EBNER STOLZ

SAP Compliance- und Risikomanagement

Herausforderungen und Anforderungen

Hamburg, 29. Juni 2023

A member of Nexia International

Inhaltsverzeichnis

Inhaltsverzeichnis

Unser Team – Ein bunter Strauß Vielfalt

Die Qualität der Prüfung steht im Vordergrund und resultiert aus unserer Fachkompetenz und der Erfahrung unserer Mitarbeiter

> 80
Mitarbeiter

Hamburg, Stuttgart, Köln, München, Düsseldorf, Frankfurt, Leipzig, Berlin, Reutlingen
9 Standorte

>7 Jahre
Durchschnittliche Berufserfahrung

Qualifikationen

alle einschlägigen und notwendigen vorhanden

18	CISA
2	CIA
2	WP und StB
10	ISO 27001 LA

sowie CISM, CASA, CFE, CDPSE, CRISC, QA DIIR, QAR IT ISACA, DSB/GDD, PMP, ...

Ihre Referenten

Matthias Ruhe

CISA – ISO 27001 LA – CASA

Senior Manager

matthias.ruhe@ebnerstolz.de

Max Moldenhauer

Senior Consultant

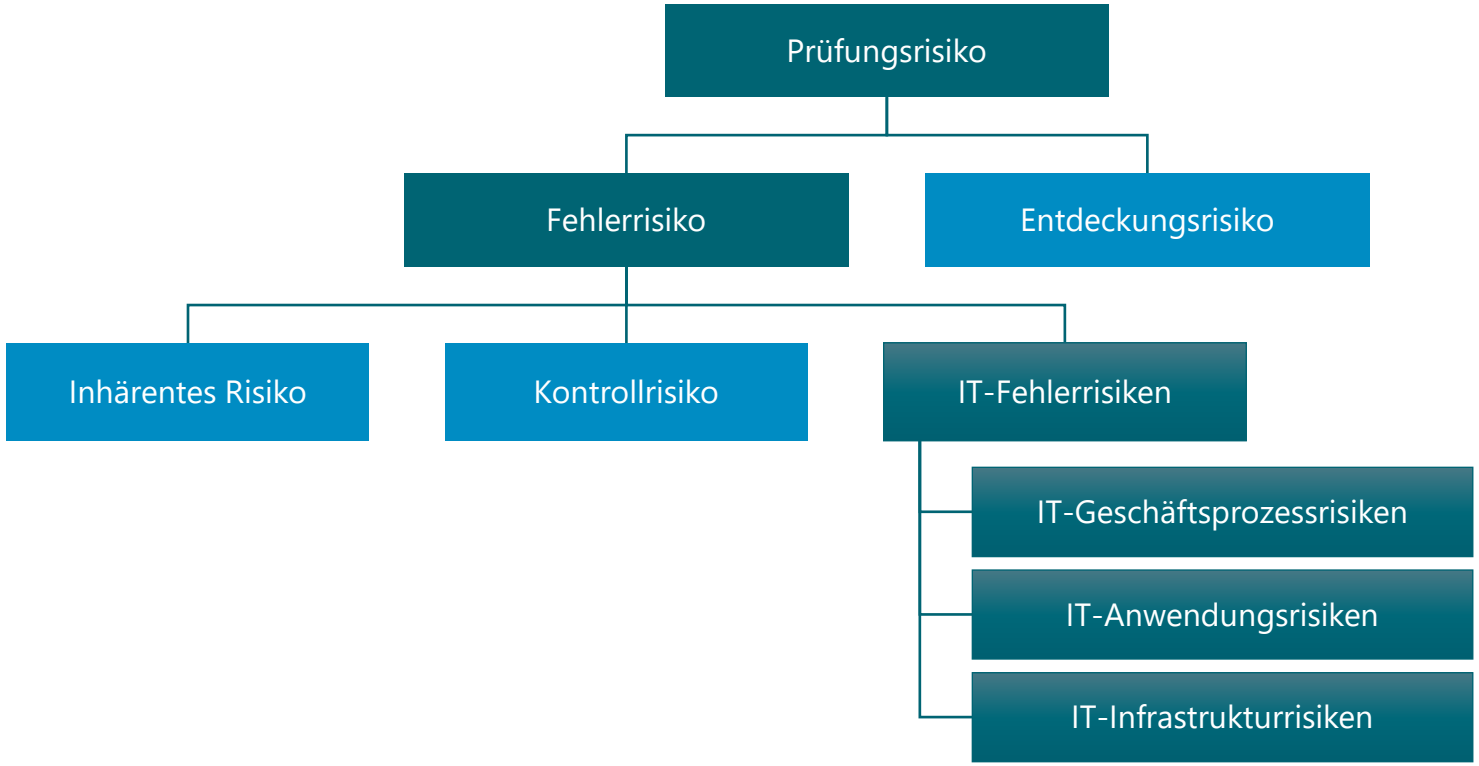
max.moldenhauer@ebnerstolz.de

Inhaltsverzeichnis

Wirtschaftsprüfer und die Jahresabschlussprüfung

1. Aufgabe des WPs: Beurteilung der Korrektheit des Jahresabschlussberichts
2. Risikoorientierter Prüfansatz
3. Behandlung von allgemeinen Fehlerrisiken
   - Darunter Fehlerrisiken die sich aus IT-Komponenten und Prozessen ergeben
   - IT-Prüfung um die relevanten IT-Komponenten zu prüfen und das Fehlerrisiko zu beurteilen

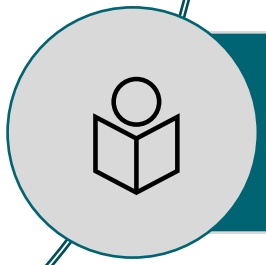
Risiken der Abschlussprüfung



Prüfungsschritte

Der ISA [DE] 315 behandelt die Verantwortlichkeit des Abschlussprüfers zur Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen im Abschluss.

Mit dem ISA [DE] 315 stellt die IT-Prüfung einen Teil der IKS-Prüfung dar, aber nun als ein integraler, nicht trennbarer Bestandteil.



Der ISA [DE] 315 ist **nicht** der Prüfungsstandard für die IT-Prüfung im Rahmen der Jahresabschlussprüfung, sondern dient zentral der Risikoidentifikation durch den Abschlussprüfer.

ISA [DE] 315 (revised) | Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen

Tz. 7

Der Prozess der Risikoidentifizierung und -beurteilung des Abschlussprüfers ist iterativ und dynamisch.

Das Verständnis des Abschlussprüfers von der Einheit und ihrem Umfeld, die maßgebenden Rechnungslegungs-grundsätze und das **interne Kontrollsystem** der Einheit sind interdependent mit Konzepten innerhalb der Anforderungen zur Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen.

Bei der Erlangung des vom ISA [DE] 315 geforderten Verständnisses können erste Risikoerwartungen entwickelt werden, die weiter verfeinert werden können während der Abschlussprüfer im Risikoidentifizierungs- und beurteilungsprozess fortschreitet.

Darüber hinaus verpflichten der ISA [DE] 315 und ISA [DE] 330 den Abschlussprüfer, basierend auf Prüfungsnachweisen, die aus den in Übereinstimmung mit ISA [DE] 330 durchgeführten weiteren Prüfungshandlungen erlangt wurden, oder wenn neue Informationen erlangt werden, die **Risikobeurteilung anzupassen** und weitere allgemeine Reaktionen sowie **weitere Prüfungshandlungen zu modifizieren**.

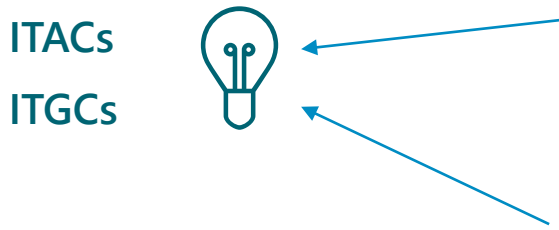
ISA [DE] 315 (revised) | Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen

Definitionen – Tz. 12

Kontrollen der Informationsverarbeitung – 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 (vgl. Tz. A6).

Definitionen - Tz. A6

Risiken für die Integrität von Informationen entstehen aus der Anfälligkeit der Informationsregelungen der Einheit – dies sind Regelungen, die die Informationsflüsse, Aufzeichnungen und Berichtsprozesse im Informationssystem der Einheit definieren – für eine unwirksame Implementierung. Kontrollen der Informationsverarbeitung sind Maßnahmen, die eine wirksame Implementierung der Informationsregelungen der Einheit unterstützen. **Kontrollen** der Informationsverarbeitung können **automatisiert** (d. h. **in IT-Anwendungen eingebettet**) oder manuell (z. B. Input- oder Output-Kontrollen) sein und **können sich auf andere Kontrollen stützen, einschließlich** anderer Kontrollen der Informationsverarbeitung oder **genereller IT-Kontrollen.**



ISA [DE] 315 (revised) | Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen

Kontrollaktivitäten – Tz. 26

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

(a) Identifizierung von Kontrollen, die die Risiken wesentlicher falscher Darstellungen auf Aussageebene in der Komponente Kontrollaktivitäten behandeln

(b) auf Grundlage der nach (a) identifizierten Kontrollen **Identifizierung von IT-Anwendungen** und anderen Aspekten der IT-Umgebung der Einheit, die sich aus dem IT-Einsatz ergebenden Risiken unterliegen (vgl. Tz. A166–A172)

(c) für solche IT-Anwendungen und anderen nach (b) identifizierten Aspekten der IT-Umgebung Identifizierung von (vgl. Tz. A173–A174):

   i. damit verbundenen, **sich aus dem IT-Einsatz ergebenden Risiken** und

   ii. die **generellen IT-Kontrollen** der Einheit, die solche Risiken behandeln

ISA [DE] 315 (revised) | Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen

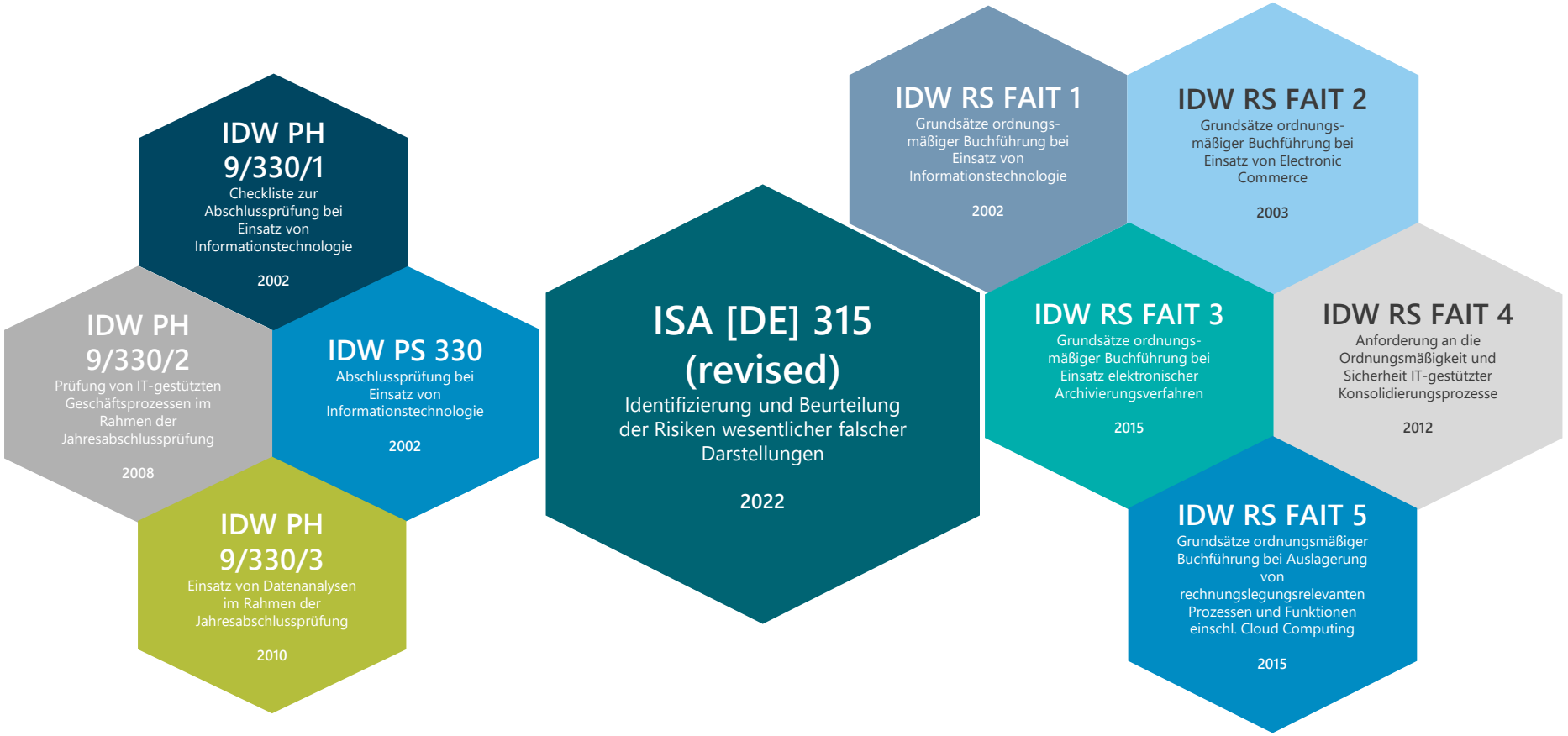
Generelle IT-Kontrollen – A 166

Hängen Kontrollen der Informationsverarbeitung von generellen IT-Kontrollen ab, kann der Abschlussprüfer festlegen **die Wirksamkeit der Funktion der generellen IT-Kontrollen zu prüfen**, die dann die Planung von Funktionsprüfungen für solche generellen IT-Kontrollen erfordert.

Legt der Abschlussprüfer unter den gleichen Umständen fest die Wirksamkeit der Funktion der generellen IT-Kontrollen nicht zu prüfen oder wird erwartet, dass die generellen IT-Kontrollen unwirksam sind, kann es erforderlich sein die verbundenen, **aus dem IT-Einsatz resultierenden Risiken durch die Planung von aussagebezogenen Prüfungshandlungen zu behandeln**.

Es kann jedoch sein, dass die aus dem IT-Einsatz resultierenden Risiken nicht behandelt werden können, wenn solche Risiken mit Risiken verbunden sind, bei denen aussagebezogene Prüfungshandlungen allein keine ausreichenden geeigneten Prüfungsnachweise erbringen. Unter solchen Umständen kann es notwendig sein, dass der Abschlussprüfer die Auswirkungen auf das Prüfungsurteil würdigt.

Überblick Prüfungsstandards und Prüfungshinweise



Ordnungsmäßigkeits- und Sicherheitsanforderungen gemäß IDW RS FAIT 1

Ordnungsmäßigkeitsanforderungen

- Vollständigkeit
- Richtigkeit
- Zeitgerechtheit
- Ordnung
- Nachvollziehbarkeit
- Unveränderlichkeit

Sicherheitsanforderungen

- **Vertraulichkeit**: kein Unbefugter kann auf Informationen zugreifen und diese lesen
- **Integrität**: Daten und Systeme stehen vollständig und richtig zur Verfügung, kein Unbefugter kann Informationen verändern
- **Verfügbarkeit**: Informationen sind dann verfügbar, wenn sie benötigt werden; Voraussetzung sind funktionsfähige Ressourcen
- **Autorisierung**: Bearbeitung und Weitergabe von Informationen oder Geschäftsvorfällen erfolgen nur durch Berechtigte
- **Authentizität**: Informationen stammen aus der vorgegebenen Quelle; eindeutige Zuordnung zum Verursacher
- **Verbindlichkeit**: die Quelle der Informationen kann deren Sendung nicht abstreiten; Herbeiführung bindender Rechtsfolgen

Zusammenspiel von Wirtschaftsprüfer und IT-Prüfer in der Prüfung

WP: Beurteilung Bilanz, GuV, Lagebericht und Anhang
IT-P: Aufnahme der IT-Landschaft, IT-gestützte Geschäftsprozesse und Kontrollen

WP und IT-P:

Einschätzung der Komplexität; Identifikation von wesentlichen prüfungsrelevanten IT-Applikationen und Geschäftsprozessen

IT-P: Prüfung und Beurteilung der Wirksamkeit der Kontrollen des allgemeinen IT-Umfelds (**IT**-**G**eneral **C**ontrols **ITGCs**)

IT-P: Prüfung und Beurteilung der Wirksamkeit der applikationsspezifischen Kontrollen (**IT**-**A**pplication **C**ontrols - **ITACs**)

IT-P: Berichterstattung an WPs hinsichtlich spezifischer Risiken aus dem IT-Bereich und allgemeiner IT-Fehlerrisiko-Beurteilung

WP: Basierend auf dem ermittelten Risiko der IT-Prüfung Erweiterung / Reduktion des Prüfungsumfangs von substanziellen Prüfungshandlungen

Aufnahme der IT-Systemlandschaft

ORGANISATION

- IT-Strategie und Berichterstattung
- IT-Aufbauorganisation
- Projektplanung
- IT-Risikomanagement und IT-Sicherheit
- Notfallmanagement
- Datenschutz
- Softwarezertifizierung

INFRASTRUKTUR

- Physische Sicherheit

IT-SUPPORT

- Betriebssysteme
- Datenbanken
- Antivirus
- Firewall/externer Zugriff

IT-Kontrollen | IT-General Controls

IT General Controls (ITGC)

- Werden aus den IT-Prozessen abgeleitet
- Haben unterstützenden Charakter
- Haben i. d. R. keinen direkten Bezug zu den Fachbereichen
- **Sind Voraussetzung für die Effizienz und Wirksamkeit von Application Controls**
- Können, soweit nicht angemessen und/oder unwirksam, zu wesentlichen Prüfungsrisiken führen
- Beeinflussen u. U. auch manuelle Kontrollen, bspw. bei der Verwendung von Reports/System-Output

ITGCs umfassen die folgenden 4 Bereiche

1. IT-Operations
2. Logical Access
3. Change Management
4. Outsourcing (sofern relevant)

IT-General Controls

LOGICAL ACCESS

Zugang zu Programmen und Daten

- System / Applikation
- Datenbank
- Betriebssystem

COMPUTER OPERATIONS

IT-Betrieb

- Datensicherung
- Hardware Monitoring
- Software Monitoring
- Schnittstellen

CHANGE MANAGEMENT

Systemänderungen

- Änderbarkeit im Produktivsystem
  - Mehrstufige Systemumgebung
  - Prozess
- Anforderung von Änderungen
- Test und Freigabe

OUTSOURCING

- Auslagerung relevanter Prozesse
  - Dienstleistersteuerung
  - Dienstleisterüberwachung
  - Sicherstellung der Wirksamkeit des dienstleistungsbezogenen internen Kontrollsystems

IT-General Controls in SAP

LOGICAL ACCESS

- Zugriffsberechtigungen (PW, SSO, Gültigkeit, Benutzertyp)
- Berechtigungskonzepte
- Can-Do Analysen (über SUIM / RSUSR002)
- Did-Do Analysen (ST03N et. al.)
- **CheckAud in der JAP**

COMPUTER OPERATIONS

- Datensicherungen
- Hardware-Monitoring
- Schnittstellen (EDIs, IDOCs, RFCs,…)
- Verbuchungsabbrüche
- Batch-Jobs

CHANGE MANAGEMENT

- Fachliche Freigaben und Testverfahren
- Funktionstrennung zwischen Entwicklern und Testern
- Systemtrennung / Mehrsystemlandschaft
- Einstellungen des TMS

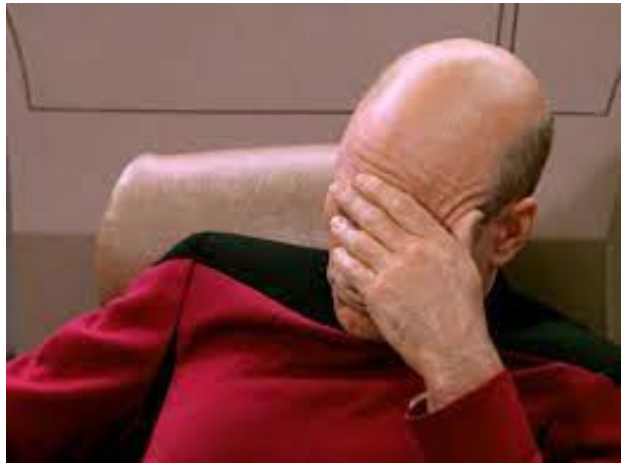
OUTSOURCING

- Was wurde ausgelagert? (RZ SAP-Basis Betrieb? Cloud-Betrieb?)
- Wie wird das IKS der Auslagerungen durch den Mandanten geprüft?
- Gibt es Prüfberichte? (ISAE 3402, SOC 1, PS 951, ….)

Was machen wir im Rahmen der JAP nicht?

Wir prüfen in erster Linie das Interne Kontrollsystem des Mandanten!

Zitat SAP-Admin zu IT-Prüfer: „*Für die Kontrolle der Berechtigungen haben wir doch Sie*“



Inhaltsverzeichnis

Rechtliche Anforderungen im Rahmen einer Migration sind…

- die handels- und steuerrechtlichen Vorschriften zur Ordnungsmäßigkeit der Buchführung (§ 238f. und § 257 HGB sowie §§145 bis 147 AO)
- die vom Bundesfinanzministerium herausgegebenen Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) (Schreiben des Bundesministers der Finanzen vom 16. Juli 2001)
- der IDW Prüfungsstandard IDW PS 330 des Fachausschusses für Informationstechnologie: Abschlussprüfung bei Einsatz von Informationstechnologie vom 24. September 2002
- der ISA [DE] 315 (revised) Identifizierung und Beurteilung der Risiken wesentlicher Falscher Darstellung, gilt für die Prüfung von Abschlüssen für Zeiträume, die am oder nach dem 15.12.2021 beginnen,
  vom 19. Mai 2022
- die IDW Stellungnahme IDW RS FAIT 1 des Fachausschusses für Informationstechnologie (FAIT) des Instituts der Wirtschaftsprüfer über die Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie
- die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) vom 28. November 2019

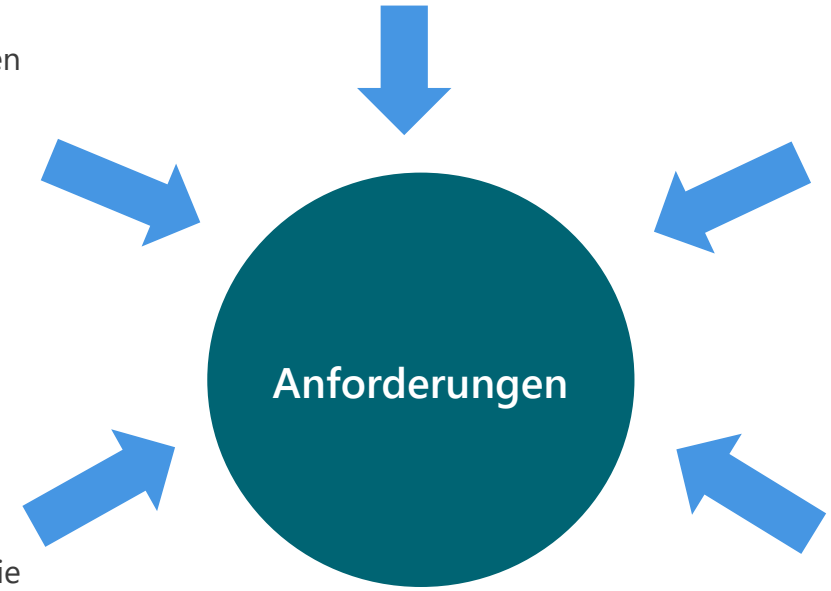
Compliance - Rechtliche Anforderungen an eine Migration

Zeitgerechtheit

- Prüfung auf formale Richtigkeit und Plausibilität
- Vermeidung von Periodenverschiebungen

Unveränderlichkeit

- Unveränderte Dokumentation und Archivierung von Migrationsaktivitäten, Überleitungstabellen, Test, Abstimmungen, Fehlerbehebungen, Freigaben und Kontrollen



Sicherheit

- Analyse und Bewertung der Risiken
- Durchführung von Massentests
- Sicherung des Altsystems nach Vorgaben des HGB und IDW RS FAIT

Vollständigkeit und Richtigkeit

- Grundsatz der Bilanzidentität
- Vollständige und richtige Migration der Einstellungen, Stamm- und Bewegungsdaten, sowie entsprechender Schnittstellenkonfigurationen

Ordnung und Nachvollziehbarkeit

- Nachvollziehbares Migrationskonzept

Aufbewahrung

Warum gibt es eine Aufbewahrungspflicht?

- Schutz von immateriellem Betriebsvermögen
- Nachweis der Einhaltung gesetzlicher Anforderungen
- Haftungssicherung
- Firmenidentität
- Gefährdung des Going Concern möglich

§ 257 Abs. 1 Nr. 4 HGB

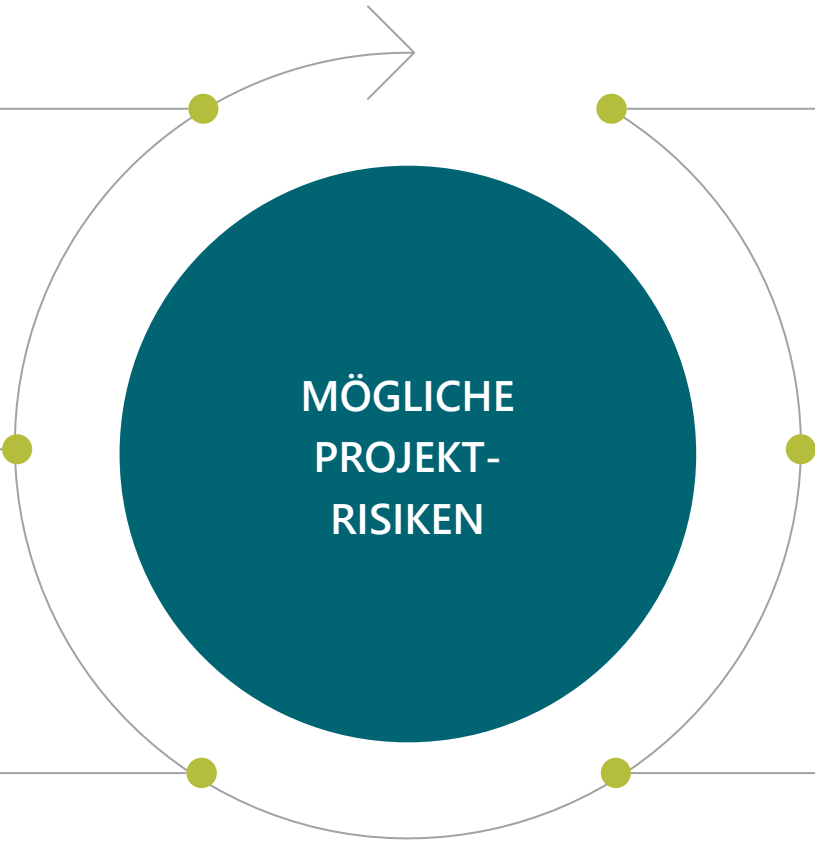
„Jeder Kaufmann ist verpflichtet die folgenden Unterlagen geordnet aufzubewahren:
(…)

4. Belege für Buchungen in den von ihm nach §238 Abs. 1 zu führenden Büchern (Buchungsbelege)“

§ 257 Abs. 4. HGB

„Die in Absatz 1 Nr. 1 und 4 aufgeführten Unterlagen sind **zehn Jahre,** die sonstigen in Absatz 1 aufgeführten Unterlagen sechs Jahre **aufzubewahren**.“

Mögliche Projektrisiken im Rahmen einer Systemeinführung



1 Projektorganisation
- Unzureichende Kommunikation und Reporting erschweren Management und Reaktion auf unerwartete Entwicklungen

2 Konzeption
- Missverständliche Vorgaben/Konzepte
- Fehlende oder nicht umsetzbare Anforderungen
- Fehlende Berücksichtigung von IKS und Compliance

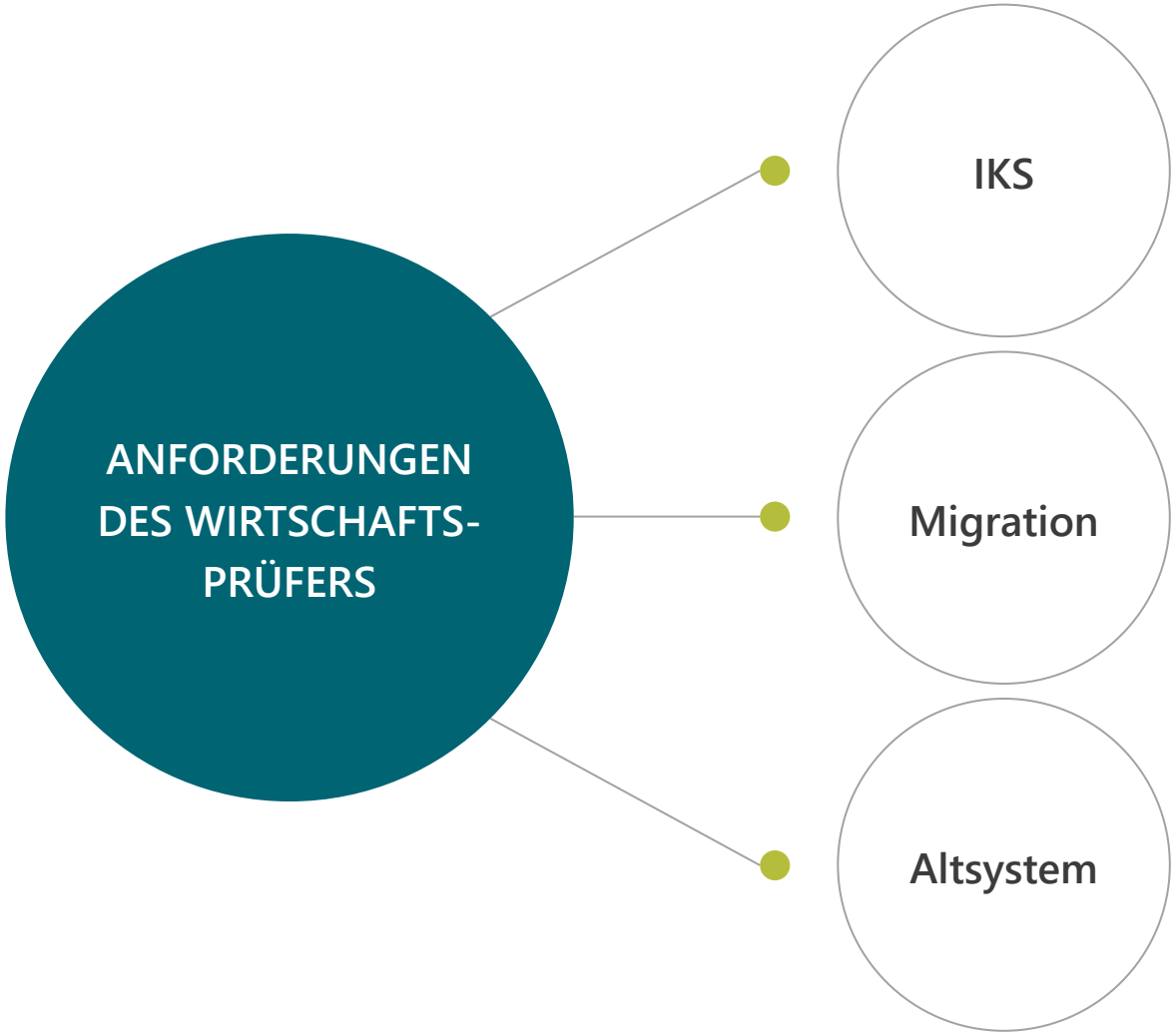
3 Implementierung
- Unvollständige Umsetzung der Konzepte
- Fehlende Funktionalität

4 Test und Freigabe
- Zu geringe oder unvollständige Tests decken nicht alle wesentlichen Fehler auf
- Fehlerhafte Datenbestände

5 Go-Live
- Folgekosten aufgrund unzureichender Abnahme
- Fehler in Cut-Over
- Kein Fall-Back-Szenario

6 Produktivbetrieb
- Fehlende Schulungen
- Zugriffsberechtigungen
- Post Go-Live Support

Anforderungen des Wirtschaftsprüfers bei einer Systemumstellung



- Die Kontrollen des IKS werden im Systemdesign berücksichtigt und implementiert
- Das (neue) IKS ist ab Go-Live genauso wirksam wie zuvor
- Die Kontrollen müssen spätestens im Rahmen der Vorprüfung geprüft werden

- Alle relevanten Daten und Systemeinstellungen werden vollständig und richtig migriert
- Die Systemeinführung und Migration sind angemessen, nachvollziehbar und vollständig dokumentiert

- Das Altsystem ist mit seinen Daten entsprechend der GoBD zu archivieren
- Zugriff auf das Altsystem wird bei unterjähriger Migration ohne Bewegungsdaten ermöglicht

Anforderungen des Wirtschaftsprüfers bei einer Systemumstellung

PHASE 01 - VORBEREITUNG

- Umstellung auf den neuen Geschäftspartneransatz in S/4HANA
- Umsetzung des hieraus folgenden neuen Kreditmanagement (vor allem Einstellungen im Customizing)
- Stammdaten für das Kreditmanagement werden im Geschäftspartner gepflegt
- Identifikation von Funktionen, die in S/4HANA nicht mehr existent sind (z.B. *S4 Readiness-Check*)
- *Umstellung auf das neue Hauptbuch*

PHASE 02 - MIGRATION

- *Übernahme der Stammdaten*
- Übernahme des Globalen Handelsmanagement
- Migration des Hauptbuchs *& Nebenbücher*
- Übernahme der Material-Bewertung: obligatorische IST-Bewertungen mit mehreren Währungen (Material-Ledger)

PHASE 03 - OPTIMIERUNG

- Einstellungen im User Interface
- Einstellungen im Bestellprozess
- Möglichkeiten für das Reporting aus dem System

Anforderungen des Prüfers

- Anforderungen an die Dokumentation der Vorgehensweise
- Erforderliche Informationen für den Abgleich der Daten vor und nach der Umstellung

Anforderungen des Wirtschaftsprüfers bei einer Systemumstellung

PROJEKTDURCHFÜHRUNG & DOKUMENTATION

- Grundlagen Systemumgebung und Datenorganisation Quellsystem / Zielsystem
- Inhalte, Umfang der Datenüberführung (Stammdaten, Bewegungsdaten)
- Migrationskonzept (Vorgehensweise, Ordnungsbegriffe, Umsetzung, Mapping etc.)
- Datenbereinigungsaktionen
- Test-Migrationen
- Überführungskontrollen, Abstimmkonzept (Kontrollzahlenkonzept)
- Dokumentation

ABGLEICH VON DATEN

Grundsätzlich sind alle Daten auf Vollständigkeit abzustimmen. Dies umfasst die:

- Stammdaten
- Bewegungsdaten
- Verkehrszahlen
- Anwendungsparameter

Abgleich kann über

- Stichproben
- ggf. Reportabgleich
- Transaktionen und Reports wie bspw. MMBE, MB52 etc. erfolgen (Bsp. MM-Bewegungsdaten)

Anforderungen des Wirtschaftsprüfers bei einer Systemumstellung - Projektdokumentation

ANFORDERUNGEN AN EINE DOKUMENTATION

- Kurzbeschreibung des Quell-/Altverfahrens
- Kurzbeschreibung des neuen Anwendungsverfahrens
- Planung der Datenübernahme – Bestandsüberführungsauftrag/Teilprojekt
- Übernahme-Stichtag
- Übernahmeverfahren
- Datenkorrekturen
- Sicherung/Archivierung und Abstimmung der Datenüberführung

DOKUMENTATION – NUR PAPIERKRAM?

- Für eine ordnungsgemäße Datenüberführung stehen im Hinblick auf die Ordnungsmäßigkeit, insbesondere Dokumentationsfragen im Vordergrund
- Erst die angemessene Dokumentation stellt letztendlich die Transparenz und Prüfungsfähigkeit und damit die Ordnungsmäßigkeit sicher
- Eine nachhaltige Dokumentation ist daher von vornherein in der Vorgehensweise angemessen zu berücksichtigen
- Relevanz aus handels- und steuerrechtlichen Vorgaben
  Kein „Nice to have“

Systemumstellung und das Interesse des Wirtschaftsprüfers:

Migration und JAP: Der Kreis schließt sich

1. Aufgabe des WPs: Beurteilung der Korrektheit des Jahresabschlussberichts
2. Risikoorientierter Prüfansatz
3. Behandlung von allgemeinen Fehlerrisiken
   - Darunter Fehlerrisiken die sich aus IT-Komponenten und Prozessen ergeben
   - IT-Prüfung um die relevanten IT-Komponenten zu prüfen und das Fehlerrisiko zu beurteilen

Inhaltsverzeichnis

FRAGEN | DISKUSSION

Kontakt

CASA / CISA / ISO 27001 LA
Matthias Ruhe

Senior Manager
Hamburg

matthias.ruhe@ebnerstolz.de
Tel. +49 40 37097-311
Mobil +49 174 1941077

Kontakt

Max Moldenhauer

Senior Consultant
Hamburg

max.moldenhauer@ebnerstolz.de
Tel. +49 40 37097-526
Mobil +49 173 5972715