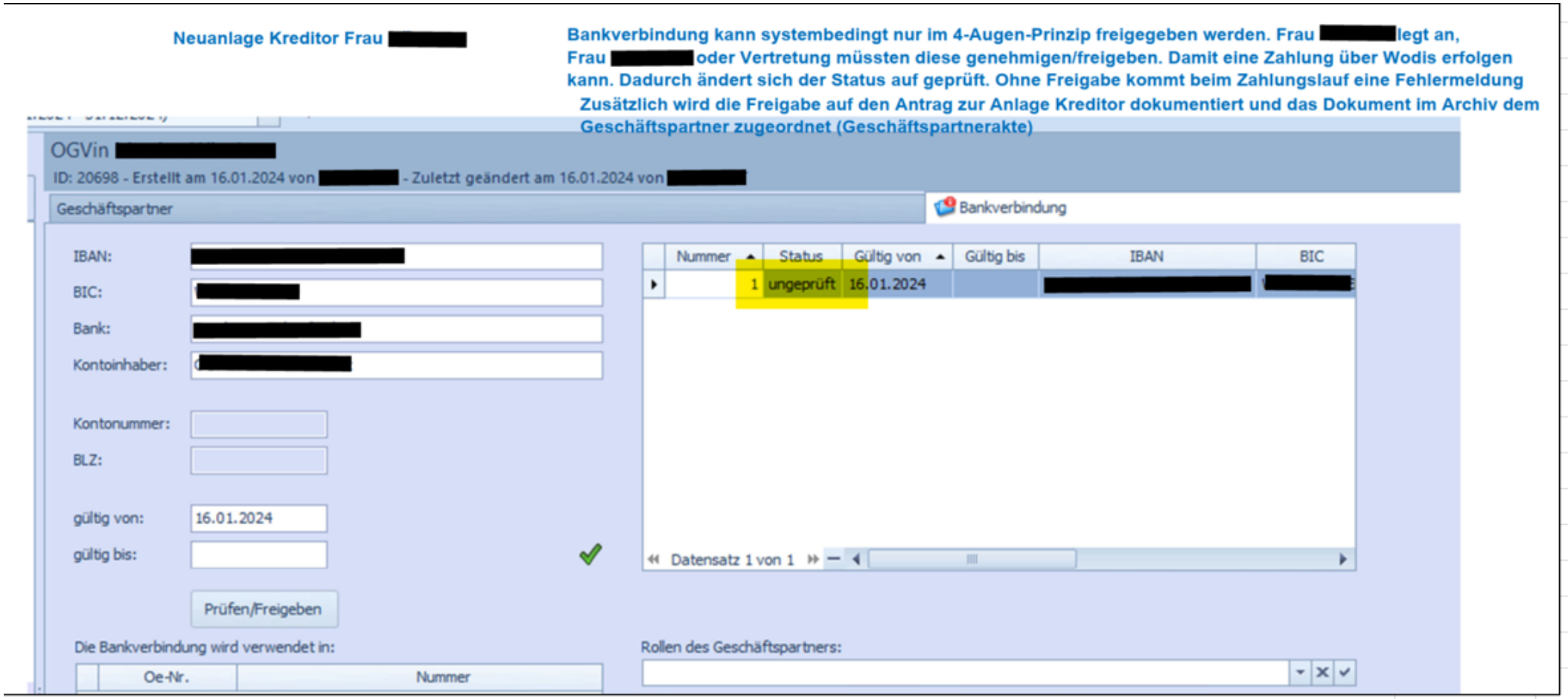
Mit freundlichen Grüßen

[redacted]
Ltrn. Wohnungswirtschaft

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT03 – Berechtigungskonzept

Beispiel



XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT03 – Berechtigungskonzept

Beispiel

Berechtigungen Sparkasse (KRL04):

Bankparameter | EBICS Benutzer | Echtzeitbenachrichtigung

EBICS Parameter: Sparkasse_neu

Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser zu gruppieren

Status	Interner Name	User-ID	Berechtigung	EU-Version	Auth.-Schlüs...	Technischer T...
bereit	[redacted]	[redacted]	Erstunterschrift (A)	A006 (2176 ...	2048 Bit	
bereit	[redacted]	[redacted]	Zweitunterschrift (B)	A006 (2176 ...	2048 Bit	
bereit	[redacted]	[redacted]	Erstunterschrift (A)	A006 (2176 ...	2048 Bit	
bereit	[redacted]	[redacted]	Zweitunterschrift (B)	A006 (2176 ...	2048 Bit	
bereit	[redacted]	[redacted]	Zweitunterschrift (B)	A006 (2176 ...	2048 Bit	
bereit	[redacted]	[redacted]	Erstunterschrift (A)	A006 (2176 ...	2048 Bit	
bereit	[redacted]	[redacted]	Zweitunterschrift (B)	A006 (2176 ...	2048 Bit	
[redacted]						

Neu | Bearbeiten | Löschen

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT03 – Berechtigungskonzept

Beispiel

Bsp. Berechtigungskonzept ERP-System

Gruppe-ID	Benutzergruppe	Beschreibung zur Gruppe	Default-Gruppe	Gruppentyp	Mibu	Fibu	ReWe	GF	Verw 1	Verw 2	Technik
150	_FREIGABE0		Nein	Benutzergruppe							
106	Administrator	Admin	Nein	Benutzergruppe				B			
103	Administratoren ReadOnly	Administratoren [S]	Nein	Benutzergruppe				B			
102	Allgemeine Systemrechte	Allgemeine Systemrechte [S]	Nein	Benutzergruppe				B			
0	Allgemeine Systemrechte1	Allgemeine Systemrechte [S]	Nein	Benutzergruppe				B			
101	Andere	Andere [S]	Nein	Benutzergruppe							
142	Anlagenbuchhaltung - ReadOnly		Nein	Benutzergruppe			B	A			
100	Anlagevermogen	Anlagevermogen [S]	Nein	Benutzergruppe			B	A			
99	Bestände/Verträge	Bestände/Verträge - Vollzugriff [K]	Nein	Benutzergruppe	B	L	L	A	L	B	L
123	Buchaltung_FiBu-Rechnungen-Buchung	Buchhaltung - Buchung der Eingangsrechnungen (zusätzliche Berechtigung) [S]	Nein	Benutzergruppe	B	B	B	A	L	L	L
124	Buchhaltung_FiBu-Rechnungen	Buchhaltung - Eingangsrechnungen (allgemeine Berechtigungen) [S]	Nein	Benutzergruppe	B	B	B	A	L	L	L

Legende	
B	Bearbeiten
L	Leseberechtigung
A	Alle Funktionen (Bearbeiten, Ändern, Lesen)
X	keine Funktionen
B, L	Teils Bearbeitungen möglich, Teils nur Leseberechtigung

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT04 – Einschaltung der systemseitigen Stammdatenänderungsprotokollierung

Muster

Identifizierte Kontrolle
KIT04 - Einschaltung der systemseitigen Stammdatenänderungsprotokollierung
Zugeordnete Risiken
RIT02 - Datenintegrität nicht gegeben (Datenmanipulation)
Aufnahme des Prozesses/Aufbauprüfung
Im Zuge einer **Befragung** des IT-Verantwortlichen - Hrn. X - wurde auch die Einrichtung und Funktion der Stammdatenänderungsprotokollierung im ERP-System Wodis Sigma hinterfragt. Nach Auskunft von Hrn. X ist die Stammdatenänderungsprotokollierung aktiv und kann auch nicht durch den Admin ausgeschalten werden. Eine Prüfung/Auswertung der Stammdatenänderungsprotokollierung erfolgt auskunftsgemäß nur bei Bedarf. Bezüglich der Stammdatenänderungsprotokollierung wird auch auf das vorliegende Softwaretestat für Wodis Sigma verwiesen (vgl. 540.1 Softwaretestat Wodis Sigma). **Einsichtnahme** ist erfolgt. (optional: Im Rahmen der Mietvertragsunterzeichnung/Neuvermietung sowie bei Mieterhöhungen erfolgen Kontrollen bei den Stammdatenänderungen...) (optional: Bei SAP-Systemen/Blue Eagle besteht die Möglichkeit die Stammdatenänderungsprotokollierung zu deaktivieren.)
Ergebnis Aufbauprüfung und Einschätzung Kontrollrisiko
Die eingerichteten Kontrollen sind teilweise angemessen. Das **Kontrollrisiko** kann als "mittel" eingeschätzt werden, da keine regelmäßige Prüfung der Stammdatenänderungen stattfindet.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT04 – Einschaltung der systemseitigen Stammdatenänderungsprotokollierung

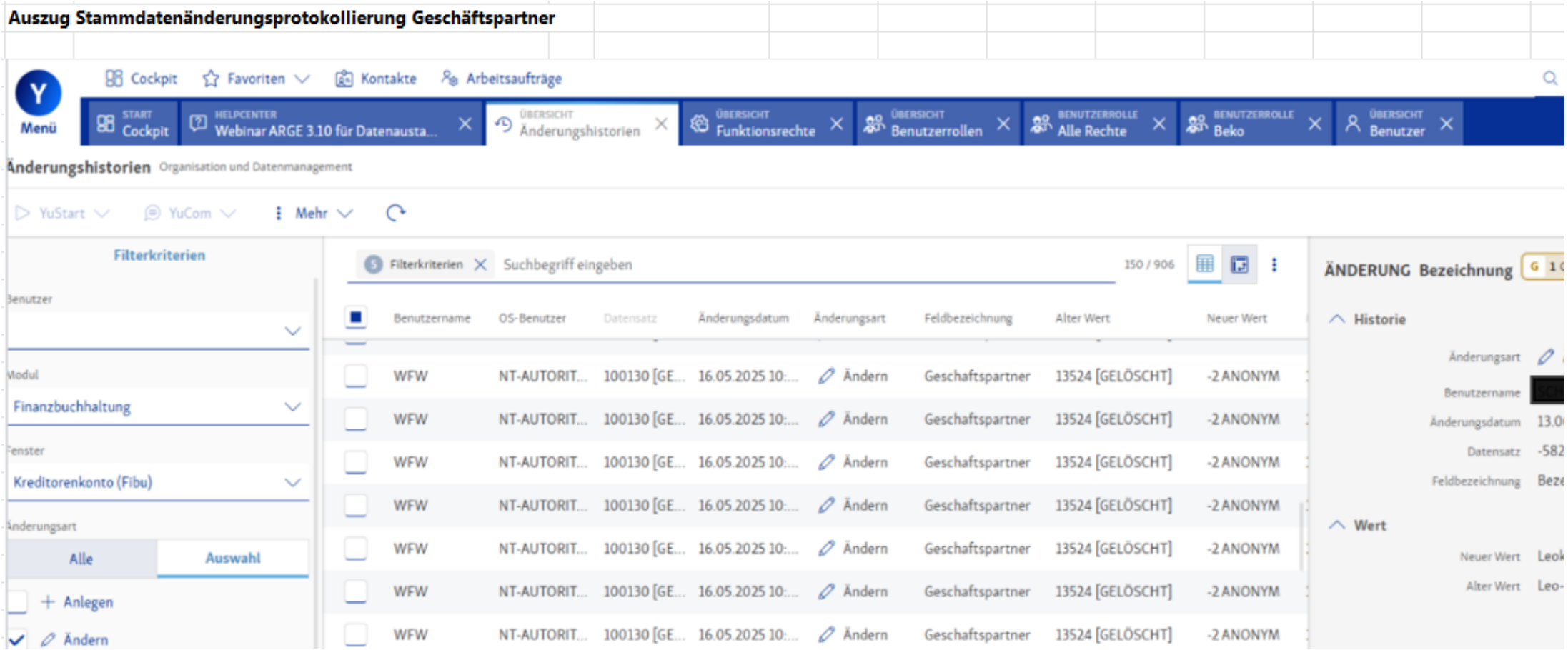
Muster

Funktionsprüfung/aussagebezogene Prüfungshandlungen: Prüfung der Umsetzung im System
Prüfung der Umsetzung im System: Änderungsprotokollierung ist aktiv, Beispiel für Geschäftspartner, Fibu-Konto und Mietvertrag => vgl. Screenshots (s.u.)
(optional: Bezüglich der Kontrolle der Stammdatenänderungen im Bereich der Neuvermietung; bei Mieterhöhungen oder Kreditoren => vgl. KRL02.. KMIxx.. etc.)
Ergebnis
Die (systemintegrierte) Kontrolle "Stammdantenänderungsprotokollierung" ist aktiv und wirksam. (optional: Kontrollen im Rahmen der Stammdatenänderungen sind eingerichtet und funktionsfähig)

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT04 – Einschaltung der systemseitigen Stammdatenänderungsprotokollierung

Beispiel - Yuneo



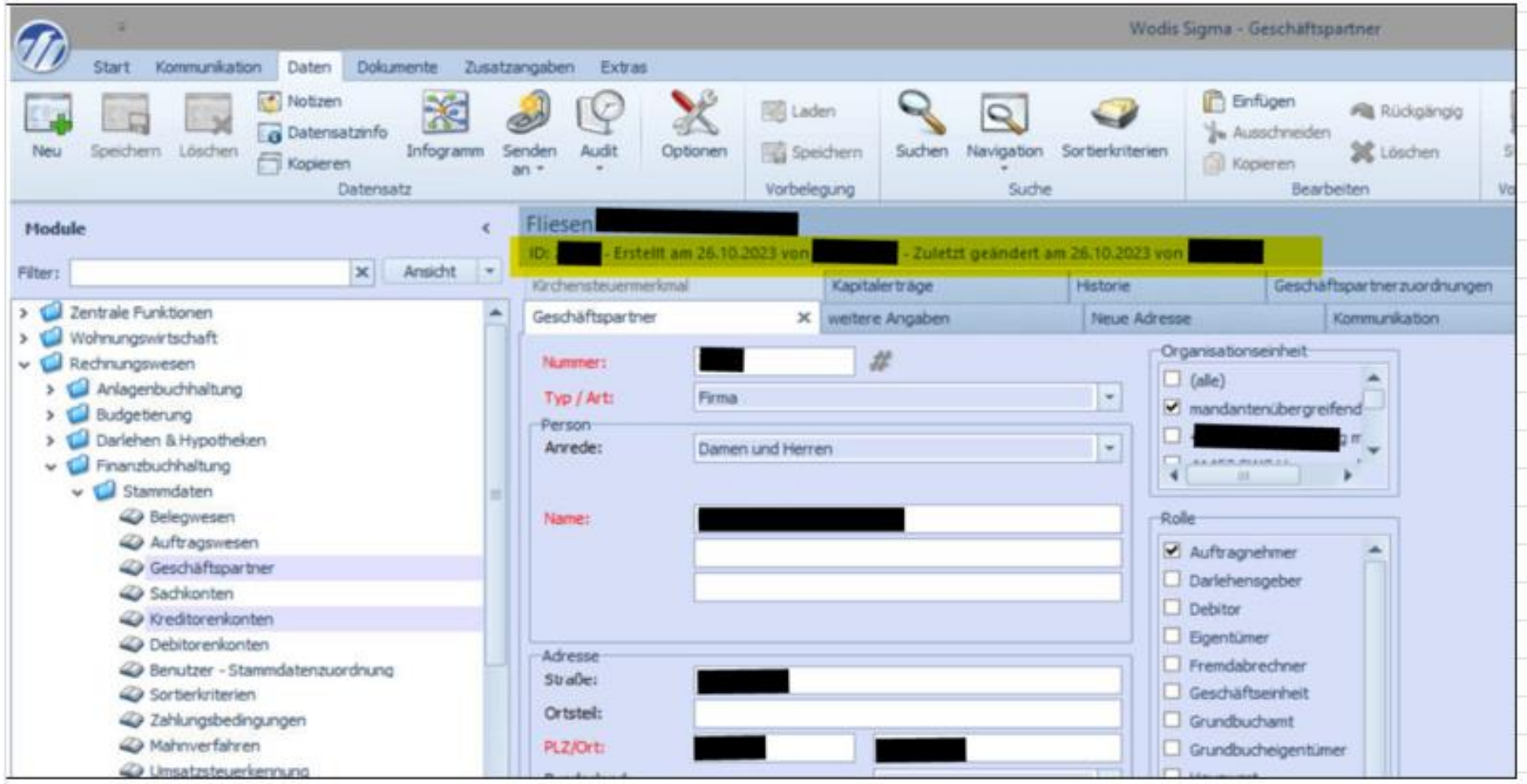
XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT04 – Einschaltung der systemseitigen Stammdatenänderungsprotokollierung

Beispiel

Sigma

Auszug Stammdatenänderungsprotokollierung Geschäftspartner



XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT04 – Einschaltung der systemseitigen Stammdatenänderungsprotokollierung

Beispiel

Auszug Stammdatenänderungsprotokollierung Mietvertrag

Nr.	Bestandtei	Art	VE	von	bis	optiert	vergünst.	Gesamtbet	nachträgl.	Betrag	Miete/m²	Mietänder	Bemerkung	Mietanpas	Erfasst am	durch	Geändert a	durch	manuell erf. Mietänderung
6800	Einzelmiet	Grundmiet	1	01.01.2023		0	0	290	0	290	6,08	1+: Neuvermietung (50N)	(Sonstig		28.11.2022	Mustermann			Vertragsbeginn
6810	Betriebsko	Umlagevor	1	01.01.2023		0	0	40	0	40	0,84	1+: Neuvermietung (50N)	(Sonstig		28.11.2022	Mustermann			Vertragsbeginn
6820	Heizkosten	Umlagevor	1	01.01.2023		0	0	100	0	100	2,1	1+: Neuvermietung (50N)	(Sonstig		28.11.2022	Mustermann			Vertragsbeginn
6830	Wasserkos	Umlagevor	1	01.01.2023		0	0	25	0	25	0,52	1+: Neuvermietung (50N)	(Sonstig		28.11.2022	Mustermann			Vertragsbeginn
																=> Neuanlage MV durch Frau Mustermann			

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT05 – Updateprozess

Muster

Identifizierte Kontrolle
KIT05 - Kontrolle durch festgelegten Updateprozess

Zugeordnete Risiken
RIT03 - Verarbeitung der Daten ist nicht richtig (laufender Betrieb, Updates)

Aufnahme des Prozesses/Aufbauprüfung
Zu dieser Kontrolle erfolgte eine **Befragung** des IT-Verantwortlichen Hrn. X. Für die Aktualisierung der beim Unternehmen eingesetzten Softwarelösungen ist er allein verantwortlich. (optional: Das ERP-System wird als SaaS betrieben. Für die Aktualisierung der Software ist der Anbieter verantwortlich, vgl. Vertrag). Die Updates für das ERP-System erfolgen regelmäßig nach Erscheinen, i.d.R. immer am auf die Veröffentlichung folgenden Freitag. Der Admin. führt diese Updates über eigene Hardware am Standort durch. Mindestens einmal monatlich erfolgen die Updates auf den Servern, dies führt Hr. X i.d.R. am Wochenende über Fernzugriff von seinem Zuhause aus durch. Ebenfalls monatlich werden die Updates der nicht-rechnungslegungsrelevanten Anwendungen mittels "Paket-Lösung" (ACMP) durchgeführt. Der Update-Prozeß als solches ist nicht schriftlich fixiert, er gehört quasi zum festen Aufgabenbereich des IT-Verantwortlichen. Besondere, planmäßige Kontrollen durch ein zweites Augenpaar erfolgen (mangels qualifizierter Mitarbeiter) nicht, lediglich im Vertretungsfall hat der IT-Dienstleister die gleichen Befugnisse wie der IT-Verantwortliche und kann, sollten nach einem Update Probleme auftreten, innerhalb kürzester Zeit die erfolgten Updates nachvollziehen und im Bedarfsfall korrigierend eingreifen.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT05 – Updateprozess

Muster

Aufnahme des Prozesses/Aufbauprüfung
Nachweise zu dieser Kontrolle wurden nicht eingefordert, bei Hr. X am Bildschirm wurde die aktuelle Update-Historie für das ERP-System und Windows Server bzw. Windows Clients **eingesehen (Beobachtung)** (das letzte aktuelle Update für das ERP-System liegt bereits vor, die Implementierung steht jedoch noch aus; Windows Server 2025 sowie für die Clients Windows 11 sind aktuell und werden automatisch nach Bereitstellung aktualisiert - vgl. KIT07). (optional: Regelungen zu Sicherheitsmaßnahmen IT-Infrastruktur finden sich im IT-Sicherheitskonzept wieder, vgl. 540.x) Updates für Firewall und Virenschutz erfolgen automatisiert (Einstellungen vor Ort am xx.xx.20xx eingesehen). (Vgl. auch KIT07.)
Hinweis: Bitte darauf achten das insbesondere bei Windows Server und bei den Clients keine "uralten" Versionen eingesetzt werden, Windows Server 2016 wird noch bis zum 12.1.2027 supportet, Windows Server 2019 bis 9.1.2029, Windows Server 2022 bis 14.10.2031 und Windows Server 2025 bis 10.2029. Windows 10 wird noch bis 14.10.2025 unterstützt (Enterprise Versionen ggf. länger), Windows 11 in der aktuellen Version bis 9.10.2029
Ergebnis Aufbauprüfung und Einschätzung Kontrollrisiko
Eingerichtete Kontrollen sind angemessen. Das **Kontrollrisiko** kann als "gering" eingeschätzt werden.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT05 – Updateprozess

Muster

Funktionsprüfung/aussagebezogene Prüfungshandlungen: Prüfung der Umsetzung im System
Überprüfung, ob das aktuellste Update eingespielt ist. Und Beobachtung der Update-Historie.
Ergebnis
Im Kontext gehen wir davon aus, daß die Kontrolle "Update-Prozeß" sachgerecht eingerichtet und auch in Funktion ist. Wünschenswert wäre, daß die "one-man-show" einer regulären Kontrolle durch ein zweites Augenpaar (ggf. auch durch den IT-Dienstleister) unterworfen wird, um das Risiko möglicher Fehler zu minimieren. Unabhängig davon gehen wir davon aus, daß Hr. X ein qualifizierter und gewissenhafter Mitarbeiter ist, welcher seine Pflichten vollumfänglich erfüllt. Wir verweisen hierzu auch auf eine qualifizierte Vertretung im Notfall durch einen ext. Dienstleister. Vgl. auch KIT09.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT05 – Updateprozess

Beispiel

Windows Update: => aktuellste Version ist eingespielt



XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT06 – Sicherheitsmaßnahmen IT-Infrastruktur

Muster

Identifizierte Kontrolle
KIT06 - Sicherheitsmaßnahmen IT-Infrastruktur
Zugeordnete Risiken
RIT01 - Daten sind nicht verfügbar bzw. vollständiger Datenverlust und RIT02 - Datenintegrität nicht gegeben (Datenmanipulation)
Aufnahme des Prozesses/Aufbauprüfung
Zu dieser Kontrolle erfolgte eine **Befragung** des IT-Verantwortlichen Hrn. X. und eine "Begehung" des Serverraumes am xx.xx.202x (**Beobachtung**). (optional: Regelungen zu Sicherheitsmaßnahmen IT-Infrastruktur finden sich im IT-Sicherheitskonzept wieder, vgl. 540.x) Die IT-Infrastruktur wird durch das Unternehmen inhouse betrieben, bei Bedarf können externe Partner gem. den vertraglichen Regelungen unterstützen. (optional: die IT-Infrastruktur hat das Unternehmen in die Cloud eines externen Dienstleisters ausgelagert. Der Betrieb erfolgt durch eigenes Personal auf fremder Infrastruktur.) (optional: die IT-Infrastruktur hat das Unternehmen in die Cloud eines externen Dienstleisters ausgelagert. Der Dienstleister kümmert sich entsprechend den vertraglichen Vereinbarungen auch um den Betrieb und die Administration.)
Ergebnis Aufbauprüfung und Einschätzung Kontrollrisiko
Eingerichtete Kontrollen sind angemessen. Das **Kontrollrisiko** kann als "gering" eingeschätzt werden.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT06 – Sicherheitsmaßnahmen IT-Infrastruktur

Muster

Funktionsprüfung/aussagebezogene Prüfungshandlungen: Prüfung der Umsetzung im System
Begehung des Serverraums am xx.xx.202x. Der Serverraum des Unternehmens entspricht den gängigen Anforderungen und ist verschlossen. Zutritt hat nur ein eingeschränkter Personenkreis (lt. Schlüsselplan). Sicherheitsmaßnahmen sind entsprechend den allg. Anforderungen umgesetzt (Klimatisierung, kein brennbares Material, Rauch-/Wärme-/Feuchtigkeits- und Bewegungssensor, USV, Brandschutztür mit Sicherheitsschließsystem, Alarmanlage). (optional: Die Netzwerkverteilerkästen sind für die Öffentlichkeit nicht zugänglich und befinden sind in abgeschlossenen Räumen.)
Ergebnis
Die Sicherheitsmaßnahmen für die IT-Infrastruktur entsprechen den gängigen Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik). Es ergeben sich keine Beanstandungen.
Prüfungsnachweise
Als Prüfungsnachweis gilt die dokumentierte Begehung des Serverraums.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT07 – Sicherheitsmaßnahmen Netzwerk

Muster

Identifizierte Kontrolle
KIT07 - Sicherheitsmaßnahmen Netzwerk

Zugeordnete Risiken
RIT03 - Verarbeitung der Daten ist nicht richtig (laufender Betrieb, Updates)

Aufnahme des Prozesses/Aufbauprüfung
Zu dieser Kontrolle erfolgte eine **Befragung** des IT-Verantwortlichen Hrn. X am xx.xx.202x und **Einsichtnahme** in die Regelungen zu den Sicherheitsmaßnahmen für das Netzwerk im IT-Sicherheitskonzept. Das Unternehmensnetzwerk wird durch ein Firewall- und Virenschutzsystem, Passwortrestriktionen und Berechtigungskonzepte geschützt. Firewall- und Virenschutzsysteme unterliegen automatischen Updates (vgl. Screenshots, s.u.). Bezüglich der Passwortrestriktionen und Berechtigungenskonzepte vgl. KIT02 und KIT03. Ein Monitoring der EDV-Systeme erfolgt derzeit nicht. Im Unternehmen ist eine Vielzahl von mobilen Endgeräten im Einsatz. Ein Mobile Device Managementsystem zur zentralen Steuerung der Geräte (vor allem Updates und bei Verlust) ist nicht im Einsatz. Die Steuerung der mobilen Endgeräte erfolgt über den Exchange Server (ist auch eine Möglichkeit). Dort ist auch eine Richtlinie hinsichtlich der Verschlüsselung der Geräte (Smartphones) eingerichtet. Laptops und Tablets werden nicht speziell verschlüsselt. Fernzugriff auf das Unternehmensnetzwerk haben Mitarbeiter im Homeoffice, Mitarbeiter mit Smartphone (Outlook) und ext. Dienstleister. Der Zugriff auf das Unternehmensnetzwerk erfolgt via VPN-Tunnel mit OpenVPN mit folgenden Standards: AES 256 bei TLS 1.2. Eine Multi-Faktor-Authentifizierung ist nicht vorgesehen.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT07 – Sicherheitsmaßnahmen Netzwerk

Muster

Aufnahme des Prozesses/Aufbauprüfung
Nach Rücksprache mit dem Geschäftsführer finden jährlich im Rahmen der Datenschutzschulung auch Mitarbeiterschulungen zum Thema IT-Sicherheit und Cybergefahren durch den Datenschutzbeauftragten statt. (optional: Durch die IT-Abteilung bzw. externen Dienstleister erfolgt weiterhin ein laufendes Monitoring der Systeme mit der Software...) Auskunftsgemäß ist die Konfiguration der Firewall ordnungsgemäß und entspricht den Bedürfnissen des Unternehmens. Eine laufende Überwachung erfolgt durch den IT-Verantwortlichen.
Ergebnis Aufbauprüfung und Einschätzung Kontrollrisiko
Kontrollen sind teilweise eingerichtet. Es gibt jedoch kein Monitoring der Systeme und insbesondere für die Zugriffe von außerhalb auf die IT-Systeme gibt es kein Zwei-Faktor-Verfahren. Weiterhin können wir die ordnungsgemäße Konfiguration der Firewall nicht beurteilen. Hinweise zum Monitoring und zur Zwei-Faktor-Authentifizierung an Unternehmensleitung und IT-Leiter wurden gegeben. Das **Kontrollrisiko** kann als "mittel" eingeschätzt werden,
Funktionsprüfung/aussagebezogene Prüfungshandlungen: Prüfung der Umsetzung im System
Überprüfung, ob der Virenscanner auf dem aktuellsten Stand ist. Ferner Überprüfung, ob die Firewall aktuell ist (vgl. Ref. oder s.u.).
Ergebnis
Sicherheitsmaßnahmen für das Unternehmensnetzwerk sind hinreichend eingerichtet und in Funktion. Updates sind aktuell. Zur weiteren Erhöhung der Sicherheit empfehlen wir Laptops/Tablets zu verschlüsseln und ein Monitoring der IT-Systeme zu prüfen.

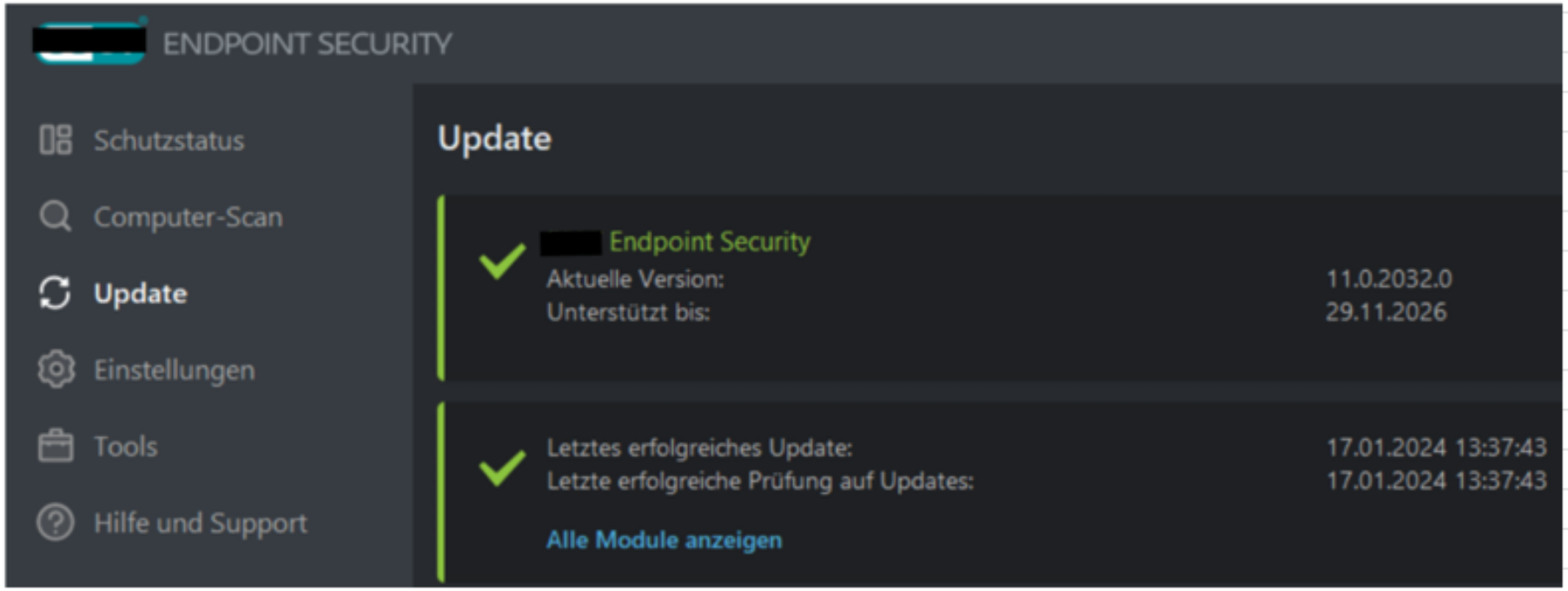
XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT07 – Sicherheitsmaßnahmen Netzwerk

Beispiel

Prüfungsnachweise

Screenshot Virenschutz



XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT07 – Sicherheitsmaßnahmen Netzwerk

Beispiel

Screenshot Firewall

Hardware Firwall [redacted] im Einsatz und aktuell, Lizenzen laufen bis 11/2026

Feature Key

Summary

Model	M270
Serial Number	[redacted]
Software Edition	Fireware XTM Pro
Signature	[redacted]

Features

FEATURE	VALUE	EXPIRATION	TIME LEFT
Model Upgrade	M270	Never	
Application Control	Enabled	08/11/2026	Expires in 938 Days
APT Blocker	Enabled	08/11/2026	Expires in 938 Days
Total Number of Authenticated Users	500	Never	
Gateway AntiVirus (AV)	Enabled	08/11/2026	Expires in 938 Days
Branch Office VPN Tunnels	50	Never	
Cloud Connect	Enabled	08/11/2026	Expires in 938 Days
Dimension Basic	Enabled	08/11/2026	Expires in 938 Days
Dimension Command	Enabled	08/11/2026	Expires in 938 Days
Fireware XTM	Enabled	Never	
Firewall Policy Maximum	Enabled	Never	
Filter Policy Throughput Maximum	Enabled	Never	
IP Addresses Allowed Outbound Access	Enabled	Never	
Intrusion Prevention (IPS)	Enabled	08/11/2026	Expires in 938 Days

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT07 – Sicherheitsmaßnahmen Netzwerk

Beispiel

Aktuelle Netzwerkübersicht	=> IT-Umfeld mittlerer Größe
23er Netz mit 8 Servern (davon drei virt.)	
drei NAS, 25 Druckern	
50 AP	
Fritz-Mesh Netzwerk	
vorgeschaltete Sophos XGS128 Firewall per LAN-Anbindung	
W-Lan + Gast-WLan	
Aufstellung eingesetzte Software/Hardware	
Microsoft W10/11, MS Office	
Aareon: Yuneo, Archiv Kompakt, Immoblue, Mareon	
Corporate Planning, SFirm, SmartTimePlus (Zeiterfassung)	

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT08 – Überprüfung der Datenverarbeitung und Datenübernahme

Muster

Identifizierte Kontrolle
KIT08 - Überprüfung Datenverarbeitung und Datenübernahme
Zugeordnete Risiken
RIT03 - Verarbeitung der Daten ist nicht richtig (laufender Betrieb, Updates)
Aufnahme des Prozesses/Aufbauprüfung
Zu dieser Kontrolle erfolgte eine **Befragung** des IT-Verantwortlichen Hrn. X und der kfm. Prokuristin Fr. Y am xx.xx.202x. Im ERP-System werden zwischen und in den Modulen Daten verarbeitet und über Schnittstellen (i.d.R. integrierte) übernommen. Eingabevalidierungen bzgl. der vollständigen und richtigen Erfassung von Daten erfolgen durch das ERP-System selbst (vgl. Testat 540.x - **Einsichtnahme**). In vielen Verarbeitungsschritten werden des Weiteren durch das ERP-System automatisch Protokolle und Fehlerlisten erzeugt, so bspw. im Bereich Sollstellung/Lastschriftlauf (Fehlerlisten), Bekolauf (Sollstellungsprotokoll), Lauf Erlösschmälerungen und Beko-Abrechungslauf. => vgl. KMI02_x und KBK01_x Eine Prüfung der Protokolle erfolgt durch die für den Bereich zuständigen Mitarbeiter. Eine gesonderte Dokumentation erfolgt nicht. Ohne Bearbeitung der Fehlerprotokolle erfolgt i.d.R. auch kein Durchlauf. Es handelt sich somit ebenfalls um automatische Systemkontrollen. (optional: Weiterhin gibt es noch eine Schnittstelle zum Handwerkerportal: Diese Schnittstelle ist automatisiert, vgl. Beschreibung KRL03_x)
Ergebnis Aufbauprüfung und Einschätzung Kontrollrisiko
Eingerichtete Kontrollen sind angemessen. Das **Kontrollrisiko** kann als "gering" eingeschätzt werden.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT08 – Überprüfung der Datenverarbeitung und Datenübernahme

Muster

Ergebnis Aufbauprüfung und Einschätzung Kontrollrisiko
Eingerichtete Kontrollen sind angemessen. Das **Kontrollrisiko** kann als "gering" eingeschätzt werden.
Funktionsprüfung/aussagebezogene Prüfungshandlungen: Prüfung der Umsetzung im System
Nachvollziehen der Protokollierung und Überprüfung der Schnittstelle zum Handwerkerportal (siehe KRL03_x).
Nachvollziehen der Protokollierung im Bereich Mietsollstellung (siehe KMIxx_x und KBKxx_x).
Ergebnis
Eine Überprüfung der Datenverarbeitung und Datenübernahme erfolgt weitestgehend durch automatisierte Eingabekontrollen seitens des ERP-Systems. Es ergeben sich keine Beanstandungen. Kontrollen sind eingerichtet und in Funktion.
Prüfungsnachweise

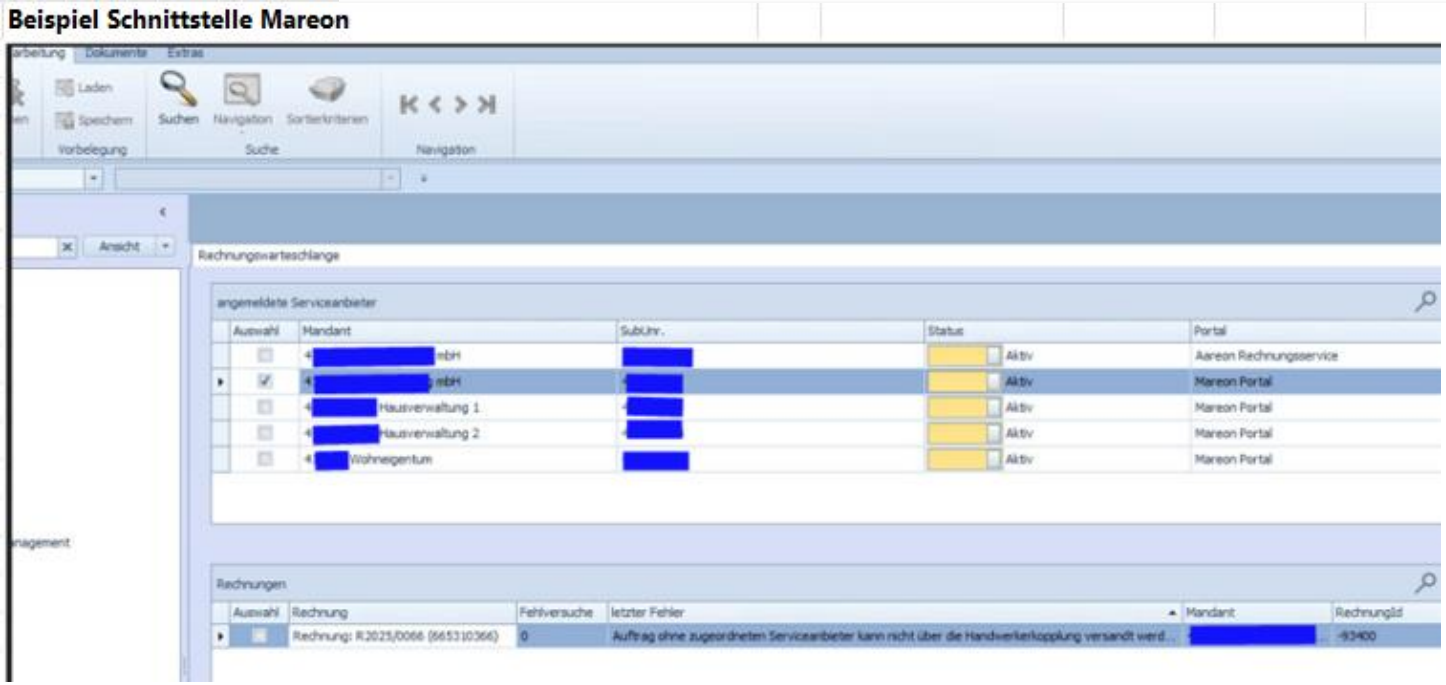
XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT08 – Überprüfung der Datenverarbeitung und Datenübernahme

Beispiel

Im Wodis erfolgt eine automatisierte Schnittstellenprüfung zum Handwerkerportal (Mareon) und zum Aareon Rechnungsservice (ARS)

Beispiel Schnittstelle Mareon



=> die Transfers zwischen Wodis und Mareon/ARS erfolgen automatisiert. Falls es zu Fehlern kommt erhält der Admin eine Mail und kann diese dann klären lassen. Dies erfolgt bspw. wenn im Mareon eine Rechnung erzeugt wurde und für diese kein Auftrag vorliegt. Für die Rechnungsart "MAR" muss zwingend ein Auftrag vorliegen, sonst kann diese in das Rechnungseingangsbuch nicht eingespielt werden.

=> automatische Kontrolle ist eingerichtet.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT08 – Überprüfung der Datenverarbeitung und Datenübernahme

Beispiel

Beispiel: Sollstellungsprotokoll Wodis Sigma

Verträge ohne Soll-Saldo (Soll < Haben)

=> Fehlerprotokoll aus Wodis zu Sollstellung => hier Verträge ohne Soll-Saldo => auf Grundlage dessen prüft Frau [redacted] die jeweiligen Verträge nochmal, warum keine Sollstellung erfolgt ist

Vertrag 13640/308/22/97; endg. Soll: 0,00; endg. Haben: 230,00; Beginn:01.06.2022; Ende: ; Kündigung:
Vertrag 1307/381/19/76; endg. Soll: 0,00; endg. Haben: 0,00; Beginn:15.11.2012; Ende: ; Kündigung: 30.06.2023
Vertrag 14438/395/19/84; endg. Soll: 0,00; endg. Haben: 0,00; Beginn:01.08.2023; Ende: ; Kündigung:
Vertrag 2069/402/73/14; endg. Soll: 0,00; endg. Haben: 0,00; Beginn:01.10.2008; Ende: ; Kündigung: 30.04.2022
Vertrag 4547/1281/29/15; endg. Soll: 579,51; endg. Haben: 1.176,00; Beginn:01.05.2008; Ende: ; Kündigung:

Listenende Uhrzeit: 11:01:53

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT09 – Notfallplan

Muster

Identifizierte Kontrolle
KIT09 - Einrichung eines IT-Notfallplans
Zugeordnete Risiken
RIT03 - Verarbeitung der Daten ist nicht richtig (laufender Betrieb, Updates)
Aufnahme des Prozesses/Aufbauprüfung
Befragung von Hrn. X (IT-Admin.) zum Vorhandensein eines Notfallplanes für die IT. Dieser ist im Intranet für jeden Mitarbeiter einsehbar. Es liegt ein IT-Notfallplan vor (optional: als Bestandteil des IT-Sicherheitskonzeptes). Dieser enthält sowohl organisatorische Maßnahmen (Ansprechpartner/Dienstleister mit Telefonnumer/Mail), als auch technische Festlegungen (bspw. zum Serverneustart, Aufbewahrung Notfalluser-Passwort etc.) (**Einsichtnahme**). Der Notfallplan wird bei Bedarf aktualisiert, bspw. bei neuer Hardware/Software oder Änderungen bei den Ansprechpartnern/Dienstleistern. Weiterhin liegt im Serverraum eine aktuelle Version in Papier aus. Bezüglich der Durchführbarkeit des Notfallplanes werden keine regelmäßigen Ernstfälle simuliert, jedoch werden auskunftsgemäß u.a. regelmäßig (ca. wöchentlich) Rücksicherungstests durchgeführt. Die Rücksicherungstests werden durch den Admin dokumentiert. Mit den externen Dienstleistern (Hardwarebetreuung Fa. xyz, vgl. Vertrag 540.x) und ERP-System Fa. Aareon (Vertrag vgl. 540.x) wurden Vereinbarungen zu Reaktionszeiten getroffen. Die Geschäftsführung geht davon aus, dass die Systeme im Notfall nach spätestens drei Werktagen wieder laufen, was der Ausfall von drei Tagen praktisch für Auswirkungen hat und, ob die Systeme dann im Worst Case wirklich wieder laufen, wurde bisher nicht näher untersucht. (Alternativ: Das Unternehmen hat kein eigenes, qualifiziertes IT-Personal. Ein schriftlich formulierter Notfallplan liegt nicht vor. Es gibt eine Liste mit den vertraglich gebundenen externen Dienstleistern, welche im Notfall unterstützen. Mit den Dienstleistern wurde entsprechende Vereinbarungen, auch zu Reaktionszeiten, getroffen. Vgl. 540.x.)

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT09 – Notfallplan

Muster

Ergebnis Aufbauprüfung und Einschätzung Kontrollrisiko
Das **Kontrollrisiko** kann als "mittel" eingeschätzt werden, da keine Notfalltests vorgenommen werden und es auch keine Definition einer maximal tolerierbaren Ausfallzeit durch die Unternehmensleitung gibt. Somit kann auch nicht beurteilt werden ob die vertraglichen Vereinbarungen hinreichend sind.
Funktionsprüfung/aussagebezogene Prüfungshandlungen: Prüfung der Umsetzung im System
Einsichtnahme in den Notfallplan und Bewertung, ob der Notfallplan für die Unternehmensgröße und Struktur ausreichend ist.
(optional: Einsichtnahme in Verträge mit den Dienstleistern hinsichtlich der Vereinbarung von Reaktionszeiten)
Ergebnis
Ein hinreichendes Notfallkonzept liegt vor, Verantwortlichkeiten und Maßnahmen sind festgelegt. Nach unserer Einschätzung ist davon auszugehen, dass im Notfall die Systeme innerhalb der vom Geschäftsführer definierten maximalen Ausfallzeit (3 Tage) wiederhergestellt werden können. (optional: Es wurde empfohlen, dass das Wideranlaufverfahren der Server beschrieben werden sollte. Dadurch kann sichergestellt werden, dass eine Wiederherstellung reibungslos, auch im Vertretungsfall, durchgeführt werden kann.) (optional: Eine maximal tolerierbare Ausfallzeit wurde durch die Unternehmensleitung nicht definiert, somit kann auch nicht beurteilt werden ob die vertraglichen Vereinbarungen mit den Dienstleistern im Notfall ausreichen.)
Prüfungsnachweise

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT09 – Notfallplan

Beispiel

Auszug Vertrag ERP-System - Reaktionszeiten Dienstleister -

4 Prioritäten und Reaktionszeiten

Die Problem- und Störungsbearbeitung erfolgt je nach Auswirkung des Problems während der Servicezeiten nach festgelegten Prioritäten. Folgende Prioritätsstufen und Reaktionszeiten sind definiert:

Priorität	Definition	Reaktionszeit Fehlermeldungen
0	Völliger Systemstillstand oder Störung zentraler Funktionen mit hohen wirtschaftlichen Konsequenzen.	30 Minuten
1	Fehlerhafte oder ausgefallene Funktionalität, die in der aktuellen Situation dringend benötigt wird; ernste Störung des gesamten produktiven Geschäftsablaufs.	2 Arbeitsstunden
2	Fehlerhafte oder ausgefallene Funktionalität; Beeinträchtigung des normalen Geschäftsablaufs.	10 Arbeitsstunden
3	Keine oder geringe Beeinträchtigung des normalen Geschäftsablaufs.	14 Arbeitstage

Die Festlegung der Priorität des jeweils aufgetretenen Problems wird von der Technischen Hotline vorgenommen und mit dem Kunden abgestimmt.

XI. Funktionsprüfungen der 9 allgemeinen IT-Kontrollen

KIT09 – Notfallplan

Beispiel

Auszug Notfallplan

5 Notfallplan und Wiederherstellung-Richtlinien

Bei Störungen mit Gefährdungspotential 1 "Notfall", die einen Ausfall von wichtigen Komponenten des IT-Systems zur Folge haben, leitet der EDV-Administrator bzw. sein Stellvertreter unverzüglich notwendige Maßnahmen ein.

5.1 Störung /Ausfall von Hardware
- Überprüfung aller Serversysteme vor Ort
- Eingrenzung des Fehlers
- Information an Geschäftsleitung
- Meldung an ViaLan, Abstimmung zur Fehlerbeseitigung
- Einleitung von Maßnahmen zur Wiederherstellung

5.2 Störungen durch Viren, Spareware und andere Bedrohungen
- Trennen des Internetzuganges
- Überprüfung der betroffenen Systeme

- bei Virenbefall entsprechende Systeme herunterfahren und isolieren
- Information an Geschäftsleitung
- Meldung an ViaLan, Abstimmung zur Fehlerbeseitigung
- Überprüfen des Datenbestandes auf unzulässige Veränderungen
- Beseitigung der Ursachen (Viren, Malware-Programme u. ä.)
- wenn notwendig, Einspielen von Datensicherungen

5.3 Störungsmeldungen
- im Brandfall:
  Die Stromversorgung ausschalten,
  wenn möglich Löschversuch mit Kohlendioxid-Löscher,
  ansonsten Alarmierung Feuerwehr,
  Information an Geschäftsleitung / EDV-Administrator

- bei Ausfall Klimagerät (Temperatur> 35°C):
  Tür Serverraum öffnen,
  Klimagerät überprüfen,
  bei defektem Gerät das Reserve-Klimagerät in Betrieb nehmen,
  Information an EDV-Administrator

5.4 Wichtige Telefonnummern bei Server-Havarien

XII. Vorgehen bei ausgelagerter rechnungslegungsbezogener IT-Systeme

XII. Vorgehen bei ausgelagerter rechnungs-legungsbezogener IT-Systeme

Für Überlegungen bei der Abschlussprüfung von Einheiten, die Dienstleister in Anspruch nehmen gilt nun der **ISA [DE] 402.**

Was ist ein Dienstleister (ISA [DE] 402.8)?

Ein Dritter (oder ein Segment davon), der für auslagernde Einheiten **Dienstleistungen** erbringt, die Teil der **rechnungslegungsbezogenen Informationssysteme** dieser Einheiten sind.

XII. Vorgehen bei ausgelagerter rechnungs-legungsbezogener IT-Systeme

Merksatz (ISA [DE] 402.3)

Von einem Dienstleister erbrachte Dienstleistungen sind für die Prüfung des Abschlusses einer auslagernden Einheit relevant, wenn diese Dienstleistungen sowie die zugehörigen Kontrollen Teil des rechnungslegungsbezogenen Informationssystems der auslagernden Einheit einschließlich der damit verbundenen Geschäftsprozesse sind.

Typische ausgelagerte Dienstleistung bei Wohnungsunternehmen:

Personalabrechnung und Nutzung eines **Rechenzentrums** zur Verarbeitung der rechnungslegungsrelevanten Daten oder auf die **Geschäftsbesorgung** durch einen Dritten

XII. Vorgehen bei ausgelagerter rechnungs-legungsbezogener IT-Systeme

Was ist das Ziel im Rahmen der Prüfung (ISA [DE] 402.7)?

Wenn die auslagernde Einheit die Dienstleistungen eines Dienstleisters in Anspruch nimmt, bestehen die **Ziele des Abschlussprüfers des Auslagernden** darin,

- ein **Verständnis** von Art und Bedeutsamkeit der von dem Dienstleister **erbrachten Dienstleistungen** und von deren Auswirkungen auf die für die Abschlussprüfung **relevanten internen Kontrollen** der auslagernden Einheit zu erlangen, das ausreicht, um die **Risiken wesentlicher falscher Darstellungen zu identifizieren und zu beurteilen**, und
- **Prüfungshandlungen** zu planen und durchzuführen, um diesen Risiken zu begegnen.

Zu beachten (ISA [DE] 402.4):
Skalierung: Art und Umfang der vom Abschlussprüfer des Auslagernden durchzuführenden Tätigkeiten im Zusammenhang mit den Dienstleistungen eines Dienstleisters hängen von **Art und Bedeutsamkeit dieser Dienstleistungen** für die auslagernde Einheit und von ihrer Relevanz für die Abschlussprüfung ab.

XII. Vorgehen bei ausgelagerter rechnungslegungsbezogener IT-Systeme

Was ist zu erfragen, um ein Verständnis von der Auslagerung zu erlangen?

- Art der vom Dienstleister erbrachten Dienstleistungen und deren Bedeutung für die auslagernde Einheit, einschließlich der Auswirkungen auf das IKS der auslagernden Einheit (Welche DL?)
- Art und Wesentlichkeit der vom Dienstleister verarbeiteten Geschäftsvorfälle, betroffene Konten, Rechnungslegungsprozesse (Was ist betroffen?)
- Grad der Wechselwirkung zwischen den Tätigkeiten des Dienstleisters und denjenigen der auslagernden Einheit (Wirksame Kontrollen beim Auslagernden vorhanden?)
- Art der Beziehung zwischen auslagernder Einheit und Dienstleister einschließlich relevanter vertraglicher Beziehungen (Vertrag? Vereinbarung? Rechte des Auslagernden? Bericht nach IDW PS 951 n.F. (03.2021) vorhanden?)

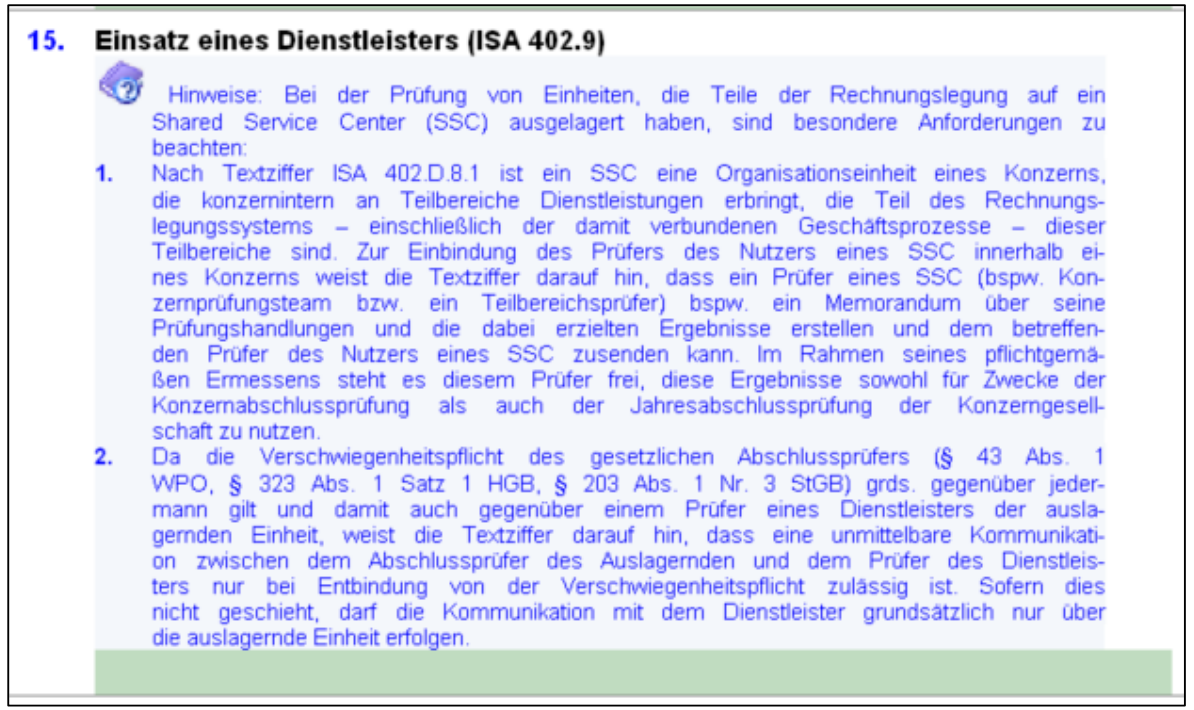
Aufgrund dieser Informationen sind ggf. Risiken wesentlicher falscher Darstellungen zu identifizieren und dann auch zu beurteilen.

XII. Vorgehen bei ausgelagerter rechnungs-legungsbezogener IT-Systeme

Das Verständnis, die Risikobeurteilung und ggf. weitere geplante Prüfungshandlungen ist hier zu dokumentieren:

MEMO.PA3 Frage 15

Hier ist jede Art der Auslagerung aufzunehmen.



15. Einsatz eines Dienstleisters (ISA 402.9)

Hinweise: Bei der Prüfung von Einheiten, die Teile der Rechnungslegung auf ein Shared Service Center (SSC) ausgelagert haben, sind besondere Anforderungen zu beachten:

1. Nach Textziffer ISA 402.D.8.1 ist ein SSC eine Organisationseinheit eines Konzerns, die konzernintern an Teilbereiche Dienstleistungen erbringt, die Teil des Rechnungslegungssystems – einschließlich der damit verbundenen Geschäftsprozesse – dieser Teilbereiche sind. Zur Einbindung des Prüfers des Nutzers eines SSC innerhalb eines Konzerns weist die Textziffer darauf hin, dass ein Prüfer eines SSC (bspw. Konzernprüfungsteam bzw. ein Teilbereichsprüfer) bspw. ein Memorandum über seine Prüfungshandlungen und die dabei erzielten Ergebnisse erstellen und dem betreffenden Prüfer des Nutzers eines SSC zusenden kann. Im Rahmen seines pflichtgemäßen Ermessens steht es diesem Prüfer frei, diese Ergebnisse sowohl für Zwecke der Konzernabschlussprüfung als auch der Jahresabschlussprüfung der Konzerngesellschaft zu nutzen.
2. Da die Verschwiegenheitspflicht des gesetzlichen Abschlussprüfers (§ 43 Abs. 1 WPO, § 323 Abs. 1 Satz 1 HGB, § 203 Abs. 1 Nr. 3 StGB) grds. gegenüber jedermann gilt und damit auch gegenüber einem Prüfer eines Dienstleisters der auslagernden Einheit, weist die Textziffer darauf hin, dass eine unmittelbare Kommunikation zwischen dem Abschlussprüfer des Auslagernden und dem Prüfer des Dienstleisters nur bei Entbindung von der Verschwiegenheitspflicht zulässig ist. Sofern dies nicht geschieht, darf die Kommunikation mit dem Dienstleister grundsätzlich nur über die auslagernde Einheit erfolgen.

Soweit ein Risiko wesentlicher falscher Darstellung aus einer Art der Auslagerung identifiziert wird und sich im mittleren bzw. oberen Rand des Spektrums der inhärenten Risiken bewegt, ist es im Risiko-dialog zu erfassen und entsprechende Prüfungshandlungen durchzuführen.

Soweit keine Auslagerungen vorliegen ist "n/a" einzutragen.

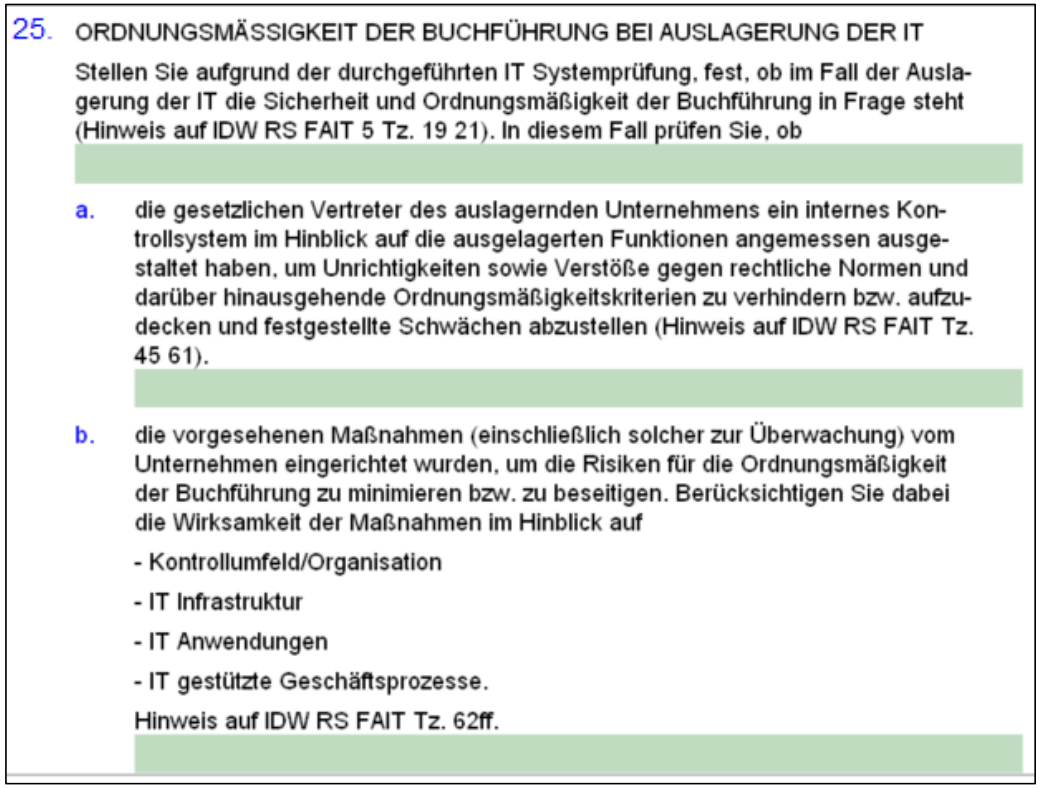
XII. Vorgehen bei ausgelagerter rechnungs-legungsbezogener IT-Systeme

Sind Teile der IT oder diese vollständig ausgelagert, sind weitere Schritte notwendig.
Z.B. Nutzung eines Rechenzentrums oder Cloud-Anwendungen

531.ORD.MIN Frage 25

Vorgehen:
- Erlangung ausreichender Informationen von der auslagernden Einheit und Prüfung bei dieser möglich und ausreichend
- ansonsten Einholung eines Berichts nach IDW PS 951 n.F. (03.2021) (Typ 1 oder 2)

Hinweis: ein Bericht nach Typ 2 ist besser, da er auch Funktionsprüfungen umfasst
Oder Zertifizierungen nach ISAE 3402 Typ 1 bzw. Typ 2 oder ISO 27001



25. ORDNUNGSMÄSSIGKEIT DER BUCHFÜHRUNG BEI AUSLAGERUNG DER IT

Stellen Sie aufgrund der durchgeführten IT Systemprüfung, fest, ob im Fall der Auslagerung der IT die Sicherheit und Ordnungsmäßigkeit der Buchführung in Frage steht (Hinweis auf IDW RS FAIT 5 Tz. 19 21). In diesem Fall prüfen Sie, ob

a. die gesetzlichen Vertreter des auslagernden Unternehmens ein internes Kontrollsystem im Hinblick auf die ausgelagerten Funktionen angemessen ausgestaltet haben, um Unrichtigkeiten sowie Verstöße gegen rechtliche Normen und darüber hinausgehende Ordnungsmäßigkeitskriterien zu verhindern bzw. aufzudecken und festgestellte Schwächen abzustellen (Hinweis auf IDW RS FAIT Tz. 45 61).

b. die vorgesehenen Maßnahmen (einschließlich solcher zur Überwachung) vom Unternehmen eingerichtet wurden, um die Risiken für die Ordnungsmäßigkeit der Buchführung zu minimieren bzw. zu beseitigen. Berücksichtigen Sie dabei die Wirksamkeit der Maßnahmen im Hinblick auf

- Kontrollumfeld/Organisation
- IT Infrastruktur
- IT Anwendungen
- IT gestützte Geschäftsprozesse.

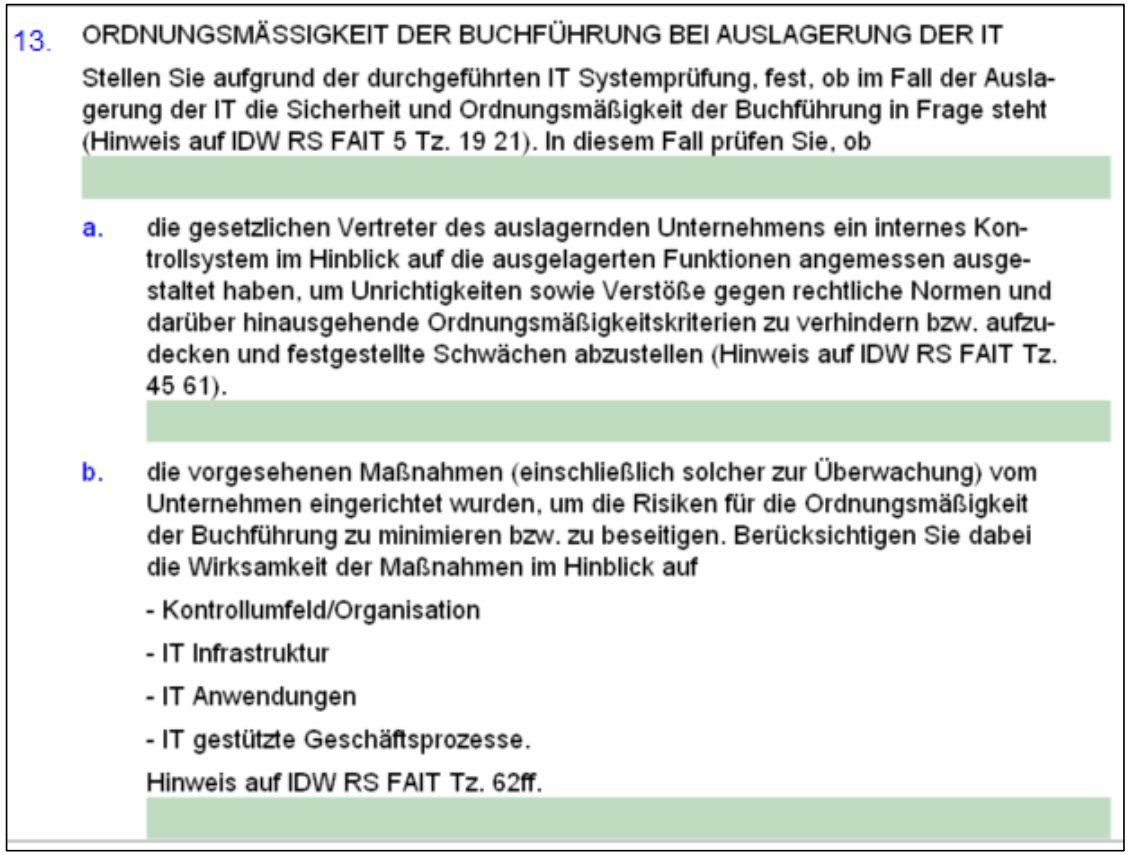
Hinweis auf IDW RS FAIT Tz. 62ff.

XII. Vorgehen bei ausgelagerter rechnungs-legungsbezogener IT-Systeme

Die gleiche Fragestellung ist bei komplexen IT-Systemen in folgendem Dokument enthalten:

ORD.PP Frage 13

Auch hier ist zu prüfen, ob durch die Auslagerung der IT ein Risiko wesentlicher falscher Darstellung vorliegt.



13. ORDNUNGSMÄSSIGKEIT DER BUCHFÜHRUNG BEI AUSLAGERUNG DER IT

Stellen Sie aufgrund der durchgeführten IT Systemprüfung, fest, ob im Fall der Auslagerung der IT die Sicherheit und Ordnungsmäßigkeit der Buchführung in Frage steht (Hinweis auf IDW RS FAIT 5 Tz. 19 21). In diesem Fall prüfen Sie, ob

a. die gesetzlichen Vertreter des auslagernden Unternehmens ein internes Kontrollsystem im Hinblick auf die ausgelagerten Funktionen angemessen ausgestaltet haben, um Unrichtigkeiten sowie Verstöße gegen rechtliche Normen und darüber hinausgehende Ordnungsmäßigkeitskriterien zu verhindern bzw. aufzudecken und festgestellte Schwächen abzustellen (Hinweis auf IDW RS FAIT Tz. 45 61).

b. die vorgesehenen Maßnahmen (einschließlich solcher zur Überwachung) vom Unternehmen eingerichtet wurden, um die Risiken für die Ordnungsmäßigkeit der Buchführung zu minimieren bzw. zu beseitigen. Berücksichtigen Sie dabei die Wirksamkeit der Maßnahmen im Hinblick auf

- Kontrollumfeld/Organisation
- IT Infrastruktur
- IT Anwendungen
- IT gestützte Geschäftsprozesse.

Hinweis auf IDW RS FAIT Tz. 62ff.

XII. Vorgehen bei ausgelagerter rechnungslegungsbezogener IT-Systeme

Soweit Risiken falscher Darstellungen identifiziert worden sind, sind die entsprechenden Reaktionen zu planen und durchzuführen (ISA [DE] 402.15):

- festzustellen, ob **ausreichende geeignete Prüfungsnachweise** zu den relevanten Aussagen im Abschluss aus **bei der auslagernden Einheit** vorhandenen Aufzeichnungen **verfügbar** sind und – wenn dies nicht der Fall
- **weitere Prüfungshandlungen** durchzuführen, um ausreichende geeignete Prüfungsnachweise zu erlangen, oder einen anderen Prüfer hinzuzuziehen, der diese Prüfungshandlungen für den Abschlussprüfer des Auslagernden bei dem Dienstleister durchführt. (Vgl. Tz. A24-A28)
- Durchführung von Funktionsprüfungen und/oder aussagebezogenen Prüfungshandlungen

XII. Vorgehen bei ausgelagerter rechnungslegungsbezogener IT-Systeme

Bei der Durchführung von Funktionsprüfungen – soweit eine Stützung auf Kontrollen bei dem Dienstleister erfolgt – ist folgendes zu beachten (ISA [DE] 402.16):

- Erlangung eines Berichts vom Typ 2, sofern verfügbar (beste Lösung!) oder ISO-Zertifizierungen
- Durchführung von geeigneten Funktionsprüfungen bei dem Dienstleister (Voraussetzung dazu ist die Einwilligung des Dienstleisters) oder
- Hinzuziehen eines anderen Prüfers, der für den Abschlussprüfer des Auslagernden Funktionsprüfungen bei dem Dienstleister durchführt.

XII. Vorgehen bei ausgelagerter rechnungs-legungsbezogener IT-Systeme

Ergebnis der durchgeführten Prüfungshandlungen (Reaktionen) (ISA [DE] 402.20):

1) Die erlangten Prüfungsnachweise sind ausreichend, um ein Prüfungsurteil zu fällen.
   => keine Auswirkungen auf den Bestätigungsvermerk/ZPE
2) Der Prüfer ist nicht in der Lage, ausreichende geeignete Prüfungsnachweise zu den von dem Dienstleister erbrachten Dienstleistungen zu erlangen, die für die Prüfung des Abschlusses der auslagernden Einheit relevant sind (ISA [DE] 402.20)
   => dann Modifizierung des Bestätigungsvermerks/ZPE

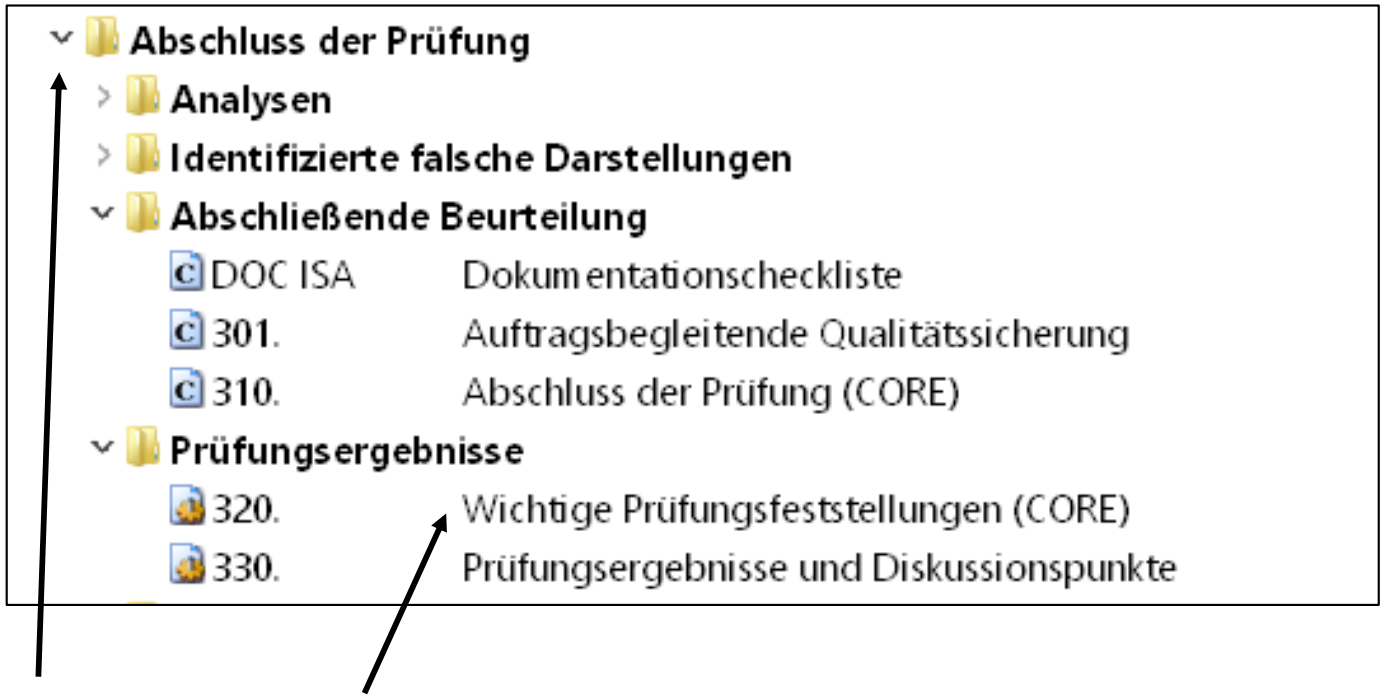
XIII. Wichtige Prüfungsfeststellungen (320)

XIII. Wichtige Prüfungsfeststellungen (320)

Wozu braucht man das Dokument?

- Alle wichtigen Prüfungsfeststellungen für den Prüfungsleiter oder verantwortlichen Wirtschaftsprüfer auf einen Blick
- Erfassung sämtlicher wichtiger Prüfungsfeststellungen
  - Feststellungen in Bezug auf Prüffelder oder Prozesse
  - IT-Feststellungen
  - Feststellungen zur Ordnungsmäßigkeit der Geschäftsführung
  - Alle weiteren Feststellungen
- Enthält die Verknüpfung zum zugrundeliegenden Dokument

XIII. Wichtige Prüfungsfeststellungen (320)



Zu finden unter Abschluss der Prüfung

XIII. Wichtige Prüfungsfeststellungen (320)

Erstellen einer wichtigen Prüfungsfeststellung

Thema	Erledigt von	Typ	Dokument	Priorität	Status	Erstellt am	Fällig am	Erle
CB-1 - Kompetenzen klären		Wichtige Prüfungsfeststellungen	ORD. PP	Normal	Nicht gestartet	04.12.2023	18.12.2023	☐

Fertiggestellt mit unten aufgeführten FeststellungenUngenügende Umsetzung von Vertretungsregeln. Unklare Aufgabenabgrenzungen zwischen den Abteilungen.CB, Montag, 4. Dezember 2023

Regelung der Kompetenzen vornehmen, klare Abgrenzungen einführen, Empfehlung: Erstellung von Stellenbeschreibungen und Organigramm überarbeiten, mit Berechtigungen abgleichen

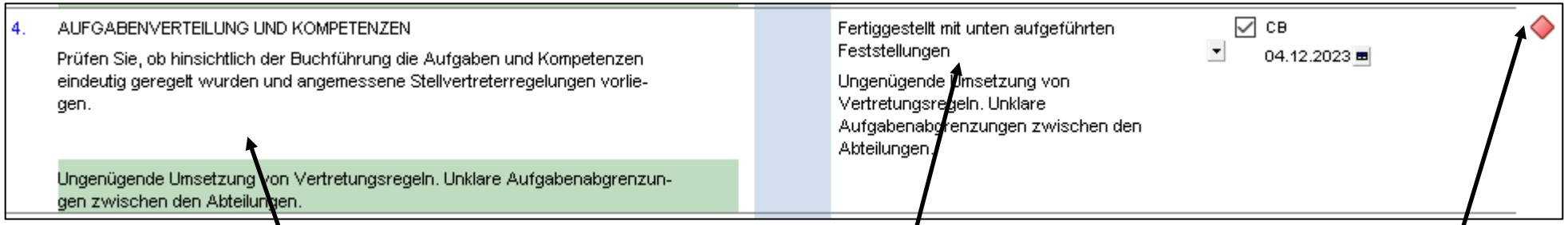
Auflistung der Prüfungsfeststellungen

Zu Grunde liegendes Dokument

Falls erledigt, hier markieren danach kann auch sortiert werden

XIII. Wichtige Prüfungsfeststellungen (320)

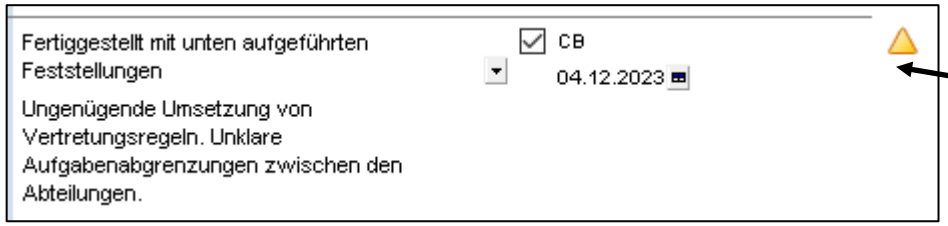
Erstellen einer wichtigen Prüfungsfeststellung



Prüfungshandlung

Prüfungsfeststellung

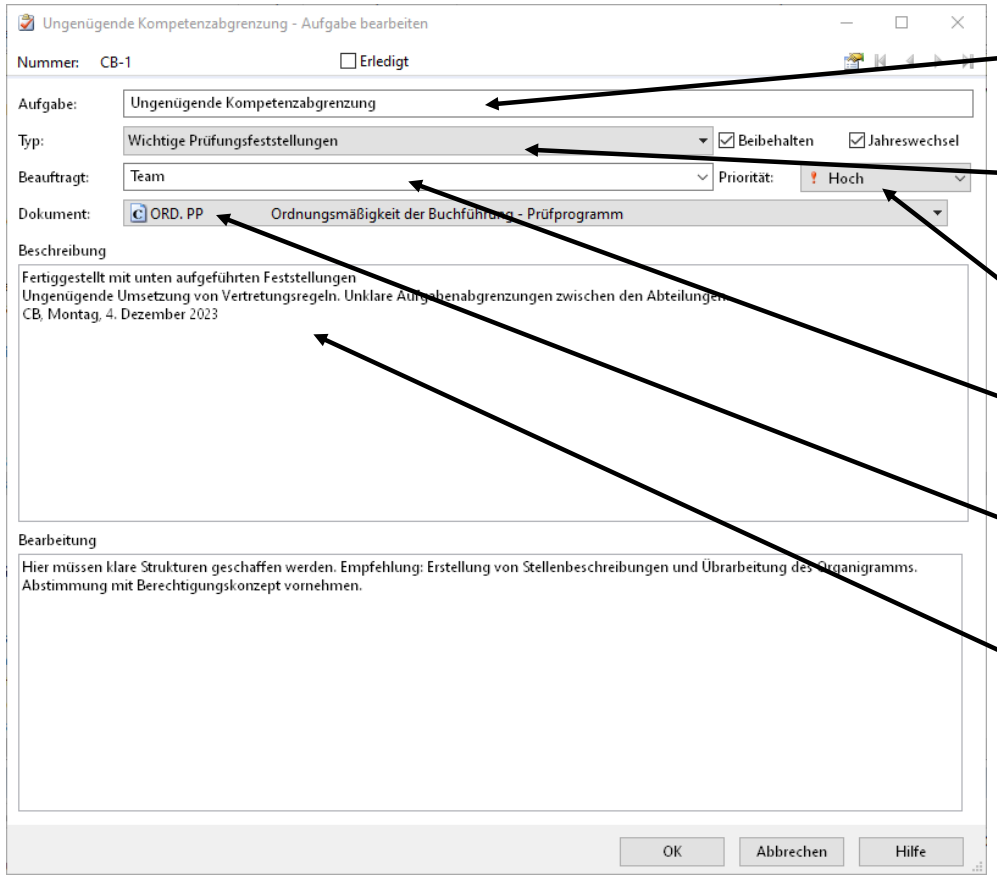
Aufgabe ist noch Nicht angelegt.



Aufgabe ist angelegt.

XIII. Wichtige Prüfungsfeststellungen (320)

Erstellen einer wichtigen Prüfungsfeststellung



Kurzbeschreibung der Prüfungsfeststellung

Typ: Wichtige Prüfungsfeststellung!!

Festlegung der Priorität

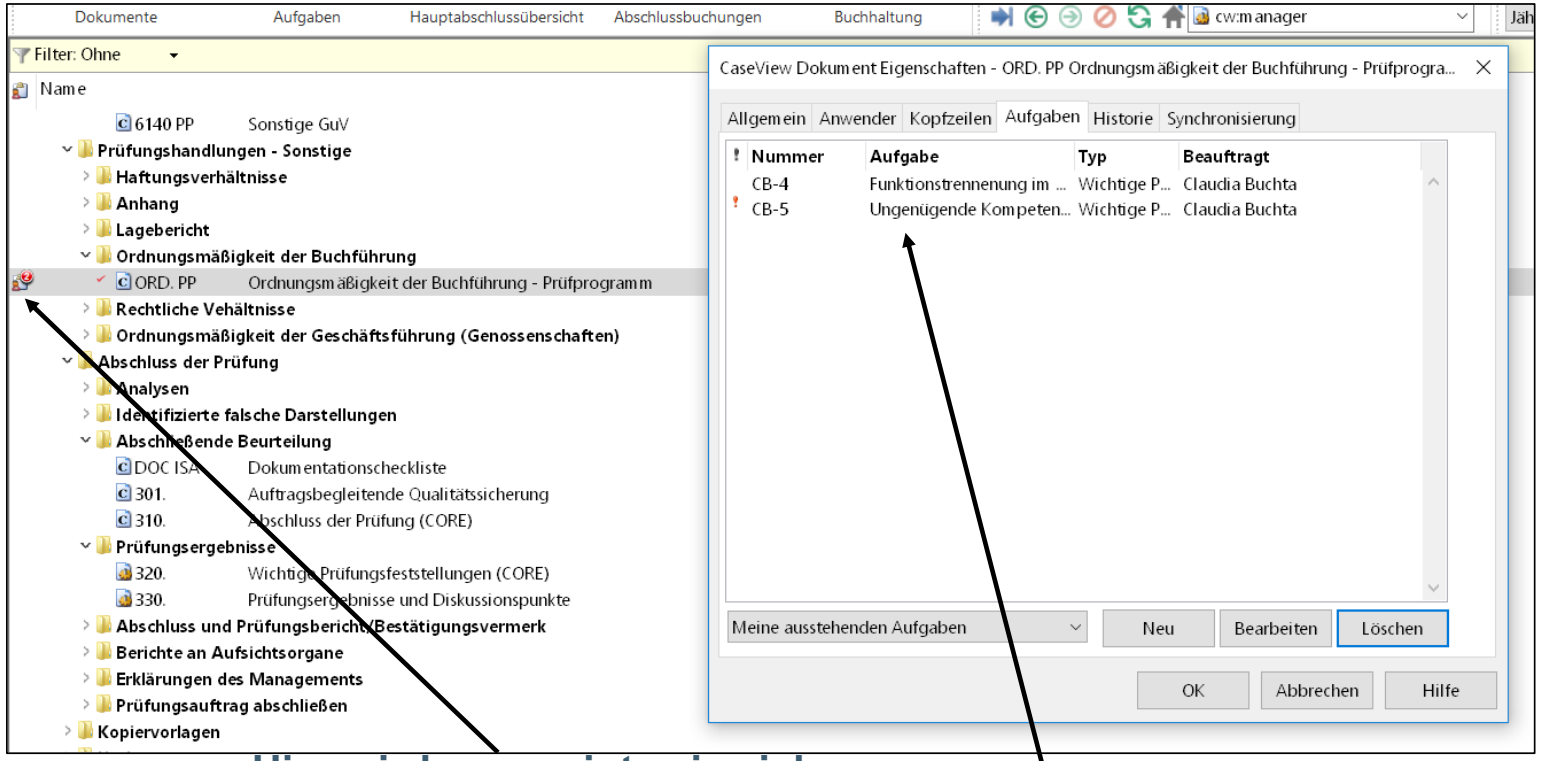
Adressat der Prüfungsfeststellung

Bezugsdokument

Genauere Beschreibung der Feststellung

XIII. Wichtige Prüfungsfeststellungen (320)

Erstellen einer wichtigen Prüfungsfeststellung



Hier wird angezeigt, wie viele Aufgaben angelegt sind

Mit Doppelklick werden die Aufgaben angezeigt

XIII. Wichtige Prüfungsfeststellungen (320)

Erstellen einer wichtigen Prüfungsfeststellung

Beispiele für bedeutsame Sachverhalte:

- Vom Management geschätzte Werte in der Rechnungslegung.
- Punkte zu Angaben und Darstellung im Abschluss.
- Anwendung von bedeutsamen Bilanzierungs- und Bewertungsmethoden.
- Beurteilungen des Managements in Bezug auf Vermögenswertänderungen.
- Festgestellte falsche Darstellungen im Abschluss.
- Zweifel an der Fähigkeit der Einheit, die Unternehmenstätigkeit fortzuführen.

Die für dieses Dokument relevanten ISAs lauten: ISA 200, ISA 230, ISA 240, ISA 260, ISA 450, ISA 540, ISA 550 und ISA 570.

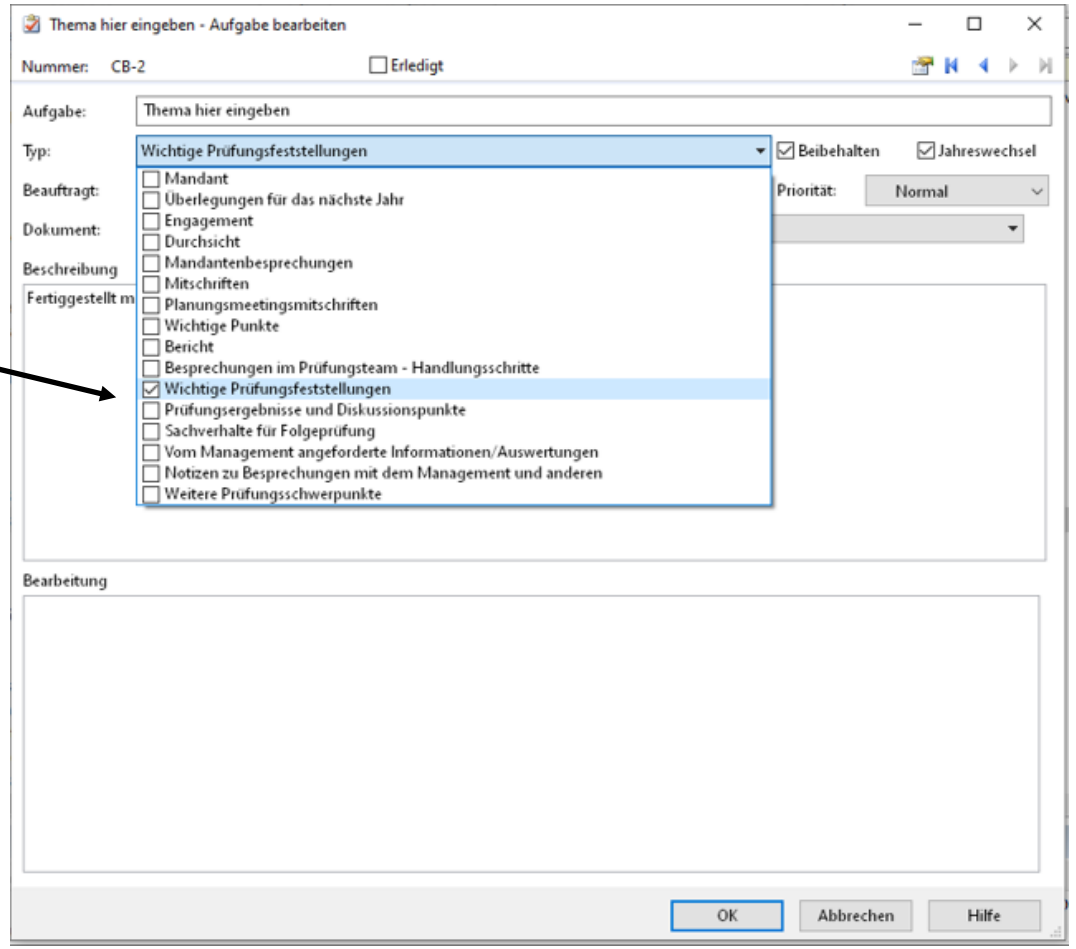
Stellen Sie sicher, dass Folgendes dokumentiert wird:
1) Die Beschreibung des wichtigen Punkts.
2) Die vorgeschlagene Lösung.
3) Die gezogenen Schlussfolgerungen.
4) Ob der Punkt den für die Überwachung Verantwortlichen gemeldet werden soll.

XIII. Wichtige Prüfungsfeststellungen (320)

Erstellen einer wichtigen Prüfungsfeststellung

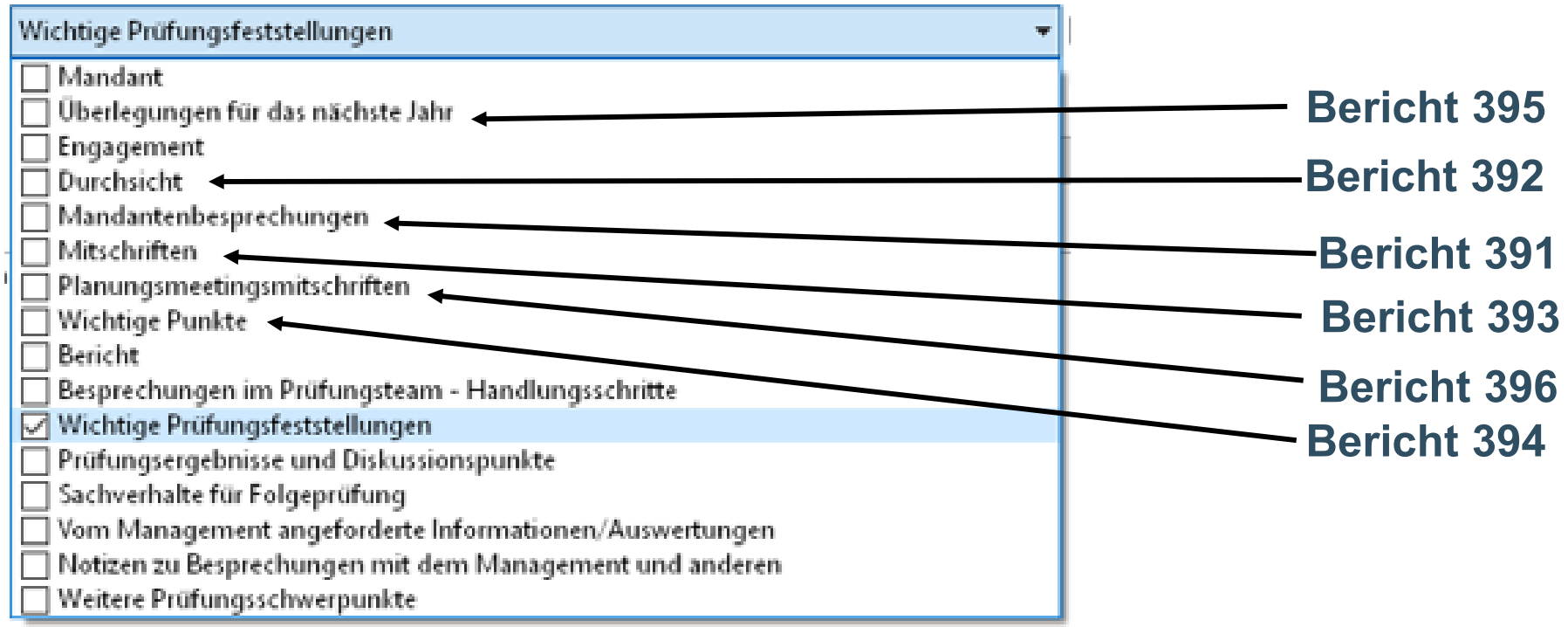
Wichtig ist die Festlegung des Berichtstypen!

Er steuert in welchen Bericht die Aufgabe dargestellt wird.
Es ist möglich mehrere Berichtsarten auszuwählen!



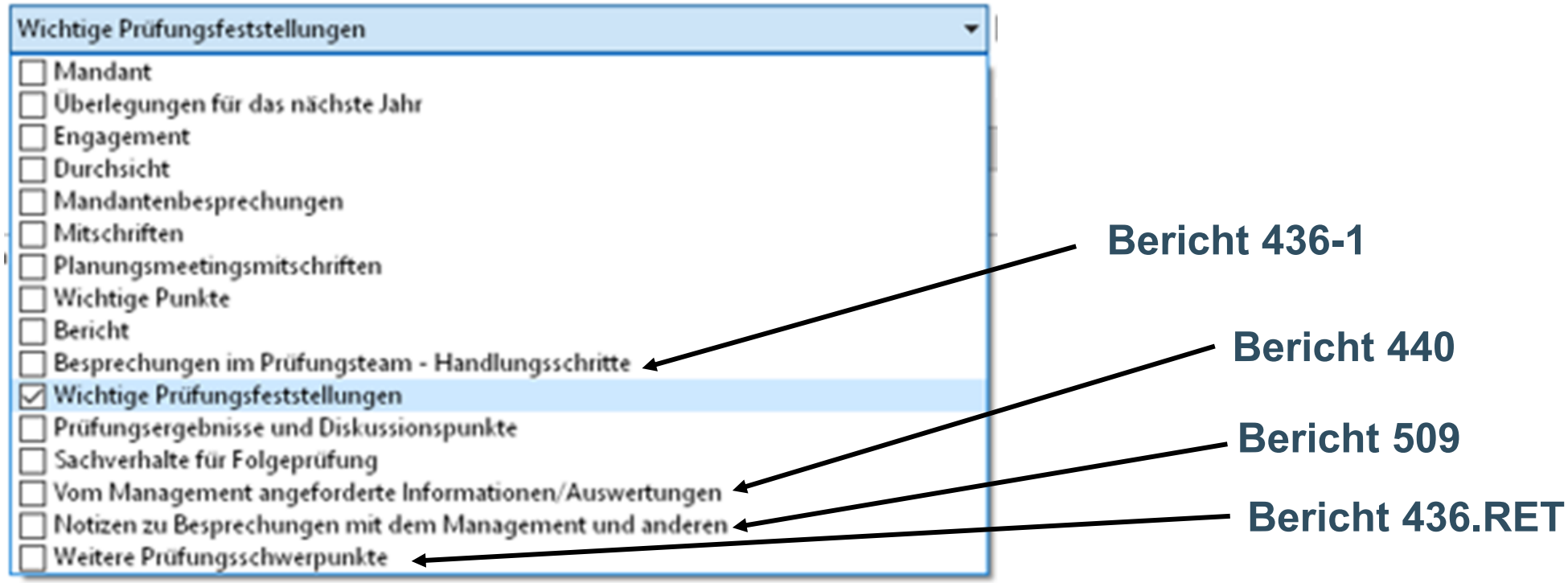
XIII. Wichtige Prüfungsfeststellungen (320)

Erstellen einer wichtigen Prüfungsfeststellung



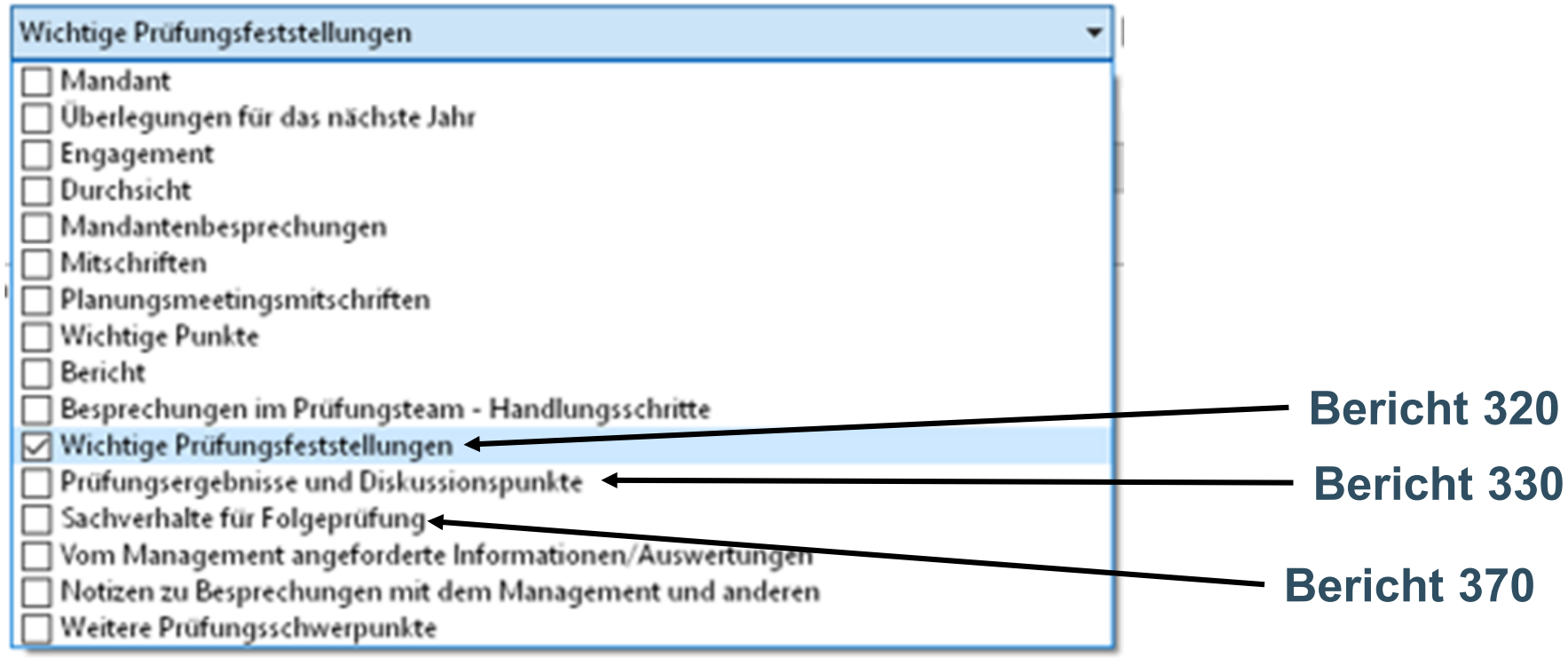
XIII. Wichtige Prüfungsfeststellungen (320)

Erstellen einer wichtigen Prüfungsfeststellung



XIII. Wichtige Prüfungsfeststellungen (320)

Erstellen einer wichtigen Prüfungsfeststellung



XIV. Arbeitspapiere und Berichterstattung

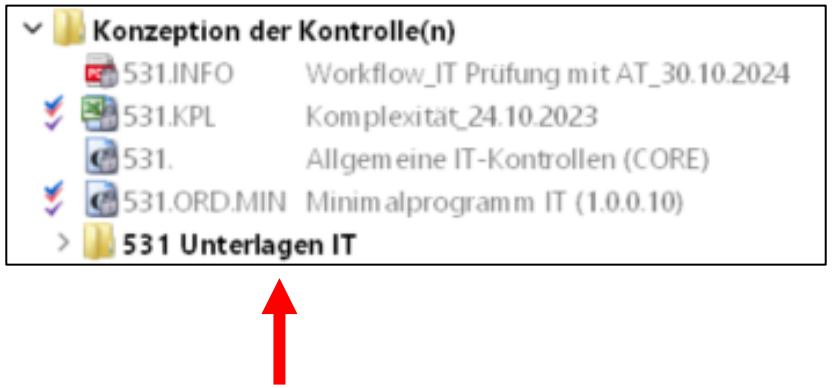
XIV. Arbeitspapiere und Berichterstattung

- Die Dokumente 531., ORD.PP und 531.ORD.MIN sind nachvollziehbar zu bearbeiten und ggf. mit Verknüpfungen zu den entsprechenden Dokumenten zu versehen.
- Ein alleiniges "Fertiggestellt ohne Beanstandungen" reicht nicht aus!!!!
- Die Prüfungshandlungen zu Aufbau- und Funktionsprüfungen sind angemessen zu dokumentieren.

  Dies betrifft auch die Walk-Throughs!
- Es gelten die allgemeinen Grundsätze für die Anlage von Arbeitspapieren (Beschriftung, Referenzierung etc.).
- Art und Umfang ist abhängig von der Komplexität des IT-Systems.
- Die Ablage der Arbeitspapiere wird empfohlen durch Einbinden in Audicon vorzunehmen.

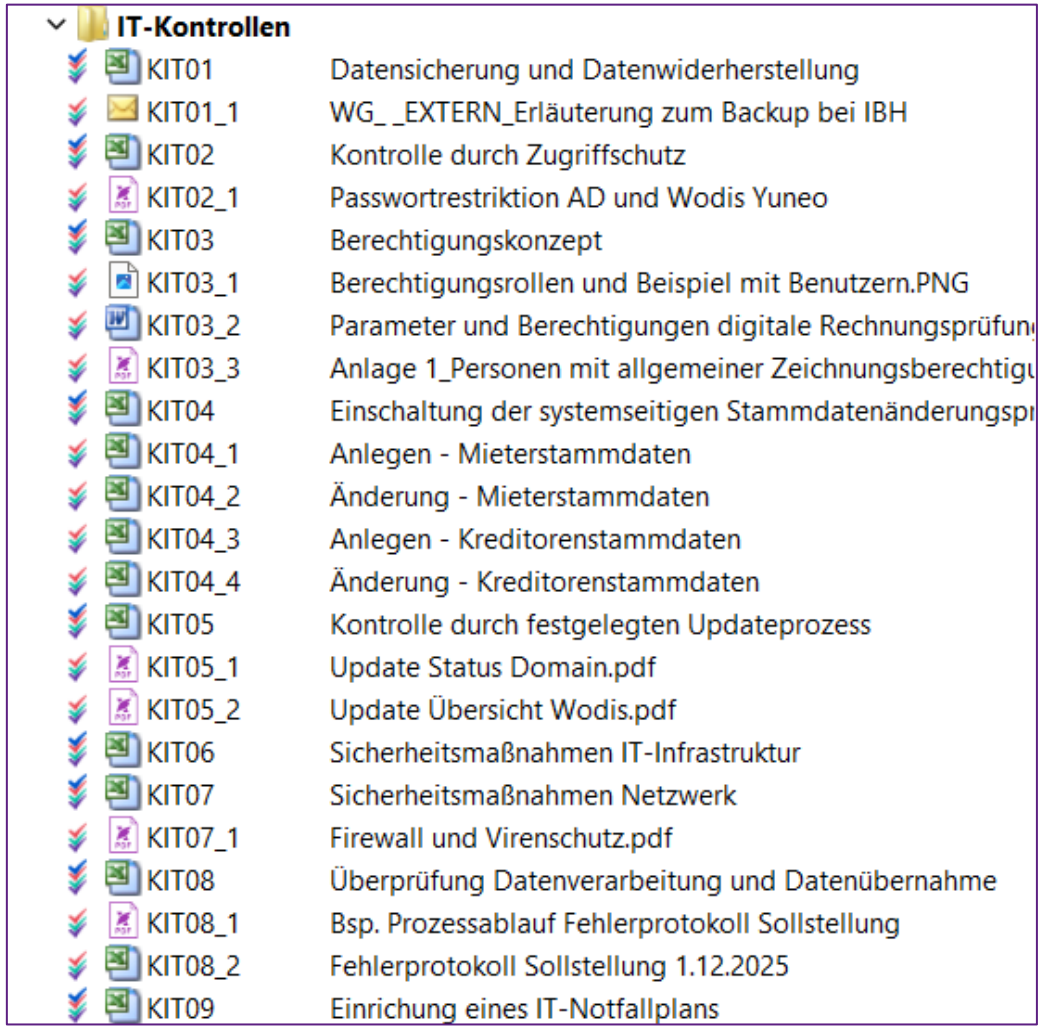
  Dauerhafte Unterlagen können in einer elektronischen Dauerakte geführt werden (z.B. Verträge).

XIV. Arbeitspapiere und Berichterstattung

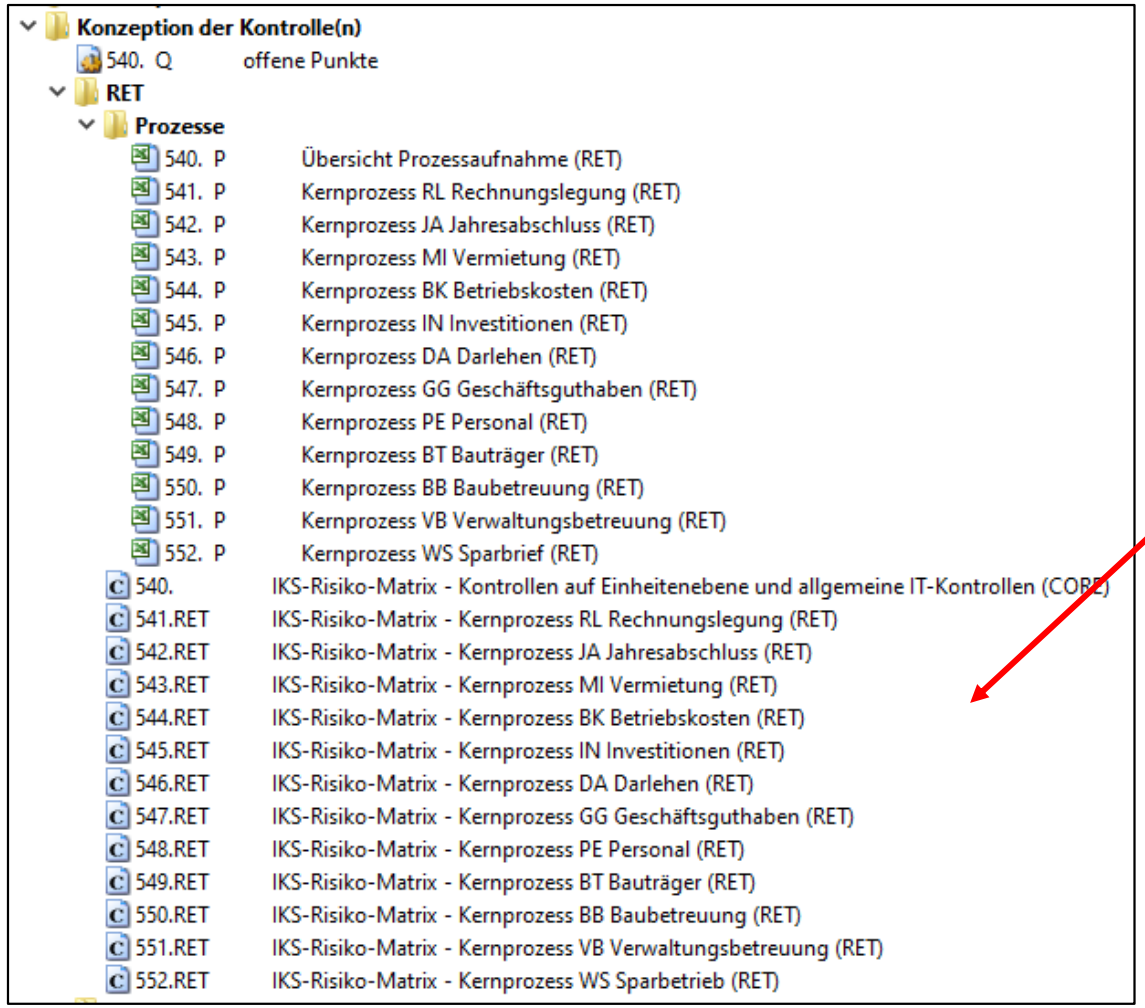


Unterlagen zu den Aufbauprüfungen hier ablegen

Unterlagen zu den Funktionsprüfungen hier ablegen und eindeutig beschriften



XIV. Arbeitspapiere und Berichterstattung



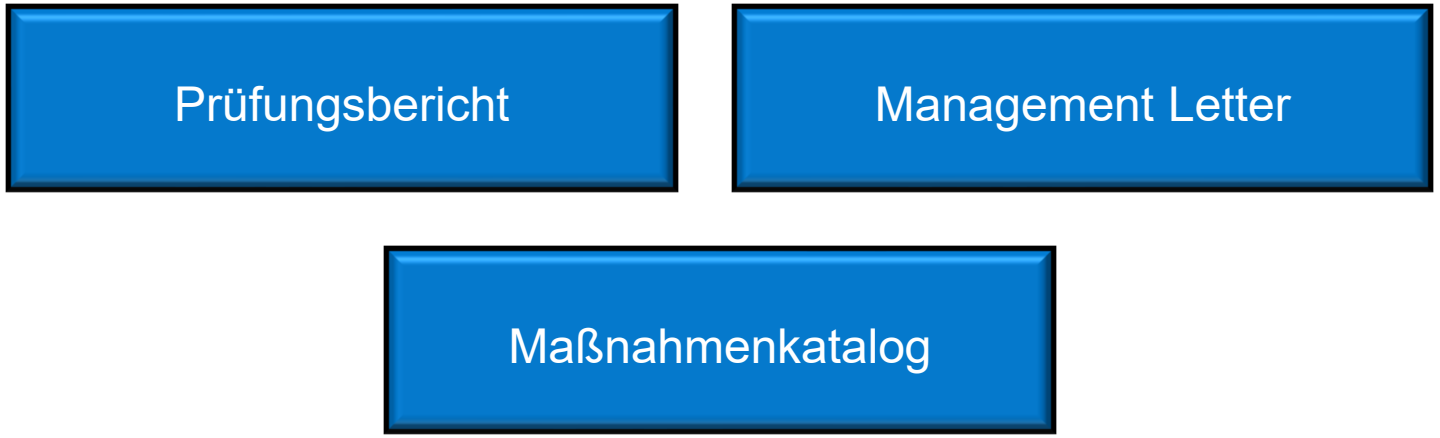
Für die Prüfung der IT-gestützten Kontrollen bzw. Report-Kontrollen

Unterlagen wie
- Walk Through oder
- Funktionsprüfungen

Könnten auch hier abgelegt werden.

In Bezug zu den einzelnen Prozessen.

XIV. Arbeitspapiere und Berichterstattung



XIV. Arbeitspapiere und Berichterstattung

Buchführung und weitere geprüfte Unterlagen

"Auf bestehende bedeutsame Mängel in der Buchführung und den weiteren geprüften Unterlagen und auf ihre Auswirkungen auf die Rechnungslegung sowie ihren Einfluss auf das Prüfungsergebnis ist hinzuweisen (vgl. Tz. 61 f.). Falls der Abschlussprüfer bedeutsame Mängel hinsichtlich der Sicherheit der für die Zwecke der Rechnungslegung verarbeiteten Daten festgestellt hat, sind diese im Prüfungsbericht darzustellen."
(IDW PS 450 n.F. (10.2021) Tz 65)

XIV. Arbeitspapiere und Berichterstattung

Bestätigungsvermerk

Wenn die festgestellten Schwächen des IT-Systems zu **bedeutsamen Mängeln** in der Rechnungslegung führen, ist eine Modifizierung des Bestätigungsvermerks zu prüfen.

Es gelten die allgemeinen Anforderungen.

XIV. Arbeitspapiere und Berichterstattung

Fragen

1. Frage:

"Im Rahmen unserer Prüfung haben wir keine Sachverhalte festgestellt, dass die Sicherheit der IT-Systeme und die Sicherheit der rechnungslegungsrelevanten Daten nicht gegeben ist."

Muss ein solcher Satz in den Prüfungsbericht aufgenommen werden?

2. Frage:

Muss im Abschnitt "Buchführung und weitere geprüfte Unterlagen" eine ausführliche Beschreibung des IT-Systems erfolgen?

3. Frage:

Gibt es Ausnahmen, bei denen eine ausführlichere Darstellung der IT notwendig ist?

XIV. Arbeitspapiere und Berichterstattung

Zusammengefasstes Prüfungsergebnis

Hier sollten die gleichen Kriterien angesetzt werden, wie bei der Berichterstattung im Bestätigungsvermerk:

Soweit festgestellte Schwächen des IT-Systems zu bedeutsamen Mängeln in der Rechnungslegung führen, sollte im zusammengefassten Prüfungsergebnis im Abschnitt "Feststellung der wirtschaftlichen Verhältnisse unter Einbeziehung von Buchführung, Jahresabschluss und Lagebericht der Genossenschaft " eine Berichterstattung erfolgen.

XIV. Arbeitspapiere und Berichterstattung

Aufgaben des Management Letters

- Berichterstattung über festgestellte Verbesserungspotentiale aus der Prüfung aus den Risiken und Kotrollen aus dem Einsatz der IT
- Adressaten: gesetzliche Vertreter

Über anlässlich der IT-Systemprüfung festgestellte **Verbesserungspotenziale** des geprüften IT-Systems empfiehlt es sich, den Auftraggeber und/oder die gesetzlichen Vertreter – unbeschadet der Darstellung im Prüfungsbericht – in geeigneter Form (z. B. Management Letter) zu informieren.

XIV. Arbeitspapiere und Berichterstattung

Beispielhafter Aufbau eines Management Letters

- Aussagekräftige Überschrift
- Ziel der Prüfung
- Vorgehensweise
- Beschreibung der Feststellung
- Darstellung des darin liegenden Risikos
- Empfehlung

Ggf. Erweiterung des Management Letter (ML) um einen **Maßnahmenkatalog**

XIV. Arbeitspapiere und Berichterstattung

Beispielhafter Aufbau eines Management Letters

Auszug aus einem Management-Letter

Oder kurz:

Feststellung
Risiko
Empfehlung

2 IT-Umfeld und IT-Organisation

2.1 IT-Umfeld und IT-Organisation

2.1.1 Ziel

Ziel der Prüfung des IT-Umfeldes war es, die Angemessenheit der IT-Strategie sowie des Sicherheitskonzeptes und der daraus abgeleiteten Maßnahmen zu beurteilen.

Ziel der Prüfung der IT-Organisation war es, festzustellen, inwieweit die vorhandene Aufbau- und Ablauforganisation einschließlich der Zusammenarbeit mit den Fachbereichen den geregelten IT-Betrieb sicherstellen kann.

2.1.2 Vorgehensweise

Sichtung relevanter Dokumentation, Interviews, persönliche Beobachtung.

2.1.3 Feststellungen

Im Unternehmen wurde durch den Vorstand keine Sicherheitsrichtlinie aufgestellt. Zum Zeitpunkt der Prüfung wurden Angebote für die Erstellung eines Sicherheitskonzeptes erstellt.

Der EDV-Administrator hat im Geschäftsjahr 2013 gleichzeitig auch die Funktion des Datenschutzbeauftragten wahrgenommen.

2.1.4 Darstellung der Risiken

Durch ein fehlendes Sicherheitsbewusstsein seitens des Vorstandes könnten notwendige Maßnahmen zur Absicherung des IT-Systems unterbleiben.

Durch die fehlende Funktionstrennung zwischen EDV-Administration und Datenschutz kann der Datenschutzbeauftragte seine Aufgaben nicht richtig wahrnehmen

2.1.5 Empfehlungen

Wir empfehlen die Aufstellung einer Sicherheitsrichtlinie durch den Vorstand. Die Sicherheitsrichtlinie sollte die Basis für das zu erstellende Sicherheitskonzept bilden. Die IT sollte in einem Risikomanagementhandbuch mit der entsprechenden Risikobewertung aufgenommen werden. Der Administrator darf nicht gleichzeitig Datenschutzbeauftragter sein, deshalb empfehlen wir die Bestellung eines betrieblichen Datenschutzbeauftragten.

XIV. Arbeitspapiere und Berichterstattung

Beispielhafter Aufbau eines Management Letters

Empfohlene Maßnahmen
IT-Systemprüfung

Risikobereich	Maßnahme Nr.	Feststellungen	Risiko-bewertung	Vorgeschlagene Maßnahme	Priorisierung 1= Umsetzung dringend empfohlen 2= Umsetzung zeitnah empfohlen 3= Umsetzung bei Gelegenheit empfohlen 0 = Hinweis	Verantwortlich
IT-Infrastruktur	1	Kein Bewegungsmelder im Serverraum		Installation eines Bewegungsmelders prüfen	2	Vorstand
	2	Keine feuerfeste Tür zum Serverraum		Einbau einer feuerfesten Tür prüfen	2	Vorstand
	3	CO_2 Feuerlöscher im Serverraum installiert		CO_2 Feuerlöscher vor dem Serverraum installieren	3	Vorstand
	4	Keine Benutzerrichtlinie		Benutzerrichtlinie schriftlich fixieren	2	Vorstand
	5	Keine Passwortrichtlinie		Passwortrichtlinie schriftlich fixieren	2	Vorstand
	6	Datensicherungskonzept nicht schriftlich vorhanden		Datensicherungskonzept schriftlich fixieren	2	Vorstand
	7	Datensicherungen (NAS) befinden sich im Serverraum		Datensicherungen nicht im Serverraum, sondern in einem anderen Brandabschnitt lagern.	2	Vorstand
	8	Kennwortparameter für Windows Sperrung erst nach 15 Anmeldeversuchen		Sperrung nach 3-5 Anmeldeversuchen	2	Vorstand
	9	Kein Notfallkonzept		Notfallkonzept schriftlich fixieren	1	Vorstand
	10	Keine Richtlinien für Internet-, E-Mail- und PC-Nutzung		Richtlinien für die Internet-, E-Mail- und PC-Nutzung schriftlich fixieren	2	Vorstand

Wichtige Internetadressen

Bundesamt für Sicherheit in der Informationstechnik
www.bsi.de

Softwarebescheinigungen (Nur noch vollständige Berichte!)
Intranet des GdW / Die Beratungsprüfer-Webseite

Datenschutzbeauftragte der jeweiligen Bundesländer, z. B.:
www.datenschutz.de

ISACA Germany Chapter (Berufsverband der IT-Revisoren)
www.isaca.de bzw. www.isaca.org

Vielen Dank für Ihre Aufmerksamkeit!

Claudia Buchta, Enrico Großer