# Block 8

# IT-Prüfung in der Jahresabschlussprüfung nach ISA [DE] 315 (Revised 2019)

**WP Claudia Buchta, GdW**

**CISA Enrico Großer, Bavaria Treu AG**

**Berlin, 06. und 07.12.2023**

# Agenda

I. Einleitung

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

III. IT-Systemprüfung mit AuditTemplate – Workflow

IV. Bestimmung der Komplexität

V. Ausgestaltung und Einrichtung von Allgemeinen IT-Kontrollen (566)

VI. Optionale Checklisten (510-2)

VII. Erfassung von IT-Risiken (540)

# Agenda

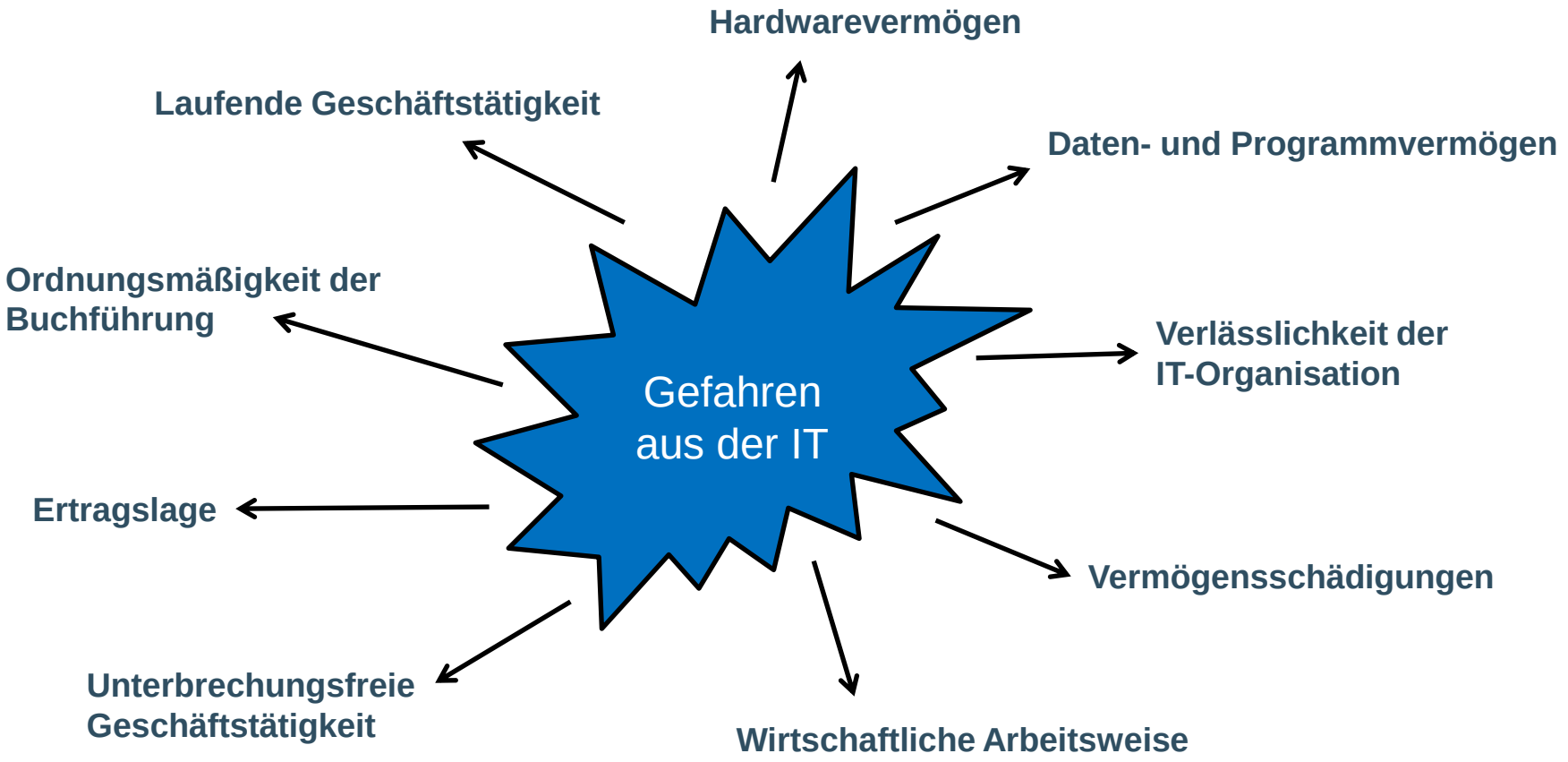
# I. Einleitung

## Warum Prüfung der IT?

- 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

# I. Einleitung

## Auswirkungen bei Gefahren aus der IT



# I. Einleitung
# Was ist neu ab 01.01.2023?

- GoA unter Einbeziehung der ISA
- Anwendung des ISA [DE] 315 (Revised 2019)
  Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen
- Keine separater IT-Prüfungsstandard mehr, die Prüfung der IT ist nun integraler Bestandteil der Jahresabschlussprüfung
- IDW PS 330 Abschlussprüfung bei Einsatz von Informationstechnologie entfällt
- Aus IDW PS 331 n.F.
  Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen
  wird
  ISA [DE] 402
  Überlegungen bei der Abschlussprüfung von Einheiten, die Dienstleister in Anspruch nehmen

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

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

# Überblick

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

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

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

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

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

# F & Q zu ISA [DE] 315 (Revised 2019) Frage 4.13

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

# F & Q zu ISA [DE] 315 (Revised 2019) Frage 4.13

- 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 durchfzuführen

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

# F & Q zu ISA [DE] 315 (Revised 2019) Frage 4.14

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

# F & Q zu ISA [DE] 315 (Revised 2019) Frage 4.14

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

# F & Q zu ISA [DE] 315 (Revised 2019) Frage 4.16

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

# F & Q zu ISA [DE] 315 (Revised 2019) Frage 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.**

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

# IDW RS FAIT 1

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

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

# IDW RS FAIT 1

**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)**

**(IDW RS FAIT 1 Tz 25 ff.)**

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

# IDW RS FAIT 1

**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**

**(IDW RS FAIT 1 Tz 23)**

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

**Übungsaufgabe 1**

**Sind die gesetzlichen Ordnungsmäßigkeitskriterien bei folgenden Softwareprodukten erfüllt?**

1) **Reporting-Tool in Excel**
2) **Projektplanungs-Tool in Excel**
3) **Baubuch in Excel**
4) **Bewertungs-Tool in Excel**
5) **Anlagenverzeichnis in Excel**
6) **Anlagenbuchhaltung in Excel**

**Zeitumfang: 5 Minuten**

**Wer: Alle**

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

## Übersicht

Übersicht 3: GoB angewandt auf Rechnungslegungssysteme

| | | | |
|---|---|---|---|
| **HGB** (GoB allgemein) | **Vollständigkeit** (§ 239 Abs. 2 HGB) | **Zeitgerechtigkeit** (§ 239 Abs. 2 HGB) | **Nachvollziehbarkeit** (§ 238 Abs. 1 Satz 2 HGB) |
| | **Richtigkeit** (§ 239 Abs. 2 HGB) | **Ordnung** (§ 239 Abs. 2 HGB) | **Unveränderlichkeit** (§ 239 Abs. 3, 257 Abs. 3 HGB) |

| | | |
|---|---|---|
| **IDW RS FAIT 1** (Anwendung auf Rechnungslegungssysteme) | **Belegfunktion** | **Vertraulichkeit** |
| | **Journalfunktion** | **Integrität** |
| | **Kontenfunktion** | **Verfügbarkeit** |
| | **Dokumentation** | **Autorisierung** |
| | **Aufbewahrung** | **Authentizität** |
| | | **Verbindlichkeit** |

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

# IDW RS FAIT 1

## Belegfunktion

- **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)

**(IDW RS FAIT 1 Tz 33 ff.)**

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

# IDW RS FAIT 1

## Journalfunktion

- 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

(IDW RS FAIT 1 Tz 41 ff.)

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

# IDW RS FAIT 1

## Kontenfunktion

- 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

(IDW RS FAIT 1 Tz 46 ff.)

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

# IDW RS FAIT 1

## (Verfahrens-)Dokumentation

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

(IDW RS FAIT 1 Tz 52 ff.)

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

# IDW RS FAIT 1

## Aufbewahrung

- 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

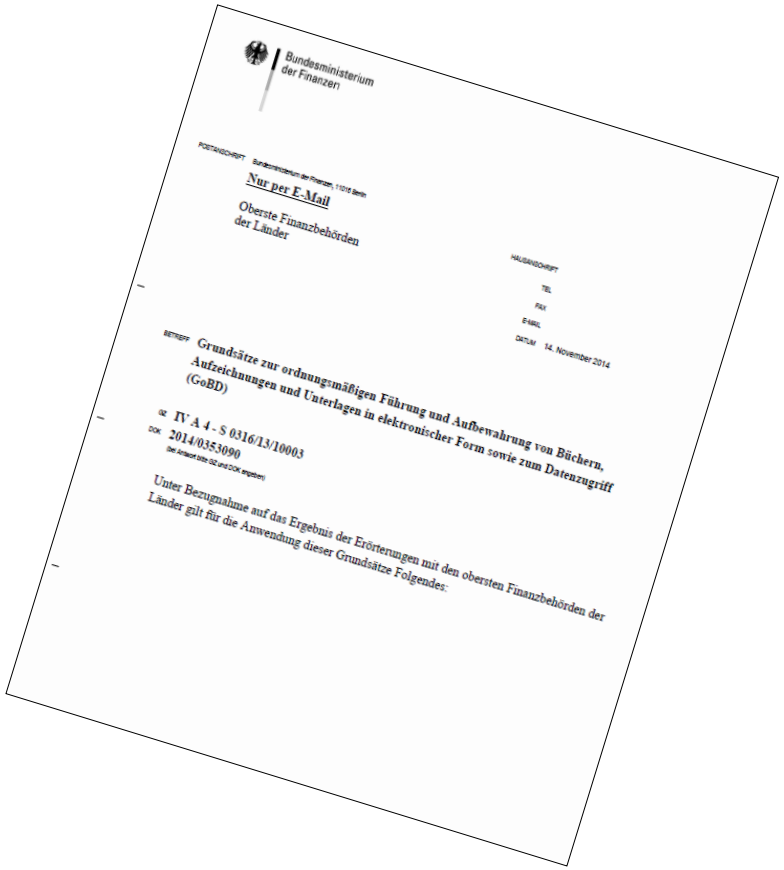
**(IDW RS FAIT 1 Tz 60 ff.)**

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

# 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**
**Neufassung der GoBD  am 28.11.2019**



Bundesministerium der Finanzen

Nur per E-Mail

Oberste Finanzbehörden der Länder

BETREFF Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)

GZ IV A 4 - S 0316/13/10003
DOK 2014/0353090

Unter Bezugnahme auf das Ergebnis der Erörterungen mit den obersten Finanzbehörden der Länder gilt für die Anwendung dieser Grundsätze Folgendes:

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

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

# GoBD - Ordnungsmäßigkeitsprinzipien

## Ordnungsmäßigkeitsprinzipien nach GoBD (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. ISA [DE] 315 (Revised 2019) / Rechtliche Grundlagen

# GoBD – Internes Kontrollsystem (IKS)

**Sicherstellung, dass alle Buchungen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden (§ 146 Abs. 1 AO)!**

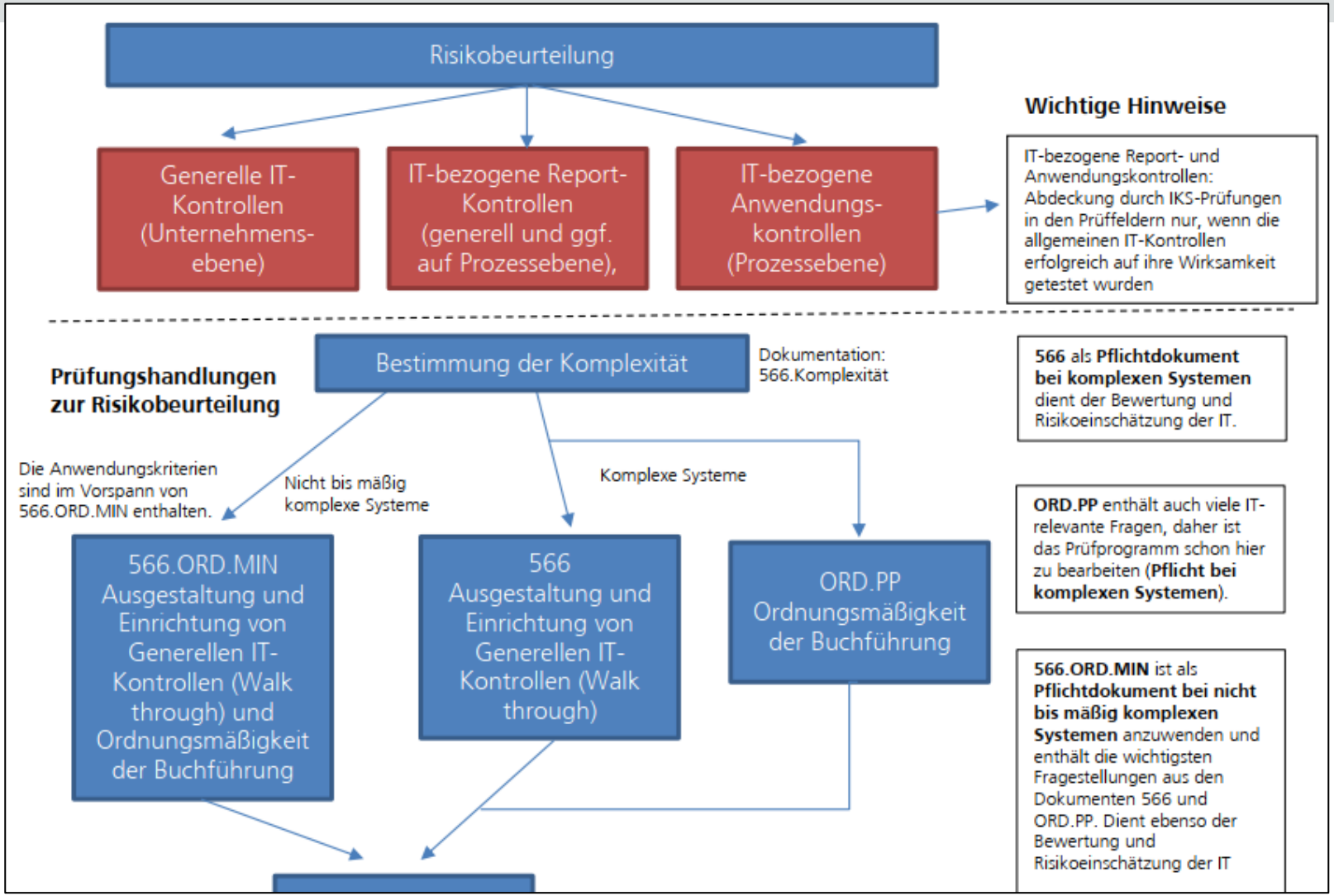
**Um dies zu gewährleisten sind Kontrollen einzurichten, auszuüben und zu protokollieren:**

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

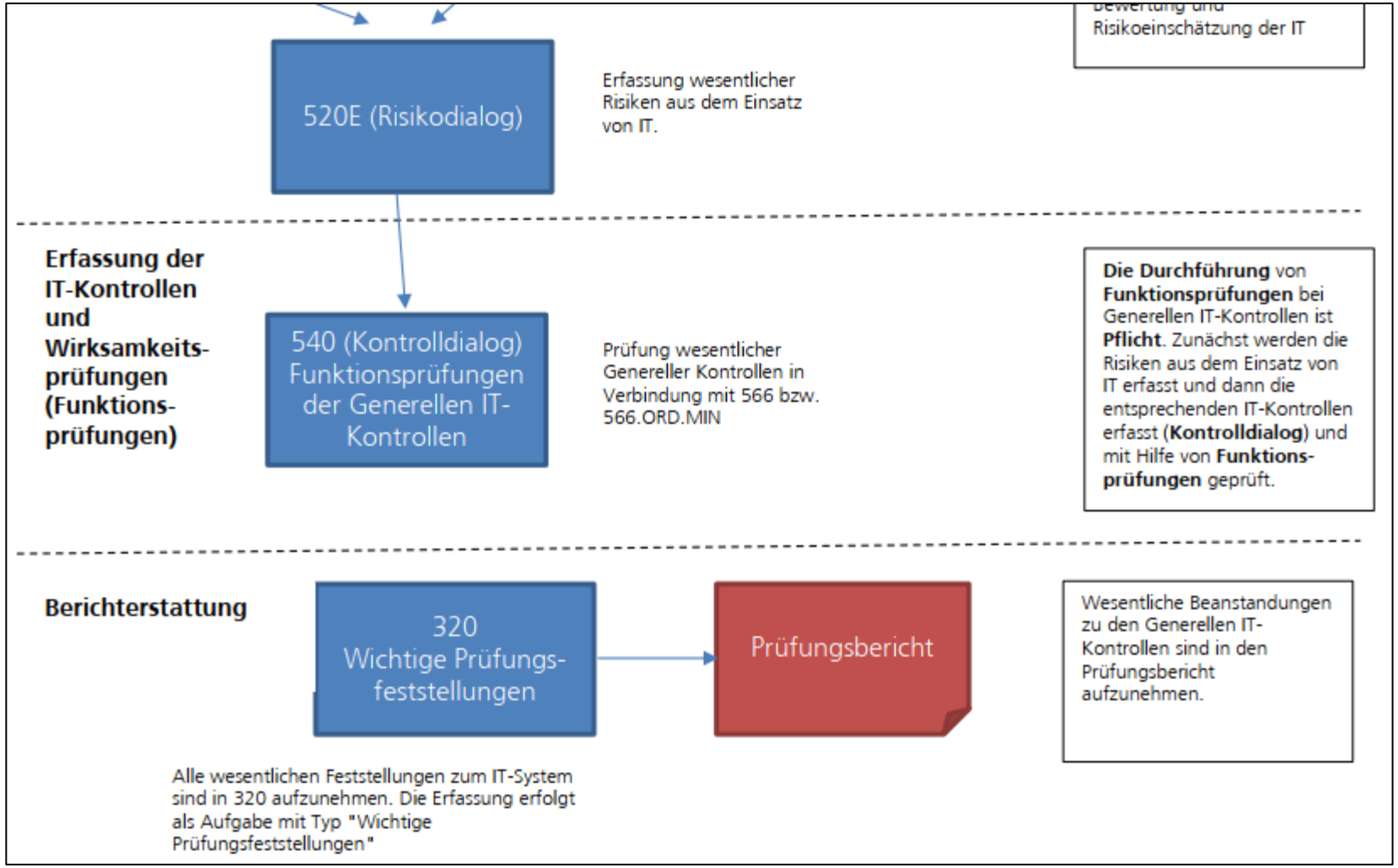
**Die Beschreibung des IKS ist Bestandteil der Verfahrensdokumentation (Tz 102)!**

# III. IT-Systemprüfung mit AuditTemplate nach ISA [DE] 315 (Revised 2019) – Workflow

# III. IT-Systemprüfung mit AuditTemplate nach ISA [DE] 315 (Revised 2019) – Workflow

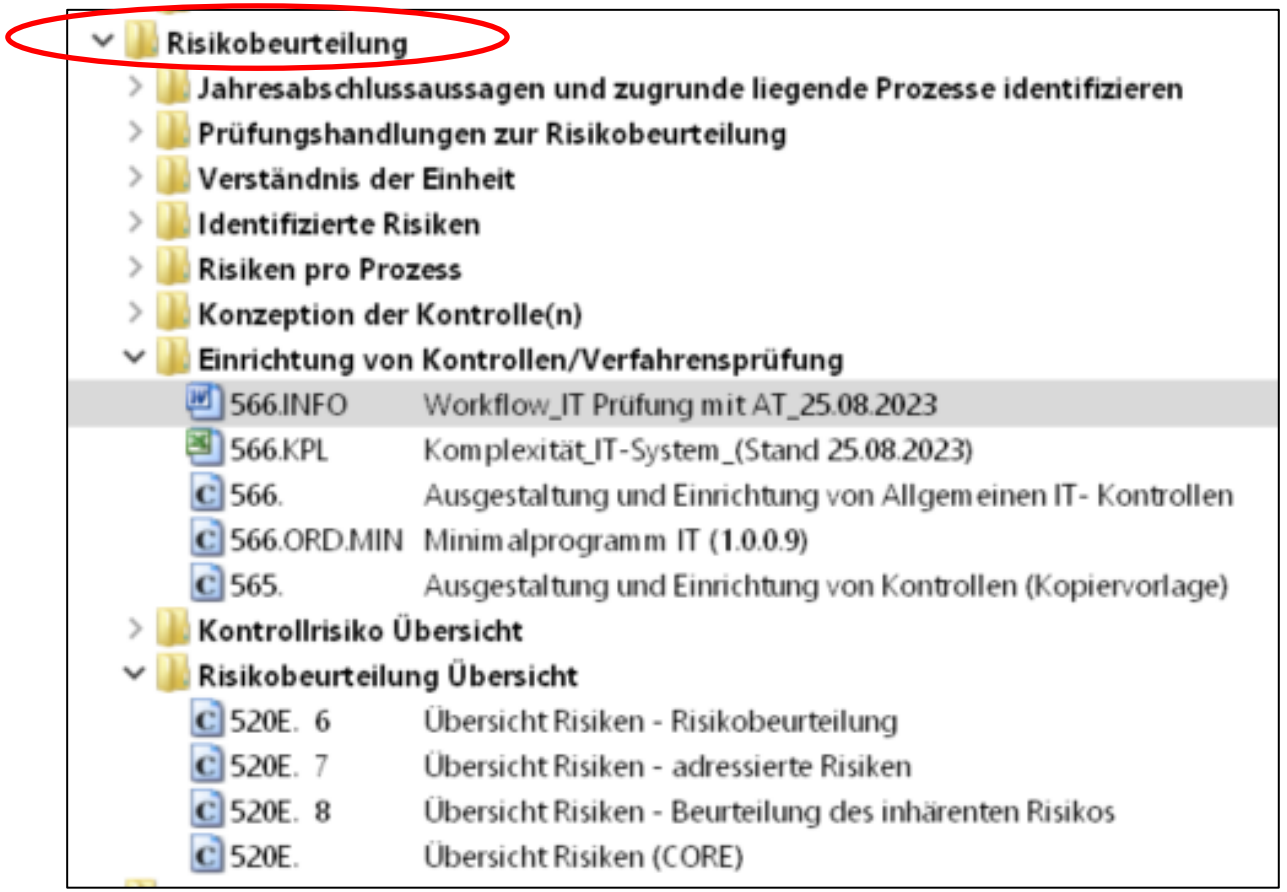


# III. IT-Systemprüfung mit AuditTemplate nach ISA [DE] 315 (Revised 2019) – Workflow



# III. IT-Systemprüfung mit AuditTemplate nach ISA [DE] 315 (Revised 2019) – Workflow

## Wo sind diese Checklisten zu finden?

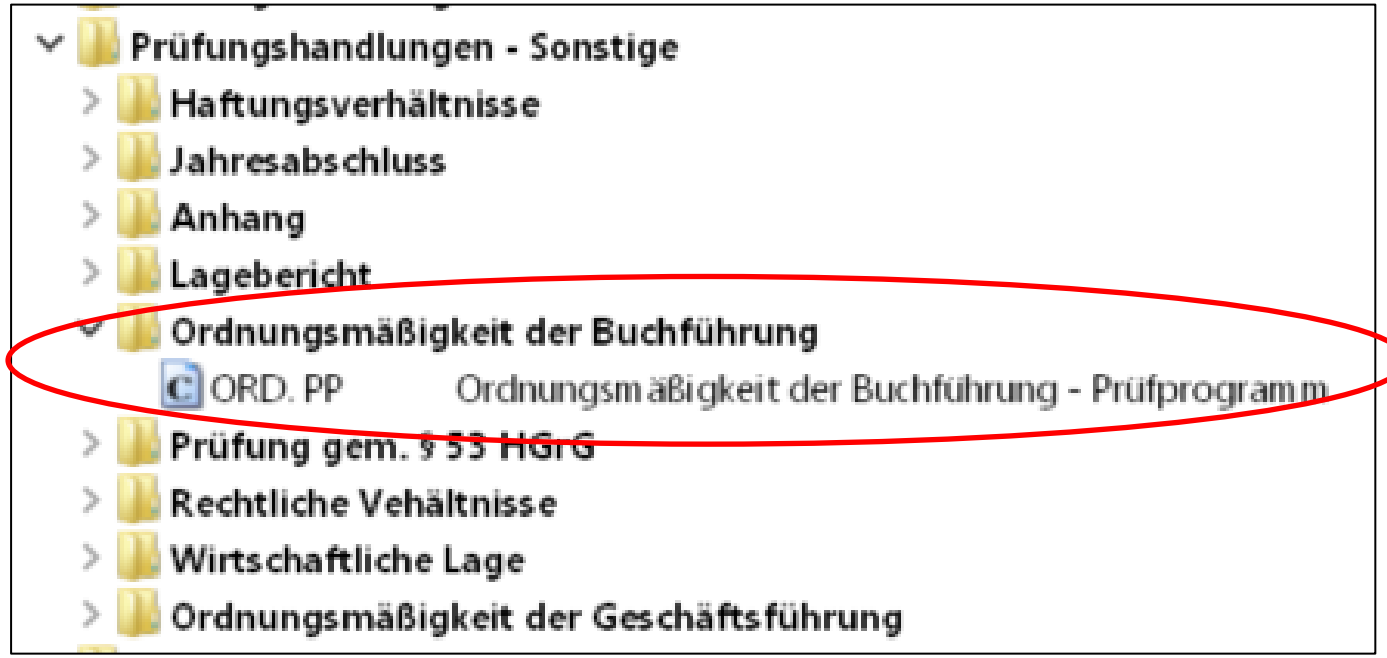


# III. IT-Systemprüfung mit AuditTemplate nach ISA [DE] 315 (Revised 2019) – Workflow

Die Wohnungswirtschaft Deutschland

GdW

## Und …

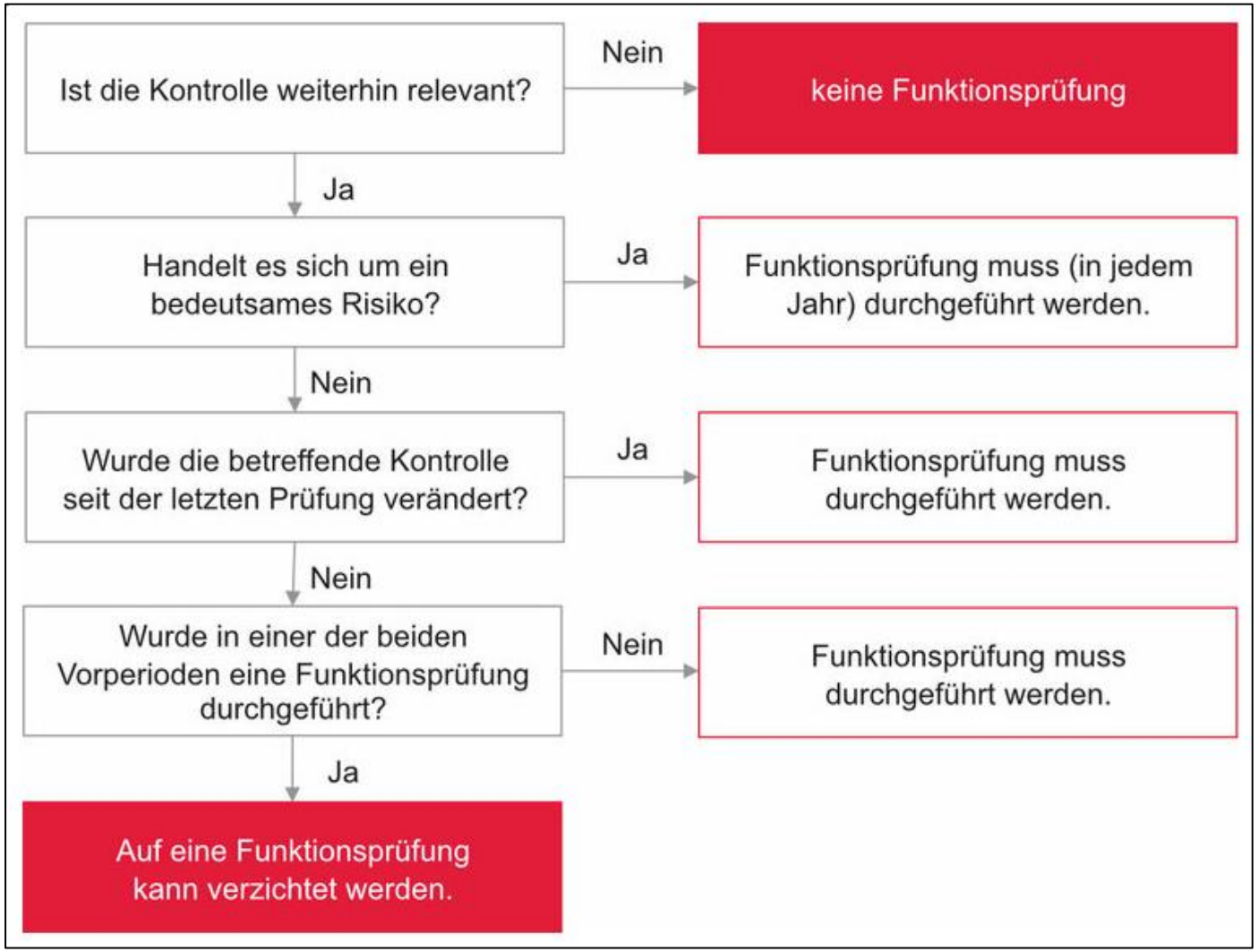


# III. IT-Systemprüfung mit AuditTemplate nach ISA [DE] 315 (Revised 2019) – Workflow

## Bearbeitung

- Jährliche Bearbeitung/Aktualisierung von 566 und ORD.PP bzw. 566.ORD.MIN
- Jährliche Aktualisierung von 566.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. IT-Systemprüfung mit AuditTemplate nach ISA [DE] 315 (Revised 2019) – Workflow



# IV. Bestimmung der Komplexität – 566.KPL

# IV. Bestimmung der Komplexität – 566.KPL

**Im Rahmen der Verständnisgewinnung muss der Abschlussprüfer 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.**
- **In Anlage 5 werden verschiedene Skalierungsmöglichkeiten in Abhängigkeit der Komplexität beschrieben.**
- **Die Checkliste 566.KPL basiert auf der Tabelle aus Anlage 5.**

# IV. Bestimmung der Komplexität – 566.KPL

**Die Checkliste 566.KPL wird wie folgt angewendet:**

**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.**

# IV. Bestimmung der Komplexität – 566.KPL

**Hinweis zum "Ergebnis der Komplexitätsbeurteilung" in 566.KPL:**

**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 566.ORD.MIN als Pflichtdokument zu bearbeiten.**
**Bei komplexen Systemen sind 566 und ORD.PP als Pflichtdokumente zu bearbeiten. Der Risiko- (520E) und Kontrolldialog (540) sind im Rahmen der IT-Prüfung immer zu bearbeiten.**

# IV. Bestimmung der Komplexität – 566.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 | Referenzen |
|---|---|---|---|---|---|---|---|---|
| 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- | mäßig komplex | | |
| | 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 | 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 | | |
| | 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 | | |
| | 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 | | |

# IV. Bestimmung der Komplexität – 566.KPL

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 | 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 |
| | 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 | mäßig komplex |
| | 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 |
| | 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 | Gemischte Nutzung von neu entstehenden Technologien über | nicht komplex |

# IV. Bestimmung der Komplexität – 566.KPL

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 | Begrenztes Personal mit IT-Kenntnissen / begrenztes für IT zweckbestimmtes Personal | Zweckbestimmte IT-Abteilungen mit sachkundigem Personal, einschließlich Programmierungskenntniss | nicht komplex |
| | 3.2 | Komplexität der Prozesse zur Verwaltung von Zugriffsrechten | Einzelne natürliche Person mit Administratorenrechten verwaltet Zugriffsrechte | Wenige natürliche Personen mit Administratorenrechten | Komplexe von der IT-Abteilung verwaltete Prozesse für Zugriffsrechte | nicht komplex |
| | 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 |
| | 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 |
| | 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 | nicht komplex |
| | 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 | Größere Versions-Upgrade, neues Release, Plattformwechsel | nicht komplex |

# IV. Bestimmung der Komplexität – 566.KPL

| | | |
|---|---|---|
| **Ergebnis der Komplexitätsbeurteilung** | Hinweis zur Bearbeitung:<br>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.<br><br>Hinweis zum Ergebnis:<br>Bei nicht komplex, nicht komplex bis mäßig komplex und bei mäßig komplexen Systemen ist 566.ORD.MIN als Pflichtdokument zu bearbeiten.<br>Bei komplexen Systemen sind 566 und ORD.PP als Pflichtdokumente zu bearbeiten.<br>Der Risiko- (520E) und Kontrolldialog (540) sind im Rahmen der IT-Prüfung immer zu bearbeiten. | nicht bis mäßig komplex |

# IV. Bestimmung der Komplexität – 566.KPL

**Die Checkliste 566.KPL wird wie folgt angewendet:**

**Hinweis zum Ergebnis:**

- **Bei nicht komplex, nicht komplex bis mäßig komplex und bei mäßig komplexen Systemen ist 566.ORD.MIN als Pflichtdokument zu bearbeiten.**
- **Bei komplexen Systemen sind 566 und ORD.PP als Pflichtdokumente zu bearbeiten.**
- **Ausnahmen:**
  - **Im Berichtsjahr erfolgte eine Systemumstellung. Dann ist nicht nur die Migration zu prüfen, sondern auch die Dokumente 566 und ORD.PP als Pflichtdokumente zu bearbeiten.**
  - **Siehe Einleitung zu 566.ORD.MIN**
- **Der Risiko- (520E) und Kontrolldialog (540) sind im Rahmen der IT-Prüfung immer zu bearbeiten.**

# IV. Bestimmung der Komplexität – 566.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 PH**
  - **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 ab und verifiziert die Berechnungen in den Berichten**

# IV. Bestimmung der Komplexität – 566.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 PH zu prüfen**

# IV. Bestimmung der Komplexität – 566.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 PH**
  - **mehr Stützung auf Report-Kontrollen, da das Management, obwohl es bei seinen Kontrollen systemgenerierte Berichte nutzt und sich auf diese Berichte verlässt.**

# IV. Bestimmung der Komplexität – 566.KPL

## Exkurs: Übung 2

## Komplexitätsgrad (1) – Fallbeispiel A

| | |
|---|---|
| Unternehmen | Wohnungsbaugenossenschaft Entenhausen eG |
| Umsatz und WE | 40 Mio. EUR und 10.000 WE |
| Mitarbeiter/<br>IT-Mitarbeiter | 25 Mitarbeiter und 16 Hausmeister<br>1 IT-Mitarb. Vollzeit, 1IT-Mitarb. zu 50% in Buchhaltung tätig |
| Outsourcing | Personalbuchhaltung durch externen Dienstleister<br>Fernwartung durch Softwarehaus |
| Software-<br>bescheinigung | letzte Softwarebescheinigung von 2022 |

# IV. Bestimmung der Komplexität – 566.KPL

## Exkurs: Übung 2

### Komplexitätsgrad (2) – Fallbeispiel A

| | |
|---|---|
| Anwendungs-software | Wodis Sigma 12.0 (Inhouse) |
| Nebenbücher | Viele Nebenbücher mit vielen Schnittstellen |
| Weitere Anwendungen | Handwerkerkopplung mit Eingabe von Rechnungsdaten<br>Zahlung anhand von Originalrechnungen<br>Bankensoftware |
| Weitere Erläuterungen | - Software wurde an die individuellen Bedürfnisse der eG angepasst |

# IV. Bestimmung der Komplexität – 566.KPL

## Exkurs: Übung 2

## Komplexitätsgrad (3) – Fallbeispiel B

| | |
|---|---|
| Unternehmen | Wohnungsgenossenschaft Regenbogen eG |
| Umsatz und WE | 4 Mio. EUR und 1.500 WE |
| Mitarbeiter/<br>IT-Mitarbeiter | 4 Mitarbeiter<br>kein IT-Mitarbeiter |
| Outsourcing | Personalbuchhaltung durch externen Dienstleister<br>Nutzung eines Rechenzentrums |
| Software-<br>bescheinigung | letzte Softwarebescheinigung von 2022 |

# IV. Bestimmung der Komplexität – 566.KPL

## Exkurs: Übung 2

### Komplexitätsgrad (4) – Fallbeispiel B

| | |
|---|---|
| Anwendungs-software | DATEV |
| Nebenbücher | Nebenbücher sind in DATEV integriert |
| Weitere Anwendungen | Bankensoftware |
| Weitere Erläuterungen | - Kein Berechtigungskonzept eingerichtet, jeder Mitarbeiter darf alles<br>- Datensicherung erfolgt einmal wöchentlich<br>- manuelle Schnittstelle zw. DATEV und LuG |

# IV. Bestimmung der Komplexität – 566.KPL

**Übungsaufgabe 2**

**Bitte füllen Sie 566.KPL aus.**

**Treffen Sie dabei auch eigene Annahmen, das die Sachverhaltsbeschreibungen nicht vollständig sind.**

**Zeitumfang: 10 Minuten**

**Wer: Alle**

# V. Verständnis der IT-Umgebung der Einheit

# V. Verständnis der IT-Umgebung der Einheit

Die Wohnungswirtschaft Deutschland GdW

### 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)

**Vom IT-Einsatz ist ein Verständnis zu erlangen. Gemäß A56 umfasst dies die Struktur und die Komplexität der IT-Umgebung der Einheit.**

# V. Verständnis der IT-Umgebung der Einheit

**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 566 oder 566.ORD.MIN einfügen, da dort neben der Erfassung der generellen IT-Kontrollen auch die IT-Umgebung zu beschrieben ist.**

**Hinweis: Die Dokumente 566 und 566.ORD.MIN sind zukünftig um Beschreibungen zu den einzelnen Fragen zu ergänzen. "Fertiggestellt ohne Beanstandungen" ohne Beschreibungen und ggf. Referenzen reicht nicht aus.**

# V. Verständnis der IT-Umgebung der Einheit

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

**Teilbereich: Informationssystem und Kommunikation**

**Dies betrifft Transaktions-flüsse und die Informationsverarbeitung.**

**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)

# V. Verständnis der IT-Umgebung der Einheit

## 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.

# V. Verständnis der IT-Umgebung der Einheit

**Dokumentiert wird dies in MEMO.PA4/1e**

**Hier ist auch auf das Dokument 566 bzw. 566.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.

# V. Verständnis der IT-Umgebung der Einheit

# Exkurs 510-2

# V. Verständnis der IT-Umgebung der Einheit

## Exkurs

A. Hardware

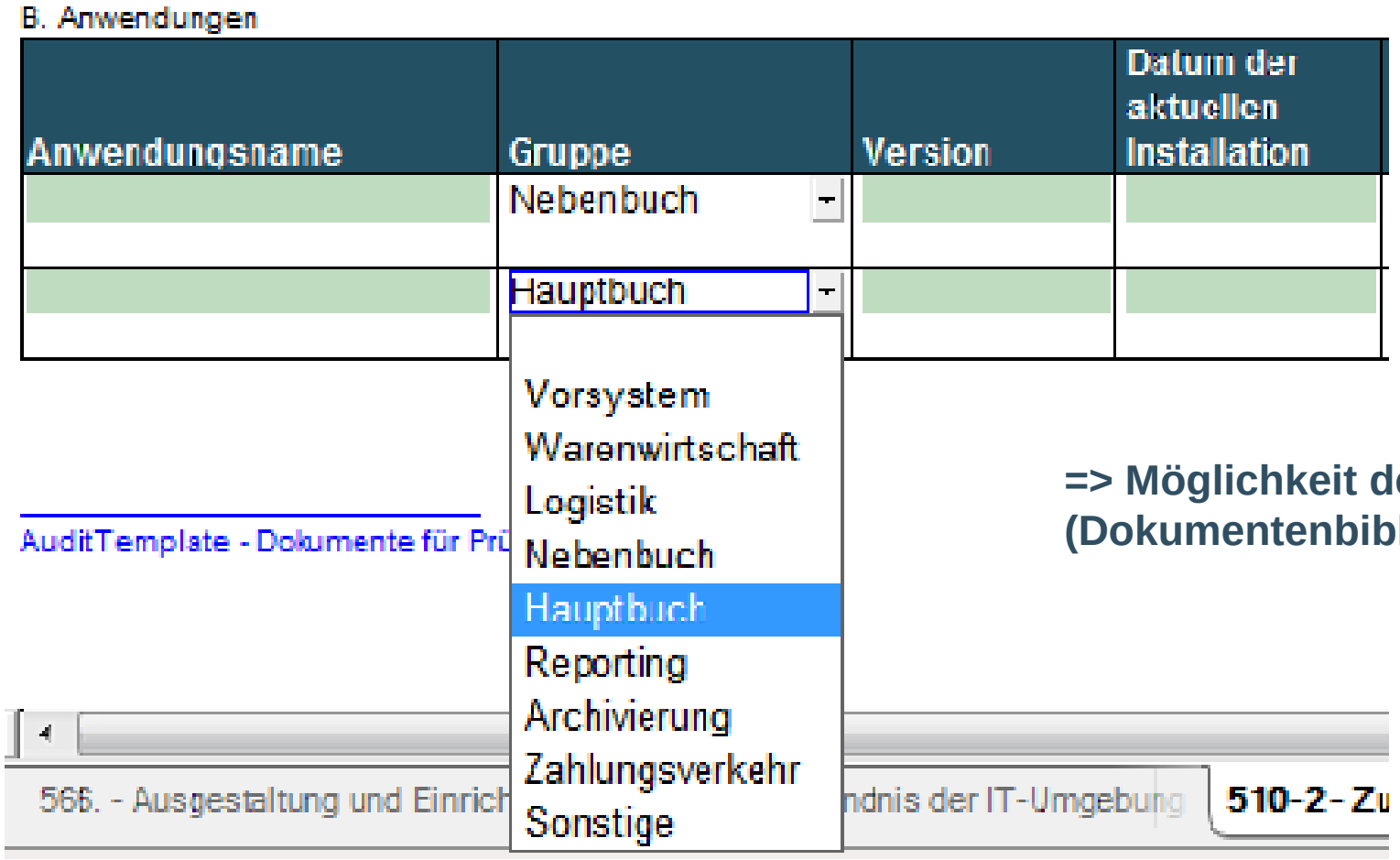
| Gerät | Hersteller und Modellbezeichnung | Seriennummer | Standort |
|---|---|---|---|
| | | | |

| Installation (Betriebssystem, Version) | Einbindung in Netzwerk (LAN/WLAN) | Anmerkung |
|---|---|---|
| | | |

**=> Möglichkeit der Hardware-Erfassung (Dokumentenbibliothek)**

# V. Verständnis der IT-Umgebung der Einheit

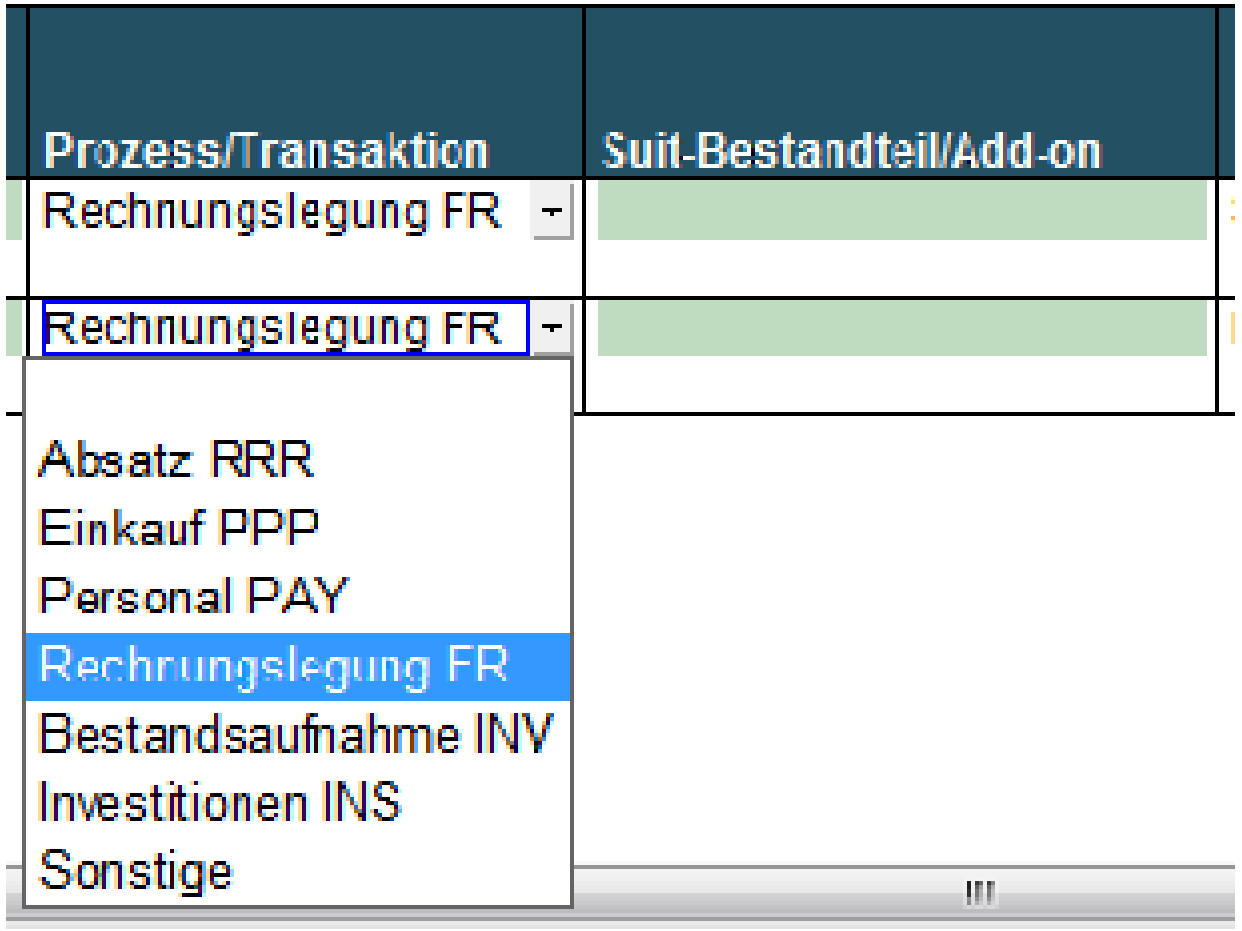
## Exkurs




**=> Möglichkeit der Software-Erfassung (Dokumentenbibliothek)**

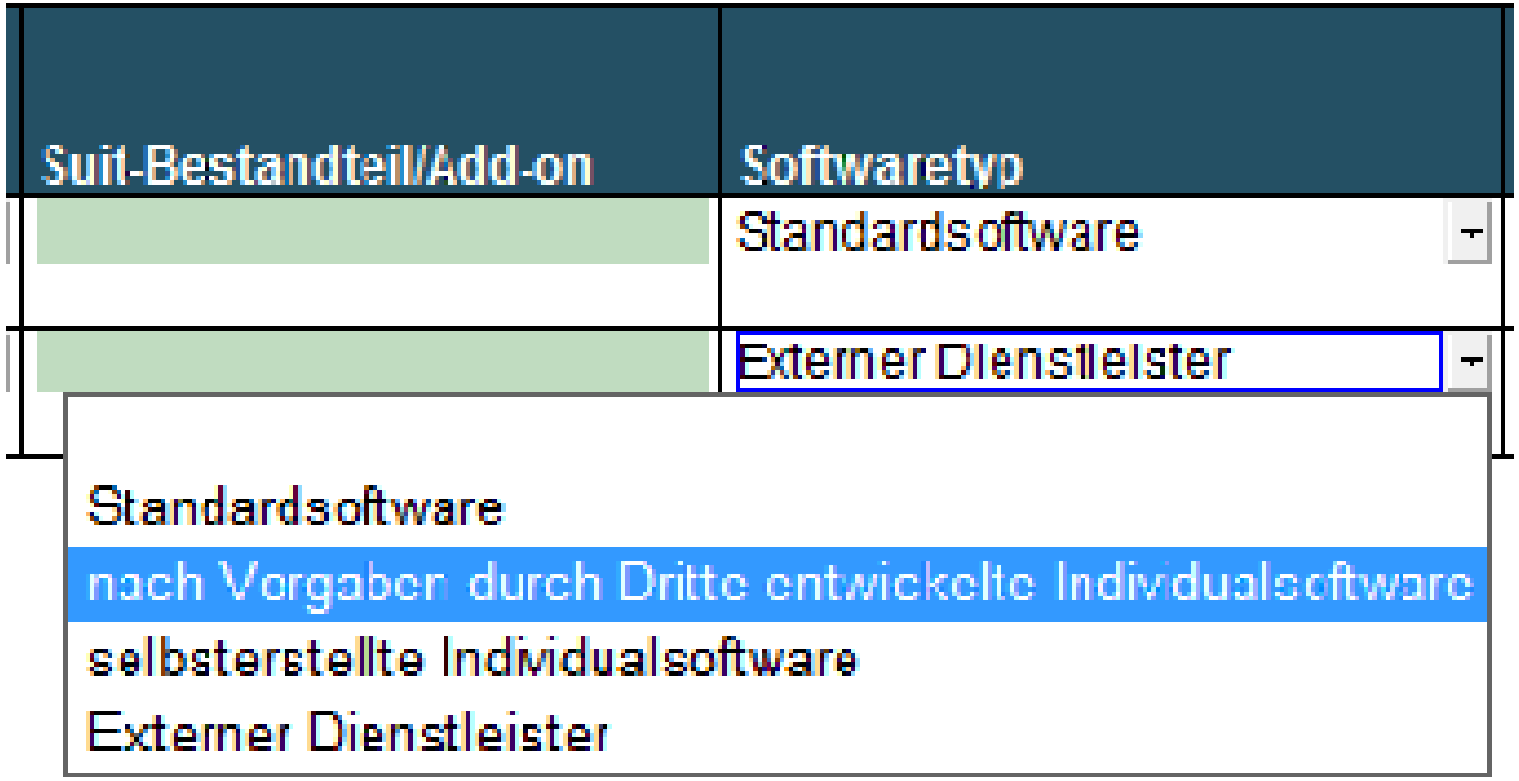
# V. Verständnis der IT-Umgebung der Einheit

## Exkurs



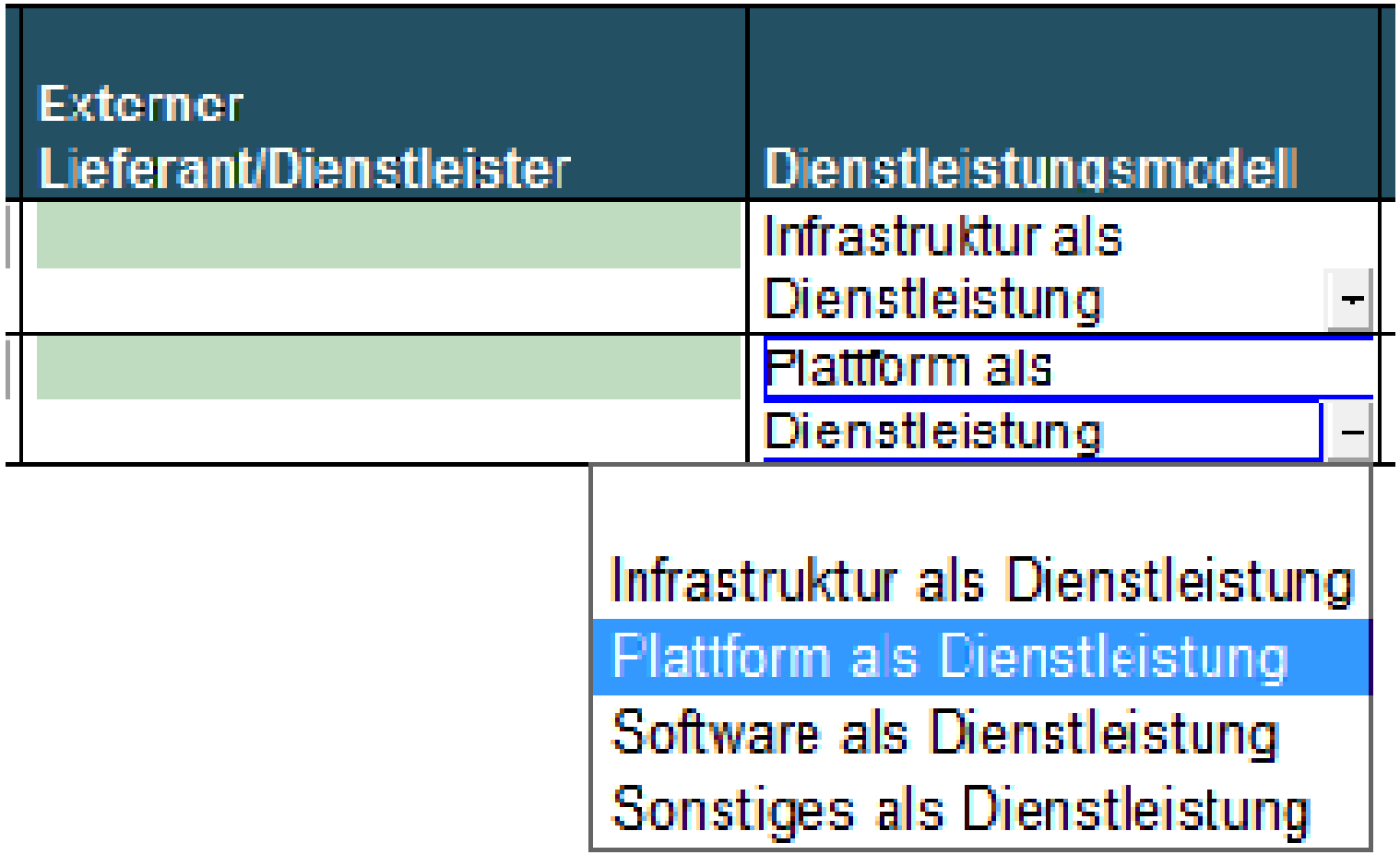
# V. Verständnis der IT-Umgebung der Einheit

## Exkurs



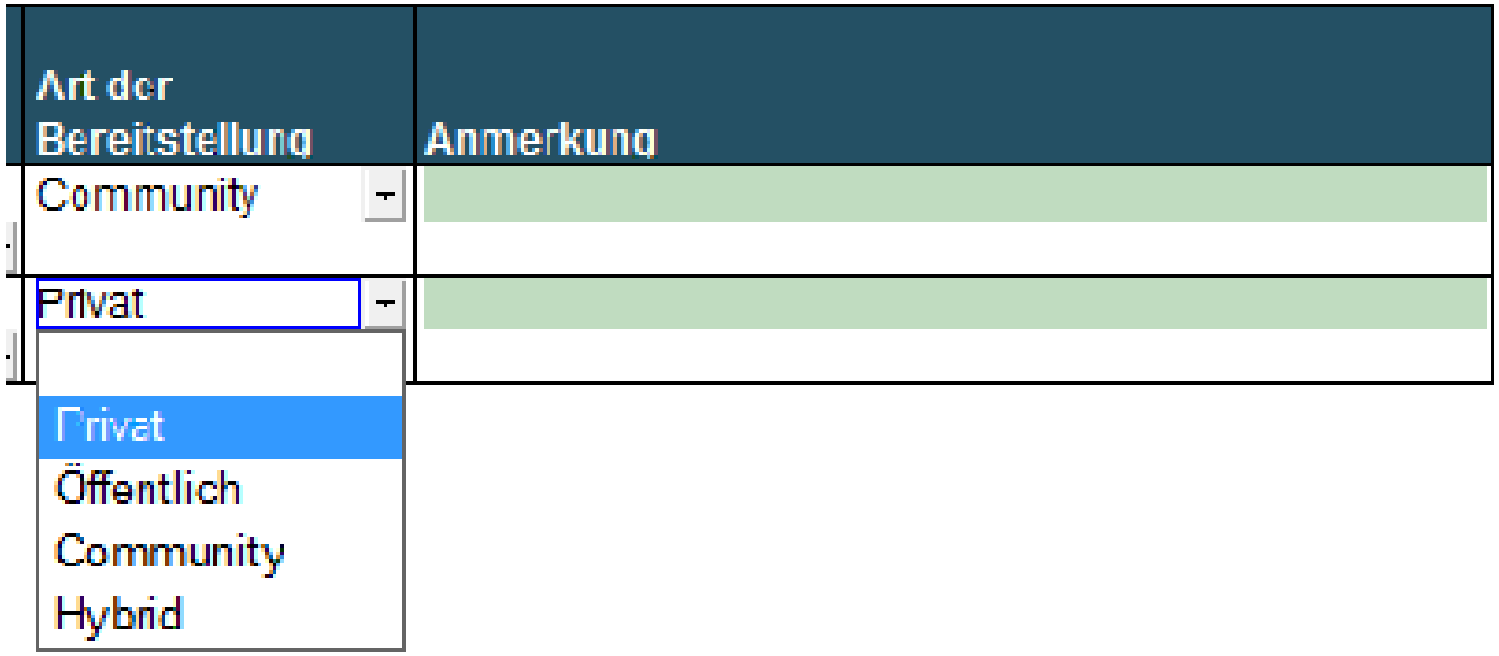
# V. Verständnis der IT-Umgebung der Einheit

## Exkurs



# V. Verständnis der IT-Umgebung der Einheit

## Exkurs



# V. Verständnis der IT-Umgebung der Einheit

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

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

# V. Verständnis der IT-Umgebung der Einheit

### 4.2.2.2.2 Kontrollaktivitäten

**26**

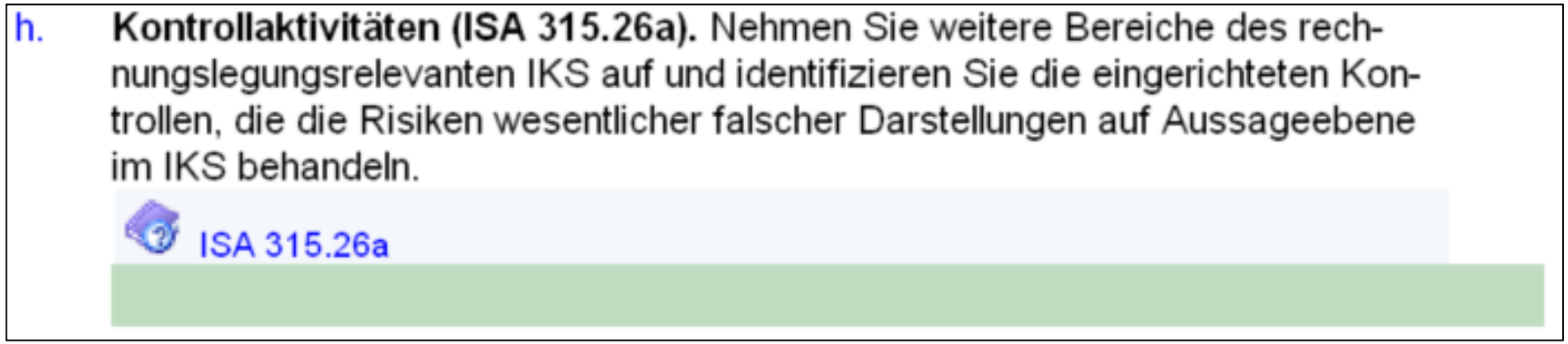
Der Abschlussprüfer hat ein Verständnis von der Komponente Kontrollaktivitäten zu erlangen durch die Durchführung von Prüfungshandlungen zur Risikobeurteilung mittels: (Vgl. Tz. A147–A157)

**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)**

# V. Verständnis der IT-Umgebung der Einheit

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




**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 566 bzw. 566.ORD.MIN zu verweisen.**

# V. Verständnis der IT-Umgebung der Einheit

**Zusammenfassung:**

Schritt 1
**Informations-gewinnung**

Verständnis des Geschäftsmodells und der IT-Umgebung (Tz 19)

Verständnis über das Informationssystem (Tz 25a)

Verständnis über die Kontrollaktivitäten (Tz 26)

Befragung, Beobachtung, Einsichtnahme
**(A22 bis A36 sowie FAQ zu ISA [DE] 315 (Revised) Frage 4.20)**

Bestimmung der Komplexität der IT-Umgebung und Berücksichtigung bei allen weiteren Schritten (Anlage 5, Tz 6 f.)

# VI. Risikoidentifizierung aus dem Einsatz von IT

# VI. Risikoidentifizierung aus dem Einsatz von IT

**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**
- **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**
- **Identifizierung genereller IT-Kontrollen, die diese Risiken behandeln**

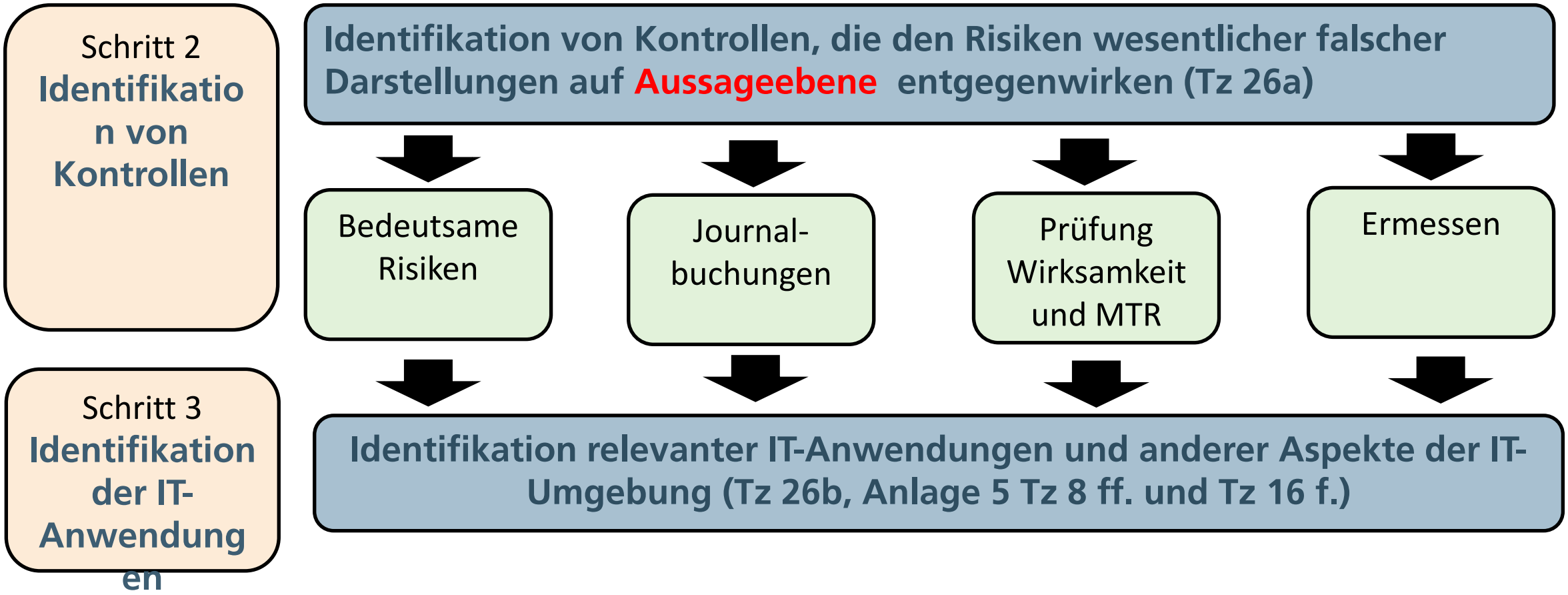
# VI. Risikoidentifizierung aus dem Einsatz von IT

**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))**

# VI. Risikoidentifizierung aus dem Einsatz von IT



# VI. Risikoidentifizierung aus dem Einsatz von IT

**Zusammenfassung:**

| | |
|---|---|
| Schritt 3<br>**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<br>**Identifikation von IT-Risiken** | **Identifikation von sich aus dem IT-Einsatz ergebenden Risiken (IT-Risiken) (Tz 26c, Anlage 5 Tz 18 ff.)** |
| Schritt 5<br>**Identifikation genereller IT-Kontrollen** | **Identifikation genereller IT-Kontrollen, die diesen Risiken begegnen (Tz 26c, Anlage 5 Tz 18 ff.)<br>aber auch die anwendungsbezogenen IT-Kontrollen** |

# VI. Risikoidentifizierung aus dem Einsatz von IT

**Zusammenfassung:**

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**

# VI. Risikoidentifizierung aus dem Einsatz von IT

**Durchführung der Aufbauprüfung / Prüfungshandlungen:**

**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)**

# VI. Risikoidentifizierung aus dem Einsatz von IT

**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)**

# VI. Risikoidentifizierung aus dem Einsatz von IT

**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)**

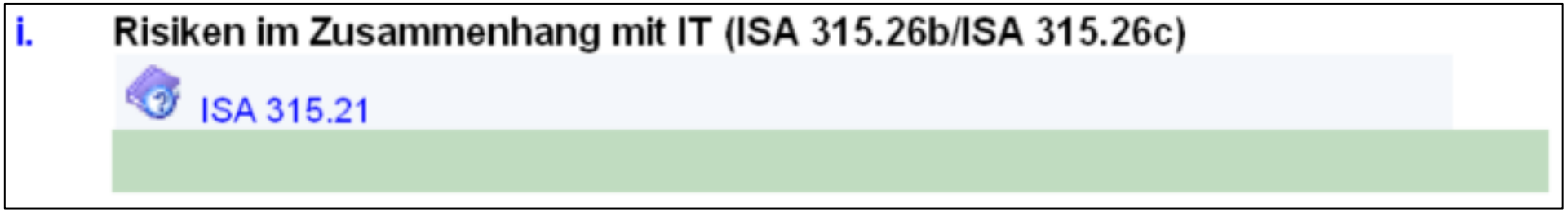
# VI. Risikoidentifizierung aus dem Einsatz von IT

**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

# VI. Risikoidentifizierung aus dem Einsatz von IT

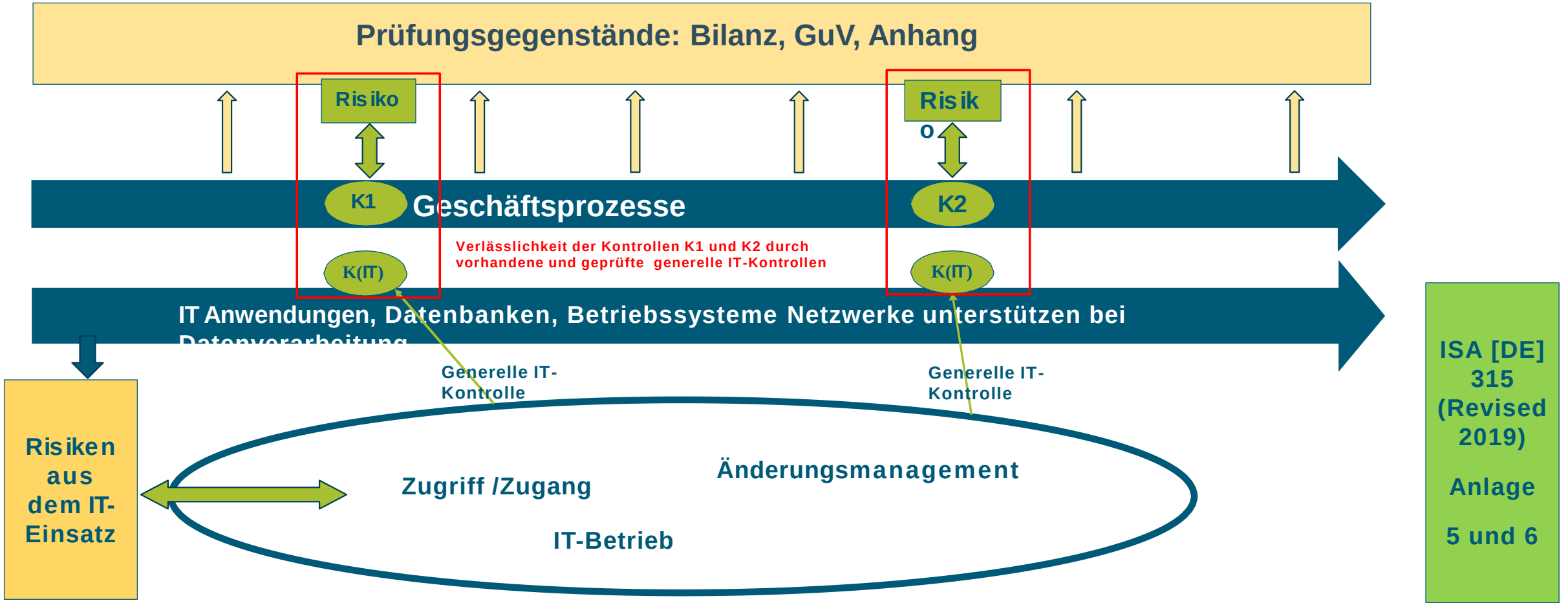
**Die Risiken aus dem Einsatz der IT sind in MEMO.PA4/1i zu dokumentieren.**




**Verweis auf folgende Dokumentationen:**

- **566 oder 566.ORD.MIN**
- **520E (IT-Risiken)**
- **540 (Kontrolldialog)**

# VI. Risikoidentifizierung aus dem Einsatz von IT




**IDW RS FAIT 1: Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität, Verbindlichkeit**

# VI. Risikoidentifizierung aus dem Einsatz von IT

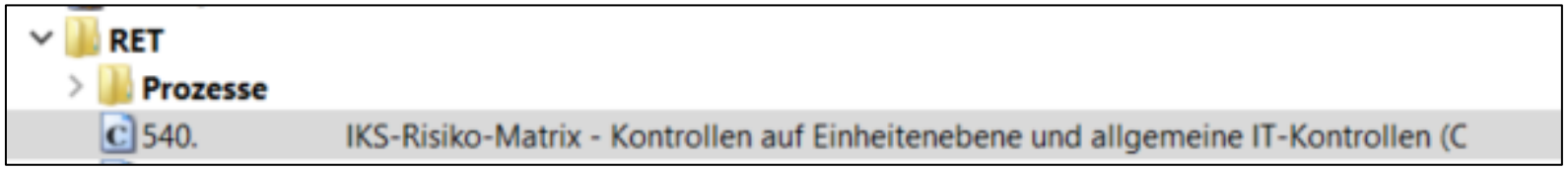
**Mit welchen Kontrollen muss man sich im Rahmen der Prüfung nun befassen?**

1. **Generelle IT-Kontrollen (=> bei jeder Prüfung!)**
   - **Selbst anlegen**
   - **Risiko-Import**
2. **Kontrollen, die Reports betreffen**
   - **Nach eigenem prüferischen Ermessen unter Berücksichtigung der Komplexität selbst anlegen**
3. **in Prozessen integrierte IT- gestützte Kontrollen**
   - **Nach eigenem prüferischen Ermessen unter Berücksichtigung der Komplexität selbst anlegen**

# VI. Risikoidentifizierung aus dem Einsatz von IT

## Generelle IT-Kontrollen:

- 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.

# VII. Erfassung von Risiken aus dem Einsatz von IT

# VII. Erfassung von Risiken aus dem Einsatz von IT

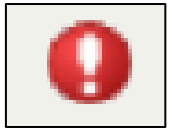
**Es gibt folgende zwei Möglichkeiten Risiken aus dem Einsatz von IT zu erfassen:**

1) **Manuelle Erfassung**

2) **Risikoimport aus der Importvorlage**

# VII. Erfassung von Risiken aus dem Einsatz von IT

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

- **Soweit sich bei der Bearbeitung der Dokumente 566 und ORD.PP bzw. 566.ORD.MIN Risken aus dem Einsatz von IT gezeigt haben**
- **Die Erfassung erfolgt z. B. über die Dokumente 566 und ORD.PP bzw. 566.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.**

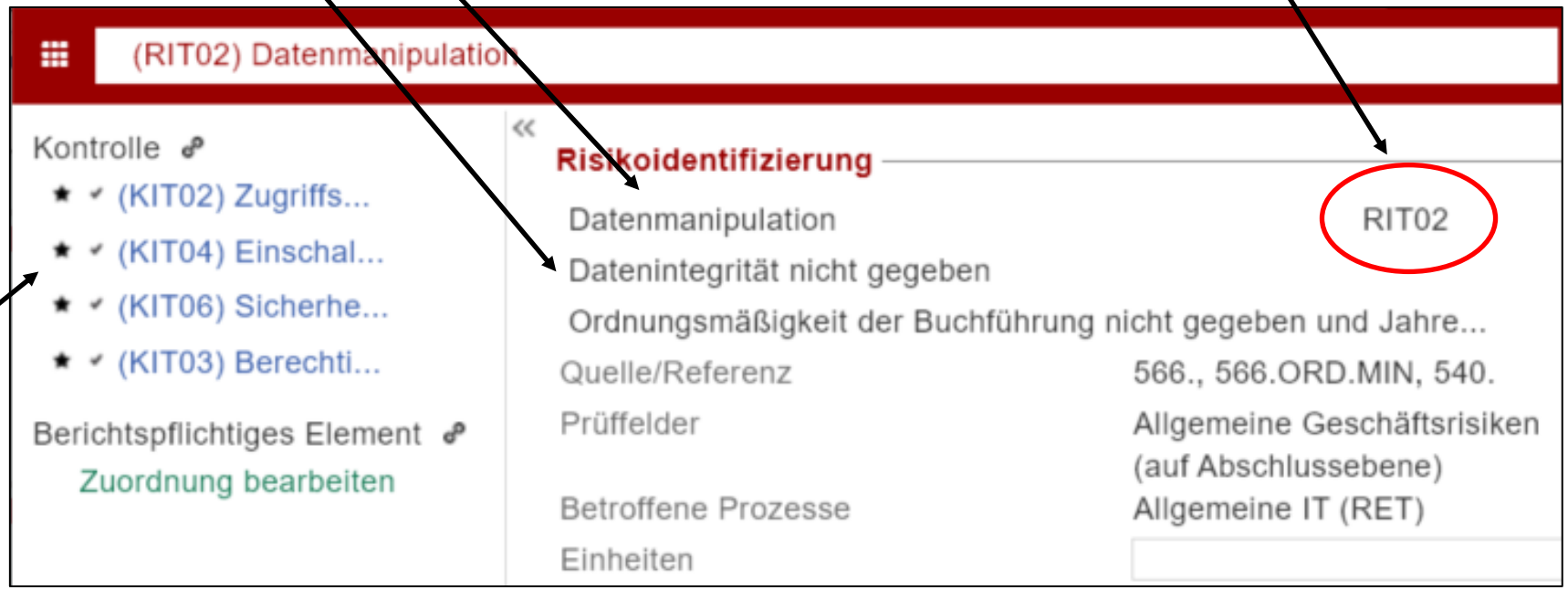
# VII. Erfassung von Risiken aus dem Einsatz von IT

**Bezeichnung und Beschreibung des Risikos**

**Kurzkennzeichen nach vorgegebenem Schema**

**Festlegung des Prüffeldes**

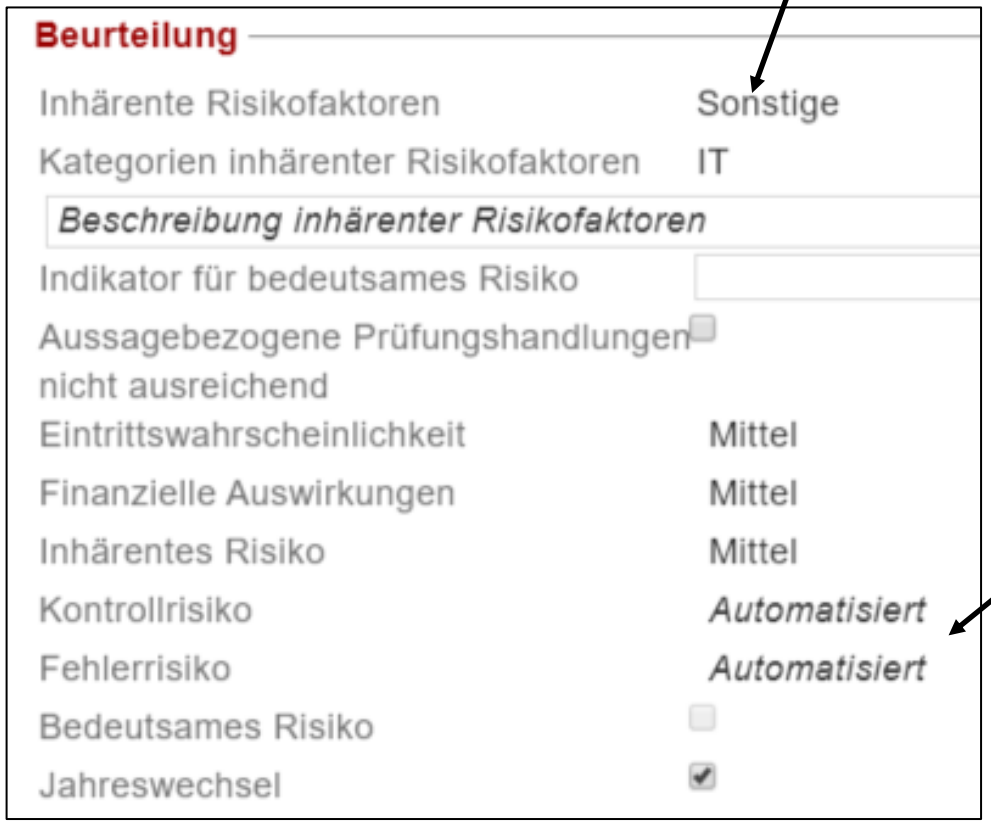
**Hier sind bereits Kontrollen zugeordnet**



# VII. Erfassung von Risiken aus dem Einsatz von IT

**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.**

# VII. Erfassung von Risiken aus dem Einsatz von IT

Reaktion des Managements eintragen.

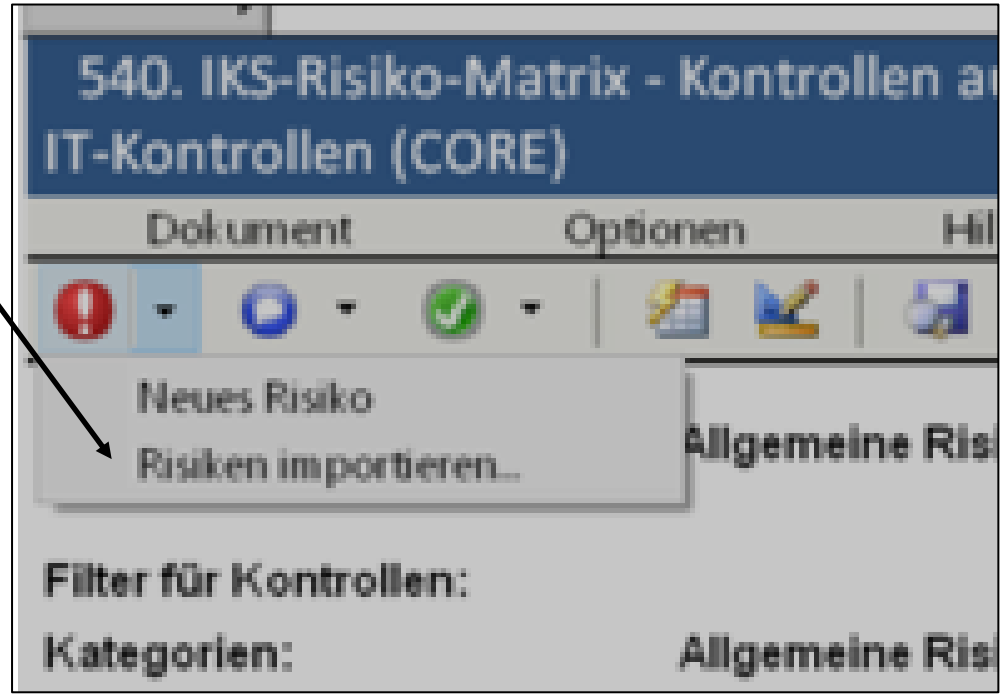
Unsere Reaktion auf das Risiko eintragen.

Jedes Risiko muss adressiert werden.


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

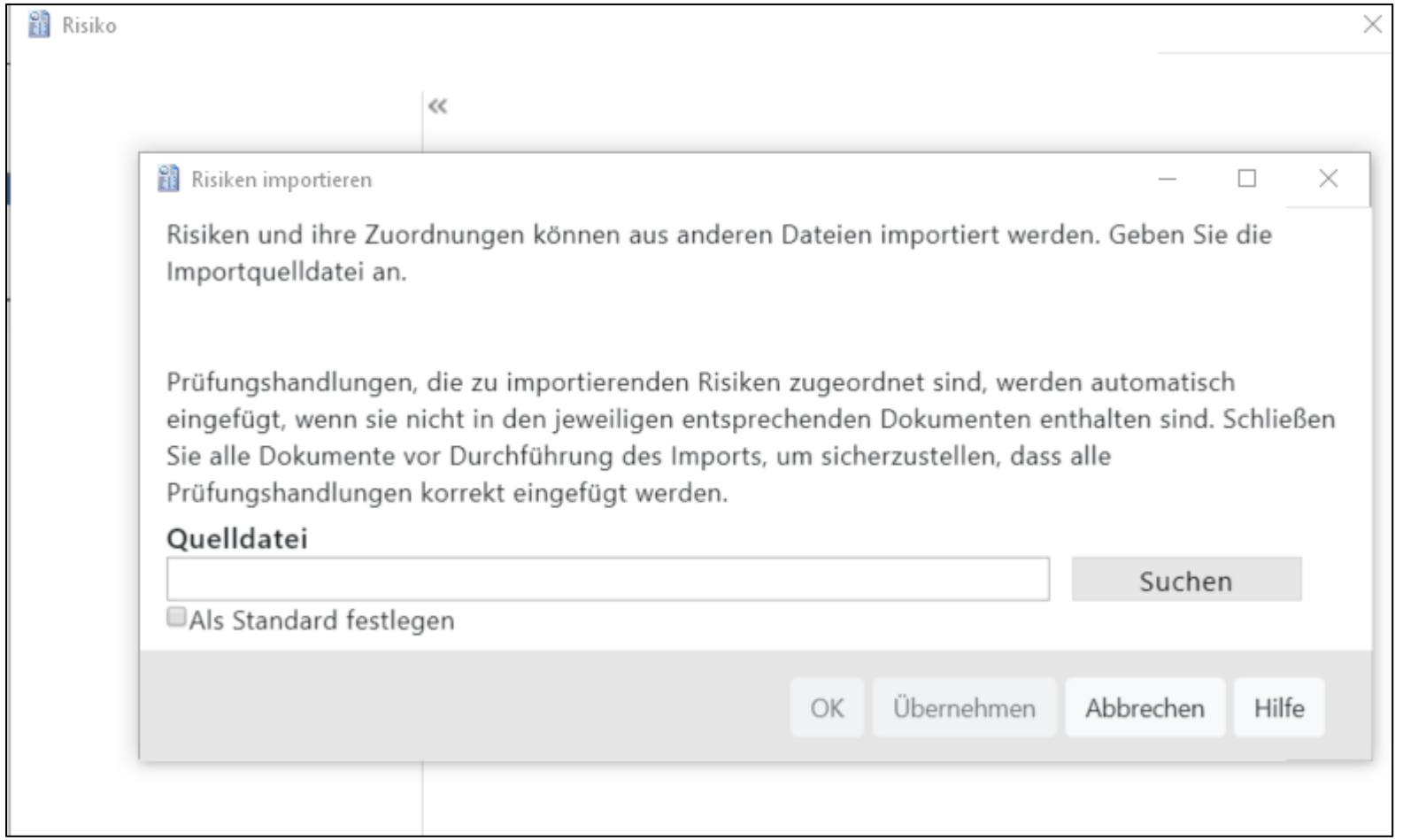
# VII. Erfassung von Risiken aus dem Einsatz von IT

**Import von IT-Risiken aus der Importvorlage**



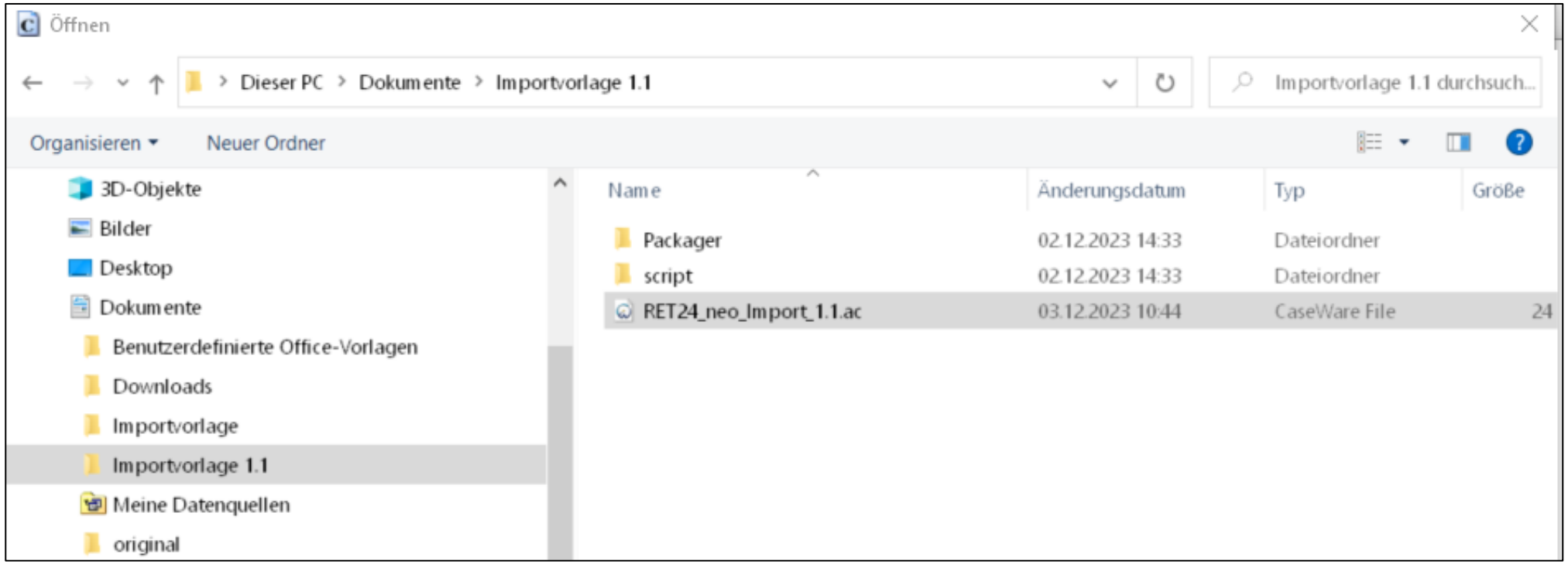
# VII. Erfassung von Risiken aus dem Einsatz von IT

**Auswahl der Quelldatei**



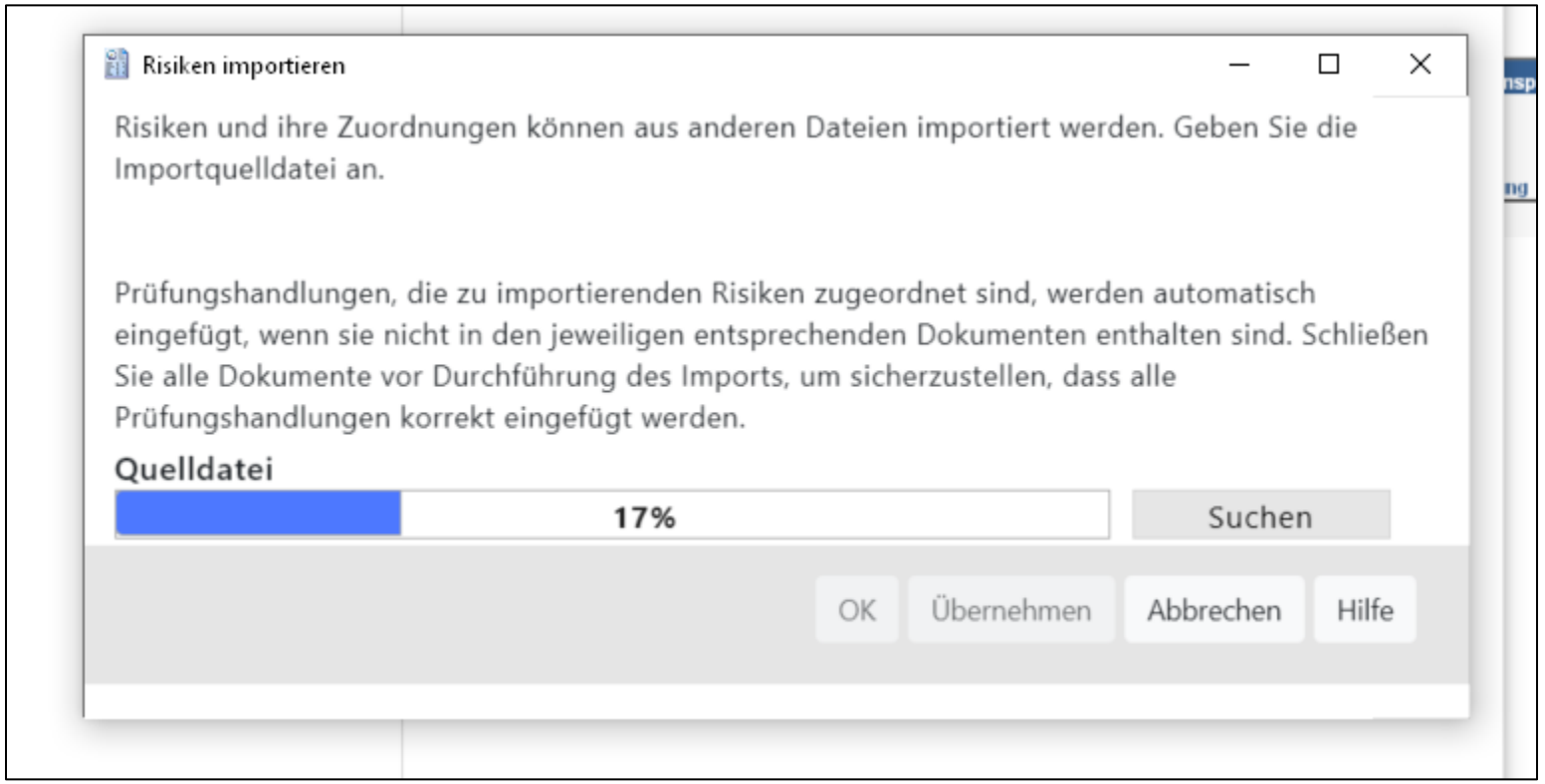
# VII. Erfassung von Risiken aus dem Einsatz von IT

## Auswahl der Quelldatei



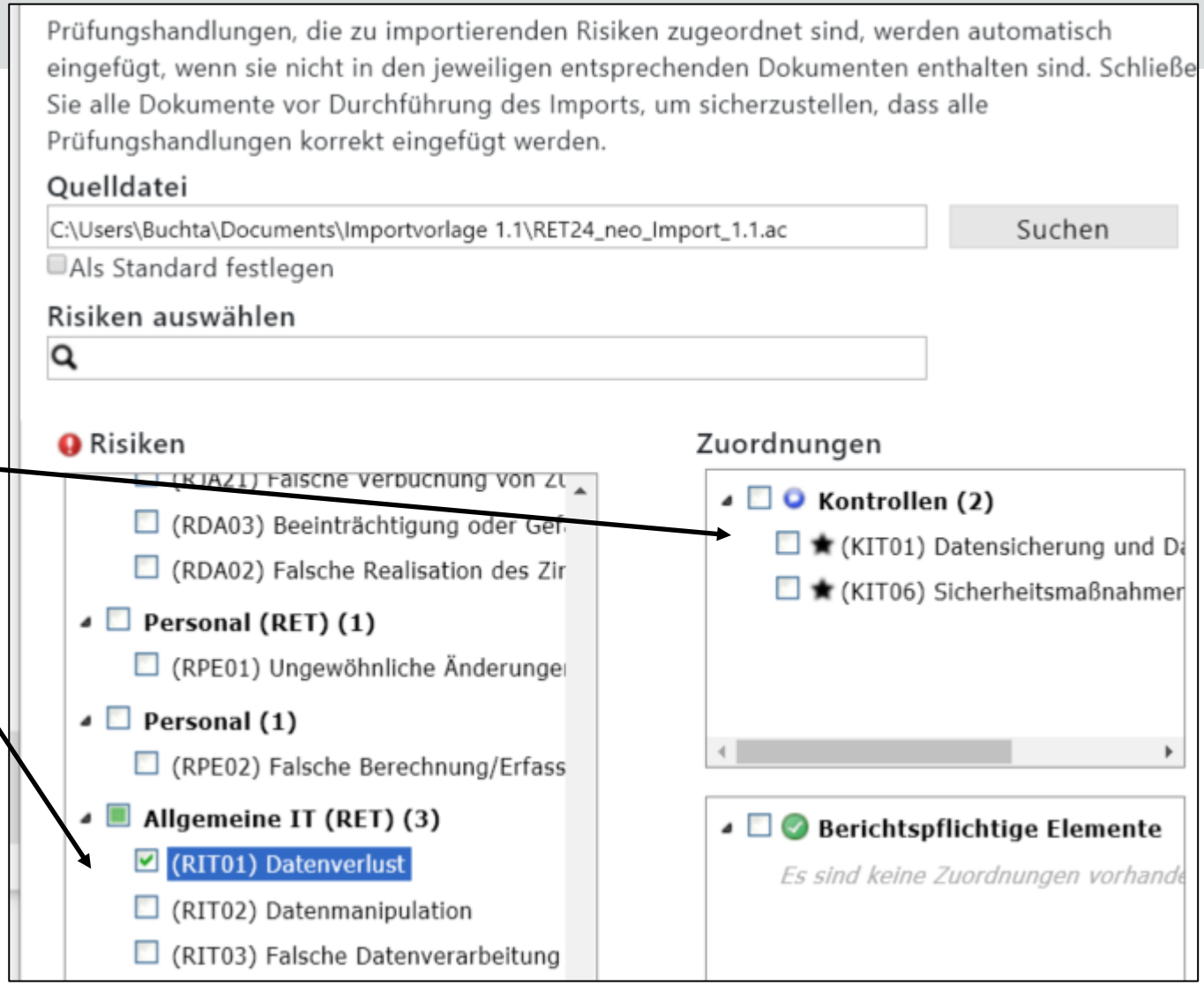
# VII. Erfassung von Risiken aus dem Einsatz von IT

## Auswahl der Quelldatei



# VII. Erfassung von Risiken aus dem Einsatz von IT

**Auswahl der Risiken und gleichzeitig der Kontrollen**

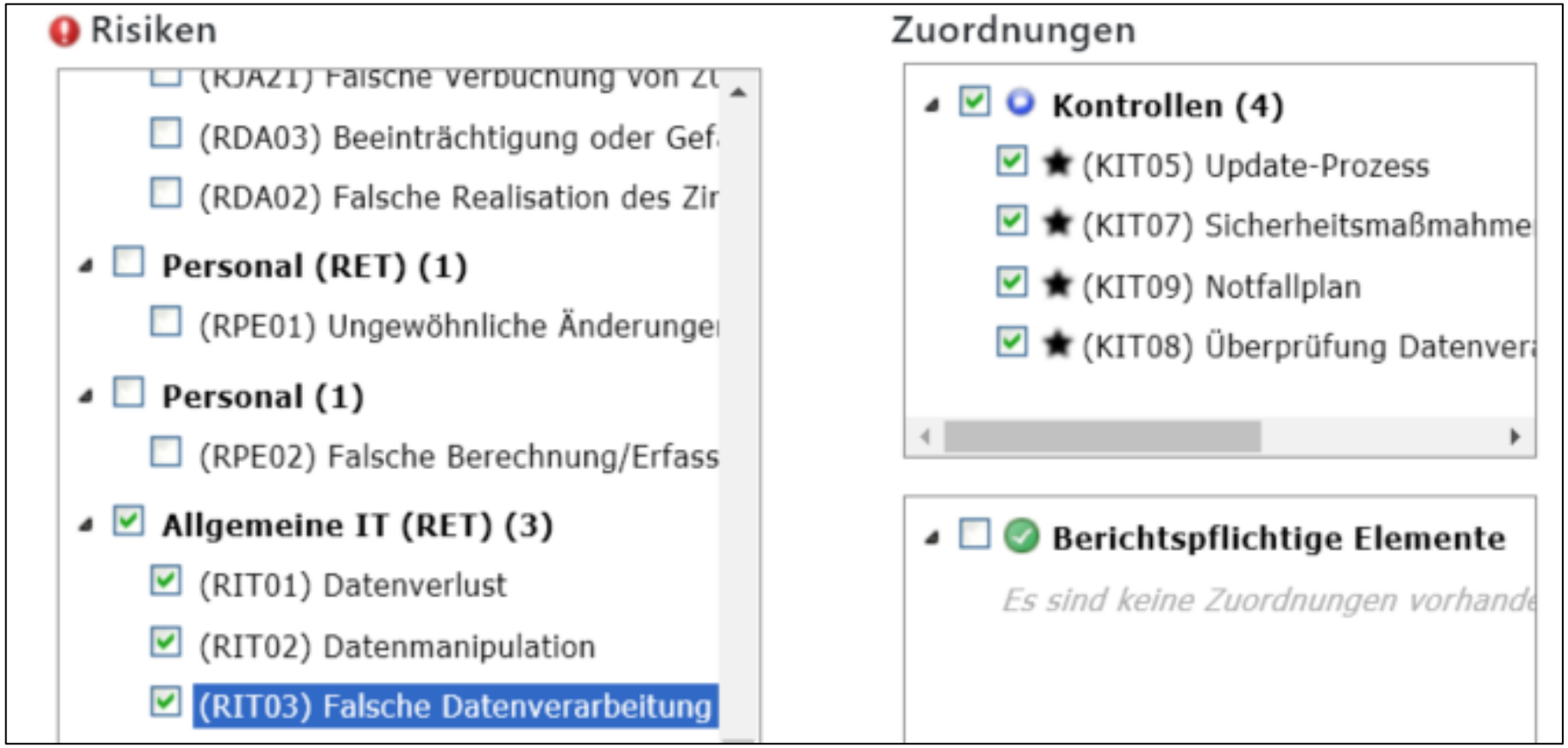


# VII. Erfassung von Risiken aus dem Einsatz von IT

Im Beispiel wurden alle IT-Risiken und Kontrollen importiert

Es handelt sich um die generellen IT-Kontrollen!

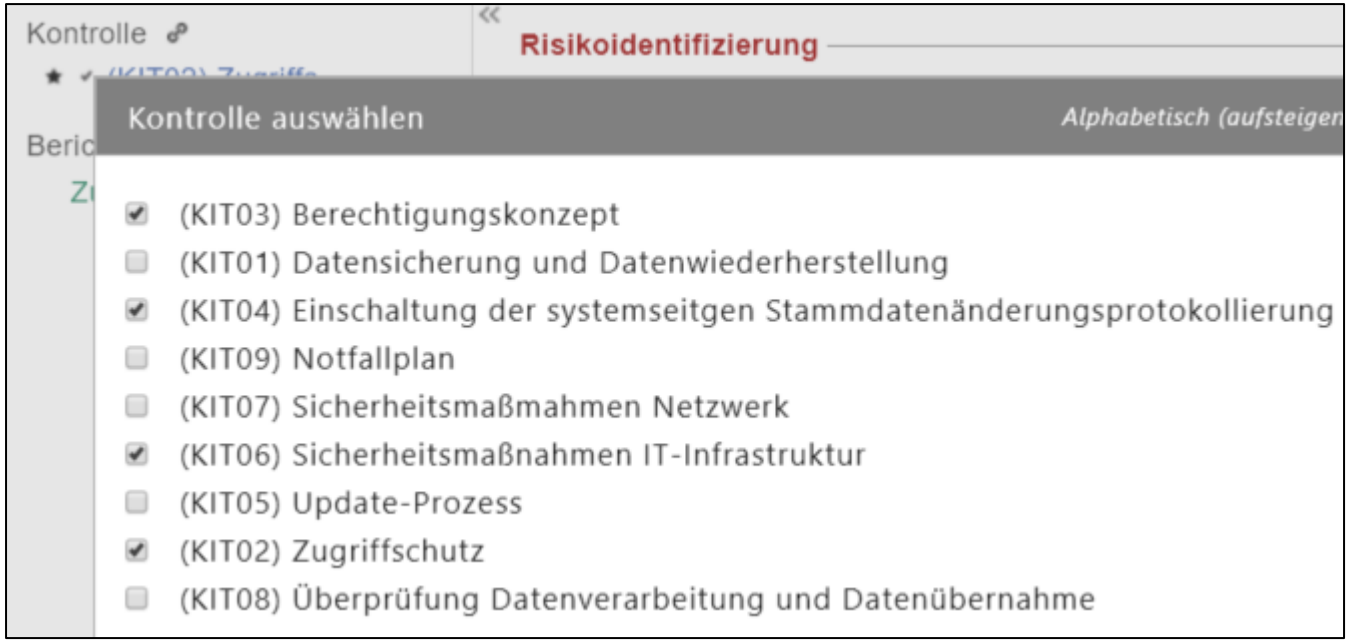
Nach der Auswahl "Übernehmen" und "OK" anklicken für jedes Risiko.



# VII. Erfassung von Risiken aus dem Einsatz von IT

**Manuelle Korrekturen:**

- **RIT01 muss die IT-Kontrolle KIT06 noch manuell zugeordnet werden.**
- **RIT02 müssen noch  die IT-Kontrollen KIT03, KIT04 und KIT06 manuell zugeordnet werden**
- **RIT03 müssen noch  die IT-Kontrollen KIT07, KIT08 und KIT09 manuell zugeordnet werden**

# VII. Erfassung von Risiken aus dem Einsatz von IT

## 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) |

# VIII. Erfassung von IT-Kontrollen und Funktionsprüfungen

# VIII. Erfassung von IT-Kontrollen und Funktionsprüfungen

**Es gibt folgende zwei Möglichkeiten IT-Kontrollen zu erfassen:**

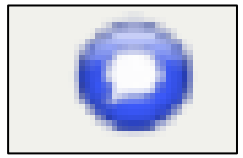
1) **Manuelle Erfassung**

2) **Kontroll-Import aus der Importvorlage (erfolgt i.d.R. gleichzeitig mit dem Import der IT-Risiken)**

# VIII. Erfassung von IT-Kontrollen und Funktionsprüfungen

## 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 566 und ORD.PP bzw. 566.ORD.MIN
- Erfassung IT-gestützter Kontrollen  in Bezug auf bestimmt Prüffelder bzw. Prozessen
- Erfassung von Report-Kontrollen in Bezug auf bestimmt Prüffelder bzw. Prozessen
- Zu sehen in der IKS-Risiko-Matrix 540 für Kontrollen auf Einheitenebene und allgemeine IT-Kontrollen sowie in den IKS-Risiko-Matrixen einzelner Prüffelder/Prozesse.
- Zu jeder Kontrolle ist auch ein Risiko erfasst.
- Erst danach werden die Funktionsprüfungen durchgeführt.

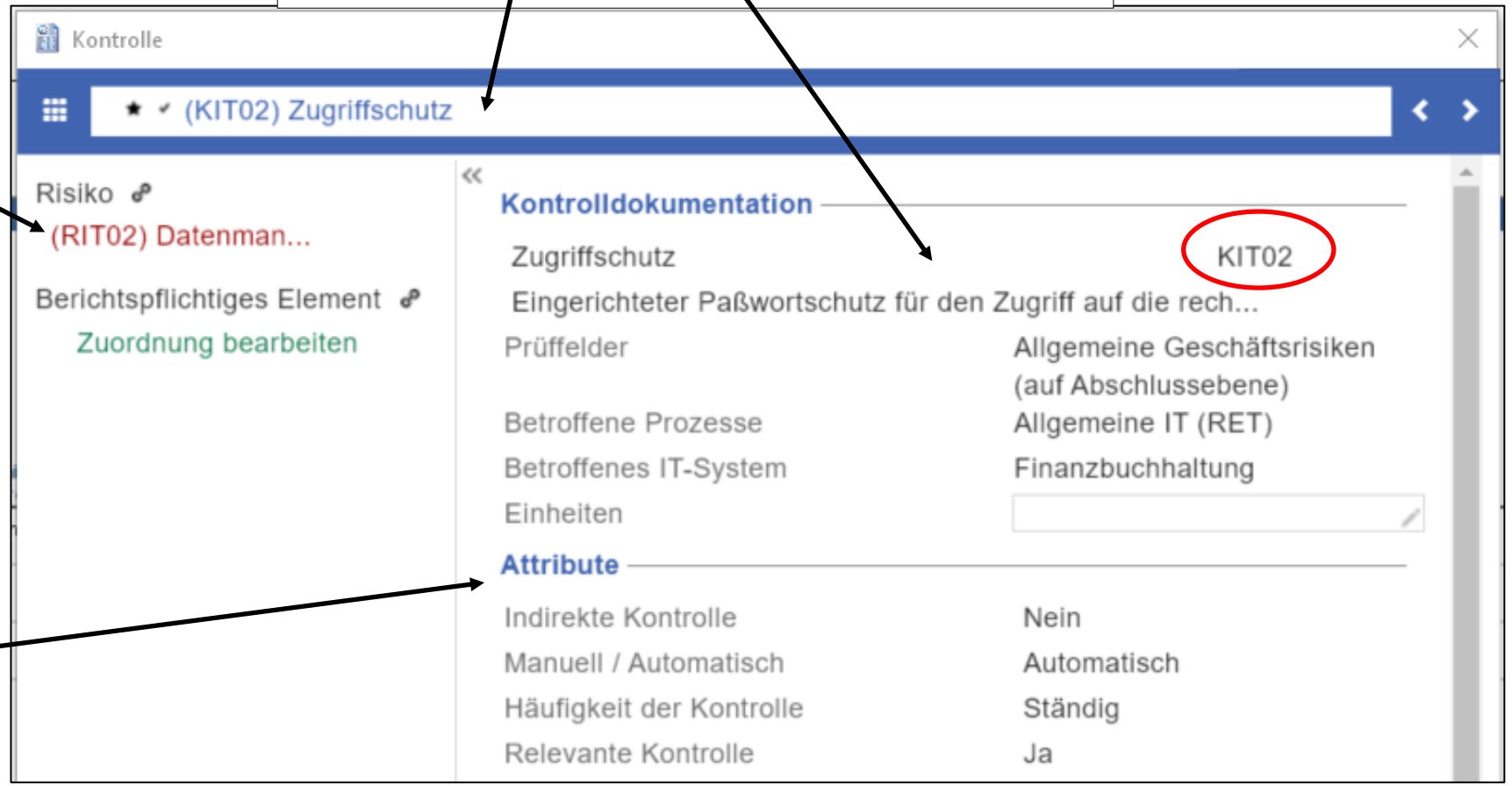


# VIII. Erfassung von IT-Kontrollen und Funktionsprüfungen

**Bezeichnung und Beschreibung der Kontrolle**

**Ver-knüpftes Risiko.**

**Eigenschaften der Kontrolle**

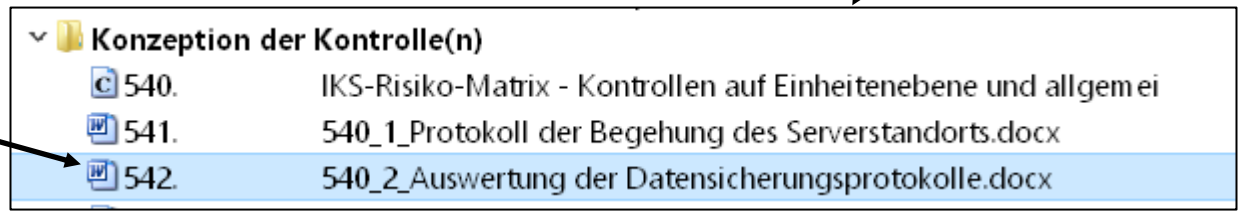


# VIII. Erfassung von IT-Kontrollen und Funktionsprüfungen

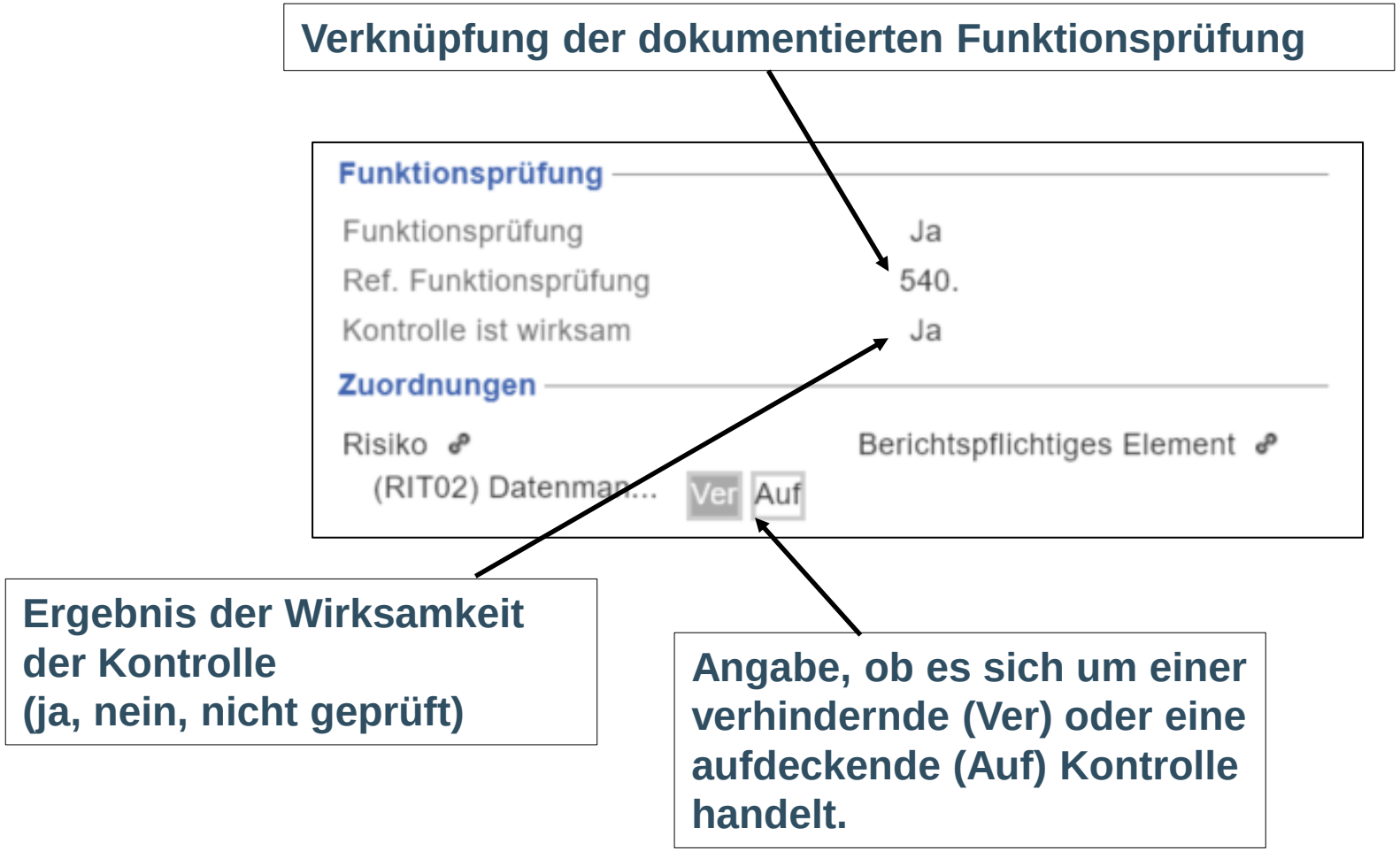
**Verknüpfung der Kontrolle mit der Aufbauprüfung**


**"zufriedenstellend" oder "nicht zufriedenstellend"**

**Referenz z. B. auf ein Word-Dokument möglich**

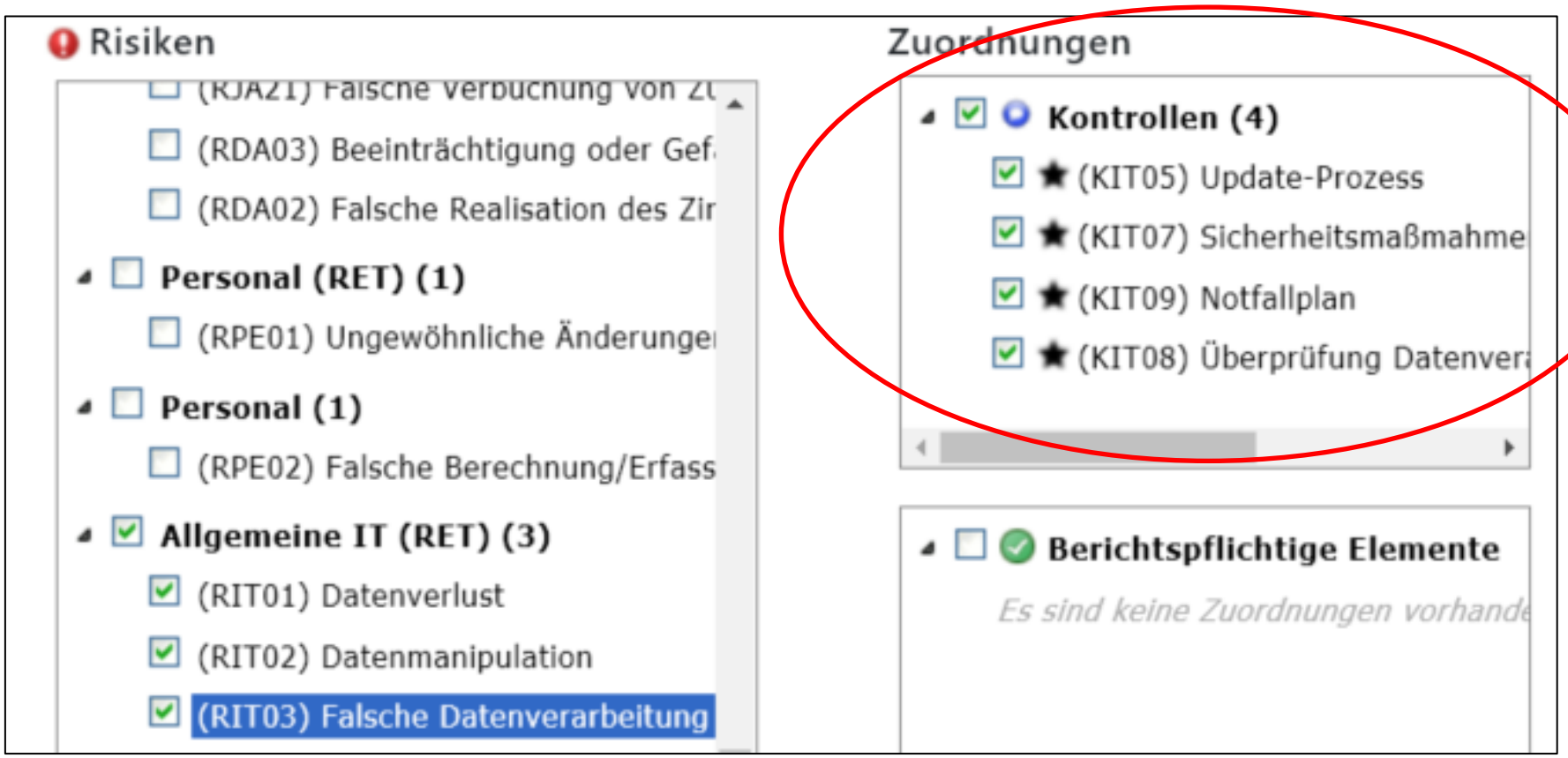


# VIII. Erfassung von IT-Kontrollen und Funktionsprüfungen



# VIII. Erfassung von IT-Kontrollen und Funktionsprüfungen

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

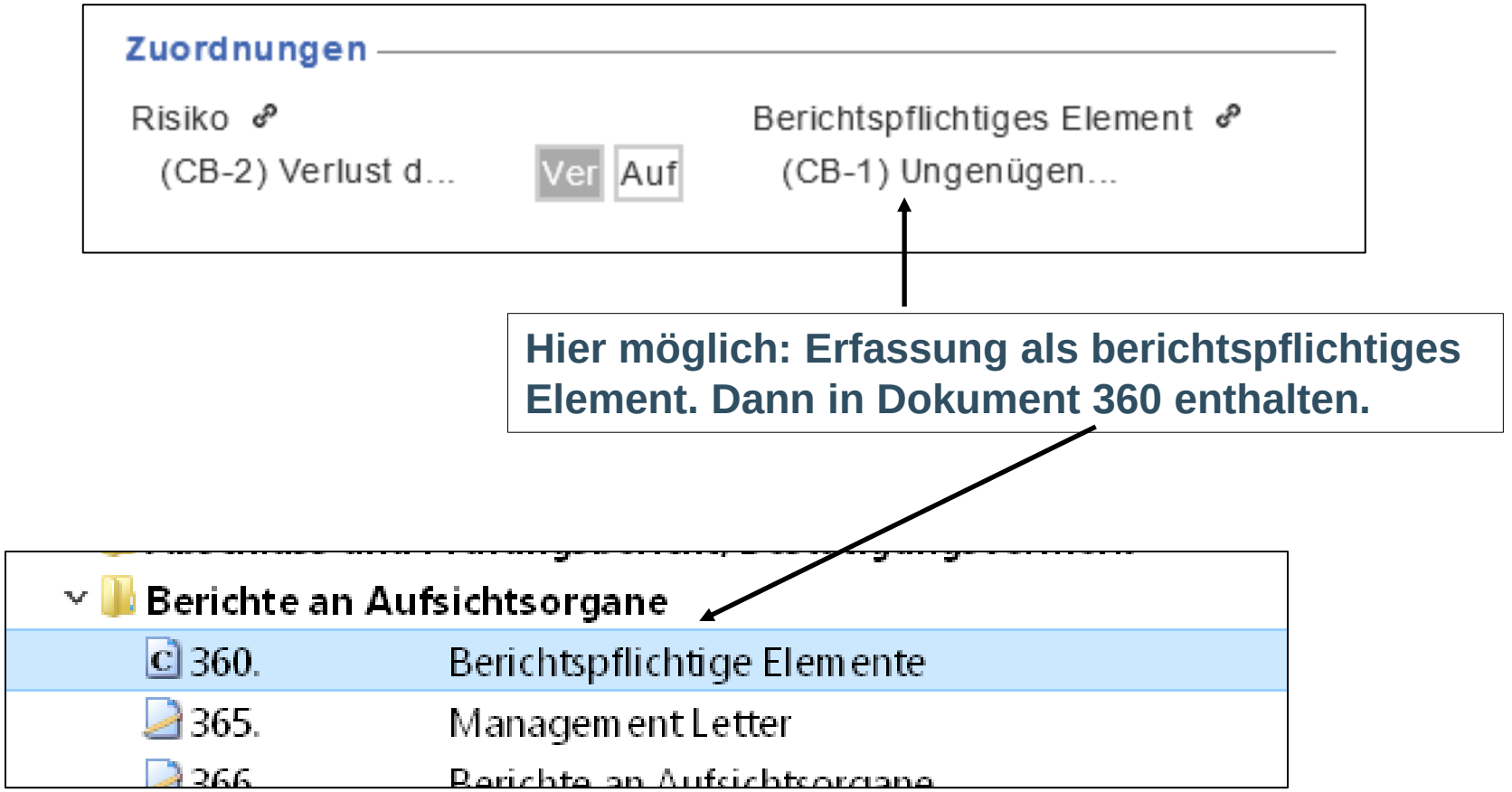


# VIII. Erfassung von IT-Kontrollen und Funktionsprüfungen

## 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) |

# VIII. Erfassung von IT-Kontrollen und Funktionsprüfungen



# VIII. Erfassung von IT-Kontrollen und Funktionsprüfungen

## Dokument 360 – Berichterstattung an den Aufsichtsrat

| Berichtspflichtige Elemente | Einheiten | Feststellungsdatum | Identifiziert von | Eingeschlossen in | | Begründung | Bewertung | Gruppier |
|---|---|---|---|---|---|---|---|---|
| | | | | Management Let... | Bericht für die f... | | | |
| **31.12.2017** | | | | | | | | |
| **Wesentliche Schwächen im internen Kontrollsystem** | | | | | | | | |
| (CB-1) Ungenügende Datensicherung | | 26.11.2018 | Claudia Buchta | Ja | Ja | Es läuft doch | Bedeutsam | |

# IX. Risiko-Kontroll-Matrix

**Zusammengefasste Darstellung in Dokument 540**

| | Kontrollen | Einheiten | Betroffenes IT-System | Feststellungsdatum | Ref. Walkthrough | Konzeption der Kontrolle(n) |
|---|---|---|---|---|---|---|
| 1 | (KIT01) Datensicherung und Datenwiederherstellung | | Finanzbuchhaltung | 08.11.2023 | | Zufriedenstellend |
| 2 | (KIT02) Zugriffschutz | | Finanzbuchhaltung | 08.11.2023 | | Zufriedenstellend |

# IX. Risiko-Kontroll-Matrix

**Zusammengefasste Darstellung in Dokument 540**

| Aufbauprüfung | | | | |
|---|---|---|---|---|
| Ref. Walkthrough | Konzeption der Kontrolle(n) | Kontrolle eingerichtet | Ergebnisse Walkthrough | Seit der vorherigen Bewertung geändert |
| | Zufriedenstellend | Ja | Zufriedenstellend | Nein |
| | Zufriedenstellend | Ja | | Nein |

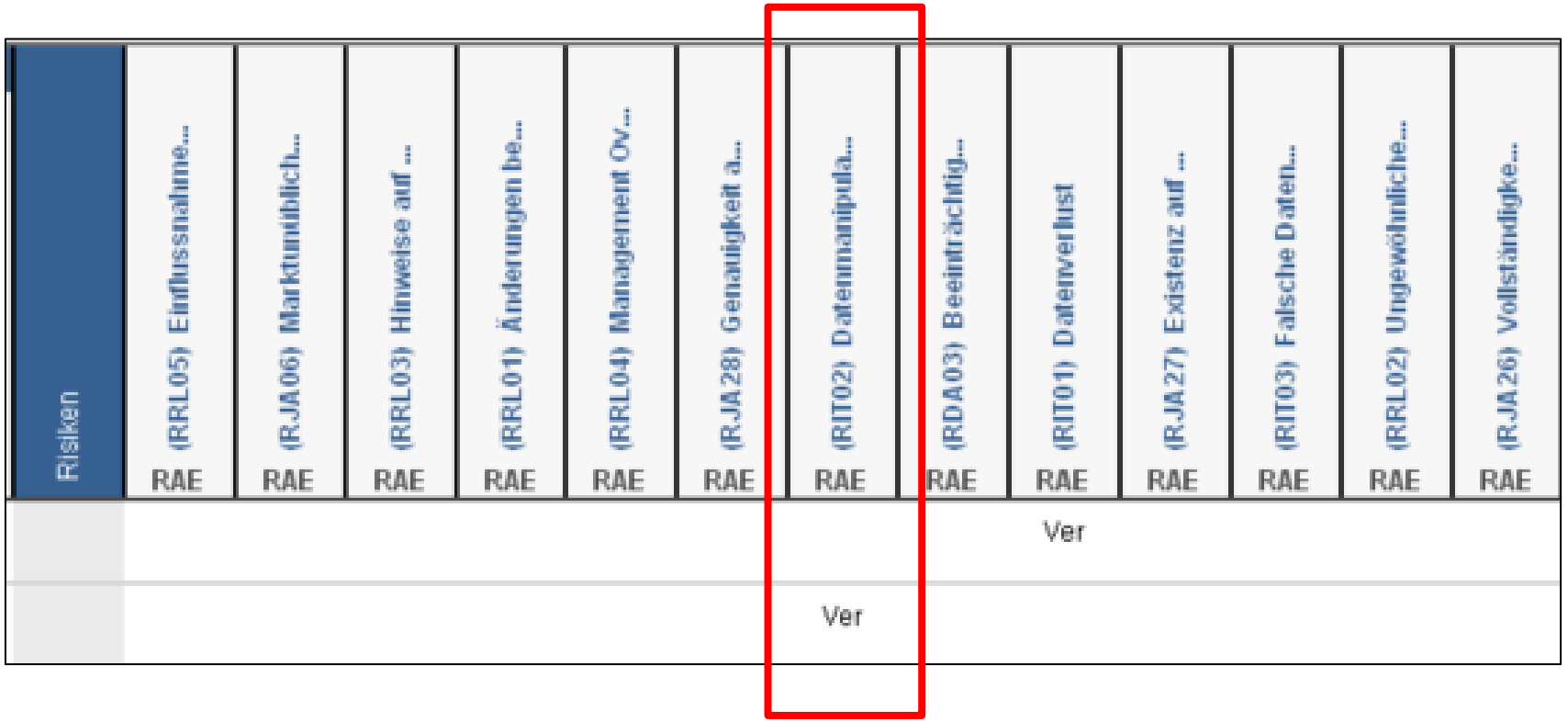
# IX. Risiko-Kontroll-Matrix

**Zusammengefasste Darstellung in Dokument 540**

| Kontrollattribute | | | | Funktionsprüfung | | | |
|---|---|---|---|---|---|---|---|
| Relevante Kontrolle | Indirekte Kontrolle | Manuell / Automatisch | Häufigkeit der Kontrolle | Funktionsprüfung | Ref. Funktionsprüfung | Kontrolle ist wirksam | Berichtspflichtiges Element |
| Ja | Ja | Manuell | Täglich | Ja | 540. | Ja | |
| Ja | Nein | Automatisch | Ständig | Ja | 540. | Ja | |

# IX. Risiko-Kontroll-Matrix

**Zusammengefasste Darstellung in Dokument 540**



# IX. Risiko-Kontroll-Matrix

## Alle Risiko-Kontroll-Matrixen in der RET Vorlage

# X. Zuordnung der IT-Risiken und generellen IT-Kontrollen

# X. Zuordnung der IT-Risiken und generellen IT-Kontrollen

**Wichtiger Hinweis:**

**Die Fragestellungen in 566, ORD.PP und 566.ORD.MIN können nicht direkt mit Risiken oder Kontrollen verknüpft werden!**

Lösungen:

- Es können entsprechende Referenzen zugefügt werden, z.B. 540 oder 520E.
- Ferner kann in der Beschreibung (grünes Kästchen) die Bezeichnung des IT-Risikos bzw. der IT-Kontrolle aufgenommen werden. Dies betrifft die generellen IT-Kontrollen.

# X. Zuordnung der IT-Risiken und generellen IT-Kontrollen

## Dokument 566

| | | |
|---|---|---|
| 2. | **Externe Prüfungsassistenz**<br>Wurden das IT-System auf Komplexität geprüft und die Notwendigkeit eines IT-Spezialisten berücksichtigt? | 566.KPL |

| | |
|---|---|
| 10. | **IT-Rollen und -Verantwortlichkeiten**<br>Existieren Richtlinien und Verfahren zur Definition IT-bezogener Rollen, Verantwortlichkeiten, Richtlinien, Standards und Verfahren sowie einer IT-Berichterstattung?<br>RIT02, KIT03 |

| | |
|---|---|
| 19. | **Sicherung**<br>RIT01, KIT01 |

| | |
|---|---|
| 20. | **Notfallpläne**<br>RIT03, KIT09 |
| a. | Existieren Pläne, um zu gewährleisten, dass kritische Geschäftsprozesse bei Unterbrechungen des normalen Geschäftsbetriebs fortgeführt bzw. unverzüglich wiederaufgenommen werden können? |

# X. Zuordnung der IT-Risiken und generellen IT-Kontrollen

## Dokument 566

| | |
|---|---|
| 22. | **Physischer Zugang**<br>Ist der physische Zugang zu IT-Systemen auf autorisiertes Personal beschränkt?<br>RIT03, KIT06 |

| | |
|---|---|
| 24. | **Logischer Zugang**<br>Ist der Zugang zu Anwendungen und Daten auf autorisiertes Personal beschränkt?<br>RIT03, KIT07 |
| 25. | **Passwortverwaltung**<br>Werden Passwörter unter Berücksichtigung folgender Punkte verwaltet?<br>▪ Einsatz personenbezogener Passwörter<br>▪ Generierung qualifizierter Kennwörter (Länge, Ziffern, Zeichen, Sonderzeichen)<br>▪ Regelmäßige erzwungene Passwortänderung<br>▪ Regelmäßige Passwortänderung oder aufgrund eines tatsächlichen oder vermuteten Sicherheitsverstoßes<br>▪ Deaktivierung bzw. Löschung von Benutzerkonten ausgeschiedener Mitarbeiter<br>RIT02, KIT02 |

# X. Zuordnung der IT-Risiken und generellen IT-Kontrollen

## Dokument 566

| | |
|---|---|
| 32. | **Änderungsprozess**<br>Existiert ein formell genehmigtes und überwachtes Verfahren für das Management von Änderungen an Hardware, Programmen, Datenbanken und Betriebssystemen?<br>RIT03, KIT05 |

| | |
|---|---|
| 39. | **Eingabevalidierungen**<br>Existieren Eingabekontrollen, um die vollständige und richtige Erfassung von Daten zu gewährleisten?<br>RIT03, KIT08 |

# X. Zuordnung der IT-Risiken und generellen IT-Kontrollen

## ORD.PP

| | |
|---|---|
| 6. | STAMMDATENPLEGE<br>Prüfen Sie, ob die Verfahren zur Anlage, Änderung und Löschung von Stammdaten den Grundsätzen ordnungsgemäßer Buchführung entsprechen (z.B. Vier-Augen-Prinzip, Genehmigung, Dokumentation).<br>RIT02, KIT04 |

| | |
|---|---|
| 10. | UNVERÄNDERBARKEIT DER DATEN<br>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).<br>RIT02, KIT04 |

# X. Zuordnung der IT-Risiken und generellen IT-Kontrollen

## 566.ORD.MIN

| | | |
|---|---|---|
| 2. | ANWENDBARKEIT<br>Liegen die in der Einführung beschriebenen Voraussetzungen für die Anwednung des Minimalprüfprogramms vor? | 566.KPL |

| | |
|---|---|
| 3. | IT-ROLLEN UND VERANTWORTLICHKEIT<br>Hat die Einheit Rollen und Verantwortlichkeiten für die IT definiert??<br>RIT02, KIT03 |

tenverwaltung

| | |
|---|---|
| 4. | SICHERUNG<br>RIT01, KIT01 |

# X. Zuordnung der IT-Risiken und generellen IT-Kontrollen

## 566.ORD.MIN

| | |
|---|---|
| 5. | NOTFALLPLÄNE<br>RIT03, KIT09 |

| | |
|---|---|
| 6. | PHYSISCHER ZUGANG<br>Ist der physische Zugang zu IT Systemen auf autorisiertes Personal beschränkt?<br>RIT03, KIT06 |
| 7. | LOGISCHER ZUGANG<br>Ist der Zugang zu Anwendungen und Daten auf autorisiertes Personal beschränkt?<br>RIT03, KIT07 |

# X. Zuordnung der IT-Risiken und generellen IT-Kontrollen

## 566.ORD.MIN

8. PASSWORTVERWALTUNG

Werden Passwörter unter Berücksichtigung folgender Punkte verwaltet?

- Einsatz personenbezogener Passwörter
- Generierung qualifizierter Kenntwörter (Länge, Ziffern, Zeichen, Sonderzeichen)
- Regelmäßige erzwungene Passwortänderung
- Regelmäßige Passwortänderung aufgrund eines tatsächlichen oder vermuteten Sicherheitsverstoßes
- Deaktivierung bzw. Löschung von Benutzerkonten ausgeschiedener Mitarbeiter

RIT02, KIT02

### Änderungsmanagement

9. ÄNDERUNGSPROZESS

Existiert ein formell genehmigtes und überwachtes Verfahren für das Management von Änderungen an Hardware, Programmen, Datenbanken und Betriebssystemen?

RIT03, KIT05

# X. Zuordnung der IT-Risiken und generellen IT-Kontrollen

## 566.ORD.MIN

| | |
|---|---|
| 11. | EINGABEVALIDIERUNGENGEN<br>Existieren Eingabekontrollen, um die vollständige und richtige Erfassung von Daten zu gewährleisten?<br>RIT03, KIT08 |
| 15. | STAMMDATENPLEGE<br>Prüfen Sie, ob die Verfahren zur Anlage, Änderung und Löschung von Stammdaten den Grundsätzen ordnungsgemäßer Buchführung entsprechen (z.B. Vier-Augen-Prinzip, Genehmigung, Dokumentation).<br>RIT02, KIT04 |
| 19. | UNVERÄNDERBARKEIT DER DATEN<br>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).<br>RIT02, KIT04 |

# X. Zuordnung der IT-Risiken und generellen IT-Kontrollen Übersicht

| Risiken aus dem Einsatz von IT | IT-Kontrolle | 566 | ORD.PP | 566.ORD.MIN |
|---|---|---|---|---|
| Datenverlust (RIT01) | Datensicherung und Datenwiderherstellung (KIT01) | 19 | | 4 |
| | Sicherheitsmaßnahmen IT-Infrastruktur (KIT06) | 22 | | 6 |
| Datenmanipulation (RIT02) | Zugriffsschutz (KIT02) | 25 | | 8 |
| | Einschaltung der systemseitgen Stammdatenänderungsprotokollierung (KIT04) | | 6, 10 | 15, 19 |
| | Sicherheitsmaßnahmen IT-Infrastruktur (KIT06) | 22 | | 6 |
| | Berechtigungskonzept (KIT03) | 10 | | 3 |
| Falsche Datenverarbeitung (RIT03) | Update-Prozess (KIT05) | 32 | | 9 |
| | Sicherheitsmaßmahmen Netzwerk (KIT07) | 24 | | 7 |
| | Überprüfung Datenverarbeitung und Datenübernahme (KIT08) | 39 | | 11 |
| | Notfallplan (KIT09) | 20 | | 5 |

# XI. Auslagerung rechnungslegungsrelevanter Prozesse

# XI. Auslagerung rechnungslegungsrelevanter Prozesse

**Für Überlegungen bei der Abschlussprüfung von Einheiten, die Dienstleister in Anspruch nehmen gilt nun der ISA [DE] 402.**

**Der ISA [DE] 402 ersetzt den IDW PS 331 n.F.!!**

**Aus ISA [DE] 402 ergeben sich keine neuen Anforderungen!**

**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.**

# XI. Auslagerung rechnungslegungsrelevanter Prozesse

**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**

# XI. Auslagerung rechnungslegungsrelevanter Prozesse

**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.**

# XI. Auslagerung rechnungslegungsrelevanter Prozesse

**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.**

# XI. Auslagerung rechnungslegungsrelevanter Prozesse

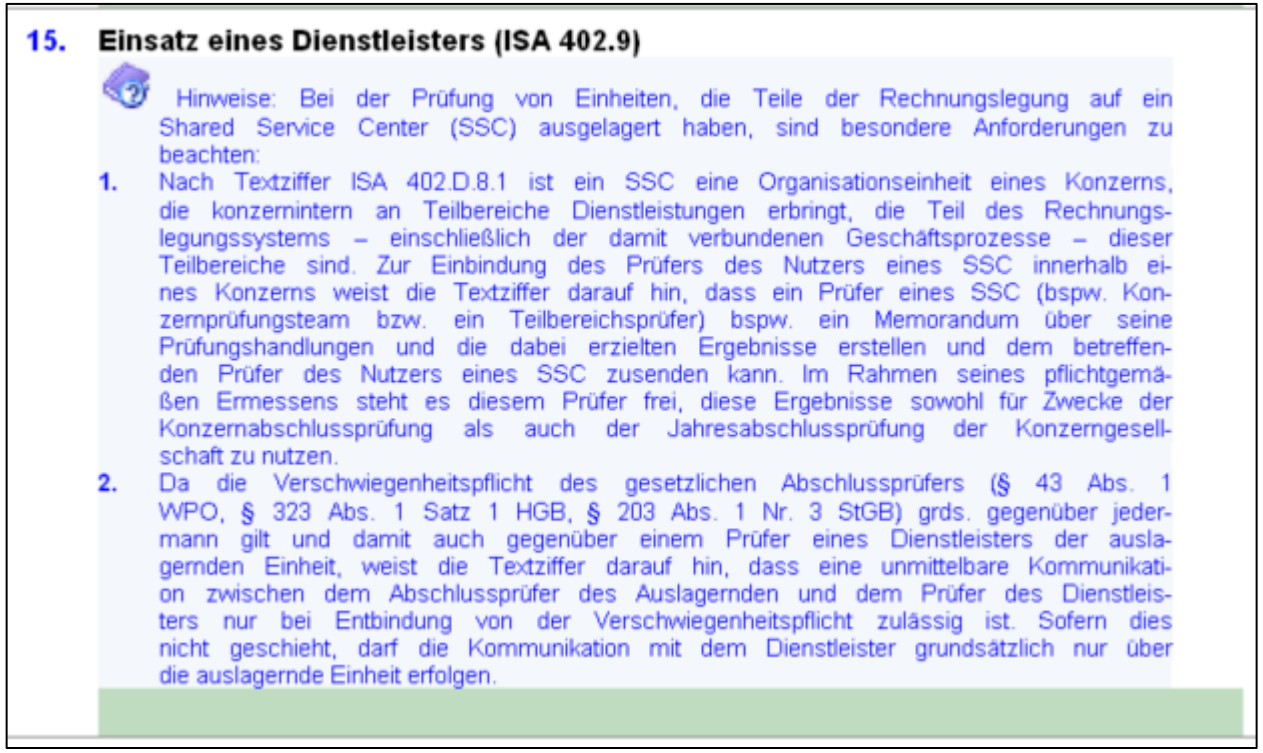
# XI. Auslagerung rechnungslegungsrelevanter Prozesse

**Das Verständnis, die Risikobeurteilung und ggf. weitere geplante Prüfungshandlungen ist hier zu dokumentieren:**

**MEMO.PA3 Frage 15**

**Hier ist jede Art der Auslagerung aufzunehmen.**

**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.**



**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 keine Auslagerungen vorliegen ist "n/a" einzutragen.**

# XI. Auslagerung rechnungslegungsrelevanter Prozesse

**Sind Teile der IT oder diese vollständig ausgelagert, sind weitere Schritte notwendig.**
**Z.B. Nutzung eines Rechenzentrums oder Cloud-Anwendungen**

**566.ORD.MIN Frage 22**

**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**

22. 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.

# XI. Auslagerung rechnungslegungsrelevanter Prozesse

**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.**

22. 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.

# XI. Auslagerung rechnungslegungsrelevanter Prozesse

**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**

# XI. Auslagerung rechnungslegungsrelevanter Prozesse

**Bei der Durchführung von Funktionsprüfungen – soweit eine Stützung auf Kontrollen bei dem Dienstleiters 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.**

# XI. Auslagerung rechnungslegungsrelevanter Prozesse

**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**

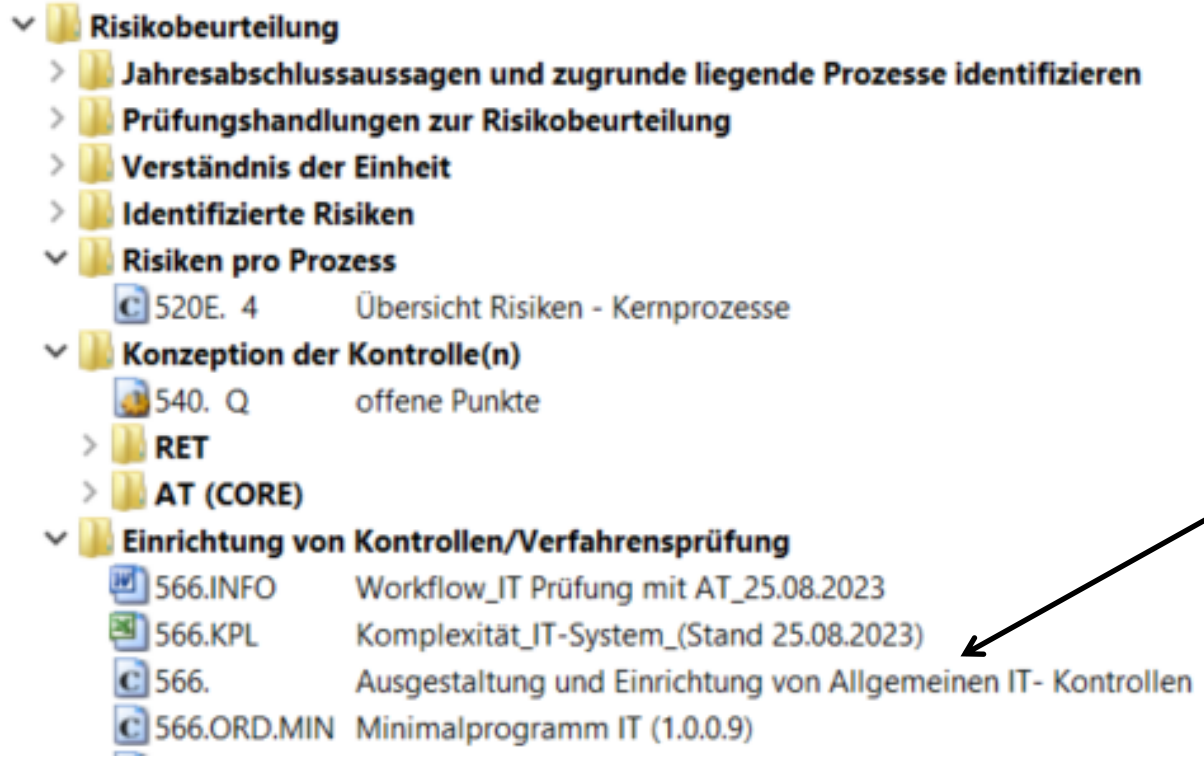
2) **Der Prüfer ist nicht in der Lage, ausreichende geeignete Prüfungsnachweise zu den von dem Dienstleister erbrachten Dienstleistungen zu erlangen, die für die Prüfung des Abschlusses der auslagernden Einheit relevant sind (ISA [DE] 402.20)**
   **=> dann Modifizierung des Bestätigungsvermerks/ZPE**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT-Kontrollen (566)

## Grundsatz - Wiederholung

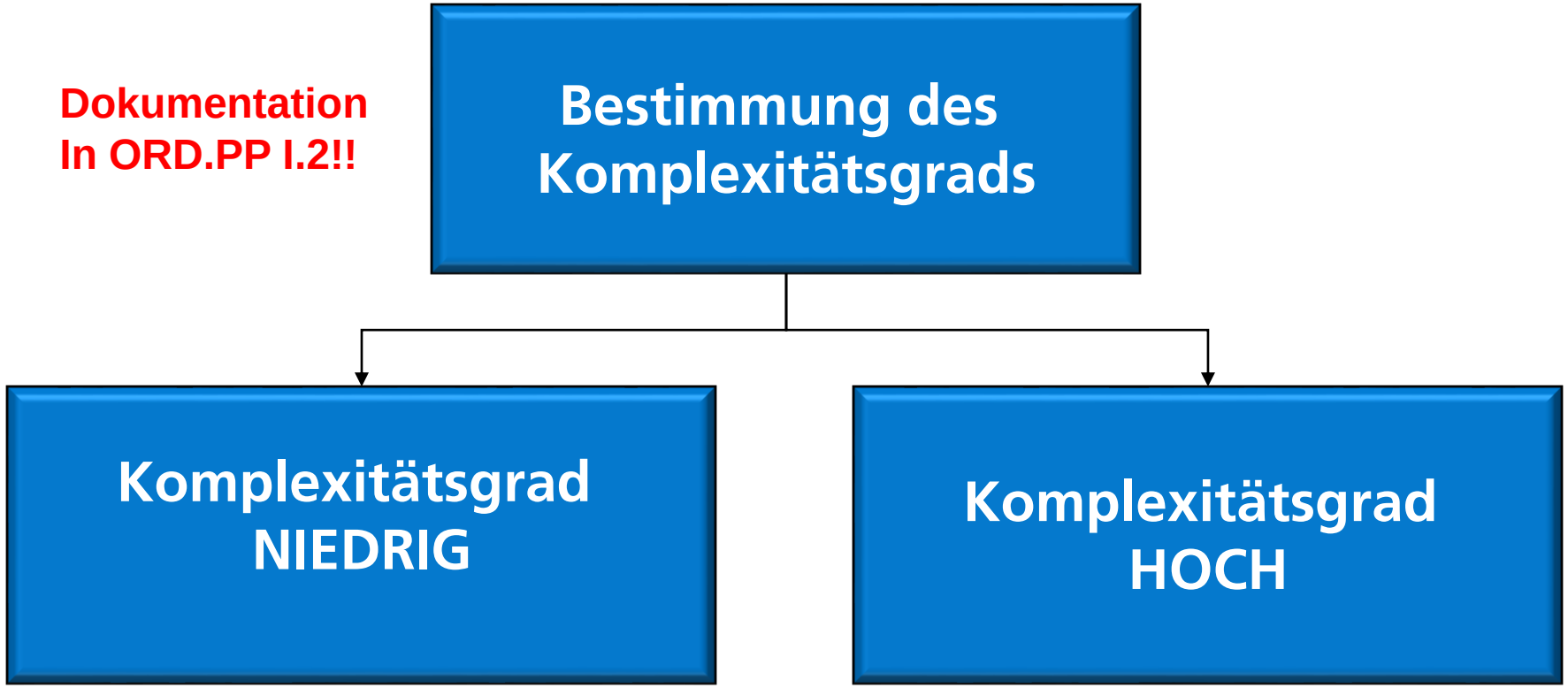



**Die Checkliste 566 ist bei jeder Prüfung zu bearbeiten, soweit nicht 566.ORD.MIN verwendet wird!**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Komplexitätsbeurteilung - Wiederholung

**Dokumentation In ORD.PP I.2!!**




566.ORD.MIN

566. ggf. Hinzuziehung von Spezialisten

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Grundlagen (1)

**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

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Grundlagen (2)

**Gefahren bei fehlenden oder ungenügenden Datensicherungs- und Auslagerungsverfahren**

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

**Die Ordnungsmäßigkeit der Buchführung ist gefährdet !**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Überblick über das IT-System

1. **Beschreibung** Ja

Haben Sie die allgemeinen Informationen über die IT-Umgebung der Einheit, einschließlich Hardware und Software, zusammengefasst?

## 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 19

(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)

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Überblick über das IT-System

| | | |
|---|---|---|
| 1. | **Beschreibung** | Ja |
| | Haben Sie die allgemeinen Informationen über die IT-Umgebung der Einheit, einschließlich Hardware und Software, zusammengefasst? | |

**Die Gesellschaft betreibt ein eigenes IT-System. Dieses umfasst auch im Rahmen einer Geschäftsbesorgung die Bereitstellung des IT-Systems für die Muttergesellschaft und die Umland WBG.**

**Die IT-Betreuung erfolgt weitestgehend durch eigene Mitarbeiter (3 Mitarbeiter). Zur Unterstützung im Bereich Hardware und Netzwerk hat die Gesellschaft einen Vertrag mit der Fa. Schnell abgeschlossen. In diesem sind auch entsprechende Reaktionszeiten definiert.**

**Derzeit umfasst das System 10 physische und 30 virtuelle Server (Win 2016/2019), ca. 50 Clients (Windows 10/11) 80 ThinClients (Linux), ca. 70 Android Smartphones bzw. 25 Mobile Geräte (Notebooks Win 10/11).**

**Als ERP-System wird Wodis Sigma (Fa. Aareon) in der derzeit aktuellen Version 12.0.22 gehalten (als SaaS im Rechenzentrum der Aareon in Mainz). Zur elektr. Archivierung wird Aareon Archiv kompakt und für die Personalbuchhaltung Sage HR Suite Enterprise (akt. Version 2021.3.0.1) verwendet. Entsprechende Supportverträge wurden mit den Softwareherstellern abgeschlossen. Für die Warenwirtschaft wird eine Eigenentwicklung genutzt.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Überblick über das IT-System

| | | |
|---|---|---|
| 2. | **Externe Prüfungsassistenz**<br>Wurden das IT-System auf Komplexität geprüft und die Notwendigkeit eines IT-Spezialisten berücksichtigt? | Ja |

**Es handelt sich um ein komplexes System mittler Größe. Neben der Standardsoftware Wodis Sigma 12.0 werden Eigenentwicklungen genutzt. Weiterhin werden weitere Gesellschaften „geschäftsbesorgt“. Ein IT-Prüfer wurde zur Unterstützung hinzugezogen.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Überblick über das IT-System

| | | |
|---|---|---|
| 3. | **Vorläufige Risikobeurteilung** | Ja |
| | Hat die Einheit während der Berichtsperiode... | |
| • | Änderungen an der IT-Umgebung vorgenommen? | |
| • | wichtige neue Betriebssysteme installiert oder Server hinzugefügt? | |
| • | eine wichtige Anwendung implementiert oder geändert? | |
| | Haben Sie – sollte dies der Fall sein – für jede Änderung dokumentiert, wie sie sich auf den Prüfungsplan auswirkt? | |

**Im Berichtsjahr wurden zwei Server ausgetauscht; 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.**

**Hier Aussage zur vorläufigen Risikobeurteilung!**

**z.B.: Das IT-Fehlerrisiko wird als gering eingeschätzt, da das IT-System bis auf den Austausch von zwei Servern zum Vorjahr unverändert ist. Ein IKS ist seitens der Geschäftsführung eingerichtet.**

**Hinweis: In der Schlussfolgerung von 566 sollte das zuvor eingeschätzte Risiko bestätigt werden oder anderes eingeschätzt.**

**Achtung: korrespondiert mit MEMO.PA4 1i. (ISA 315.26b/ISA 315.26c)!**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Dienstleister (1)

| | | |
|---|---|---|
| 4. | **Dienstleister**<br>Existiert eine eindeutig formulierte Vereinbarung, aus der die Hauptaspekte der getroffenen Absprachen hervorgehen? | Ja |

**Die Gesellschaft hat einen Support- und Wartungsvertrag mit der Aareon Deutschland GmbH abgeschlossen. Die ERP-Software wird in einem Rechenzentrum (kurz: RZ) der Aareon in Mainz betrieben. Zum RZ-Betrieb liegt ein Datenverarbeitungsvertrag mit AVB (Allgemeinen Vertrags-bedingen) vor.**

**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!**

**Bei Cloud-Diensten sind die Anforderungen der DSGVO nur sichergestellt, wenn die Server in Deutschland oder der EU stehen.**

**Amerika und Großbritannien gelten nicht als sichere Drittländer!**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Dienstleister (2)

| | | |
|---|---|---|
| 4. | **Dienstleister**<br>Existiert eine eindeutig formulierte Vereinbarung, aus der die Hauptaspekte der getroffenen Absprachen hervorgehen? | Ja |

**Verträge und Vereinbarungen (AGBs) müssen immer vorliegen. Besonders bei der Dienstleistung der System-administration 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.**

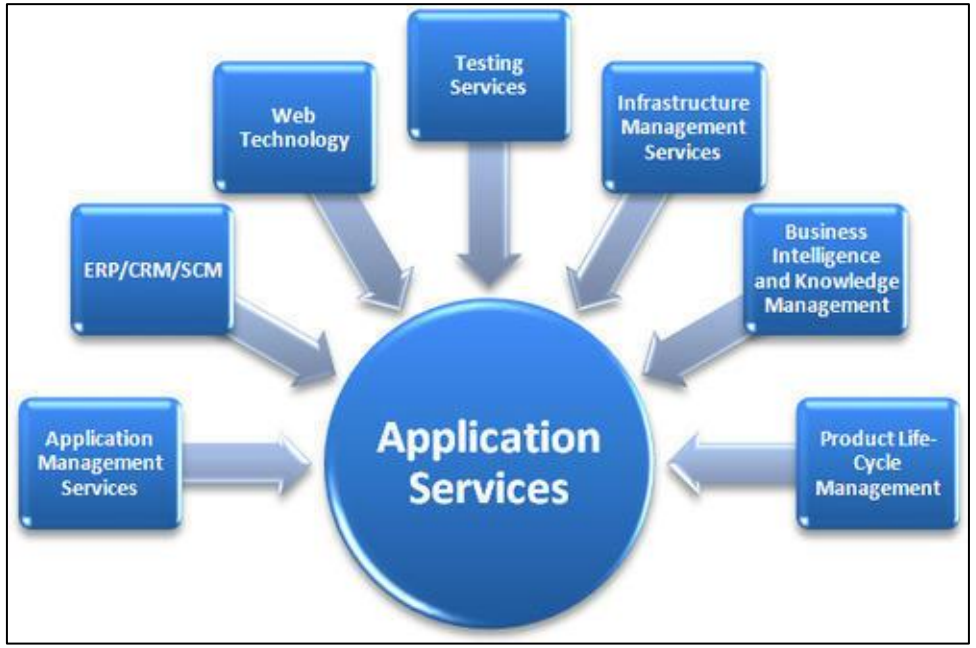
**Der Buchführende ist immer für die Daten verantwortlich, deshalb muss er sich durch geeignete Kontrollmaßnahmen von der Richtigkeit der Dienstleistung überzeugen.**

**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).**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Verträge mit Dienstleistern (ASP) - Exkurs



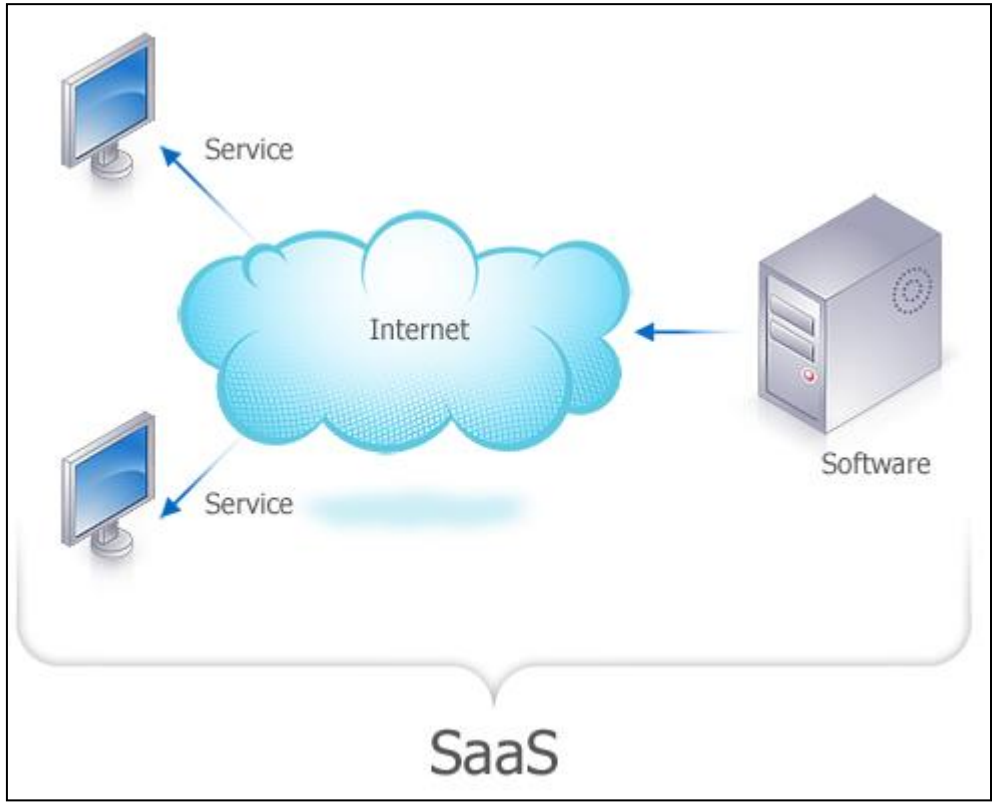

Bei einer ASP (Applikation Service Providing) Lösung laufen die Anwendungen in einem Rechenzentrum, die Anwendungen werden über eine spezielle Verbindung (Terminalserver-Technologie) zur Verfügung gestellt.

Jedem Betreiber wird eine individuelle Anwendung bereitgestellt

Die Software wird im Regelfall gemietet.

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Verträge mit Dienstleistern (SaaS) - Exkurs

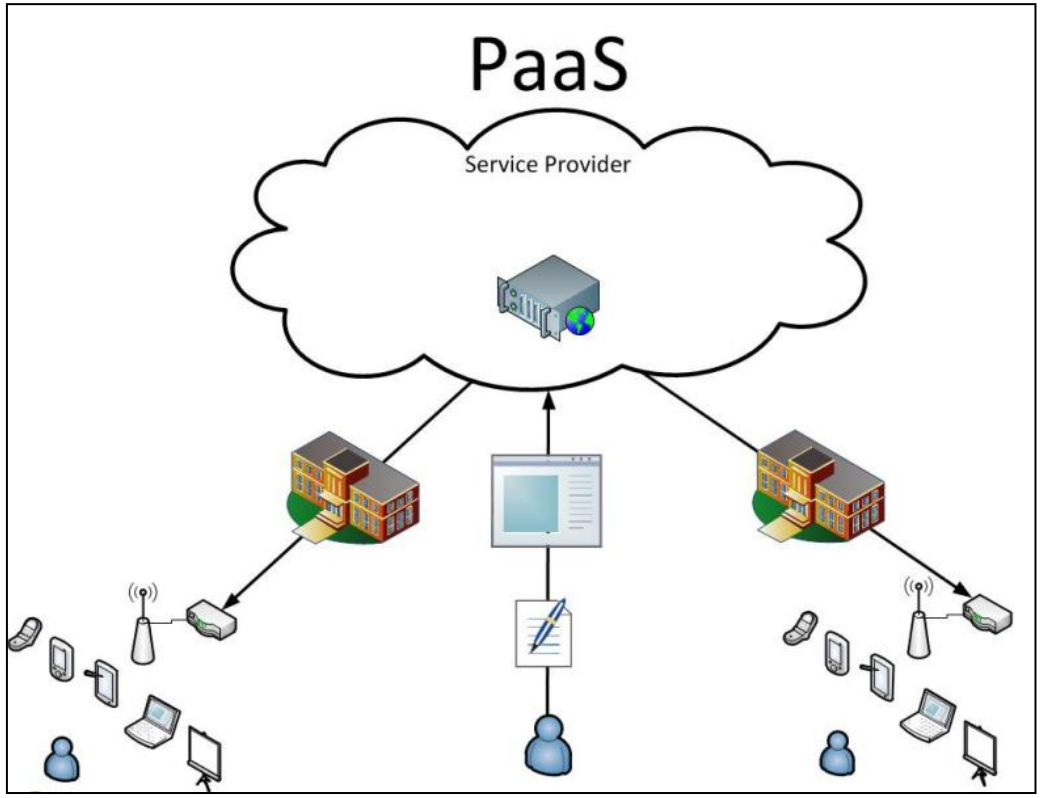



**Bei einer SaaS (Software as a Service) Lösung erfolgt der Zugriff auf die zentral (für eine Vielzahl von Kunden) bereitgestellten Anwendungen über das Internet und einen Browser.**

**Die Software wird im Regelfall gemietet.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Verträge mit Dienstleistern (PaaS) - Exkurs




Bei einer PaaS (Platform 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.

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Verträge mit Dienstleistern (IaaS) - Exkurs

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

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Verträge mit Dienstleistern (Server-Hosting) - Exkurs

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

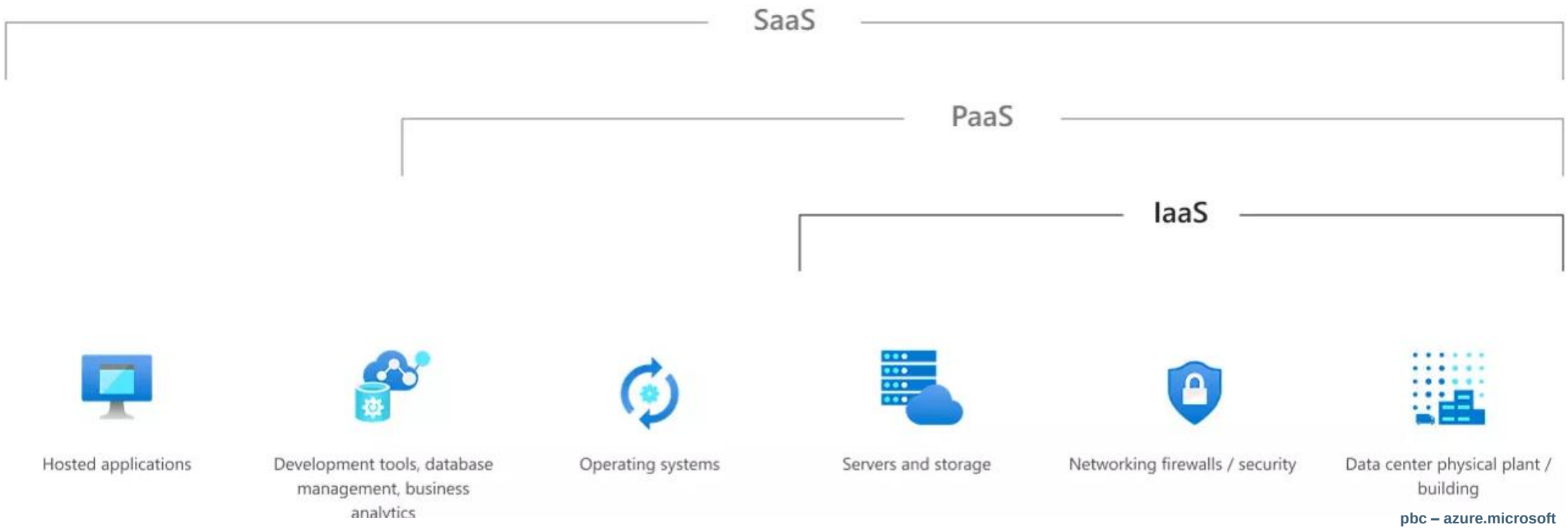
# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Verträge mit Dienstleistern (Serverhousing) (2) - Exkurs

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

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Verträge mit Dienstleistern - Überblick




pbc – azure.microsoft

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Dienstleister

5. **Einhaltung von IT-Richtlinien** Ja

Wird die Einhaltung der vertraglichen Vereinbarungen bzw. der SLA überwacht??

**Die Dienstleister müssen ihre Dienstleistungen regelmäßig dokumentieren (Zeitnachweise, Aufzeichnungen von Fernwartungssitzungen etc. Diese Unterlagen werden regelmäßig vom IT/EDV-Mitarbeiter des Unternehmens kontrolliert.**

**Servicelevel Agreement (SLA) ist eine Vereinbarung zwischen einem Servicegeber und Servicenehmer über Quantität und Qualität von Serviceleistungen.**

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

**Bestandteile eines SLA**

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

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Sonstiges

6. **E-Commerce**

Existieren geeignete Kontrollen im Hinblick auf...

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

| | | |
|---|---|---|
| a. | betrügerische Handlungen? | N/A |
| b. | den Datenschutz? | N/A |
| c. | die Verarbeitung von Geschäftsvorfällen, einschließlich Maßnahmen zur Vermeidung diesbezüglicher Doppelungen oder Versäumnisse? | N/A |

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Sonstiges

| | | |
|---|---|---|
| 7. | **EDI** | N/A |
| | Existieren geeignete Vereinbarungen und Protokolle den elektronischen Informations-austausch (EDI) betreffend? | |

**EDI-Verfahren werden nicht genutzt.**

**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.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

8. **Strategie** Ja

Trägt das Management Verantwortung für die Entwicklung und Fortschreibung der IT-Strategie?

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

**Mindestinhalte der IT-Strategie sind:** **oft Bestandteil des RMS – bei Großunternehmen**

(a) **Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation sowie IT-Dienstleistungen und sonstige wichtige Abhängigkeiten von Dritten**

(b) **Strategische Entwicklung der IT-Architektur**

(c) **Zuordnung der gängigen Standards**

(d) **Ziele, Zuständigkeiten und Einbindung der Informationssicherheit**

(e) **Aussagen zum IT-Notfallmanagement**

(f) **Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hardware- und Software-Komponenten).**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

| | | |
|---|---|---|
| 9. | **IT-Plan**<br>Erfolgt ein Abgleich der aktuellen IT-Aktivitäten mit dem IT-Plan (kurz- und mittelfristig? | Ja |

**Es liegt für den IT-Bereich ein langfristiger Investitions- und ein kurzfristiger Umsetzungsplan (Bestandteil des Wirtschaftsplans) vor. Durch regelmäßige Berichterstattungen des IT-Verantwortlichen kann sich die Geschäftsführung jederzeit ein aktuelles Bild der Umsetzung der IT-Planung machen.**

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

**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

**Planung sollte über den Zeitraum der IT-Strategie und jährlich erfolgen (Bestandteil des Wirtschaftsplanes)**

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

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

10. **IT-Rollen und -Verantwortlichkeiten**

Existieren Richtlinien und Verfahren zur Definition IT-bezogener Rollen, Verantwortlichkeiten, Richtlinien, Standards und Verfahren sowie einer IT-Berichterstattung?

**Die Gesellschaft hat Benutzerrichtlinien erlassen und eine Funktionstrennung eingerichtet. Die Berichterstattung erfolgt mündlich in regelmäßigen Geschäftsführerrunden und bei Bedarf.**

a. Hat die Einheit Rollen und Verantwortlichkeiten für die IT definiert? Ja

**Über Benutzerrichtlinien sind entsprechende Rollen im Netzwerk und auf ERP-Systemebene definiert.**

b. Werden die Richtlinien und Verfahren zur Definition IT-bezogener Rollen und Verantwortlichkeiten umgesetzt? Ja

**Aufgrund der Unternehmensgröße gibt es keine Definition und von Verfahren zur Definition IT-bezogener Rollen. Es gibt jedoch eine klare Trennung der Rollen von Admin-Aufgaben und laufender Tätigkeiten des IT-Mitarbeiters.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

11. **IT-Sicherheitsrichtlinie**

a. Existiert eine formelle IT-Sicherheitsrichtlinie, die von der zuständigen Führungsebene genehmigt und den Mitarbeitern bekanntgegeben wurde? — Ja

**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 der Größe und Komplexität der Einheit angemessen? — Ja

**ja, diese entspricht den Anforderungen der Gesellschaft und orientiert sich am IT-Grundschutzkatalog des BSI**

c. Wird die Umsetzung der IT-Sicherheitsrichtlinie überwacht? — Ja

**Jährlich erfolgt eine IT-Analyse durch den IT-Mitarbeiter, er berichtet bei Bedarf in Dienstberatungen, für Unternehmensgröße hinreichend**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

11. IT-Sicherheitsrichtlinie

### Exkurs (1) – Aufbau einer IT-Sicherheitsrichtlinie

| | |
|---|---|
| 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 |

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

11. **IT-Sicherheitsrichtlinie**

### Exkurs (1) – Aufbau einer IT-Sicherheitsrichtlinie - 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 |

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

| | | |
|---|---|---|
| 12. | **Überwachung der Wirksamkeit** | Ja |
| | Werden regelmäßig IT-Kontrollen auf ihre Wirksamkeit überprüft und die diesbezüglichen Ergebnisse dem Management gemeldet? | |

**Das Management oder die interne Revision führen in regelmäßigen Abständen Kontrollen durch.**

**Ein Internes Kontrollsystem (IKS) besteht aus systematisch gestalteten technischen und organisatorischen Regeln des methodischen Steuerns und von Kontrollen im Unternehmen zum Einhalten von Richtlinien und zur Abwehr von Schäden.**

**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**

**Regelmäßige Treffen mit der Geschäftsführung gibt es dazu nicht, Probleme sollten jedoch sofort kommuniziert werden.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

| | | |
|---|---|---|
| 13. | **Kompetenzen des IT-Personals**<br>Kann nachgewiesen werden, dass das IT-Personal angemessen geschult wird und seine Kenntnisse stets den erforderlichen Stand aufweisen? | Ja |

**Der IT-Mitarbeiter lässt sich regelmäßig schulen, des Weiteren bestehen Supportvereinbarungen mit IT-Dienstleistern die in jedem Fall aktuelle Kenntnisse zu den Systemen haben.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

| | | |
|---|---|---|
| 14. | **Dokumentation von Anwendungen**<br>Liegen Dokumentationen vor, in denen die Methoden zur ordnungsgemäßen Verarbeitung von Geschäftsvorfällen in jeder Anwendung erläutert werden? | Ja |

**vgl. Softwaretestat Wodis Sigma, Mareon (Handwerkerkopplung) und Archiv kompakt, es liegt eine entsprechende Anwenderdokumentation sowie eine Betriebsdokumentation vor**

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

**(a) Allgemeine Beschreibung**

**(b) 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.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

| | | |
|---|---|---|
| 14. | **Dokumentation von Anwendungen**<br>Liegen Dokumentationen vor, in denen die Methoden zur ordnungsgemäßen Verarbeitung von Geschäftsvorfällen in jeder Anwendung erläutert werden? | Ja |

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

**(a) 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.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

| | | |
|---|---|---|
| 14. | **Dokumentation von Anwendungen**<br>Liegen Dokumentationen vor, in denen die Methoden zur ordnungsgemäßen Verarbeitung von Geschäftsvorfällen in jeder Anwendung erläutert werden? | Ja |

**Die Dokumentation der Anwendung umfasst mindestens folgende Inhalte:**

**(a) 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.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

15. **Automatisierte Prozesse**

**keine derartigen Prozesse, Prozesse wie die Sollstellung, Abschreibungen, Aktivierung unfertige Leistungen etc. laufen nicht selbständig und unterliegen einer Kontrolle/ Freigabe**

| | | |
|---|---|---|
| a. | Werden automatisierte Prozesse, sofern sich die Einheit auf solche stützt, überwacht? | N/A |
| b. | Werden Abweichungsberichte generiert und wie werden diese behandelt? | N/A |

**Beispiele für automatisierte Prozesse können bspw. die Verbuchung der Bestandserhöhung/unfertige Leistungen bei den Betriebskosten oder auch die Darlehenssollstellung sein. Bei manchen Systemen erfolgt auch die mtl. Sollstellung der Mieten oder auch Mieterhöhungen voll automatisiert.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Organisation und Management auf Unternehmens- und IT-Ebene

| | | |
|---|---|---|
| 16. | **Lizenzierung**<br>Werden geeignete Verfahren eingesetzt, um zu gewährleisten, dass Gesetze und Vorschriften, die sich auf die Lizenzierung und auf den Umgang mit wesentlichen urheberrechtlichen bzw. immaterialgüterrechtlichen Sachverhalten beziehen, eingehalten werden? | Ja |

**Die Überwachung der ordnungsgemäßen Lizenzierung erfolgt durch den IT-Mitarbeiter. Er führt entsprechende Listen und gleicht diese regelmäßig ab.**

**Exkurs - Überwachung von Lizenzen ist 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 wir Lizenzen vorhanden sind (insbesondere bei SaaS-Lösungen).**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

17. **Klassifizierung und Vertraulichkeit von Daten** Ja

Sind Richtlinien bzw. Methoden vorhanden und dokumentiert, die sicherstellen, dass die Informationen bzw. Daten nur Berechtigten verfügbar sind?

**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 - In der Wohnungswirtschaft wird durch die verwendeten ERP-Systeme im Rahmen des Berechtigungsmanagements bereits eine einfache Datenklassifizierung der rechnungsrelevanten Daten vorgenommen.**

**Die Unternehmen sollten für sich eine Datenklassifizierung konzipieren, um sicherzustellen, dass alle verarbeiteten Daten klassifiziert werden.**

**Die DSGVO fordert eine Datenklassifizierung (auch wegen des Löschkonzepts) für personenbezogene Daten, das Gesetz zum Schutz von Geschäftsgeheimnissen auch für die anderen Daten.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

### 18. Verfügbarkeit der Daten

**Die Gesellschaft hat Maßnahmen ergriffen und dokumentiert, die die gesetzlichen Aufbewahrungsfristgen sicherstellen (vgl. IT-Sicherheitskonzept)**

| | | |
|---|---|---|
| a. | Sind Richtlinien bzw. Methoden vorhanden und dokumentiert, die sicherstellen, dass die Daten über die gesetzlichen oder vertraglichen Aufbewahrungsfristen verfügbar sind? | Ja |

**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 Daten auf geeigneten Datenträger unter Beachtung von Vertraulichkeit und Verfügbarkeit ausgelagert? | Ja |

**Es erfolgt eine Auslagerung einer Bandsicherung in ein Bankschließfach entsprechend des Datensicherungskonzeptes. Weiterhin erfolgen laufend Datensicherungen auf Festplatten, welche im Serverraum sowie in einem Tresor gelagert werden.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

### 18. Verfügbarkeit der Daten

**Exkurs - Tresor**

**Werden die Datensicherungen so gelagert, dass nur autorisierte Personen Zugriff haben?**
**Sind die Daten vor Zerstörung durch Feuer gesichert?**
**Ein normaler Tresor ist für Datenträger (CD, DVD, Magnetbänder, Festplatten etc.) nicht geeignet!**

**Wie lange ist der Tresor feuerfest?**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Exkurs: Feuerfeste Tresore


Prüfsiegel Datensicherungsschrank

**Angabe der Feuerschutzgüteklasse**

*Tresor nach Feuertest*

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Exkurs: Feuerfeste Tresore

**Feuerschutzgüteklassen**

**Papier**

S 60 P // Schrank / **60** Minuten / **P**apier
Der Schrank wurde 60 Minuten bei 960° C getestet, ohne dass die Temperatur während der Erhitzung und der folgenden Abkühlungsphase im Schrankinnenraum über 150 ° C gestiegen ist. Papier bleibt vollständig erhalten.

S 120 P // Schrank / **120** Minuten / **P**apier
Der Schrank wurde 120 Minuten bei 1090 ° C getestet, ohne dass die Temperatur während der Erhitzung und der folgenden Abkühlungsphase im Schrankinnenraum über 150° C gestiegen ist. Papier bleibt vollständig erhalten.

**Datenträger**

S 60 DIS // Schrank / **60** Minuten / **DIS**ketten
Der Schrank wurde 60 Minuten bei 960 ° C getestet, ohne dass sich die Temperatur im Schrankinnenraum während der Erhitzung und der folgenden Abkühlungsphase um mehr als 30 ° C erhöht hat. Disketten (und alle magnetischen Datenträger) bleiben vollständig erhalten und nutzbar.

S 120 DIS // Schrank / **120** Minuten / **DIS**ketten
Der Schrank wurde 120 Minuten bei 1090 ° C getestet, ohne dass sich die Temperatur im Schrankinnenraum während der Erhitzung und der folgenden Abkühlungsphase um mehr als 30 ° C erhöht hat. Disketten (und alle magnetischen Datenträger) bleiben vollständig erhalten und nutzbar.

**! Tresore sterben langsam aus – Zukunft: Cloud-Sicherungen!**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

### 19. Sicherung

**Es existiert ein Datensicherungskonzept für die lokalen Server. Die Daten vom ERP-System, Handwerkerkopplung und Archivsystem werden im Rechenzentrum gehalten. Dazu liegen vertragliche Regelungen mit dem RZ-Betreiber (Fa. Aareon) vor.**

a. Existieren geeignete Richtlinien und Verfahren zur Sicherung von Systemen, Anwendungen, Daten und Dokumentationen? — Ja

**Es liegt ein Datensicherungskonzept für die lokalen Server und es bestehen vertragliche Regelungen mit dem RZ-Betreiber (Fa. Aareon).**

b. Werden die Richtlinien regelmäßig überarbeitet und ordnungsgemäß dokumentiert? — Ja

**Eine interne Überprüfung findet in der Regel jährlich statt. Für das Rechenzentrum liegt ein Testat nach IDW PS 951 Typ 2 vor.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

### 19. Sicherung

**Exkurs Datensicherung (1)**

**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?**

**Datensicherungen sollten in einen anderen Brandabschnitt ausgelagert werden!**

**– NICHT bei Mitarbeitern zu Hause! –**

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

- **Vollsicherung?**
- **Inkrementelle Sicherung?**
- **Differentielle Sicherung?**
- **Generationenprinzip?**

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

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

**Exkurs Datensicherung (2)**

**Wesentliche Arten der Sicherung**

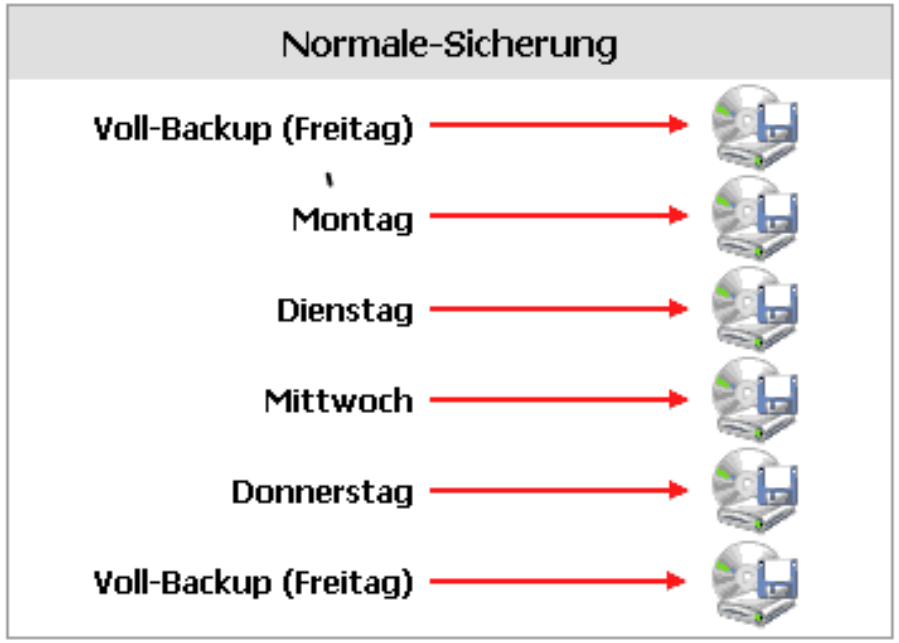
- **Differenzialsicherungen**
  - Sicherung der seit dem letzten kompletten Backup geänderten Daten
- **Inkrementelle Sicherungen**
  - Sicherung nur der seit der letzten Datensicherung geänderten Daten
- **Komplettsicherungen**
  - Sicherung aller Daten unabhängig von der letzten Sicherung

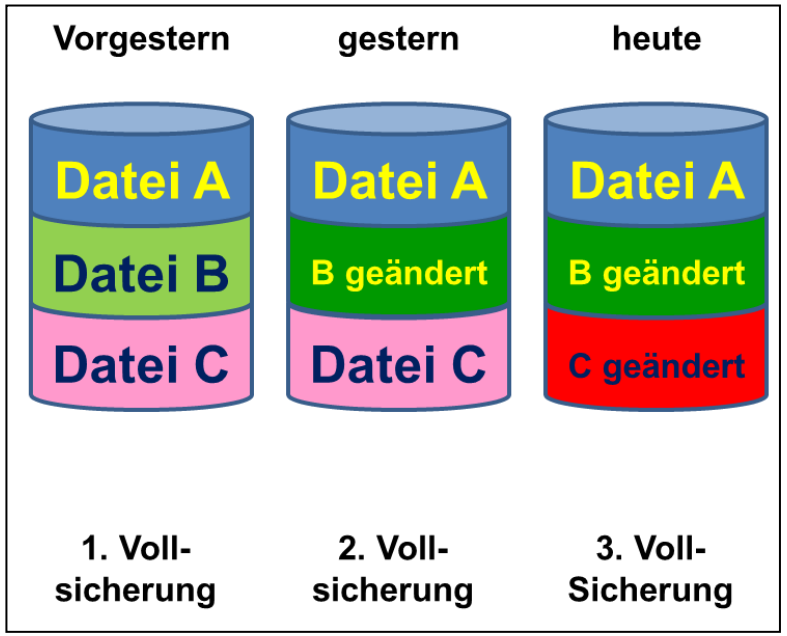
# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

### Exkurs – Datensicherung (3)

**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.**



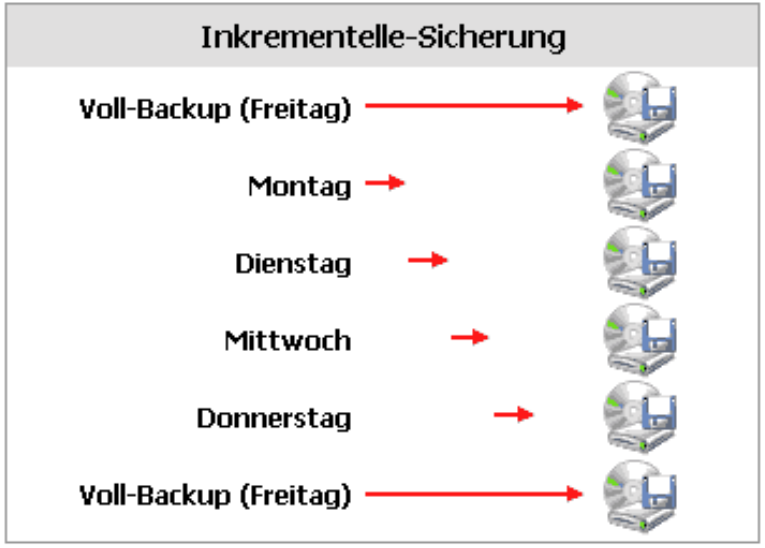



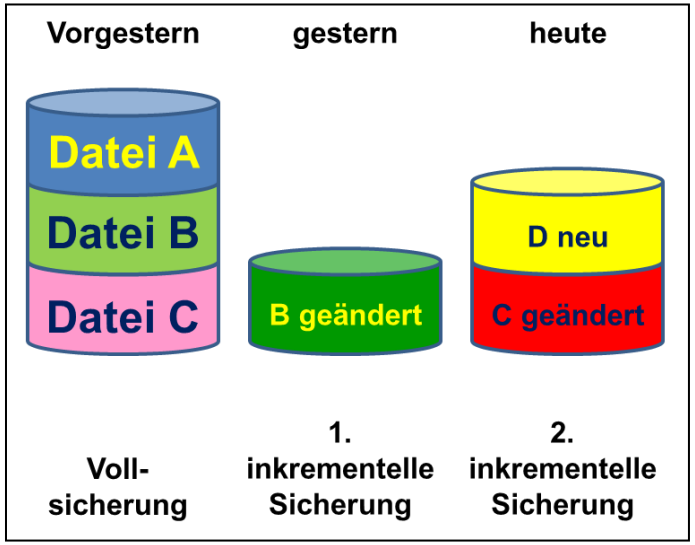
# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

### Exkurs – Datensicherung (4)

**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.**



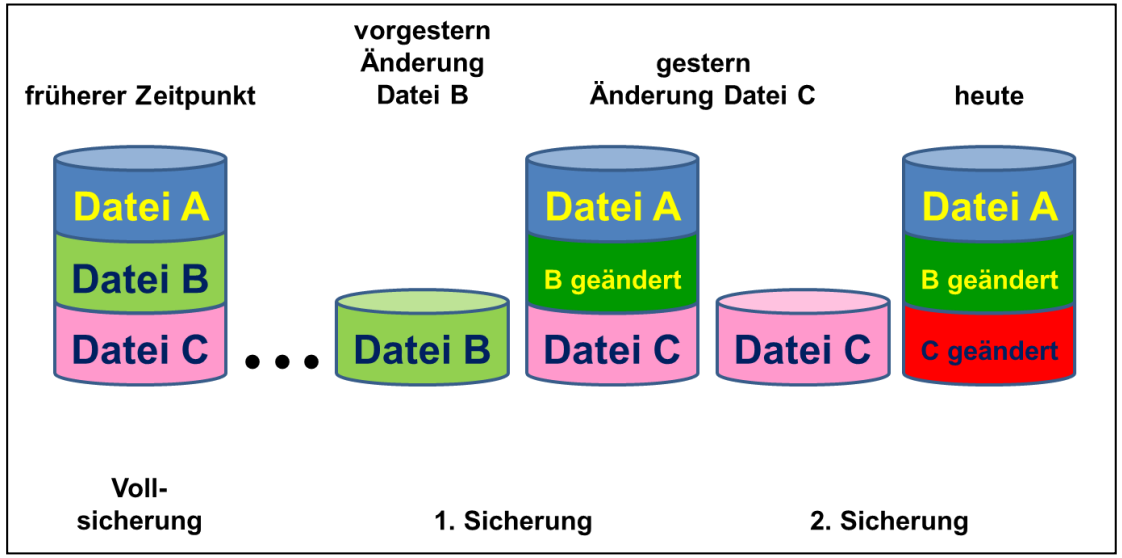



# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

### Exkurs – Datensicherung (5)

**Bei der umgekehrt inkrementellen Sicherung ist es möglich, die ältesten Sicherungen zu löschen kann, um z.B. wieder Platz für neue Sicherungen zu schaffen. Bei der umgekehrt inkrementellen Sicherung befindet sich der letzte Stand in der letzten Sicherung.**
**Mit der umgekehrt inkrementellen Sicherung ist eine ständige (forever) inkrementelle Sicherung möglich. Einmal wird eine Vollsicherung durch-geführt, danach werden für immer nur noch umgekehrt inkrementelle Sicherungen durchgeführt. Zur Sicherheit sollte aber auch ab und zu eine Vollsicherung durchgeführt werden**

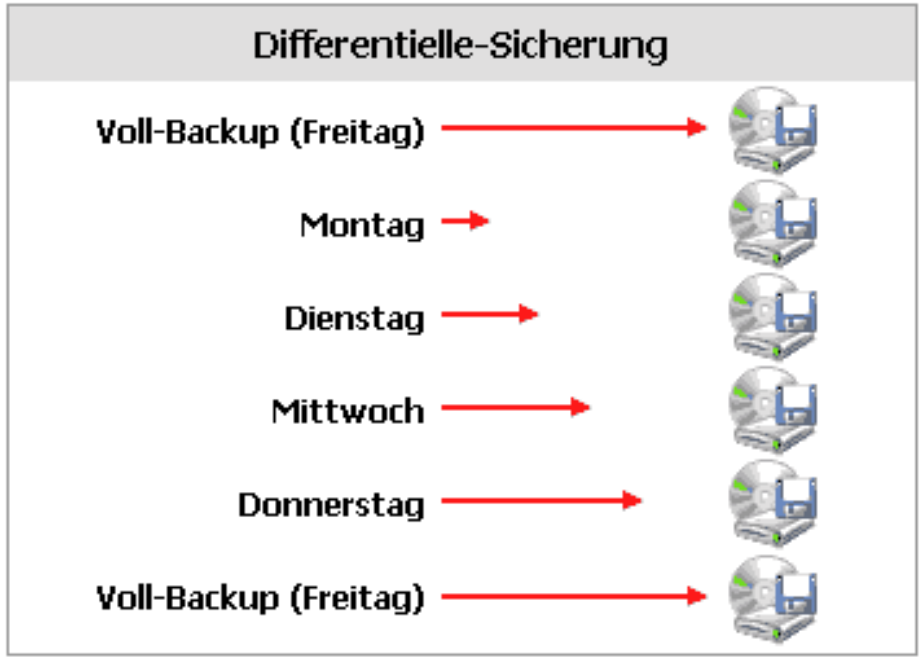


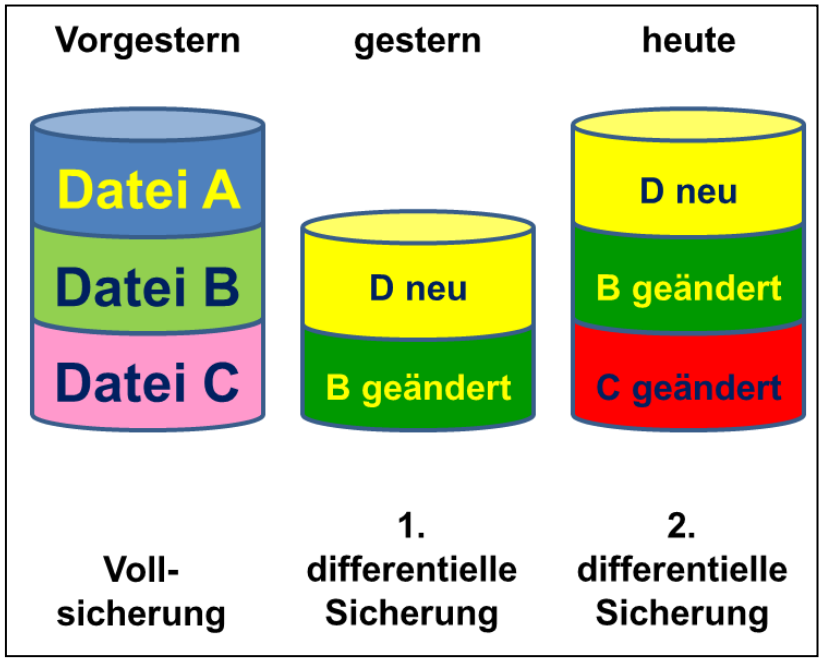
# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

### Exkurs – Datensicherung (6)

**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.**



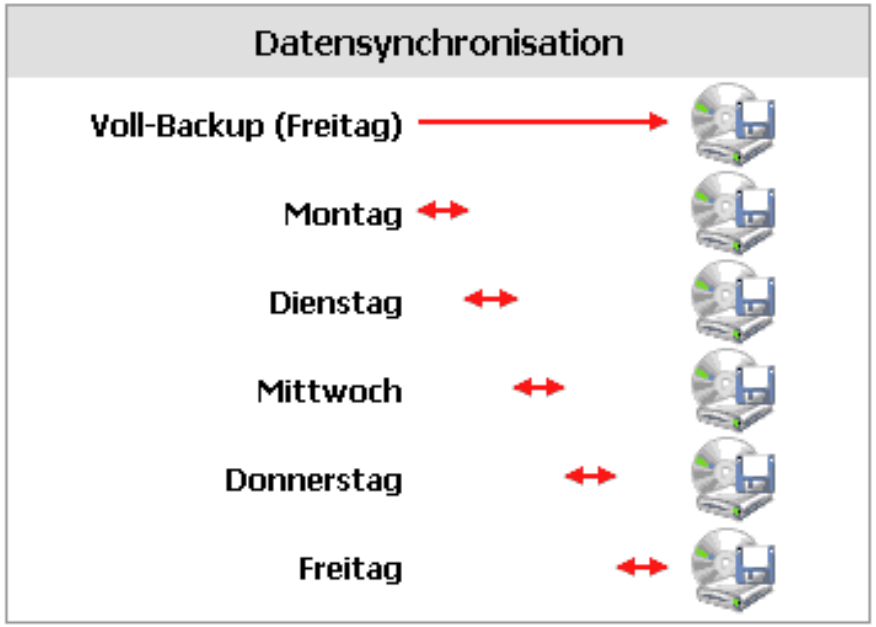



# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

### Exkurs – Datensicherung (7)

**Es werden nur aktuellere oder im Ziel nichtvorhandene Daten von der Quelle ins Ziel kopiert. Dateien und Ordner aus dem Ziel werden automatisch gelöscht, wenn diese in der Quelle nicht mehr vorhanden sind. Bei jeder Sicherung entsteht eine exakte Kopie der original Daten (Spiegelung) auf dem Sicherungs-Medium.**

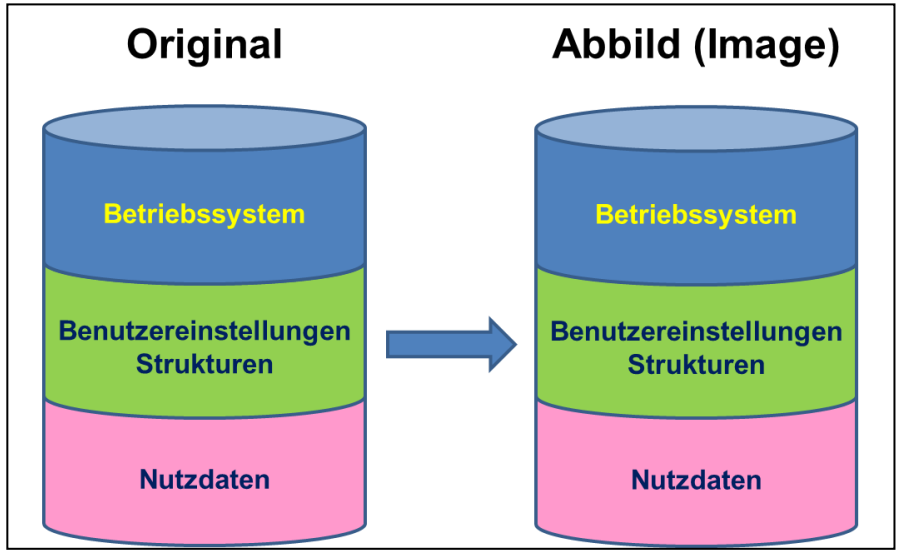


# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

### Exkurs – Datensicherung (8)

**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 einen neuen System wieder hergestellt werden können, auf dem neuen System wird die Originalstruktur wieder hergestellt**



# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Datenverwaltung

**Exkurs – Datensicherung (8)**

**Wie lange kann ich auf eine Datensicherung zurückgreifen (Generationen-Prinzip)?**

**Werden die gesetzlichen Aufbewahrungsfristen durch die Datensicherung sichergestellt?**

**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 bei einem Verschlüsselungstroianer (Ransomware) unbrauchbar werden.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Notfallpläne

20. **Notfallpläne**

**Für die im Rechenzentrum ausgelagerten Daten ist ein Notfallplan vorhanden (vgl. Testat Rechenzentrum IDW PS 951 Typ 2). Weiterhin hat die Gesellschaft als Anlage zum IT-Sicherheitskonzept einen Notfallplan aufgestellt.**

| | | |
|---|---|---|
| a. | Existieren Pläne, um zu gewährleisten, dass kritische Geschäftsprozesse bei Unterbrechungen des normalen Geschäftsbetriebs fortgeführt bzw. unverzüglich wiederaufgenommen werden können? | Ja |

**Es existieren Pläne (s.o.). Die Geschäftsführung geht davon aus das kritische Geschäftsprozesse innerhalb von einem Werktag wieder laufen.**

| | | |
|---|---|---|
| b. | Werden die Notfallpläne regelmäßig überarbeitet und ordnungsgemäß dokumentiert? | Ja |

**In Bezug auf das Rechenzentrum liegt die Verantwortung beim Dienstleister. Der eigene Notfallplan wird bei Bedarf angepasst.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Notfallpläne

**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!**

**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:¶

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Notfallpläne

**Exkurs – Notfallpläne (2)**

**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 PC-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)**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Notfallpläne

### Exkurs – Notfallpläne (3)

**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)**

**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!**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Notfallpläne - Tests

21. **Tests** Ja

Werden die Notfallpläne anhand von regelmäßigen Notfallübungen bzw. tatsächlicher Notfälle validiert und angepasst?

**Die Gesellschaft führt keine Notfalltests (bis auf Test von Datenrücksicherungen in unregelmäßigen Abständen) durch, dafür gibt es keine personellen Kapazitäten. Das Risiko ist durch Datenauslagerung (Rechenzentrum Aareon) und div. Dienstleistungsverträge für Betreuung Hard- und Software insgesamt überschaubar.**

**Wirksamkeit und Angemessenheit des Notfallmanagements ist durch regelmäßige Tests zu überprüfen.**
**Einem Test sind die getroffenen Vorsorgemaßnahmen, die organisatorischen Strukturen und die geplanten Abläufe zu unterziehen.**
**Testformen:**

- **Planbesprechung (z.B. Befall Ransomeware)**
- **Funktionstest (z.B. Wiederherstellung Daten, Server, DB..)**
- **Alarmierungstest**

**Test sollten geplant und die Durchführung muss dokumentiert werden => Schwachstelle in den meisten Unternehmen!**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

22. **Physischer Zugang** Ja

Ist der physische Zugang zu IT-Systemen auf autorisiertes Personal beschränkt?

**Der Zutritt zum Serveraum ist auf den Administrator, der kfm. Leitung (Vertretung) und der Geschäftsführung (Brandfall) beschränkt. Bzgl. der Zutrittsregelungen im Rechenzentrum vgl. Testat.**

**Exkurs – Physischer Zugang**

**Es entstehen Risiken bei fehlenden oder ungenügenden physischen Sicherungsmaßnahmen:**

- **Diebstahl von Hardware**
- **Diebstahl von Daten**

**Verlust von Daten durch**

- **Feuer, Wasser**
- **Stromausfall**
- **Sabotage**

**Datenmanipulation durch unautorisierte Zugriffe**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Exkurs: Übung 3

**Aufgaben und Fragestellungen:**

1. **Beurteilen Sie den auf den folgenden 4 Fotos abgebildeten Serverraum (Hinweis: Es handelt sich um ein großes Unternehmen) und das Fallbeispiel.**
2. **Beschreiben Sie die Risiken.**
3. **Besteht nur ein Verbesserungspotential oder liegt in den Risiken ein Problem hinsichtlich der Ordnungsmäßigkeit der Buchführung?**
4. **Welche Empfehlung gibt es, um das Risiko abzustellen oder ggf. zu minimieren?**

**Zeitumfang: 5 Minuten**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Exkurs: Übung 3

### Fallbeispiel

| | |
|---|---|
| Unternehmen | Wohnungsbaugenossenschaft Entenhausen eG |
| Anzahl WE | 14.000 WE |
| IT Infrasrtruktur | 75 PC Arbeitsplätze, Server-Raum verschließbar aber offen, der Schlüssel zum Serverraum hängt in der Teeküche nebenan. |
| Serverraum | Die Server stehen in einem unverschlossenen Serverschrank, der Schlüssel hängt im Server-Raum. |
| Brandschutz | Es ist keine Brandmeldeeinrichtung vorhanden, es gibt keinen $CO_2$ Feuerlöscher |

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Exkurs: Übung 3

### Foto Nr. 1

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

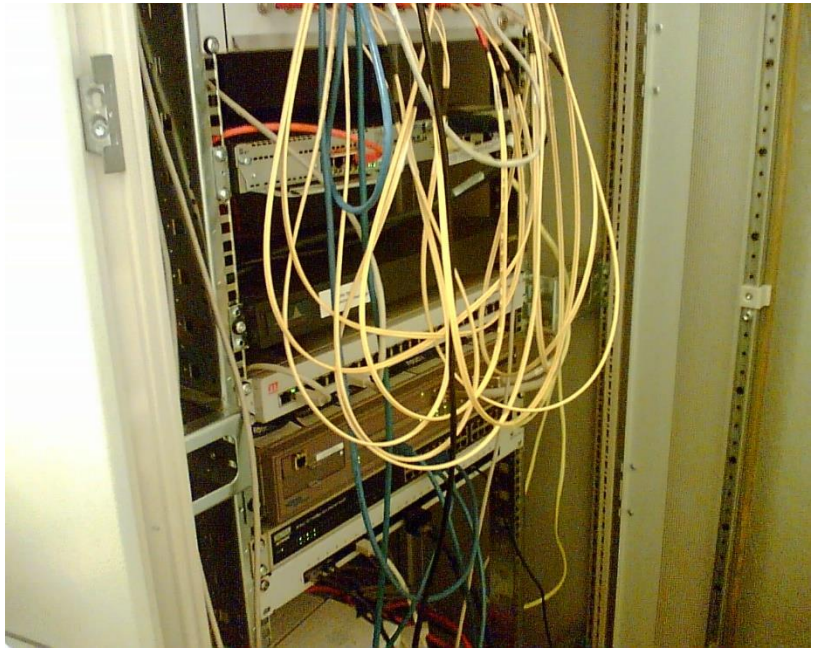
## Exkurs: Übung 3

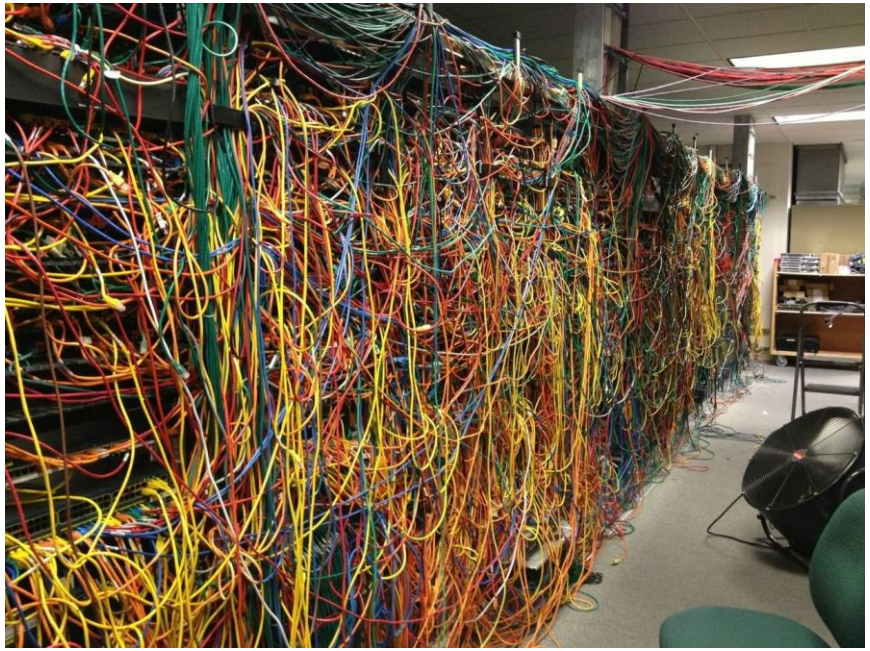
### Foto Nr. 2

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Exkurs: Übung 3

### Foto Nr. 3





# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Exkurs: Übung 3

### Foto Nr. 4

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

| | | |
|---|---|---|
| 23. | **Sicherheitsverwaltung**<br>Sind Administratorkonten/-user nur für autorisiertes Personal eingeschränkt zugänglich und wird der Zugriff auf sie überwacht? Werden dabei ausschließlich personalisierte Administratorenkonten genutzt? | Ja |

**Die Administratorenkonten sind durch entsprechende Passwörter gesichert. Eine entsprechende Passwortrichtlinie liegt vor. Die Admin-Zugänge für das ERP-System wurden von der Gesellschaft geändert und müssen für die Administratoren der Aareon AG neu freigegeben werden. Dies gilt besonders für das Konto „WFW“, dass als Mehrfachuser genutzt wurde.**

**Es sollten ausschließlich personalisierte Administratorkonten verwendet werden.**

**Für die Absicherung der Administratorenkonten sollte eine 2-Faktor-Authentisierung oder eine Multifaktor-Authentisierung verwendet werden.**

**Die Verwendung eines Administratorkontos sollte protokolliert werden inklusive wer das Konto genutzt hat (falls kein personalisierter Admin im Einsatz war).**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

24. **Logischer Zugang** Ja

Ist der Zugang zu Anwendungen und Daten auf autorisiertes Personal beschränkt?

**Sowohl Netzwerk (Windows), als auch das ERP-System sind über ein entsprechendes Berechtigungskonzept abgesichert. Dabei ist eine funktionale Berechtigungsvergabe nach Gruppen nach dem Minimalprinzip implementiert.**

**Exkurs – Logische Zugriffskontrollen (1)**

**Zwei Konzepte:**

**Minimalprinzip (Benutzer bekommt nur die Rechte die er benötigt)**

**Maximalprinzip (Benutzer bekommt die Rechte „weggenommen“ die er nicht benötigt)**

**=> Minimalprinzip ist besser, Maximalprinzip (jeder kann erst einmal ALLES ist aber die Regel)**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

### Exkurs – Logische Zugriffskontrollen (2)

**Definition nach IDW:**

**Logische Zugriffskontrollen sind wesentliche Elemente der Datensicherheit und des Datenschutzes und Voraussetzung zur Gewährleistung von Vertraulichkeit.**

**Die Sicherheitsanforderungen Autorisierung und Authentizität bedingen logische Zugriffskontrollen.**

**(IDW RS FAIT 1 Tz 84 ff)**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

### Exkurs – Logische Zugriffskontrollen (3)

**Begriffe**

**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.**

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

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

25. **Passwortverwaltung** Ja

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

25. **Passwortverwaltung** Ja

Werden Passwörter unter Berücksichtigung folgender Punkte verwaltet?

- Einsatz personenbezogener Passwörter
- Generierung qualifizierter Kennwörter (Länge, Ziffern, Zeichen, Sonderzeichen)
- Regelmäßige erzwungene Passwortänderung
- Regelmäßige Passwortänderung oder aufgrund eines tatsächlichen oder vermuteten Sicherheitsverstoßes
- Deaktivierung bzw. Löschung von Benutzerkonten ausgeschiedener Mitarbeiter

**Bei der Gesellschaft ist für jeden User im Netzwerk und ERP-System ein eigenes Konto mit Passwort angelegt. Die Kennwortlänge beträgt 8 Zeichen, die letzten 5 Kennwörter dürfen nicht wieder benutzt werden. Benutzerkonten ausgeschiedener Personen werden unverzüglich durch den Admin deaktiviert, alle Rechte werden dem Benutzerkonto entzogen. Die Verfahrensweise entspricht den Regelungen der Passwortrichtlinie**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

### Exkurs – Passwortverwaltung (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 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)?**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

### Exkurs – Passwortverwaltung (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 Passwortrichtlinie 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 (Passwortrichtlinie).**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

### Exkurs – Passwortverwaltung (3)

Müssen die Benutzer regelmäßig ihr Kennwort ändern? **(wird nicht mehr empfohlen)**
„früher“ alle 30 oder 60 Tage.
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?

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

### Exkurs – Passwortverwaltung (4)

**Wenn die Passwortlängen zu groß sind und ein komplexes Passwort gefordert wird, sind die Mitarbeiter schneller bereit, das Passwort aufzuschreiben.**

**Ist die Passwortlänge zu kurz (3 Zeichen oder weniger), stimmt das Passwort mit dem Benutzernamen oder Unternehmens-namen überein ist das Risiko hoch.**

**Werden nicht mehr benötigte Benutzerkonten gesperrt?**
**Inzwischen wird ein regelmäßiger Passwortwechsel nicht mehr empfohlen.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

### Exkurs – Passwortverwaltung (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 |

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

**Fragestellung:**

**Welche Risiken sehen Sie in Bezug auf die Fallbeispiele zum Thema "Logische Zugriffskontrollen"?**

**Zeitumfang: 5 Minuten**

**Fallbeispiel A oder Fallbeispiel B**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

### Fallbeispiel A

| | |
|---|---|
| Unternehmen | Wohnungsbaugenossenschaft Entenhausen eG |
| Anzahl WE | 4.000 WE |
| Berechtigungen | Es gibt einen Sammelbenutzer, mit dem sich alle Mitarbeiter anmelden |
| Kennwörter | Da nur ein Benutzer eingerichtet ist, haben alle Mitarbeiter das gleiche Kennwort |

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

### Fallbeispiel B

| | |
|---|---|
| Unternehmen | Wohnungsbaugenossenschaft Entenhausen eG |
| Anzahl WE | 14.000 WE |
| Benutzereinrichtung | Jeder Mitarbeiter hat eigene Benutzereinstellungen, die Kennwörter sind komplex und individuell |
| Berechtigungen | Von insgesamt 60 Benutzern haben 25 Mitarbeiter alle Berechtigungen (inkl. Administratorrechte) |
| Berechtigungen | Die Einrichtung von Berechtigungen wird nicht kontrolliert und erfolgt per Telefon zwischen den Abteilungsleitern und den Administratoren |

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

26. **Zugriffsverletzungen** Ja

Werden Sicherheitsverstöße (z. B. fehlerhafte Anmeldeversuche) überwacht und nachverfolgt?

**Bei mehr als 5 fehlerhaften Anmeldungen wird das Konto automatisch für 30 Minuten gesperrt.**

**Wie werden Falschanmeldungen behandelt?**

- **dauerhafte Sperre**
- **Sperre für eine gewisse Zeit, abhängig von der Anzahl der Fehlversuche**
- **keine Reaktion auf Fehlversuche**

**Der Zugriff auf das Internet wird immer risikoreicher, sind die Mitarbeiter unaufmerksam oder unwissend steigt das Risiko, die Systeme mit Schadsoftware zu infizieren!**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## 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.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## 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.

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## 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.

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## 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.

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## 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.

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

| | | |
|---|---|---|
| 27. | **Mobile Computing**<br>Werden sämtliche mobile Computer (Notebooks etc.), einschließlich mobiler Endgeräte (Smartphone, Tablet), angemessen kontrolliert bzw. ist ein MDM (Mobile Device Management) im Einsatz? | Ja |

**Variante 1)**

**auskunftsgemäß derzeit noch nicht im Einsatz, nur Smart Phones (Outlook)**
**=> Steuerung/Administration über Exchange**

**Variante 2)**

**Ein Mobile-Device-Managmentsystem (MDM) von XX ist seit Juni 2020 und ein Application Management System (MAM) von der Fa. YY Mobile ist im Einsatz.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

**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)?**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

28. **Remote-Zugriff** Ja

Unterliegen der Remote-Zugriff und die Autorisierung zum Remote-Zugriff angemessenen Kontrollen?

Berücksichtigen Sie Folgendes:

- VPN
- Remote-Desktop (RDP), Citrix
- Software für den Remote-Zugriff

**Der Remote Zugriff wird über das Programm TeamViewer realisiert. Der Zugang ist nur mit Genehmigung des Admin zulässig.**
**Die Aareon AG setzt das Programm Desk Share ein, der Zugriff muss von der Gesellschaft (betroffener Mitarbeiter) zugelassen werden.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

**Exkurs – Remote-Zugriff**

**Setzt das Unternehmen VPN Verbindungen ein, um Mitarbeiter, die beispielsweise 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?**

**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!**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Informationssicherheit

29. **Verschlüsselung** Ja

Werden sensible Informationen verschlüsselt, um ihre Vertraulichkeit zu wahren?

**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)**

**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, Handy).**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Änderungsmanagement

30. **Hardware**

Existiert ein formell genehmigtes und überwachtes Verfahren für das Management

**Die Gesellschaft hat kein Verfahren für das Management von Hardwareveränderungen eingerichtet. Die Anschaffung von Hardware ist über Investitionen Bestandteil des Wirtschaftsplanes und Unterliegt somit der Zustimmung durch die Geschäftsführung.**

**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“?**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Änderungsmanagement

31. **Genehmigte Systeme**

Führt die Einheit eine Liste mit genehmigten Programmen, Datenbanken und Betriebssystemen?

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

**Dürfen im Unternehmen nur genehmigte Programme eingesetzt werden?**

**Dürfen die Anwender selbständig Software installieren?**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Änderungsmanagement

32. **Änderungsprozess**

Existiert ein formell genehmigtes und überwachtes Verfahren für das Management von Änderungen an Hardware, Programmen, Datenbanken und Betriebssystemen?

**Die Gesellschaft hat kein Verfahren für das Management von Änderungen an Hardware, Software, Datenbanken oder Betriebssystemen eingerichtet. Alle Fragestellungen müssen mit der Geschäftsführung besprochen werden (Bestandteil des Wirtschaftsplanes).**

**Wie werden im Unternehmen Änderungen an Hardware, Software oder Prozessen initiiert?**

**Werden Änderungen vor Produktivsetzung getestet?**

**Führt das Unternehmen Eigenentwicklungen, auch Excel-Anwendungen, durch?**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Änderungsmanagement

33. **Dokumentation**

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

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

**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**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Änderungsmanagement

### 34. Testumgebung

Werden alle wesentlichen Änderungen an Hardware, Programmen, Datenbanken und Betriebssystemen vor ihrer Umsetzung getestet?

**Es handelt sich um eine ERP-Software im SaaS-Model. Im RZ existiert eine isolierte Testumgebung. Die bei der Softwareeinführung genutzte Schulungsdatenbank kann jetzt auch zu Testzwecken verwendet werden.**
**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.**

**Werden Änderungen an der Software durch Updates vor der Installation auf einem isolierten Testsystem getestet?**

**Wird neue Hardware auf Kompatibilität mit der eingesetzten Software geprüft und getestet?**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Genauigkeit, Vollständigkeit und Echtheit

35. **Datengenauigkeit**

Existieren Kontrollen, um zu gewährleisten, dass Informationen valide, korrekt und vollständig sind?

**Die Dateneingaben werden mit Hilfe von Eingabenachweisen kontrolliert. Eine Rechnungskontrolle (bei Eingangsrechnungen) wird durchgeführt und dokumentiert. Die Zahlungslisten werden durch den Leiter ReWe vor der endgültigen Zahlung geprüft und freigegeben.**
**Für Instandhaltungsaufträge existieren Freigabegrenzen, die über das ERP-System kontrolliert werden (automatische Kontrolle). Eine Überschreitung der Grenzen ist ohne Genehmigung des Vorgesetzten nicht möglich.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Genauigkeit, Vollständigkeit und Echtheit

### 36. Autorisierung

Ist die Integrität der Belege, Daten und Transaktionen sichergestellt?

**Stammdatenänderungen sind nur für berechtigte Personen zulässig. Es werden Stammdatenänderungsprotokolle automatisiert im ERP-System erzeugt. Eine Kontrolle erfolgt Anlassbezogen.**

**Werden Daten, die aus einem externen Programm stammen hinreichend geprüft, bevor sie endgültig gebucht werden?**

**Wer ist dazu autorisiert?**

**Ein Beispiel ist die Anlagenbuchhaltung in Excel (Fehleranfällig).**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Genauigkeit, Vollständigkeit und Echtheit

37. **Fehlervermeidung**

Welche fehlervermeidenden manuellen oder automatischen Kontrollen sind eingerichtet?

**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 Aareon AG gemeldet und beseitigt.**

**Sind bei der Anwendungssoftware Fehler bekannt?**

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

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Genauigkeit, Vollständigkeit und Echtheit

### 38. Fehlerbehandlung

Ist die Behandlung von Fehlern geregelt?

**Ein schriftlich dokumentiertes Verfahren zur Fehlerbehandlung ist nicht eingerichtet. Fehler werden zentral über das Ticketsystem der Aareon AG 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)**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Genauigkeit, Vollständigkeit und Echtheit

39. **Eingabevalidierungen**

Existieren Eingabekontrollen, um die vollständige und richtige Erfassung von Daten zu gewährleisten?

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

**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?**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Genauigkeit, Vollständigkeit und Echtheit

### Prüfpfad Eingabevalidierungen Rechnungen - Exkurs

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

**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 Prüfpfad zwischen Rechnung und Leistung" schafft.**

**Dieser verlässliche Prüfpfad 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.**

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Genauigkeit, Vollständigkeit und Echtheit

**Prüfpfad, 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 Prüfpfad zwischen Rechnung und Leistung schaffen kann, gewährleistet werden**
( § 14 Abs. 1 Satz 5 und 6 UStG ).

**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**? | | |

# XII. Ausgestaltung und Einrichtung von Allgemeinen IT- Kontrollen (566)

## Trennung von Funktionen

40. **Elektronische Funktionstrennung**

Ist eine elektronische Funktionstrennung implementiert, die gewährleisten soll, dass die Initiierung und Autorisierung eines Geschäftsvorfalls sowie dessen Ausführung und Überprüfung getrennt voneinander erfolgen? Liegen die technischen und organisatorischen Voraussetzungen (keine Mehrfachuser, restriktive Zuweisung von Admin-Rechten) vor?

**Die Funktionstrennung wird durch das in Wodis Sigma eingerichtete Berechtigungskonzept sicher gestellt. Weiterhin gibt es elektr. Funktionstrennungen im Bereich des Zahlungsverkehrs (elektr. Unterschrift). Hier erfolgt eine Hinterlegung bei den Banken (vgl. Bankbestätigung).**

**Exkurs Funktionstrennung:**

**Gibt es eine Funktionstrennung zwischen IT-Leitung (Administration) und dem Datenschutzbeauftragten? Da der Datenschutzbeauftragte den IT-Bereich kontrollieren soll, darf der IT-Leiter grundsätzlich nicht Datenschutzbeauftragter sein.**
**Gibt es keinen Datenschutzbeauftragten, kann je nach Unternehmensgröße ein Verstoß gegen die Datenschutzgrundverordnung (DSGVO) oder das Bundesdatenschutzgesetz (BDSG) vorliegen.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

# XIII. Ordnungsmäßigkeit der Buchführung (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 566.ORD.MIN liegen vor!**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

## I. Systemüberblick

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.

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

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

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

## Exkurs: Softwaretestat

**Inhaltsverzeichnis** **Seite**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

## Exkurs: Softwaretestat

Bescheinigung über die Durchführung einer Softwareprüfung

An die gesetzlichen Vertreter der Aareon Deutschland GmbH

Die Aareon Deutschland GmbH, Mainz, hat uns am 24. Februar 2023 beauftragt, eine Folgeprüfung des Softwareprodukts

Aareon Wodis Yuneo Release 23.77.0

mit den Modulen

Finanzbuchhaltung, Mietenbuchhaltung, Betriebskostenabrechnung, Mitgliederverwaltung, Fremdverwaltung (Eigentümerbuchhaltung und -abrechnung), Sparverkehr, Anlagenbuchhaltung, Darlehen & Hypotheken, Kautionsverwaltung und Konfiguration

vorzunehmen.

Wir sind der Auffassung, dass unsere Prüfung eine hinreichend sichere Grundlage für unsere Beurteilung bildet.

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

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

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 (Wodis Sigma) mit den typischen Nebenbüchern (Anbu, Darlehen, Miete, BK, Debitoren/Kreditoren etc.) eingesetzt. Weiterhin gibt es eine eigenentwickelte Warenwirtschaft zur Tochtergesellschaft, 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.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

## II. Organisation und allgemeine Buchhaltungsfunktionen

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.

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

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

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

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

4. AUFGABENVERTEILUNG UND KOMPETENZEN

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

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

Fertiggestellt mit unten aufgeführten Feststellungen

Kompetenzen sind nicht klar geregelt

**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?**

**Hier beispielhaft erfasst als "Wichtige Prüfungsfeststellung" im Dokument 320.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

**Frage 4 ist die Einstiegsfrage. Diese zielt nun konkret auf die Funktionstrennung. Dazu ist auch das Berechtigungskonzept einzusehen. Lassen Sie sich ggf. dazu die notwendigen Einstellungen vom Leiter IT erläutern.**


**Im Rahmen der IKS-Prüfungen auf Prozessebene haben sich keine Feststellungen ergeben, die gegen eine Einhaltung der Funktionstrennung sprechen.**

**Hier sind sensible Bereiche der Funktionstrennung insbesondere im Zahlungsbereich zu untersuchen. Dies kann auch im Rahmen der IKS-Prüfungen vorgenommen werden.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

6. 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).

**Besprechung mit IT-Verantwortlichen geführt. Änderungsprotokollierung im ERP-System ist aktiv. Vor Ort am 1.12.2023 eingesehen.**

**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 Stammdaten-änderungen eingerichtet ist. ! Bspw. im SAP lässt sich die Protokollierung ausschalten! Argument ist meistens die Performance.**

**Wenn möglich lassen Sie sich die entsprechenden Einstellungen zu einem Beispiel zeigen.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

7. 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).

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

**Nehmen Sie Einsicht ins Buchungsjournal. Sind alle notwendigen Angaben enthalten? Ggf. vollziehen Sie dies für einen manuellen Beleg (Rechnung) und einen automatischen Beleg nach (z. B. automatische AfA-Buchungen oder monatlichen Sollmietenstellung [kann auch bei der IKS-Prüfung erfolgen]) – Anhaltspunkt: Softwarebescheinigung**

**IDW RS FAIT 1 Tz 33 ff.:**
**Keine Buchung ohne Beleg!**
**=> Konventioneller Beleg oder maschineller Beleg!**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

8. 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).

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

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

**IDW RS FAIT 1 Tz 41 ff.:**
**Sicherstellung der zeitlichen Ordnung!**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

9. 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).

**Die Kontenfunktion wird eingehalten (vgl. auch Softwaretestat).**

**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 46 ff.:**
**Sicherstellung der sachlichen Ordnung!**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

10. 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).

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

**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)**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

11. 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)

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

**Finden Sie heraus, ob die gesetzlichen Aufbewahrungsvorschriften eingehalten werden (Befragung).**

**Aufbewahrungsvorschriften: § 257 HGB und § 146 AO**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

12. ELEKTRONISCHE AUFBEWAHRUNG

Prüfen Sie, ob die nach handelsrechtlich und steuerlichen Vorschriften aufzeichnungspflichtigen und nach § 147 Abs. 1 AO aufbewahrungspflichtigen Unterlagen zulässigerweise elektronisch (auf einem Bild oder Datenträger) aufbewahrt werden.

a. Prüfen Sie hierfür, ob die gewählte Form der Aufbewahrung den GoB entspricht und sichergestellt ist, dass die Wiedergabe oder die Daten

- mit den empfangenen Handels- oder Geschäftsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden,
- während der Aufbewahrungsfrist jederzeit verfügbar sind,
- unverzüglich lesbar gemacht und
- maschinell ausgewertet werden können (IDW RS FAIT 5 Tz. 16).

**Elektronische Daten können im Rahmen der gesetzlichen Aufbewahrungsfristen jederzeit lesbar gemacht werden. Im Rahmen der Prüfung nichts gegenteiliges festgestellt.**

**Nehmen Sie Einsicht in eine bestehende Datenschutzrichtlinie. Ist diese mit den gesetzlichen Vorgaben vereinbar? Oder führen Sie ein Gespräch mit dem Leiter IT. Ggf. ist zu diesem Punkt der Vertrag mit einem Dienstleister (Rechenzentrum) einzusehen.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

b. Sofern Papierdokumente durch den Scanvorgang in elektronische Dokumente umgewandelt werden, ist festzustellen, ob das angewandte Verfahren den gesetzlichen Ordnungsmäßigkeitsanforderungen unter Beachtung der GoBD "Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff") entspricht (IDW RS FAIT 5 Tz. 36). Das Verfahren ist zu dokumentieren.

**Diese Frage ist nur wichtig, soweit die Unterlagen (z. B. Rechnungen) nach dem Scannen vernichtet werden und damit die elektronischen Belege zu Originalen werden.**

**Im Unternehmensverbund wird noch kein ersetzendes Scannen umgesetzt. Ist aber ab 2024 geplant. Belege werden derzeit noch papierhaft vorgehalten.**

**Alternativ:**

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

**Achtung: Zukünftig wird sich dies immer mehr ändern. Z. B. durch den Einsatz von Dokumentenmanagementsystemen.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

## Exkurs – Verfahrensdokumentation ersetzendes Scannen

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

Erarbeitet von der

**Inhaltsverzeichnis**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

13. ORDNUNGSMÄSSIGKEIT DER BUCHFÜHRUNG BEI AUSLAGERUNG DER IT

Stellen Sie aufgrund der durchgeführten IT-Systemprüfung (Hinweis auf die Dokumente 510-1/566) 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

**Datenauslagerung erfolgt in ein Rechenzentrum**

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).

**Ja, ein IKS ist eingerichtet. Die Kontrollmaßnahmen sind angemessen ausgestaltet (vgl. IKS-Prüfungen)**

**Hier Angabe der bestehenden Auslagerung.**

**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.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

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 Wirksamkeitsprüfung der eingerichteten Kontrollen.**

**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). Die Personalbuchhaltung wird mtl. durch Leitung Personal und ReWe geprüft.**

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

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

## III. KONTENZUORDNUNG UND SCHNITTSTELLEN

### 14. KONTENZUORDNUNG

Prüfen Sie, ob die Konten den Posten der Bilanz sowie der Gewinn und Verlustrechnung richtig zugeordnet worden sind.

**Ja, alle Konten sind vollständig zugeordnet.**

**Überprüfung erfolgt schon beim Einlesen der SuSaLi in Audicon.**

**Hier ist die lückenlose Kontenzuordnung zu bestätigen.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

15. 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.

**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?**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

16. AUSGLEICH DER HAUPTABSCHLUSSÜBERSICHT

Prüfen Sie, ob die Hauptabschlussübersicht (HÜ) auf „Null“ aufgeht.

**Ja, die HÜ geht auf, vgl. Ref.**

**Referenz bspw. auf CaseWare 5.2.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

## IV. PERIODENABSCHLUSS

### 17. SALDOVORTRAG

Prüfen Sie, ob sichergestellt ist, dass sämtliche Salden zutreffend auf das Berichtsjahr vorgetragen wurden.

**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.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

## V. 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.

**Die letzte Betriebsprüfung in 2022 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.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

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.

**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.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

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.**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

| | | |
|---|---|---|
| 20. | ANFORDERUNGEN AN KASSEN/ KASSENSYSTEME<br>Prüfen Sie das Vorhandensein der nach GoB/GoBD erforderlichen Unterlagen für manuelle Kassen bzw. elektronische Kassensysteme.<br>§ 146 Abs. 1 AO<br>es gibt entpsrechende Kassenrichtlinie, folgende Kassen werden betrieben:<br><br>1) Arena => elektr. Kassensystem<br>2) Campingplatz => elektr. Kassensystem<br>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.<br>Beantworten Sie diese Frage mit "Ja" oder "Nein".<br>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.<br>bei 1) und 2) elektr. Kasse und 3) händisches Kassenbuch (Kassenbesandsprotokoll vgl. IKS Finanzdispo) => des Weiteren gelten entsprechende DO | Ja |
| c. | Prüfen Sie bei Einsatz von elektronischen Registrierkassen, ob<br>entsprechende Schreiben des EB liegen vor | |
| i. | die Speicherung der Einzelaufzeichnungen Folgendes beachtet:<br>• Vollständigkeit der Daten (Bonierungen, Stornierungen, Zahlungsvorgänge)<br>• Unveränderbarkeit der gespeicherten Daten<br>• Datenexportmöglichkeit für das Finanzamt (Hinweis auf die besonderen Anforderungen und Aufbewahrungsmodalitäten nach dem BMF-Schreiben vom 26.10.2010, BStBl. I 2010, S. 1342).<br>Exportmöglichkeit gegeben, durch zuständige Mitarbeiterin bei Frau XY am PC auch die entsprechenden Protokolle zeigen lassen, des weiteren gilt die entsprechende DA | Ja |

## Exkurs – elektr. Kassensysteme

| | | |
|---|---|---|
| ii. | die Speicherung der Einzelaufzeichnungen Folgendes beachtet:<br>• Vollständigkeit der Daten (Bonierungen, Stornierungen, Zahlungsvorgänge)<br>• Unveränderbarkeit der gespeicherten Daten<br>• Datenexportmöglichkeit für das Finanzamt (Hinweis auf die besonderen Anforderungen und Aufbewahrungsmodalitäten nach dem BMF-Schreiben vom 26.10.2010, BStBl. I 2010, S. 1342).<br>Exportmöglichkeit gegeben, durch zuständige Mitarbeiterin bei Frau XY am PC auch die entsprechenden Protokolle zeigen lassen, des weiteren gilt die entsprechende DA | Ja |
| 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).<br>im Rahmen der Prüfung nichts gegenteiliges festgestellt, da die Kassen insgesamt von untergeordneter Natur sind auch keine Tiefenprüfung durchgeführt | N/A |
| 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).<br>vgl. ORD.4, alle eingesetzten Kassen entsprechen gem. vorliegenden Unterlagen den Anforderungen der GoBD | N/A |

# XIII. Ordnungsmäßigkeit der Buchführung (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).

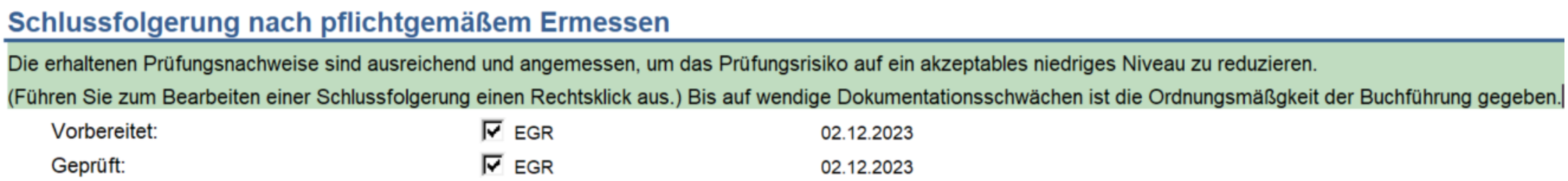
**Es haben sich keine bedeutsamen berichtspflichtigen Beanstandungen ergeben.**

**Soweit nicht bedeutsame Beanstandungen vorliegen sind dies als "Wichtige Prüfungsfeststellungen" im Dokument 320 (als Aufgaben) zu erfassen.**

**Eine 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).**

# XIII. Ordnungsmäßigkeit der Buchführung (ORD.PP)

**Am Ende der Prüfungshandlungen wird noch eine abschließende Beurteilung abgegeben.**



## Schlussfolgerung nach pflichtgemäßem Ermessen

Die erhaltenen Prüfungsnachweise sind ausreichend und angemessen, um das Prüfungsrisiko auf ein akzeptables niedriges Niveau zu reduzieren.

(Führen Sie zum Bearbeiten einer Schlussfolgerung einen Rechtsklick aus.) Bis auf wendige Dokumentationsschwächen ist die Ordnungsmäßgkeit der Buchführung gegeben.

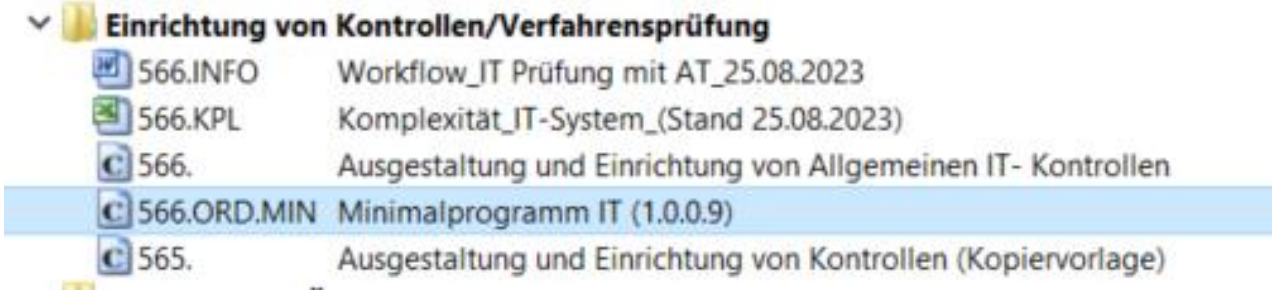
| | | |
|---|---|---|
| Vorbereitet: | ☑ EGR | 02.12.2023 |
| Geprüft: | ☑ EGR | 02.12.2023 |

**Um diese einzufügen muss dort mit der rechten Maustaste hingeklickt werden. Es erscheint "Schlussfolgerung bearbeiten".**

**Danach wird das Dokument abgezeichnet.**

# XIV. Minimalprogramm IT (566.ORD.MIN)

# XIV. Minimalprogramm IT (566.ORD.MIN)




**Bei komplexen Systemen wird 566 und ORD.PP angewendet.**
**Bei nicht komplexen Systeme wird 566.ORD.MIN bearbeitet. Dieses Dokument ersetzt dann 566 und ORD.PP!**

**Das IT-System gilt als nicht komplexes System, wenn es die Anwendungskriterien im Vorspann von 566.ORD.MIN erfüllt. Alle anderen Systeme gelten als komplexe Systeme.**

# XIV. Minimalprogramm IT (566.ORD.MIN)

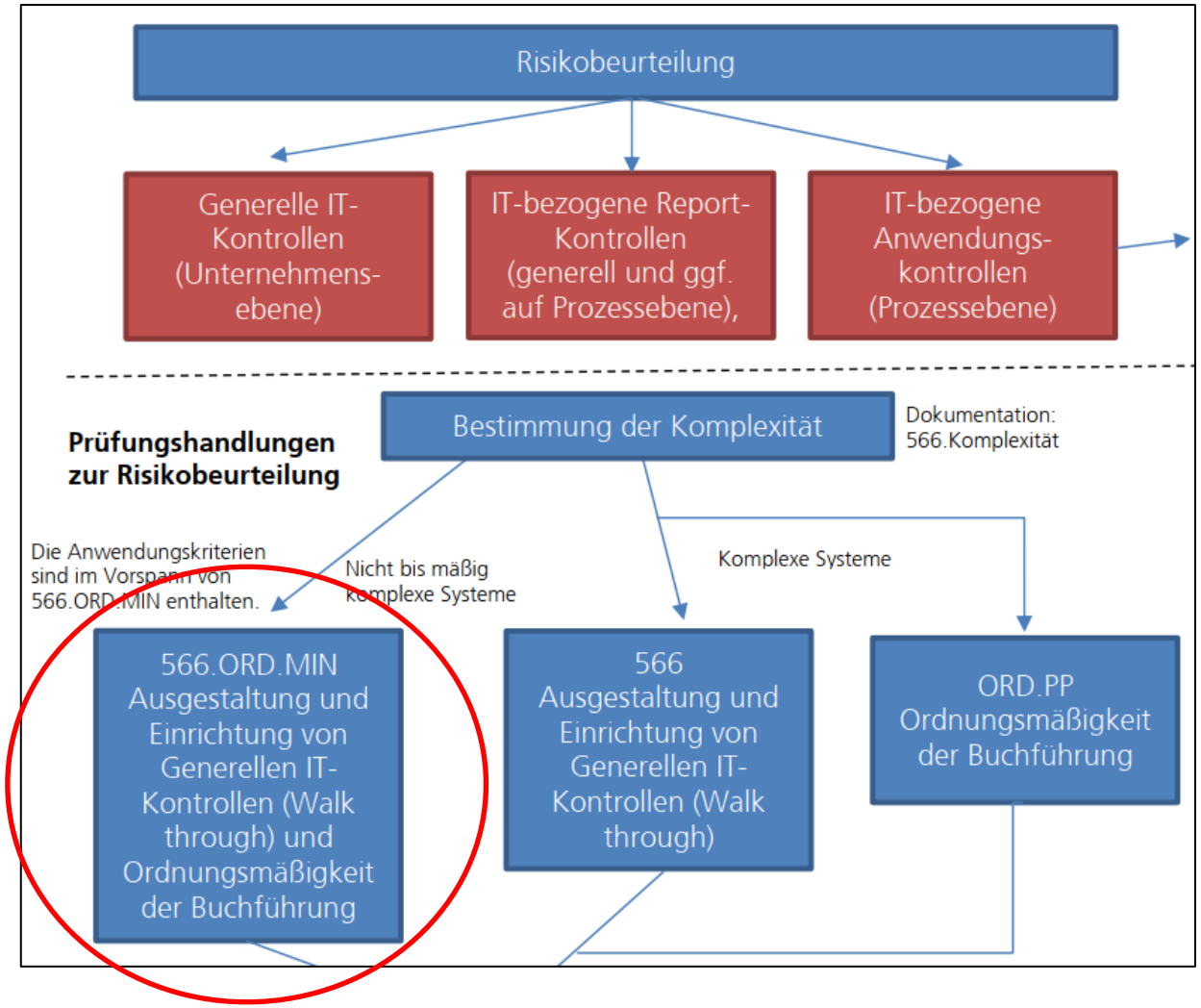
## Kriterien für eine Anwendung von 566.ORD.MIN:

**Diese Checkliste ist bei nicht bis mäßig komplexen IT-Systemen (gemäß Komplexitätseinschätzung "566.Komplexität") anzuwenden und ersetzt die Checklisten 566. sowie das Prüfprogramm ORD.PP unter den folgenden Voraussetzungen:**

- **Risikobewusstsein und Risiokultur 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"**
- **keine Softwareumstellung/Migration im Berichtsjahr**
- **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)**

**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.**

# XIV. Minimalprogramm IT (566.ORD.MIN)



# XIV. Minimalprogramm IT (566.ORD.MIN)

**Was ist 566.ORD.MIN eigentlich?**

⇒ **566.ORD.MIN ist eine Zusammenstellung der wichtigsten Fragen aus 566 und ORD.PP.**

⇒ **Die Bearbeitung von 566 und ORD.PP entfällt damit ersatzlos.**

⇒ **Ist nur ein Teil des RET-Ansatzes.**

# XIV. Minimalprogramm IT (566.ORD.MIN)

## Überblick über das IT-System

1. BESCHREIBUNG — Fertiggestellt ohne Beanstandungen — EGR — 03.12.2023 — 565.

Haben Sie die allgemeinen Informationen über die IT-Umgebung der Einheit, einschließlich Hardware und Software, zusammengefasst?

**Die Gesellschaft betreibt ein eigenes IT-System [Windows Server 2012 R2; Clients Win 8 + Win 10] mittlerer Größe (ca. 50 IT-Arbeitsplätze)**

**Als ERP-System wird Wodis Sigma (Version 12.0.23) der Fa. Aareon als SaaS eingesetzt und im Rechenzentrum der Fa. Aareon in Mainz gehostet.**

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

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

**Verlinkung mit den zu Grunde liegenden Unterlagen und Dokumenten!**

**Entspricht 566/1**

# XIV. Minimalprogramm IT (566.ORD.MIN)

| | | | | |
|---|---|---|---|---|
| 2. | ANWENDBARKEIT<br>Liegen die in der Einführung beschriebenen Voraussetzungen für die Anwednung des Minimalprüfprogramms vor? | Fertiggestellt ohne Beanstandungen | EGR<br>03.12.2023 | 566.KPL |

**Die Voraussetzungen für die Anwendung des Minimalprüfungs-programms liegen vor, die Software wird über ein Rechenzentrum betrieben. Im Berichtsjahr gab es keine Softwareumstellung, es gibt keine Schnittstellen zu externen Systemen die rechnungslegungs-relevanten Daten verarbeiten (Gehaltsdaten werden manuell bearbeitet). Im Vorjahr gab es keine Beanstandungen.**

**Vgl. auch Ref. auf Matrix 566.KPL**

# XIV. Minimalprogramm IT (566.ORD.MIN)

## Organisation und Management auf Unternehmens- und IT-Ebene

3. IT-ROLLEN UND VERANTWORTLICHKEIT

Hat die Einheit Rollen und Verantwortlichkeiten für die IT definiert??

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

**Neue Frage ab AT 24. Entspricht in 566/10**

# XIV. Minimalprogramm IT (566.ORD.MIN)

## Datenverwaltung

4. SICHERUNG

**Die Gesellschaft nutzt ein mehrstufiges Sicherungskonzept. 2x täglichen werden die Daten via Snapshot im laufenden Betrieb gesichert und auf einem Storage abgelegt. Darüberhinaus erfolgt eine inkrementelle Datensicherung auf einem NAS-System, welches auf einem weiteren NAS-System gespiegelt wird. => vgl. auch Datensicherungskonzept (Ref.)**

a. Existieren geeignete Richtlinien und Verfahren zur Sicherung von Systemen, Anwendungen, Daten und Dokumentationen?

**Ja, vgl. Datensicherungskonzept (Ref.)**

b. Werden die Richtlinien regelmäßig überarbeitet und ordnungsgemäß dokumentiert?

**Das Datensicherungskonzept wird bei Bedarf überarbeitet.**

**Entspricht 566/19**

# XIV. Minimalprogramm IT (566.ORD.MIN)

## Notfallpläne

5. NOTFALLPLÄNE

**Bei Störungen (kompletter Ausfall der Systeme) erfolgt durch den IT-Dienstleister eine Bearbeitung innerhalb von 2 Stunden. Vgl. Verträge und IT-Sicherheitskonzept in eDA. Die Kontaktdaten zu den Dienstleistern sind zentral hinterlegt.**

a. Existieren Pläne, um zu gewährleisten, dass kritische Geschäftsprozesse bei Unterbrechungen des normalen Geschäftsbetriebs fortgeführt bzw. unverzüglich wiederaufgenommen werden können?

**Durch die vertraglichen Vereinbarungen mit den Dienstleistern geht die Geschäftsführung davon aus, das innerhalb der maximal tolerierbaren Ausfallzeit von 1-2 Werktagen die Systeme auch bei größeren Störungen wieder Lauffähig zur Verfügung stehen.**

b. Werden die Richtlinien regelmäßig überarbeitet und ordnungsgemäß dokumentiert?

**Die Richtlinien werden bei Bedarf überarbeitet.**

**Entspricht 566/20**

# XIV. Minimalprogramm IT (566.ORD.MIN)

## Informationssicherheit

6. PHYSISCHER ZUGANG

Ist der physische Zugang zu IT Systemen auf autorisiertes Personal beschränkt?

**Der Zutritt zum Serveraum ist auf den Administrator, der kfm. Leitung (Vertretung) und der Geschäftsführung (Brandfall) beschränkt. Bzgl. der Zutrittsregelungen im Rechenzentrum vgl. Testat.**

**Neue Frage ab AT24; Entspricht 566/22**

# XIV. Minimalprogramm IT (566.ORD.MIN)

7. LOGISCHER ZUGANG

Ist der Zugang zu Anwendungen und Daten auf autorisiertes Personal beschränkt?

**Sowohl Netzwerk (Windows), als auch das ERP-System sind über ein entsprechendes Berechtigungskonzept abgesichert. Dabei ist eine funktionale Berechtigungsvergabe nach Gruppen nach dem Minimalprinzip implementiert.**

**Neue Frage ab AT24; Entspricht 566/24**

# XIV. Minimalprogramm IT (566.ORD.MIN)

8. PASSWORTVERWALTUNG

Werden Passwörter unter Berücksichtigung folgender Punkte verwaltet?

- Einsatz personenbezogener Passwörter
- Generierung qualifizierter Kenntwörter (Länge, Ziffern, Zeichen, Sonderzeichen)
- Regelmäßige erzwungene Passwortänderung
- Regelmäßige Passwortänderung aufgrund eines tatsächlichen oder vermuteten Sicherheitsverstoßes
- Deaktivierung bzw. Löschung von Benutzerkonten ausgeschiedener Mitarbeiter

**Bei der Gesellschaft ist für jeden User im Netzwerk und ERP-System ein eigenes Konto mit Passwort angelegt. Die Kennwortlänge beträgt mind. 8 Zeichen, Groß-/Kleinschreibung, Zahlen, Sonderzeichen etc. Pflicht, die letzten 5 Kennwörter dürfen nicht wieder benutzt werden. Benutzerkonten ausgeschiedener Personen werden unverzüglich durch den Admin deaktiviert, alle Rechte werden dem Benutzerkonto entzogen. Die Verfahrensweise entspricht den Regelungen der Passwortrichtlinie (vgl. Ref).**

**Entspricht 566/25**

# VIV. Minimalprogramm IT (566.ORD.MIN)

## Änderungsmanagement

9. ÄNDERUNGSPROZESS

Existiert ein formell genehmigtes und überwachtes Verfahren für das Management von Änderungen an Hardware, Programmen, Datenbanken und Betriebssystemen?

**Die Gesellschaft hat kein Verfahren für das Management von Änderungen an Hardware, Software, Datenbanken oder Betriebssystemen eingerichtet. Alle Fragestellungen müssen mit der Geschäftsführung besprochen werden (Bestandteil des Wirtschaftsplanes).**

**Neue Frage ab AT24; Entspricht 566/32**

# XIV. Minimalprogramm IT (566.ORD.MIN)

## Genauigkeit, Vollständigkeit und Echtheit

10. AUTORISIERUNG

Ist die Integrität der Belege, Daten und Transaktionen sichergestellt?

**Stammdatenänderungen sind nur für berechtigte Personen zulässig. Es werden Stammdatenänderungsprotokolle automatisiert im ERP-System erzeugt. Eine Kontrolle erfolgt anlassbezogen.**

**Entspricht 566/36**

# XIV. Minimalprogramm IT (566.ORD.MIN)

11. EINGABEVALIDIERUNGENGEN

Existieren Eingabekontrollen, um die vollständige und richtige Erfassung von Daten zu gewährleisten?

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

**Entspricht 566/39**

# XIV. Minimalprogramm IT (566.ORD.MIN)

## Trennung von Funktionen

12. ELEKTRONISCHE FUNKTIONSTRENNUNG

Ist eine elektronische Funktionstrennung implementiert, die gewährleisten soll, dass die Initiierung und Autorisierung eines Geschäftsvorfalls sowie dessen Ausführung und Überprüfung getrennt voneinander erfolgen? Liegen die technischen und organisatorischen Voraussetzungen (keine Mehrfachuser, restriktive Zuweisung von Admin-Rechten) vor?

**Die Funktionstrennung wird durch das in Wodis Sigma eingerichtete Berechtigungskonzept sicher gestellt. Weiterhin gibt es elektr. Funktionstrennungen im Bereich des Zahlungsverkehrs (elektr. Unterschrift). Hier erfolgt eine Hinterlegung bei den Banken (vgl. Bankbestätigung).**

**Entspricht 566/40**

# XIV. Minimalprogramm IT (566.ORD.MIN)

## Ordnungsmäßigkeit der Buchführung

13. 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.

**Zu dem im Einsatz befindlichen ERP-Sysem gibt es kein aktuelles Testat (letztes von 2018). Die geringfügigen Änderungen zwischen den Versionen betreffen keine rechnungslegungsrelevanten Daten. Die Folgeversion soll lt. Aussage des Herstells wieder testiert werden.**

**Entspricht ORD.PP/1**

# XIV. Minimalprogramm IT (566.ORD.MIN)

14. 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)

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

**Entspricht ORD.PP/11**

# XIV. Minimalprogramm IT (566.ORD.MIN)

15. 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).

**Besprechung mit IT-Verantwortlichen geführt. Änderungsprotokollierung im ERP-System ist aktiv. Vor Ort am 1.12.2023 eingesehen.**

**Entspricht ORD.PP/6**

# XIV. Minimalprogramm IT (566.ORD.MIN)

16. 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).

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

**Entspricht ORD.PP/7**

# XIV. Minimalprogramm IT (566.ORD.MIN)

17. 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).

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

**Entspricht ORD.PP/8**

# XIV. Minimalprogramm IT (566.ORD.MIN)

18. 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).

**Die Kontenfunktion wird eingehalten (vgl. auch Softwaretestat).**

**Entspricht ORD.PP/9**

# XIV. Minimalprogramm IT (566.ORD.MIN)

19. 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).

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

**Entspricht ORD.PP/10**

# XIV. Minimalprogramm IT (566.ORD.MIN)

20. KONTENZUORDNUNG

Prüfen Sie, ob die Konten den Posten der Bilanz sowie der Gewinn und Verlustrechnung richtig zugeordnet worden sind.

**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.**

**Entspricht ORD.PP/14**

# XIV. Minimalprogramm IT (566.ORD.MIN)

21. 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.

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

**Entspricht ORD.PP/15**

# XIV. Minimalprogramm IT (566.ORD.MIN)

22. 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

**Datenauslagerung erfolgt in ein Rechenzentrum**

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).

**Ja, ein IKS ist eingerichtet. Die Kontrollmaßnahmen sind angemessen ausgestaltet (vgl. IKS-Prüfungen)**

**Hier Angabe der bestehenden Auslagerung.**

**Frage neu ab AT24; ORD.PP/13**

# XIV. Minimalprogramm IT (566.ORD.MIN)

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.

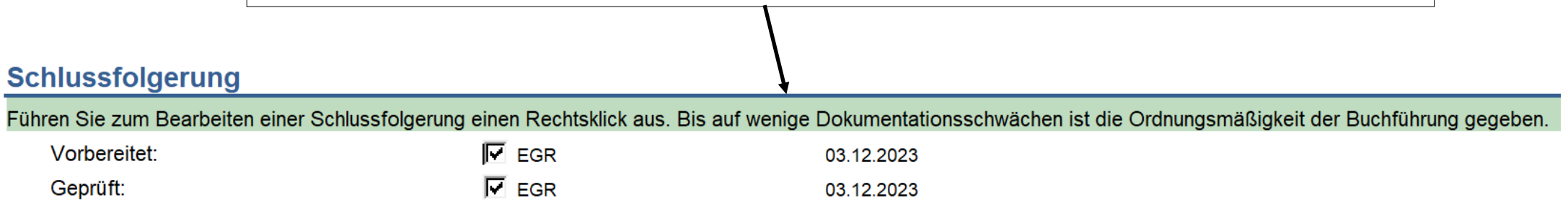
**Hier Wirksamkeitsprüfung der eingerichteten Kontrollen.**

**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). Die Personalbuchhaltung wird mtl. durch Leitung Personal und ReWe geprüft.**

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

# XIV. Minimalprogramm IT (566.ORD.MIN)

**Am Ende der Prüfungshandlungen wird noch eine abschließende Beurteilung abgegeben.**




**Um diese einzufügen muss dort mit der rechten Maustaste hingeklickt werden.**
**Es erscheint "Schlussfolgerung bearbeiten".**

**Danach wird das Dokument abgezeichnet.**

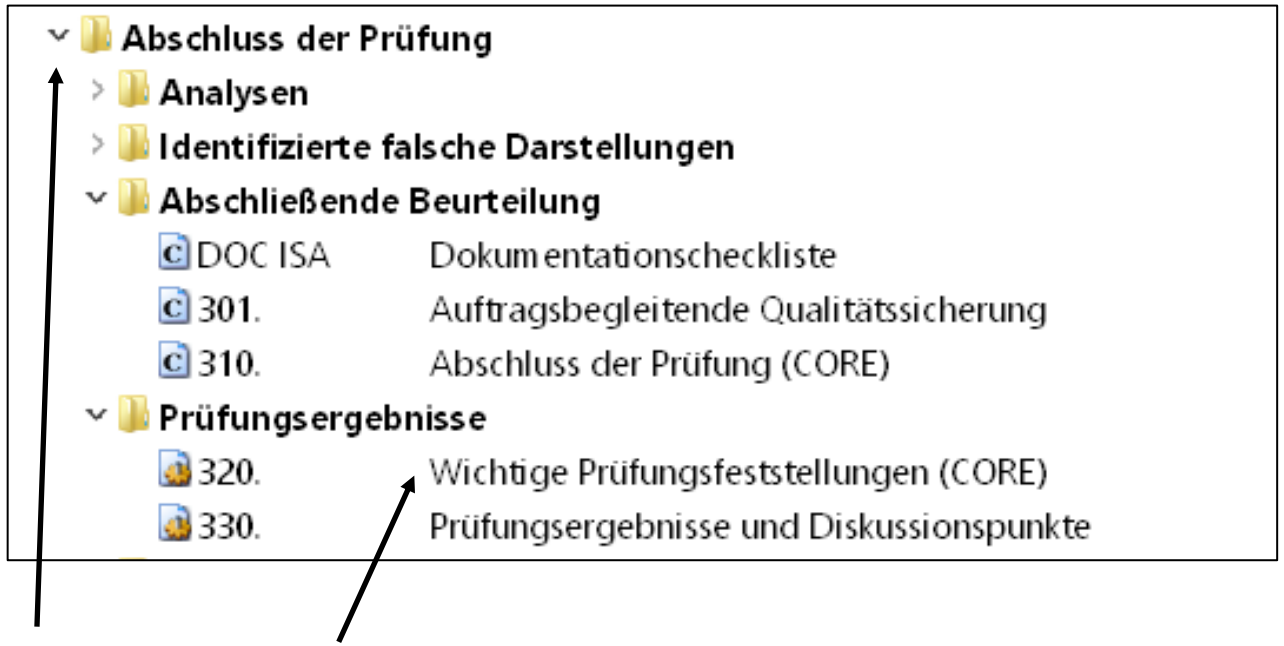
# XV. Wichtige Prüfungsfeststellungen (320)

# XV. 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

# XV. Wichtige Prüfungsfeststellungen (320)




**Zu finden unter Abschluss der Prüfung**

# XV. 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*

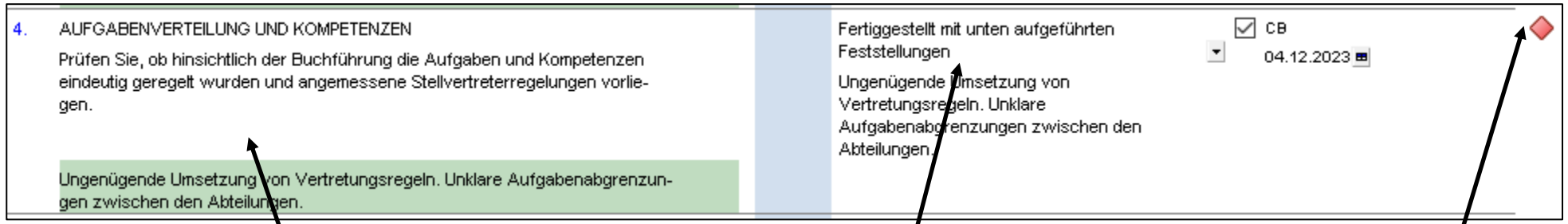
**Auflistung der Prüfungsfeststellungen**

**Zu Grunde liegendes Dokument**

**Falls erledigt, hier markieren danach kann auch sortiert werden**

# XV. Wichtige Prüfungsfeststellungen (320)

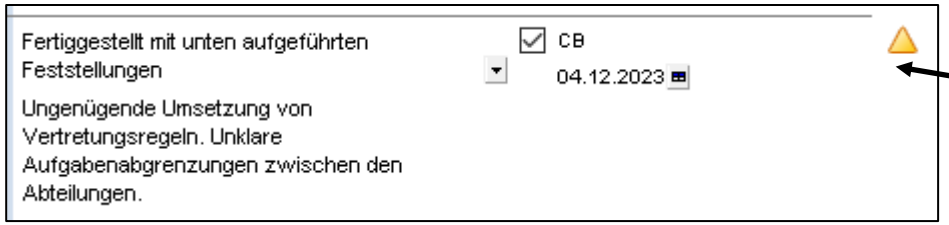
## Erstellen einer wichtigen Prüfungsfeststellung




**Prüfungshandlung**

**Prüfungsfeststellung**

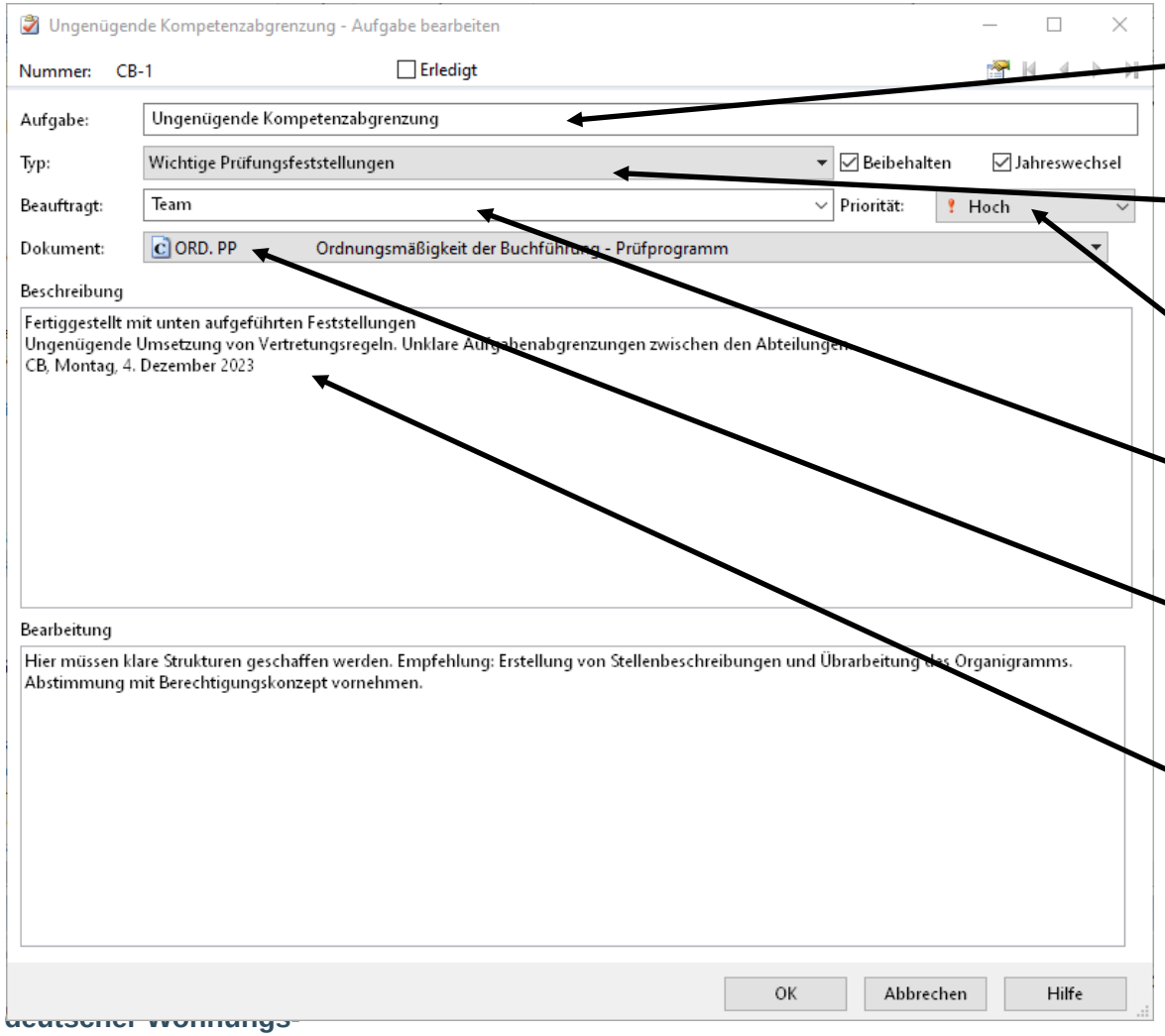
**Aufgabe ist noch Nicht angelegt.**




**Aufgabe ist angelegt.**

# XV. Wichtige Prüfungsfeststellungen (320)

## Erstellen einer wichtigen Prüfungsfeststellung




**Kurzbeschreibung der Prüfungsfeststellung**

**Typ: Wichtige Prüfungsfeststellung!!**

**Festlegung der Priorität**

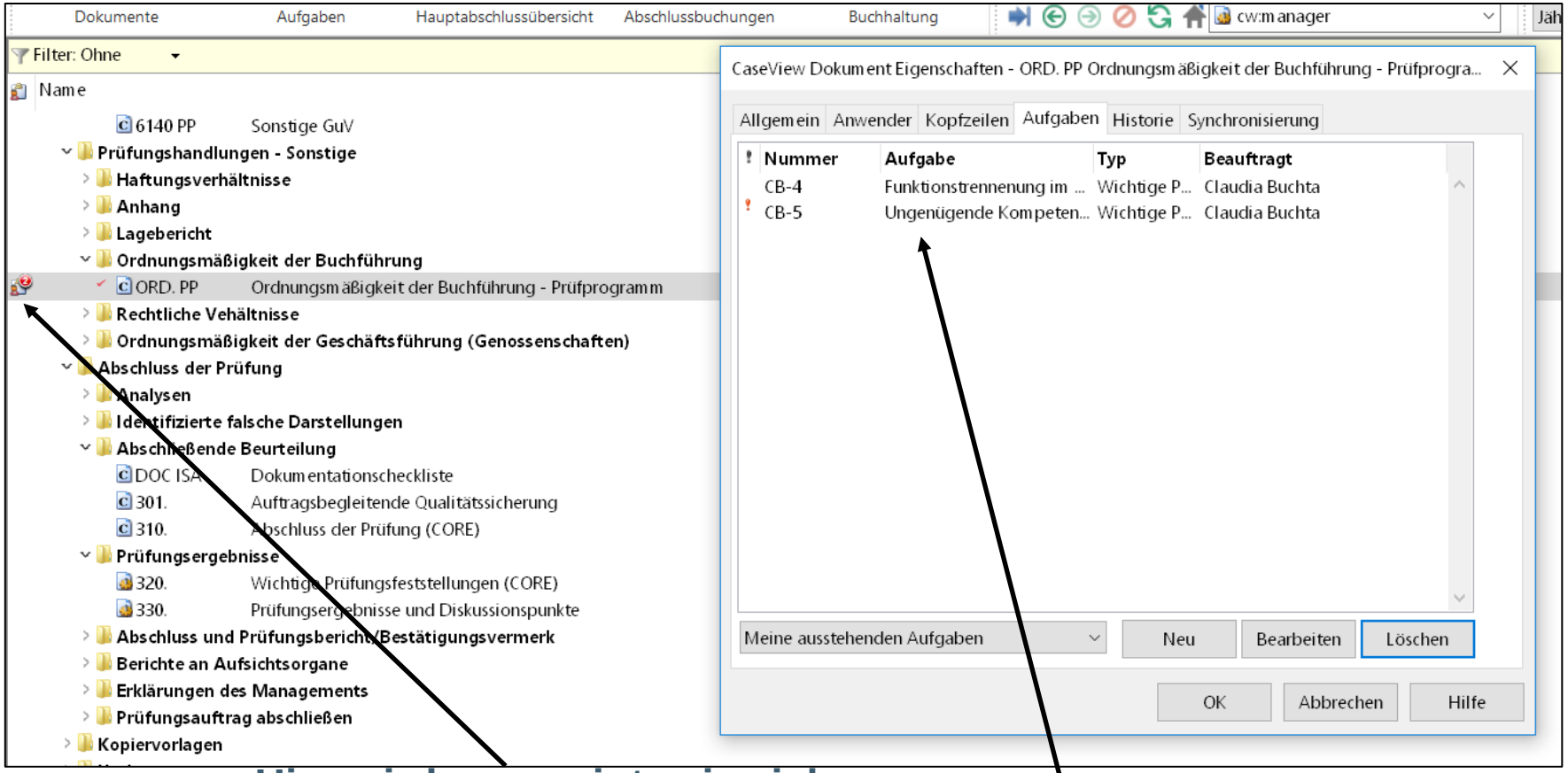
**Adressat der Prüfungsfeststellung**

**Bezugsdokument**

**Genauere Beschreibung der Feststellung**

# XV. Wichtige Prüfungsfeststellungen (320)

## Erstellen einer wichtigen Prüfungsfeststellung




**Hier wird angezeigt, wie viele Aufgaben angelegt sind**

**Mit Doppelklick werden die Aufgaben angezeigt**

# XV. 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.

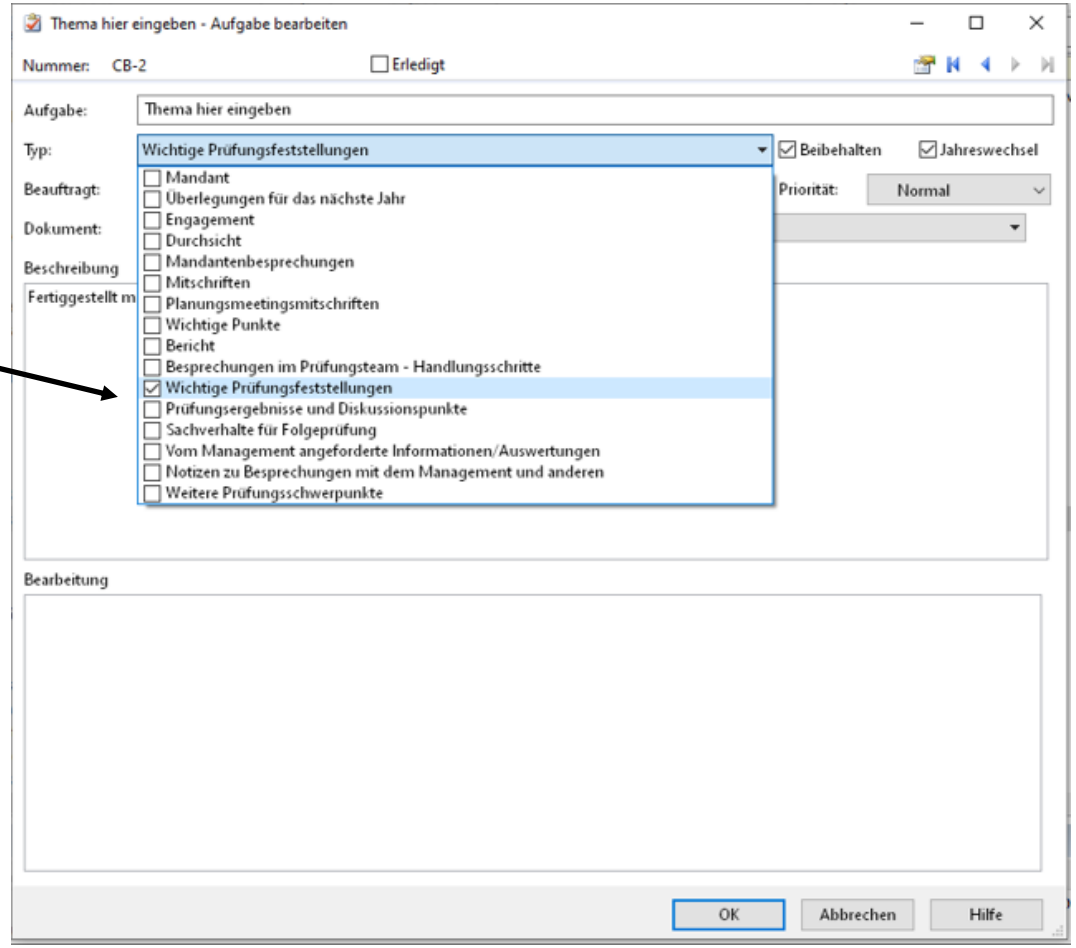
Stellen Sie sicher, dass Folgendes dokumentiert wird:
1) Die Beschreibung des wichtigen Punkts.
2) Die vorgeschlagene Lösung.
3) Die gezogenen Schlussfolgerungen.
4) Ob der Punkt den für die Überwachung Verantwortlichen gemeldet werden soll.

# XV. Wichtige Prüfungsfeststellungen (320)

## Erstellen einer wichtigen Prüfungsfeststellung

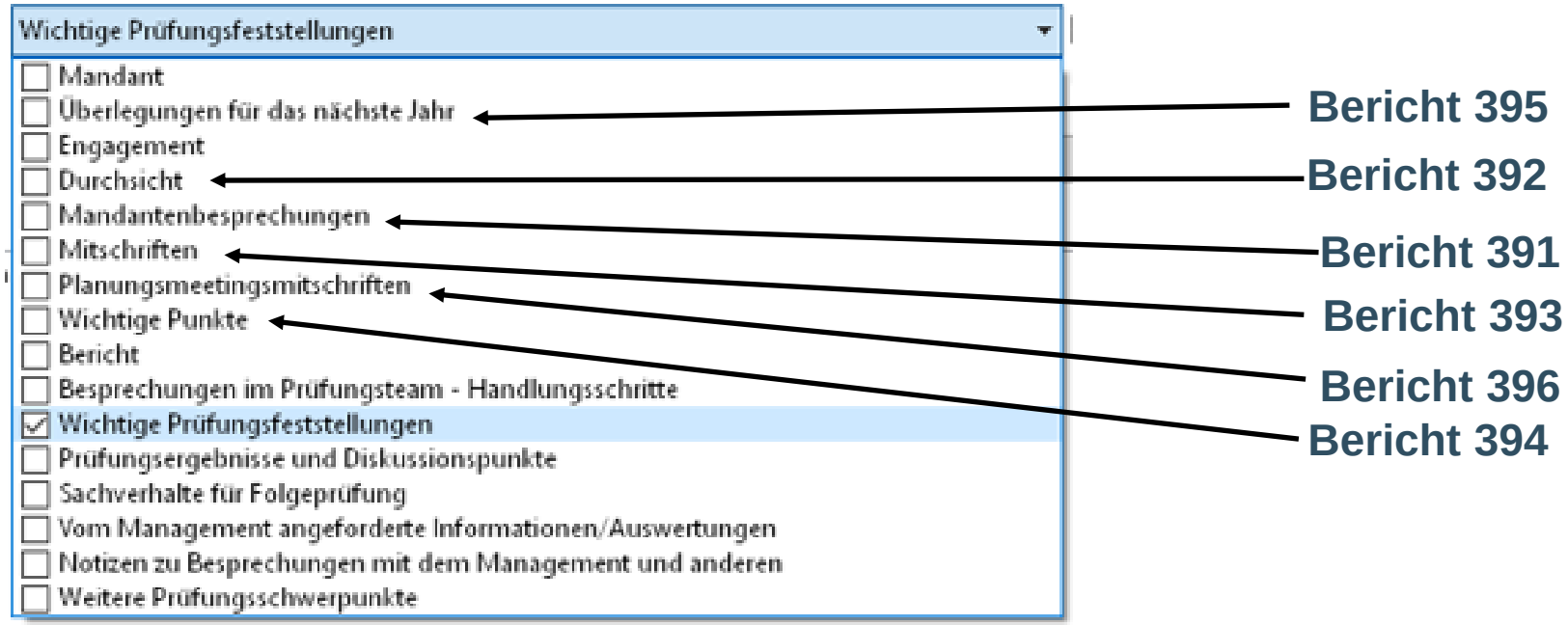
**Wichtig ist die Festlegung des Berichtstypen!**

**Er steuert in welchen Bericht die Aufgabe dargestellt wird.**
**Es ist möglich mehrere Berichtsarten auszuwählen!**



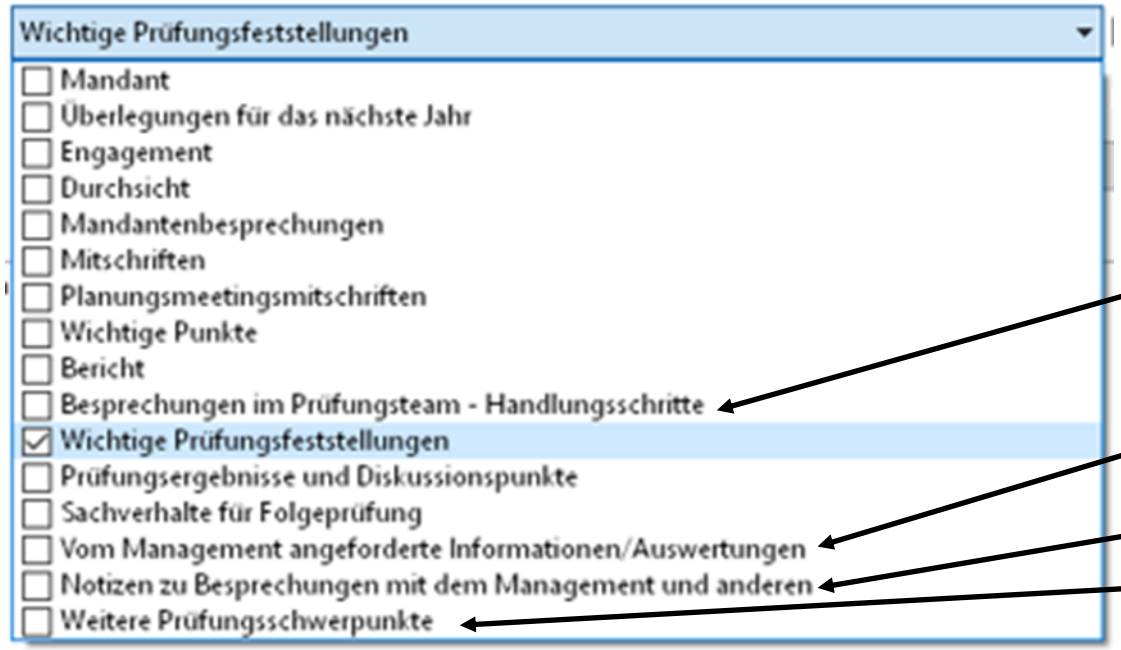
# XV. Wichtige Prüfungsfeststellungen (320)

## Erstellen einer wichtigen Prüfungsfeststellung



# XV. Wichtige Prüfungsfeststellungen (320)

## Erstellen einer wichtigen Prüfungsfeststellung




Bericht 436-1

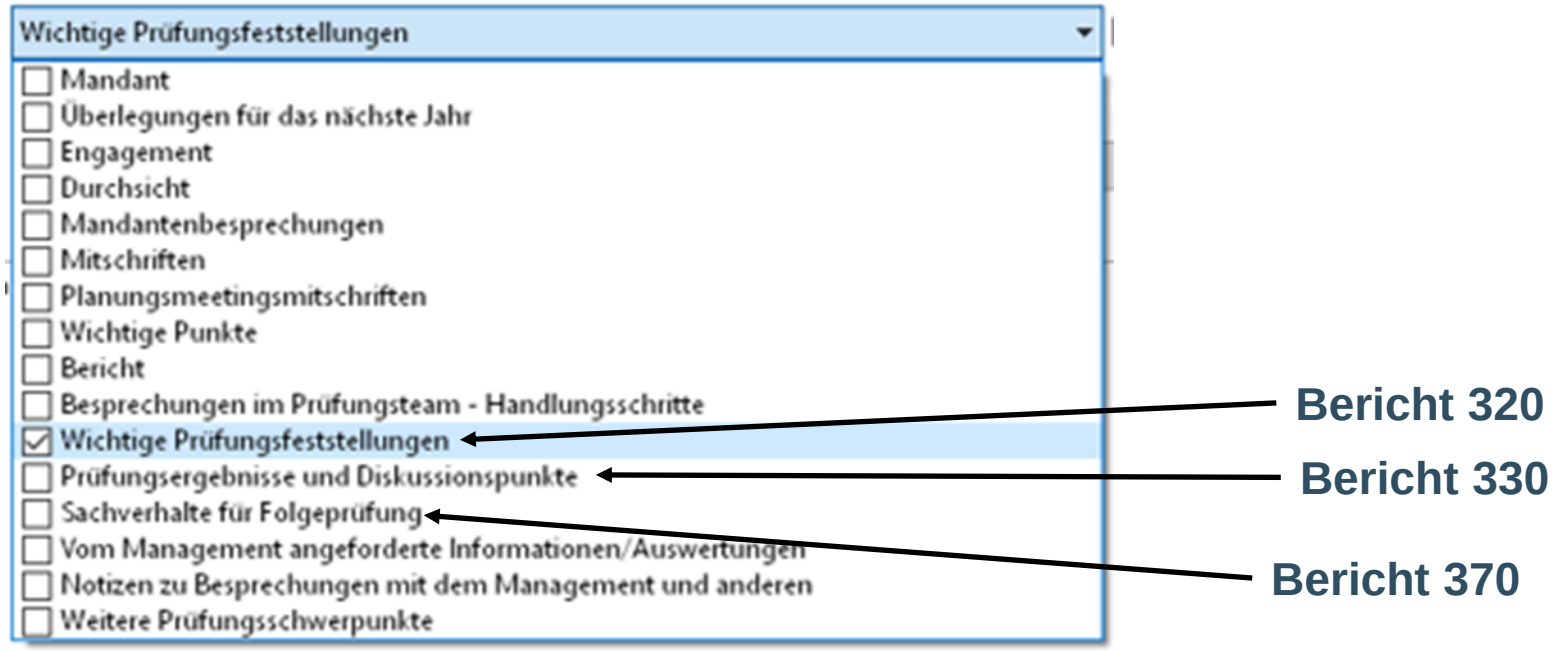
Bericht 440

Bericht 509

Bericht 436.RET

# XV. Wichtige Prüfungsfeststellungen (320)

## Erstellen einer wichtigen Prüfungsfeststellung

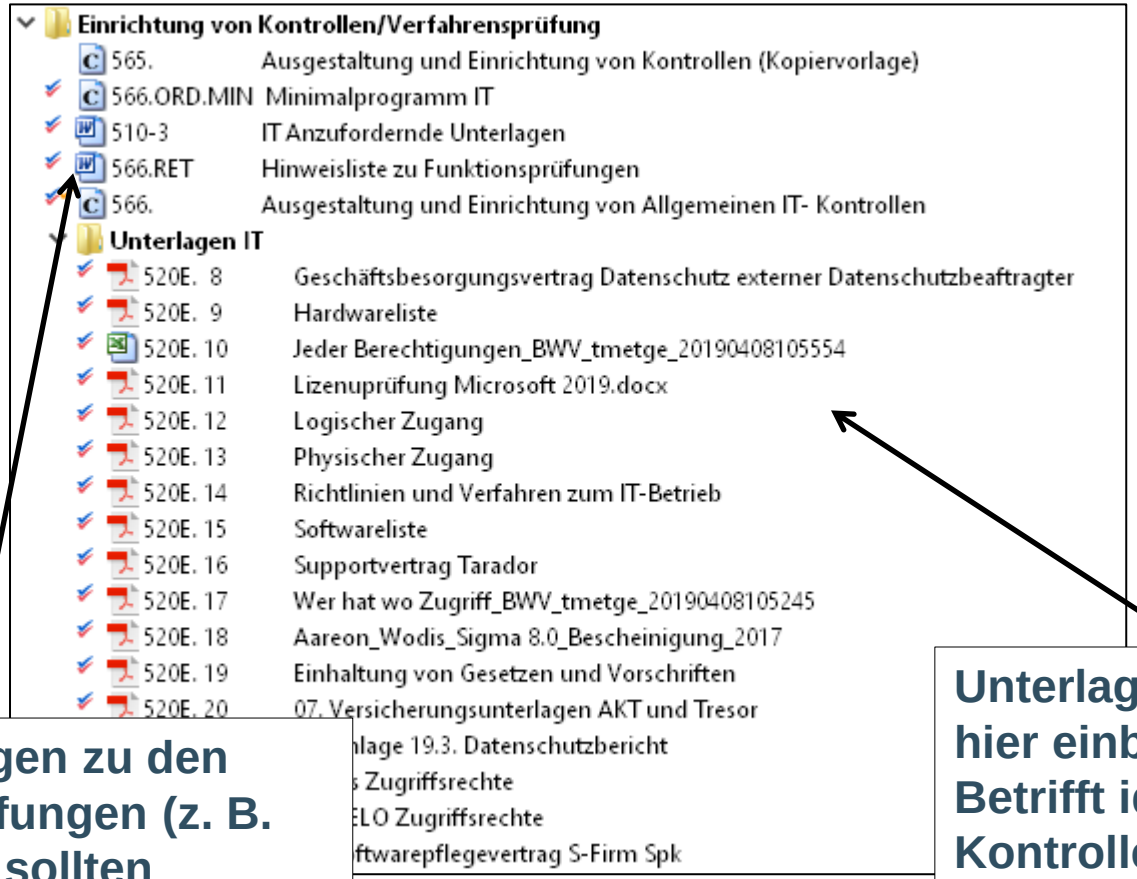


# XVI. Arbeitspapiere und Berichterstattung

# XVI. Arbeitspapiere und Berichterstattung

- Die Dokumente 566, ORD.PP und 566.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).

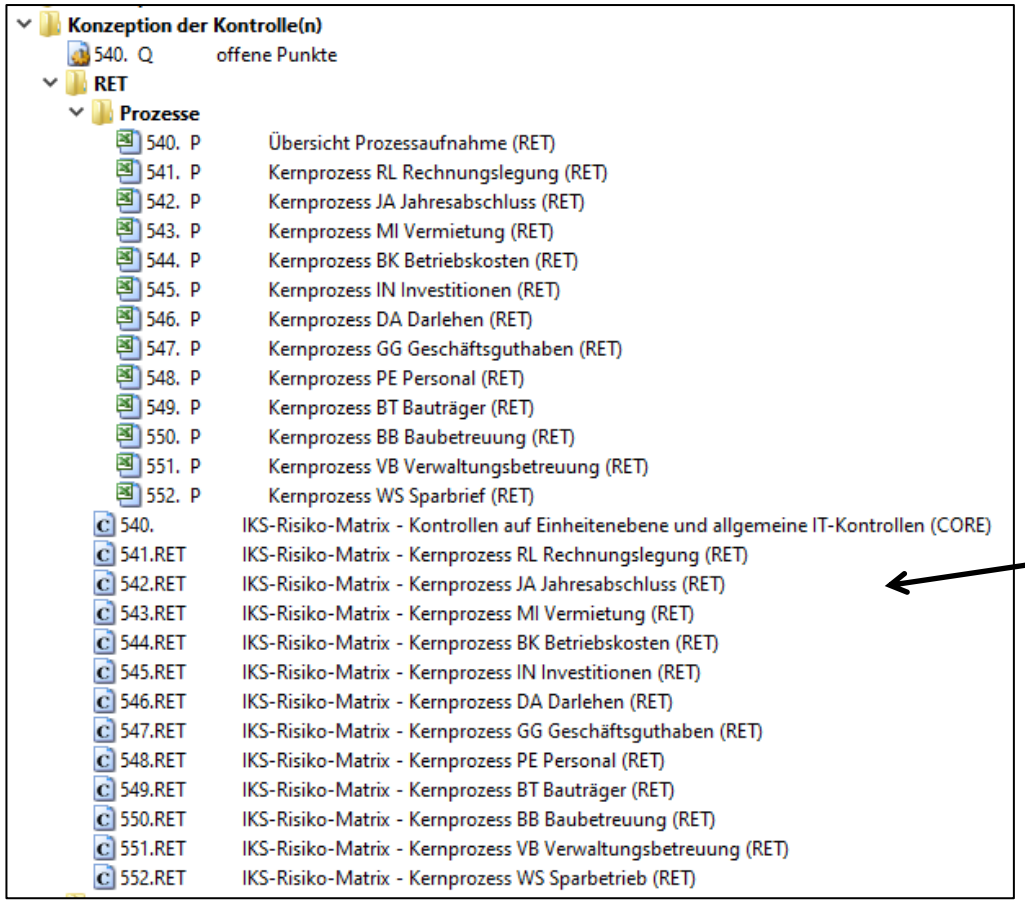
# XVI. Arbeitspapiere und Berichterstattung




**Auch Unterlagen zu den Funktionsprüfungen (z. B. Screenshots) sollten eingebunden werden.**

**Unterlagen zur IT am besten hier einbinden.
Betrifft idR die generellen IT-Kontrollen.**

# XVI. Arbeitspapiere und Berichterstattung




**Für die Prüfung der IT-gestützten Kontrollen bzw. Report-Kontrollen**

**Unterlagen wie**
**- Walk Through oder**
**- Funktionsprüfungen**
**könnten hier abgelegt werden.**
**In Bezug zu den einzelnen Prozessen.**

# XVI. Arbeitspapiere und Berichterstattung
# Formen der Berichterstattung

Prüfungsbericht

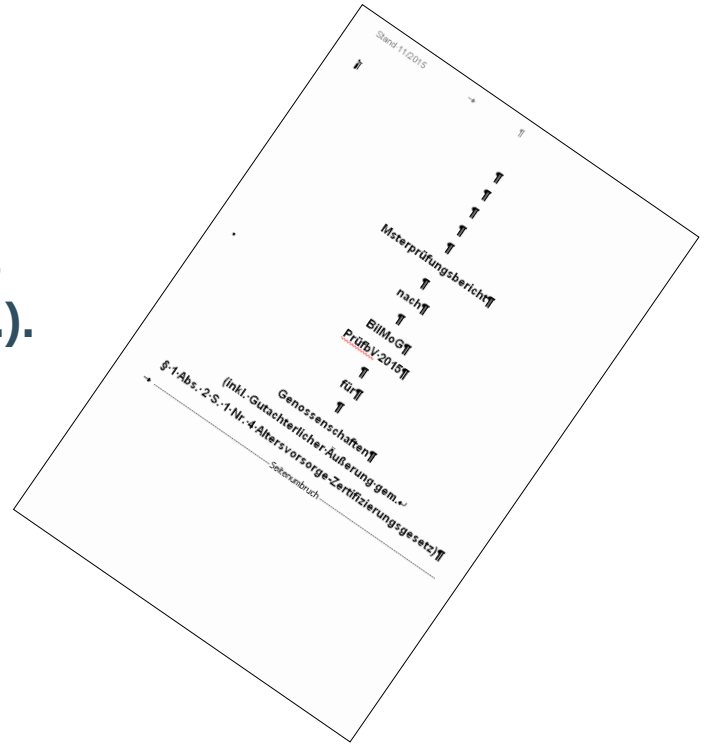
Management Letter

Maßnahmenkatalog

# XI. Arbeitspapiere und Berichterstattung Prüfungsbericht

**>> 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)



# XVI. Arbeitspapiere und Berichterstattung
# Prüfungsbericht

**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?**

# XVI. 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.**

# XVI. 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.**

# XVI. Arbeitspapiere und Berichterstattung
# Management Letter

**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.**

# XVI. Arbeitspapiere und Berichterstattung
# Management Letter

**Beispielhafter Aufbau eines Management Letter:**

- **Aussagekräftige Überschrift**
- **Ziel der Prüfung**
- **Vorgehensweise**
- **Beschreibung der Feststellung**
- **Darstellung des darin liegenden Risikos**
- **Empfehlung**

**Ggf. Erweiterung des Management Letter (ML) um einen Maßnahmenkatalog**

# XVI. Arbeitspapiere und Berichterstattung
# Management Letter

**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.

# XVI. Arbeitspapiere und Berichterstattung
# Maßnahmenkatalog

**Empfohlene Maßnahmen**
**IT-Systemprüfung**

| Risikobereich | Maßnahme Nr. | Feststellungen | Risiko-bewertung | Vorgeschlagene Maßnahme | Priorisierung<br>1= Umsetzung dringend empfohlen<br>2= Umsetzung zeitnah empfohlen<br>3= Umsetzung bei Gelegenheit empfohlen<br>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 |

# XVI. Arbeitspapiere und Berichterstattung
# Gruppenübung

**Fragestellung:**

**Bei der IT-Systemprüfung wurden verschiedene Feststellungen getroffen.  Wählen Sie verschiedene Feststellungen aus und formulieren Sie jeweils die Berichterstattung im Prüfungsbericht und im Maßnahmenkatalog. Schlagen Sie Verbesserungspotentiale vor.**

**Zeitumfang: 20 Minuten**

**Wer:**

**Aufteilung in 4 Gruppen**

# XVI. Arbeitspapiere und Berichterstattung
# Gruppenübung

**Fallbeispiele:**

a. Es ist kein Notfallkonzept vorhanden.
b. Eine PC-Richtlinie existiert nicht.
c. Das Datensicherungskonzept ist nicht dokumentiert.
d. Die Anwendungssoftware erfüllt nicht die gesetzlichen Ordnungsmäßigkeitskriterien.
e. Leere Passwörter sind möglich.
f. Es gibt keinen Datenschutzbeauftragten.
g. Das Berechtigungskonzept weist wesentliche Schwächen auf.
h. Die Anlagenbuchhaltung wird in Excel geführt.
i. Der Virenschutz ist nicht aktuell.
j. Der Zugriff der Fernwartung wird nicht protokolliert.
k. Stammdatenänderungen werden nicht protokolliert.

# XVII. Wichtige Internetadressen

# XVII. 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**