DORNBACH Consulting GmbH
Anton-Jordan-Straße 1
56070 Koblenz

JAHRESABSCHLUSSPRÜFUNG IM SAP-UMFELD

- **IT-Systemprüfung als Teilbereich der Prüfung des internen Kontrollsystems (IKS)**

Unser Angebot für WirtschaftsprüferInnen und Wirtschaftsprüfungsgesellschaften

Ihre Ziele sind unsere Aufgaben

DORNBACH Consulting GmbH
Anton-Jordan-Straße 1
56070 Koblenz

Inhaltsübersicht:

DORNBACH Consulting GmbH
Anton-Jordan-Straße 1
56070 Koblenz

1. VORWORT (GESELLSCHAFT, DIENSTLEISTUNGSPORTFOLIO)

Die DORNBACH Consulting GmbH ist spezialisiert in den Bereichen IT-Systemprüfung/-Revision, Datenanalyse sowie GoBD-Beratung. Diese Broschüre beschreibt, ergänzend zu den Beschreibungen unserer allgemeinen Broschüre „Prüfungs- und Beratungsdienstleistungen“, explizite Prüfungshandlungen für eine IT-Systemprüfung im SAP-Umfeld.

Eine fundierte IT-Systemprüfung im Rahmen der Jahresabschlussprüfung erfordert insbesondere im SAP-Umfeld, neben dem grundsätzlichen IT-Knowhow, weiterführende Kenntnisse der Software, der dieser zugrunde liegenden Datenbankprodukte und umfassendes Wissen, um die Anforderungen an ein ordnungsgemäßes Rechnungswesen.

Unsere Prüfprojekte werden daher stets durch erfahrene Praktiker (Zertifizierungsbeispiele: SAP FI Berater, Bilanzbuchhalter, IT Auditor [IDW]) durchgeführt, welche vor der Tätigkeit als Auditor, in verantwortlicher Position, in den zu prüfenden Bereichen (IT sowie Rechnungswesen) operativ tätig waren.

Speziell für Prüfungsprojekte im SAP-Bereich haben wir, unter Beachtung der einschlägigen Normen, einen Prüfungsansatz für die effiziente Durchführung von Prüfprojekten (IT-Systemprüfung, IT-Revision, Migrationsprüfung, GoBD-Check, Sicherheitsscheck DS-GVO) entwickelt. Dieser berücksichtigt beispielsweise im Falle der IT-Systemprüfung auftragsabhängig auch den Bereich Datenanalysen, so dass wir unsere Kunden, als Komplettdienstleister, mit skalierbaren Prüfungs- und Beratungsdienstleistungen, vollumfänglich unterstützen.

Betreffend den Bereich Datenanalysen verweisen wir auf unsere separate Broschüre „Analytic Factory“, welche unsere Dienstleistungen für eine effiziente und zielgerichtete Analyse der GoBD-Buchungsdatenausgabe beschreibt.

Mittels Einsatz moderner Revisionstools bearbeiten wir unsere Prüfaufträge sehr effizient. So werden beispielsweise ein Großteil der für die IT-Systemprüfung erforderlichen Informationen, mittels speziell für Belange einer IT-Systemprüfung im SAP-Umfeld entwickelter Datenabfragen, automatisiert aus dem SAP-System extrahiert, was in Folge die Prüfungstätigkeiten am System und die hiermit verbundenen Kosten auf ein Minimum reduziert.

Die Basis für die vorbeschriebenen Tätigkeiten bilden die Software Audicon Audit Solutions („Elektronische Prüfungsakte“), die Software Audicon Smart Exporter (zertifiziert für SAP ERP sowie S/4 HANA / „Extraktion der SAP-Daten“), das Analysetool Idea Smart Analyser („Datenanalyse“), sowie insbesondere die eigenentwickelte Analyse-App MK Solutions (Module: SAP-REVI / SAP-IKS), basierend auf der Entwicklungsumgebung der Software Idea Smart Analyser.

DORNBACH Consulting GmbH
Anton-Jordan-Straße 1
56070 Koblenz

2. IT-SYSTEMPRÜFUNG

2.1 KURZBESCHREIBUNG DER ANFORDERUNGEN

Die Prüfung des IT-gestützten Rechnungslegungssystems ist ein fester Bestandteil einer Abschlussprüfung. Es geht darum zu beurteilen, ob die rechtlichen Anforderungen (Ordnungsmäßigkeits-, Sicherheitsanforderungen) erfüllt werden und zu erkennen, ob Risiken wesentlicher Fehler in der Rechnungslegung bestehen. In diesem Zusammenhang ist zu beachten, dass gemäß HGB §322 Abs. 3, der Wirtschaftsprüfer im Rahmen des Bestätigungsvermerkes bescheinigt, dass die Grundsätze ordnungsgemäßer Buchführung oder sonstiger maßgeblicher Rechnungslegungsgrundsätze eingehalten wurden.

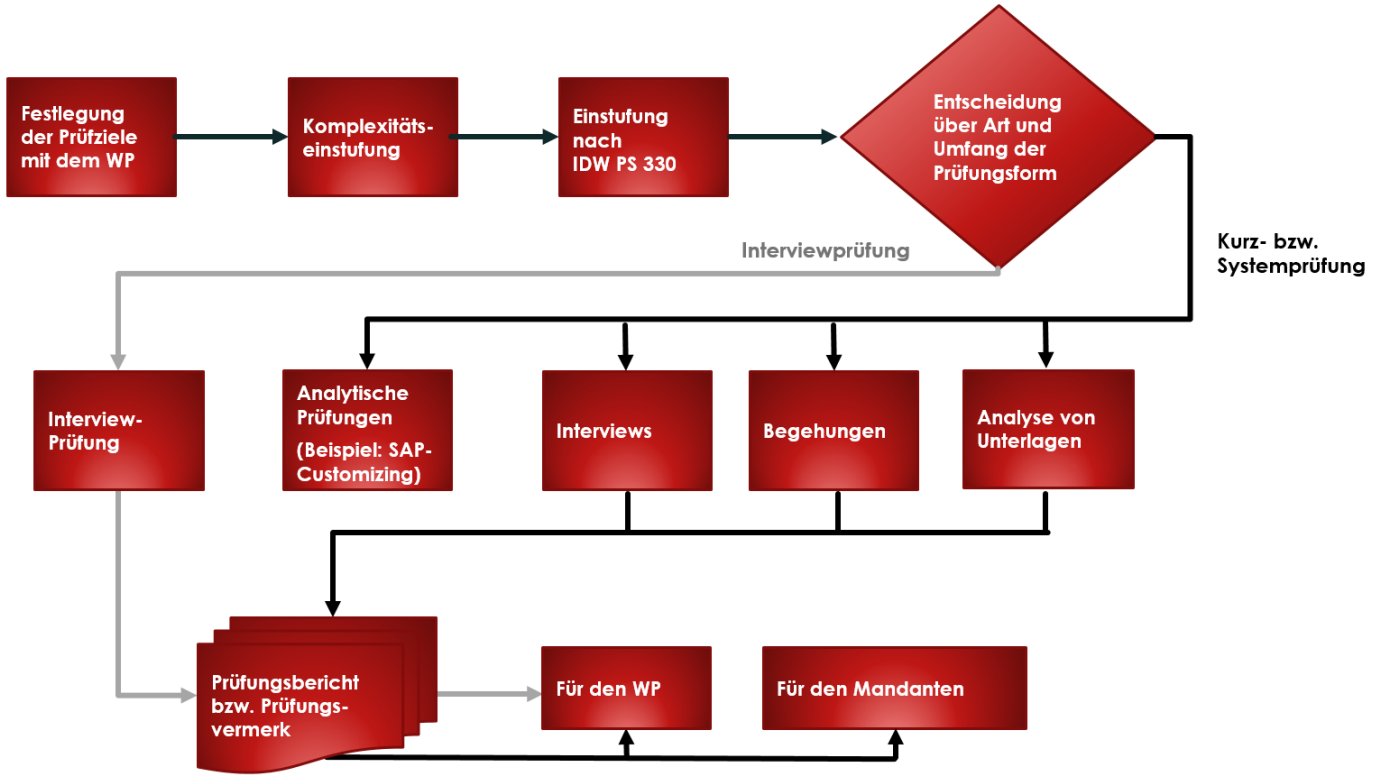
Letzteres stellt auch eine besondere Anforderung an die IT-Systemprüfung. Ergänzend zu den Aussagen betreffend die Ordnungsmäßigkeit und Sicherheit der Systeme, dient sie dem Wirtschaftsprüfer, Informationen zum inhaltlichen Rechnungswesen („Buchhaltung“) als Grundlage für weitere gezielte Kontrollen zu erhalten.

Die IT-Systemprüfung ist somit keine losgelöste Prüfung, sondern vielmehr ein Teilbereich der Prüfung und Beurteilung des internen Kontrollsystems im Rahmen der Jahresabschlussprüfung. In enger Abstimmung mit unseren Kunden wird ein individuell auf die zu prüfende Gesellschaft abgestimmter Prüfungsplan erstellt.

Eine Übersicht unserer Vorgehensweise, sowie detaillierte Informationen zu den Inhalten unseres skalierbaren Prüfungsmodells, finden Sie nachfolgend in den Punkten 2.2 bis 2.13. Letztere vermitteln eine Übersicht der nach unserem Ermessen wesentlichen Kontrollen, jedoch ohne Anspruch auf Vollständigkeit.

Weiterführende Prüfungshandlungen, begründet in einem individuell definierten Scope, sind selbstverständlich möglich.

2.2 VORGEHENSMODELL BEI EINER IT-SYSTEMPRÜFUNG (SYSTEMUNABHÄNGIGE DARSTELLUNG)



2.3 DOKUMENTATION DES CUSTOMIZING DES ZU PRÜFENDEN SYSTEMS (STANDARD BEI ALLEN PROJEKTEN)

Die Dokumentation der zu prüfenden SAP-Umgebung („Produktivsystem“) erfolgt voll automatisiert und beinhaltet im Wesentlichen Folgendes:

- Customizing der SAP Organisationseinheit Mandant
- Customizing der SAP Organisationseinheit Geschäftsbereich
- Customizing der SAP Organisationseinheit Finanzkreis
- Customizing der SAP Organisationseinheit Funktionsbereich (Hinweis: relevant bei Einsatz UKV)
- Customizing der SAP Organisationseinheit Buchungskreis
- Customizing der SAP Organisationseinheit Kostenrechnungskreis
- Customizing der SAP Organisationseinheit Werk/NL
- Customizing der SAP Organisationseinheit Lager
- Customizing der SAP Organisationseinheit Versandstelle
- Customizing der SAP Organisationseinheit Verkaufsorganisation
- Customizing der SAP Organisationseinheit Vertriebsweg
- Customizing der SAP Organisationseinheit Kreditkontrollbereich

- Customizing der SAP Organisationseinheit Einkaufsorganisation (nebst Referenz-Einkaufsorganisation(en))
- Customizing der SAP Organisationseinheit Einkäufergruppe
- Customizing der SAP Organisationseinheit Einkaufsorganisation
- Customizing der SAP Applikationsserver
- Customizing der SAP-Belegarten
- Customizing der SAP-Belegnummernkreise
- Customizing der Kontenpläne
- Customizing der Berechtigungsprofile (ABAP-Stack)
- Customizing der Berechtigungsrollen (dito)
- Customizing betreffend die Protokollierung (Tabellen)
- Übersicht der SAP-Tabellen, klassifiziert nach dem Namensraum
- etc.

Neben den Dokumentationen dienen die erstellten Analysen insbesondere als Grundlage für die durchzuführenden Prüfungshandlungen!

2.4 SAP SYSTEMKONFIGURATION/-ORGANISATION (ANFORDERUNGEN DER ORDNUNGSMÄSSIGKEIT)

Prüfbereich	**Bemerkungen**	
Fiskalisch relevante Datenflüsse	1. Dokumentation des geprüften Systems (Nachvollziehbarkeit). 2. Schaffung erforderlicher Grundlagen für nachgelagerte Prüfungshandlungen.	●
Verantwortlichkeiten betreffend die SAP-System-Administration	Kontrollen betreffend die Gewährleistung der Ordnungsmäßigkeitsanforderungen (Funktionstrennung, Vertretungsregelungen, etc.).	●
Bestandsaufnahme des fiskalisch relevanten Customizing im Produktivsystem	1. Dokumentation des geprüften Systems (Nachvollziehbarkeit). 2. Schaffung erforderlicher Grundlagen für nachgelagerte Prüfungshandlungen.	●
Aktivierung der Tabellenprotokollierung (Produktivsystem)	*Risiko:* *Gefährdung der Grundsätze der GoBD, keine Nachvollziehbarkeit von Updates („Change Managementprozess (Transporte von Programmen und Sonstigem)).*	●
Aktivierung der Tabellenprotokollierung (Qualitätssicherungssystem – Hinweis: In Abhängigkeit von der Ausprägung der SAP-Systemlandschaft)	*Risiko:* *Gefährdung der Grundsätze der GoBD, keine Nachvollziehbarkeit von Updates („Change Managementprozess (Transporte von Programmen und Sonstigem)).*	●
Aktivierung der Tabellenprotokollierung (Entwicklungssystem)	*Risiko:* *Gefährdung der Grundsätze der GoBD, keine Nachvollziehbarkeit („Eigenentwickelte Programme“, Change Managementprozess, etc.).*	●

Prüfbereich	**Bemerkungen**	
Aktivierung des SAP-Security Audit Log	1. Dokumentation des geprüften Systems (Nachvollziehbarkeit). 2. Schaffung erforderlicher Grundlagen für nachgelagerte Prüfungshandlungen. *Risiko:* *Gefährdung der Grundsätze der GoBD sowie DS-GVO.*	●
Konfiguration des SAP-Security Audit Log sowie organisatorisches Umfeld (Detailprüfung)	Gewährleistung der Ordnungsmäßigkeitsanforderungen, der Anforderungen der GoBD sowie der DS-GVO. *Risiko:* *Gefährdung der Grundsätze der GoBD sowie DS-GVO.*	❍

● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (In der Regel wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

2.5 SAP SYSTEMKONFIGURATION/-ORGANISATION (ANFORDERUNGEN DER SICHERHEIT)

Prüfbereich	**Bemerkungen**	
Kontrolle: Konfiguration der Transportwege („Changemanagement“)	Gewährleistung der Anforderungen betreffend die Ordnungsmäßigkeit, Sicherheit sowie insbesondere die GoBD sowie die DS-GVO. *Risiko:* *Gefährdung der Grundsätze Sicherheit sowie der Unveränderlichkeit.*	●
Kontrolle: Ausgewählte Parameter betreffend die Transporte („Changemanagement“)	Gewährleistung der Anforderungen betreffend die Ordnungsmäßigkeit, Sicherheit sowie insbesondere die GoBD sowie die DS-GVO. *Risiko:* *Gefährdung der Grundsätze Sicherheit sowie der Unveränderlichkeit.*	❍
Weiteres sicherheitsrelevantes Customizing im SAP-Produktivsystem	1. Dokumentation des geprüften Systems (Nachvollziehbarkeit). 2. Schaffung erforderlicher Grundlagen für nachgelagerte Prüfungshandlungen. *Risiko:* *Gefährdung der Grundsätze der GoBD sowie DS-GVO.*	●

● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (In der Regel wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

2.6 KONZEPTE (ANFORDERUNGEN DER ORDNUNGSMÄßIGKEIT SOWIE DER SICHERHEIT)

Prüfbereich	**Bemerkungen**	
Datensicherung und Datenwiederherstellung (1)	Kontrolle betreffend die Gewährleistung der Anforderungen (Vollständigkeit der Inhalte, Regelungen betreffend die Verantwortlichkeiten, Regelungen betreffend die Dokumentation (Bewertungsmaßstab: GoBD, DS-GVO, etc.)). *Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.*	●
Dito - Stichprobenprüfung der Wirksamkeit der diesbezüglich implementierten Kontrollmechanismen (Hinweis: Sinnvoll und wichtig, sofern eine Bescheinigung ISAE 3402 oder Adäquates nicht vorliegt)	*Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den beim vorherigen Punkt vorbeschriebenen Regelwerken, bedingt durch ein mangelhaftes internes Kontrollsystem.*	○
IT-Notfallkonzept (dito)	Kontrolle betreffend die Gewährleistung der Anforderungen (Vollständigkeit der Inhalte, Regelungen betreffend die Verantwortlichkeiten, Regelungen betreffend die Dokumentation (Bewertungsmaßstab: GoBD, DS-GVO, etc.)). *Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den vorgenannten Regelwerken.*	○
IT-Sicherheitskonzept (dito)	Kontrolle betreffend die Gewährleistung der Anforderungen (Vollständigkeit der Inhalte, Regelungen betreffend die Verantwortlichkeiten, Regelungen betreffend die Dokumentation (Bewertungsmaßstab: GoBD, DS-GVO, etc.)). *Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den vorgenannten Regelwerken.*	○

Prüfbereich	**Bemerkungen**	
Betriebskonzept FireWall-Lösung (dito)	Kontrolle betreffend die Gewährleistung der Anforderungen (Vollständigkeit der Inhalte, Regelungen betreffend die Verantwortlichkeiten, Regelungen betreffend die Dokumentation (Bewertungsmaßstab: GoBD, DS-GVO, etc.)) *<u>Risiko:</u> Gefährdung der Erfüllung der Anforderungen aus den vorgenannten Regelwerken.*	○
Bestandsaufnahme und Bewertung der getroffenen Maßnahmen betreffend die IT-Betriebs- und IT-Funktionssicherung (dito)	Kontrolle betreffend die Gewährleistung der Anforderungen (Vollständigkeit der Inhalte, Regelungen betreffend die Verantwortlichkeiten, Regelungen betreffend die Dokumentation (Bewertungsmaßstab: GoBD, DS-GVO, etc.)) *<u>Risiko:</u> Gefährdung der Erfüllung der Anforderungen aus den vorgenannten Regelwerken.*	○
Stichprobenprüfung betreffend die Wirksamkeit des internen Kontrollsystems bezüglich der in den vorgenannten Konzepten definierten Prozesse und Kontrollmechanismen („Prüfungszeitraum“)	*<u>Risiko:</u> Gefährdung der Erfüllung der Anforderungen aus den in den vorherigen Punkten vorbeschriebenen Regelwerken, bedingt durch ein mangelhaftes internes Kontrollsystem.*	○
Bestandsaufnahme der erforderlichen SAP-spezifischen Konzepte (Ausgewähltes, in Abstimmung zum Scope der Prüfung) <u>Beispiele:</u> - Konzept „SAP Notfallbenutzer“ - Konzept „SAP Sonderbenutzer“	*<u>Risiko:</u> Gefährdung der Erfüllung der Anforderungen betreffend die Erfüllung der Anforderungen an die Ordnungsmäßigkeit, Sicherheit sowie insbesondere die Vollständigkeit, mangels fehlender Regelungen für ein adäquates internes Kontrollsystem (IKS).*	○

Prüfbereich	Bemerkungen	
- Konzept „Änderungsverfahren betreffend die System- und Mandantenänderbarkeit“ - Konzept „Betrieb des Security Audit Log“ - Konzept „Betrieb HANA Audit Log“ - Konzept „Datenreorganisation“ - Konzept „Verbuchungsabbrüche“ - Konzept „Konsistenzprüfung Datenbestände“ Hinweis: Nur bei SAP ERP erforderlich! - SAP-spezifisches „Löschkonzept DS-GVO“ - etc.		
Detailprüfung ausgewählter Konzepte („Vollständigkeit“), nebst wahlweisen Kontrollen („Stichproben“) der Wirksamkeit der in den Prozessen implementierten Kontrollmechanismen.	*Risiko:* *Gefährdung der Erfüllung der Anforderungen betreffend die Erfüllung der Anforderungen an die Ordnungsmäßigkeit, Sicherheit sowie insbesondere die Vollständigkeit, aufgrund eines nicht wirksamen IKS.*	❍

- ● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
- ❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (In der Regel wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

2.7 SAP-CUSTOMIZING 01 (ANMELDEVERFAHREN/BERECHTIGUNGSVERGABE)

Prüfbereich	**Bemerkungen**	
SAP-Anmeldeinstanzen	1. Dokumentation des geprüften Systems (Nachvollziehbarkeit). 2. Zwingende Grundlage für nachgelagerte Prüfungshandlungen (Prüfung der Startprofilparameter für die Kennwortsicherheit, etc.).	●
Anmeldeverfahren	Schaffung erforderlicher Grundlagen für nachgelagerte Prüfungshandlungen.	●
Ausprägung des Customizing betreffend die Verwendung von individuellen Anmeldepolicies („Produktivsystem“)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). *<u>Risiko:</u> Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.*	●
Customizing wesentlicher Systemprofilparameter zur Steuerung der Kennwortvergabe sowie der Abwehr fehlerhafter Zugriffe („Produktivsystem“)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). *<u>Risiko:</u> Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.*	○

Prüfbereich	**Bemerkungen**	
Dito. (Kontrolle bezüglich im Prüfungszeitraum durchgeführter Veränderungen)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). *Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.*	○
Customizing betreffend die Protokollierung und Nachvollziehbarkeit von fehlerhaften Anmeldeversuchen („Produktivsystem“)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). *Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.*	○
Dito. (Kontrolle bezüglich im Prüfungszeitraum durchgeführter Veränderungen)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). *Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.*	○
Customizing i.S. „verbotene Kennwörter“ (Hinweis: Bedarfsweise bzw. in Abhängigkeit zum Resultat der Prüfungshandlungen beim vorherigen Punkt („Produktivsystem“)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). *Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.*	○

Prüfbereich	**Bemerkungen**	
Customizing der Kennwortrestriktionen für die Anmeldung am Netzwerk / Windowsdomäne bzw. Novell – individuell abhängig vom IT-Umfeld der zu prüfenden Gesellschaft	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). *Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.*	❍
Customizing der Startprofilparameter zur Steuerung der Berechtigungsprüfung - ABAP-STACK („Produktivsystem“)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). *Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.*	❍
Dito. (Kontrolle bezüglich im Prüfungszeitraum durchgeführter Veränderungen)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). *Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.*	❍
Customizing betreffend die Deaktivierung von Berechtigungsobjekten („Produktivsystem“)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). *Risiko:* *Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.*	❍

- ● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
- ❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (In der Regel wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

2.8 SAP-CUSTOMIZING 02 (SONDERBENUTZER, BENUTZERSTAMM GRUNDLAGENPRÜFUNG)

Prüfbereich	**Bemerkungen**	
Absicherung der SAP Sonderbenutzer (Diverse Kriterien)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). Risiko: Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.	●
Verfahren zur Vergabe, dem Entzug und der Änderung von Berechtigungen im SAP-System (technische Vorgehensweise im SAP-System)	Schaffung der erforderlichen Grundlagen für nachgelagerte Prüfungshandlungen.	●
Erstellung diverser Benutzeranalysen	Dokumentation des geprüften Systems sowie der erforderlichen Grundlagen für nachgelagerte Prüfungshandlungen.	●
Zuweisung von Berechtigungsprofilen an nicht mehr gültige Benutzer	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). Risiko: Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.	●

Prüfbereich	**Bemerkungen**	
Zuweisung von Benutzerrollen an nicht mehr gültige Benutzer	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). Risiko: Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.	●

- ● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
- ❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (In der Regel wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

2.9 SAP-CUSTOMIZING 03 (SONDERBENUTZER, BENUTZERSTAMM ERWEITERTE PRÜFUNG)

Prüfbereich	Bemerkungen	
Benutzer ohne Anmeldung in einem längeren Zeitraum	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). Risiko: Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.	○
Referenzbenutzer	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO, etc.). Risiko: Gefährdung der Erfüllung der Anforderungen aus den vorbeschriebenen Regelwerken.	○
Verwendung von Sammelbenutzern (ca. 30 Suchmuster)	Risiko: 1. Gefährdung der Erfüllung der Anforderungen betreffend die Sicherheit (GoBD, DS-GVO). 2. Keine Nachvollziehbarkeit der Erfassungen durch die Verwendung von nicht personalisierten Benutzer-IDs.	○
Zuweisung von SAP-Sammelprofilen für das Modul Finanzbuchhaltung	Risiko: Bei Zuweisung dieser Profile wird die gemäß Berechtigungskonzept definierte Funktionstrennung unterlaufen.	○
Zuweisung von SAP-Sammelprofilen für das Modul Anlagenbuchhaltung	Risiko: Bei Zuweisung dieser Profile wird die gemäß Berechtigungskonzept definierte Funktionstrennung unterlaufen.	○

Prüfbereich	**Bemerkungen**	
Zuweisung von SAP-Sammelprofilen für das Modul Einkauf	Risiko: Bei Zuweisung dieser Profile wird die gemäß Berechtigungskonzept definierte Funktionstrennung unterlaufen.	❍
Zuweisung von SAP-Sammelprofilen für das Modul Vertrieb (Fakturierung)	Risiko: Bei Zuweisung dieser Profile wird die gemäß Berechtigungskonzept definierte Funktionstrennung unterlaufen.	❍
Zuweisung von SAP-Sammelprofilen für die Rechnungsprüfung	Risiko: Bei Zuweisung dieser Profile wird die gemäß Berechtigungskonzept definierte Funktionstrennung unterlaufen.	❍
Zuweisung von SAP-Sammelprofilen für das Modul Personalbuchhaltung	Risiko: Bei Zuweisung dieser Profile wird die gemäß Berechtigungskonzept definierte Funktionstrennung unterlaufen.	❍
Zuweisung von SAP-Sammelprofilen für das Modul Konsolidierung	Risiko: Bei Zuweisung dieser Profile wird die gemäß Berechtigungskonzept definierte Funktionstrennung unterlaufen.	❍

● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (In der Regel wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

2.10 SAP-CUSTOMIZING 04 (VERGABE KRITISCHER BERECHTIGUNGEN)

Prüfbereich	**Bemerkungen**	
Zuweisung von kritischen Profilen (Kontrolle der 8 wesentlichen Profile)	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen betreffend die Sicherheit (GoBD, DS-GVO).* 2. *Keine Funktionstrennung bei Einsatz dieser Profile.* 3. *Gefährdung der Grundsätze der Unveränderlichkeit (Datenverlust oder ungewollte Veränderung durch den Einsatz nicht autorisierter Programme).* 4. *Verstoß gegen das Radierverbot durch manipulativen Einsatz von nicht autorisierten Programmen.*	•
Berechtigung zum Debugging	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen betreffend die Sicherheit (GoBD, DS-GVO).* 2. *Gefährdung der Erfüllung der Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit.* 3. *Gefährdung der Grundsätze der Unveränderlichkeit (Datenverlust oder ungewollte Veränderung durch den Einsatz nicht autorisierter Programme).* 4. *Verstoß gegen das Radierverbot durch manipulativen Einsatz von nicht autorisierten Programmen.*	•
Berechtigung zum Einsatz der SE16N-Emergency-Funktionalität	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen betreffend die Sicherheit (GoBD, DS-GVO).* 2. *Gefährdung der Erfüllung der Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit.*	•

Prüfbereich	Bemerkungen	
	3. *Gefährdung der Grundsätze der Unveränderlichkeit (Datenverlust oder ungewollte Veränderung durch den Einsatz nicht autorisierter Programme).* 4. *Verstoß gegen das Radierverbot durch manipulativen Einsatz von nicht autorisierten Programmen.*	
Berechtigung zur Änderung der System- und Mandantenänderbarkeit	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen betreffend die Sicherheit (GoBD, DS-GVO).* 2. *Gefährdung der Erfüllung der Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit.* 3. *Gefährdung der Grundsätze der Unveränderlichkeit (Datenverlust oder auch Veränderung, bedingt durch manipulative oder auch ungewollte Veränderung des Customizing.)*	●
Berechtigung zur Pflege der Belegobjekte	*Risiko:* *Gefährdung der Erfüllung der Anforderungen betreffend die Vergabe einer fortlaufenden Belegnummer (siehe UStG §14 bzw. UStAE 14.5) durch ungewollte oder auch unberechtigte Veränderung des Customizing von fiskalisch relevanten Belegobjekten.*	○
Berechtigung zur Pflege der Nummernkreisintervalle	*Risiko:* *Gefährdung der Erfüllung der Anforderungen betreffend die Vergabe einer fortlaufenden Belegnummer (siehe UStG §14 bzw. UStAE 14.5) durch ungewollte oder auch unberechtigte Veränderung des Customizing von fiskalisch relevanten Belegobjekten.*	○
Berechtigung zur Änderung/Pflege der Buchungsperioden (Ebene: Applikation)	*Risiko:* *Werden die Buchungsperioden geändert und vor allem für die Vergangenheit geöffnet, kann in vergangene Perioden gebucht werden. Dieses gefährdet den Grundsatz der Zeitgerechtheit.*	○

Prüfbereich	**Bemerkungen**	
Berechtigung zur Änderung/Pflege der Buchungsperioden (Ebene: Applikation oder mittels der Funktionen der Tabellenpflege)	*Risiko:* *Werden die Buchungsperioden geändert und vor allem für die Vergangenheit geöffnet, kann in vergangene Perioden gebucht werden. Dieses gefährdet den Grundsatz der Zeitgerechtheit.*	○
Zuweisung von kritischen Datenbankberechtigungen, bei Einsatz einer HANA-Datenbank i. V. m. SAP ERP (3. Generation der SAP-Software) sowie Einsatz der neuen S/4 HANA Software (4. Generation der SAP-Software)	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen betreffend die Ordnungsmäßigkeit, Sicherheit sowie insbesondere die Vollständigkeit bedingt durch nicht berechtigten Zugriff auf die Datenbank und hiermit verbunden manipulativer oder auch unbeabsichtigter Veränderung von Daten (Löschung, Änderung, Einfügen neuer Datensätze) außerhalb der Software.* 2. *Gefährdung der Erfüllung der Anforderung der DS-GVO, bedingt durch unberechtigte Einsichtnahme in Daten auf der Ebene der Datenbank.*	○
Berechtigung zur Löschung der Änderungsbelege	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen der GoBD (Nachvollziehbarkeit), bedingt durch unbeabsichtigte oder auch manipulative Löschung von Änderungsbelegen.* 2. *Verstoß gegen das Radierverbot, bedingt durch unbeabsichtigte oder auch manipulative Löschung von Änderungsbelegen.*	○
Berechtigung zur Löschung der Änderungsbelege sowie die Pflege der Änderungsbelegobjekte	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen der GoBD (Nachvollziehbarkeit), bedingt durch unbeabsichtigte oder auch manipulative Löschung von Änderungsbelegen.* 2. *Verstoß gegen das Radierverbot, bedingt durch unbeabsichtigte oder auch manipulative Löschung von Änderungsbelegen.* 3. *Verlust der GoBD-Konformität des elektronisch geführten Rechnungswesens, bedingt durch manipulative oder auch ungewollte Veränderung der SAP-Standard-Belegobjekte.*	○

Prüfbereich	**Bemerkungen**	
Weitere Analysen gemäß individuellem Scope, mittels der Software AddCube (Beispiel: Ermittlung von kritischen Berechtigungskombinationen)	Einsatzbereiche: Modul FI (Finanzbuchhaltung), Modul AA (Anlagenbuchhaltung), Modul MM (Materialwirtschaft), Modul SD (Vertriebsmodul („Fakturierung")), Modul HR (Personalbuchhaltung).	○

- ● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung")
- ○ Optionale Ergänzungen zu den Standardprüfungshandlungen (In der Regel wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

2.11 SAP-CUSTOMIZING 05 (WEITERES SICHERHEITSRELEVANTES CUSTOMIZING)

Prüfbereich	**Bemerkungen**	
Status: Customizing betreffend die Systemänderbarkeit (Produktivsystem)	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen betreffend die Sicherheit (GoBD, DS-GVO).* 2. *Gefährdung der Erfüllung der Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit.* 3. *Gefährdung der Grundsätze der Unveränderlichkeit (Datenverlust oder auch Veränderung, bedingt durch manipulative oder auch ungewollte Veränderung des Customizing).*	●
Dito (Kontrolle betreffend Veränderungen im Prüfungszeitraum)	Überprüfung der Wirksamkeit des internen Kontrollsystems.	○
Status: Customizing betreffend die Mandantenänderbarkeit (Produktivsystem)	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen betreffend die Sicherheit (GoBD, DS-GVO).* 2. *Gefährdung der Erfüllung der Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit.* 3. *Gefährdung der Grundsätze der Unveränderlichkeit (Datenverlust oder auch Veränderung, bedingt durch manipulative oder auch ungewollte Veränderung des Customizing).*	●
Dito (Kontrolle betreffend Veränderungen im Prüfungszeitraum)	Überprüfung der Wirksamkeit des internen Kontrollsystems.	○

Prüfbereich	**Bemerkungen**	
Status: Customizing der Mandantentabelle (Produktivsystem)	*Risiko:* *Gefährdung der Erfüllung der Anforderungen betreffend die Nachvollziehbarkeit (GoBD).*	●
Dito (Kontrolle betreffend Veränderungen im Prüfungszeitraum)	Überprüfung der Wirksamkeit des internen Kontrollsystems.	○
Status Customizing: Absicherung der SAP Auslieferungs- und Sondermandanten (Produktivsystem)	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen betreffend die Sicherheit (GoBD, DS-GVO).* 2. *Gefährdung der Erfüllung der Anforderungen an die Ordnungsmäßigkeit, die Vollständigkeit sowie die Nachvollziehbarkeit (Gefahr durchgeführter Veränderungen im Sondermandanten, mit globaler Auswirkung auf den Datenbestand im Produktivmandanten, ohne jegliche Nachvollziehbarkeit im Produktivmandanten.).*	●
Vergabe von Entwickler- und Objektschlüsseln (Produktivsystem)	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen betreffend die Sicherheit (GoBD, DS-GVO).* 2. *Gefährdung der Erfüllung der Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit, bedingt durch den Einsatz nicht autorisierter Programme.* 3. *Gefährdung der Grundsätze der Unveränderlichkeit (Datenverlust oder ungewollte Veränderung durch den Einsatz nicht autorisierter Programme).* 4. *Verstoß gegen das Radierverbot durch manipulativen Einsatz nicht autorisierter Programme.*	●

Prüfbereich	Bemerkungen	
Customizing der Tabelle Entwicklerschlüssel (Produktivsystem)	<u>Risiko:</u> *Gefährdung der Erfüllung der Anforderungen betreffend die Nachvollziehbarkeit (GoBD).*	
Vergabe von Entwickler- und Objektschlüsseln (Qualitätssicherungssystem - Hinweis: Abhängig von der Ausprägung der SAP Systemlandschaft der zu prüfenden Gesellschaft)	<u>Risiko:</u> *Manipulation von neuen Quellcodes auf dem vordefinierten Transportweg und hiermit verbunden:* 1. *Gefährdung der Erfüllung der Anforderungen betreffend die Sicherheit (GoBD, DS-GVO).* 2. *Gefährdung der Erfüllung der Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit, bedingt durch den Einsatz nicht autorisierter Programme.* 3. *Gefährdung der Grundsätze der Unveränderlichkeit (Datenverlust oder ungewollte Veränderung durch den Einsatz nicht autorisierter Programme).* 4. *Verstoß gegen das Radierverbot durch manipulativen Einsatz nicht autorisierter Programme.*	●
Customizing der Tabelle Entwicklerschlüssel (Qualitätssicherungssystem - Hinweis: Abhängig von der Ausprägung der SAP Systemlandschaft der zu prüfenden Gesellschaft)	<u>Risiko:</u> *Gefährdung der Erfüllung der Anforderungen betreffend die Nachvollziehbarkeit (GoBD).*	●
Dito (Kontrolle betreffend Veränderungen im Prüfungszeitraum)	Überprüfung der Wirksamkeit des internen Kontrollsystems.	○

Prüfbereich	**Bemerkungen**	
Customizing der Tabelle Entwicklerschlüssel (Entwicklungssystem)	*Risiko:* *Gefährdung der Erfüllung der Anforderungen betreffend die Nachvollziehbarkeit (GoBD).*	●
Dito (Kontrolle betreffend Veränderungen im Prüfungszeitraum)	Überprüfung der Wirksamkeit des internen Kontrollsystems.	○

● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
○ Optionale Ergänzungen zu den Standardprüfungshandlungen (In der Regel wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

2.12 SAP-CUSTOMIZING 06 (FISKALISCH RELEVANTES CUSTOMIZING - BASIS/GOBD)

Prüfbereich	**Bemerkungen**	
Kontrolle: Customizing Parameter zur Steuerung der Verbuchung im System	*Risiko:* 1. *Fehlerhafte Verarbeitung.* 2. *Datenverlust.*	●
Kontrolle: Customizing Parameter zur Steuerung der Verbuchung im System (Durchgeführte Veränderungen im Prüfungszeitraum)	*Risiko:* 1. *Fehlerhafte Verarbeitung.* 2. *Datenverlust.*	●
Kontrolle: Bezüglich ggf. erfolgter Veränderungen der Objekte betreffend die SAP-Standard-Änderungsbelege	*Risiko:* 1. *Gefährdung der Erfüllung der Anforderungen betreffend die GoBD.* 2. *Verstoß gegen das Radierverbot durch Veränderung der im Systemstandard definierten Protokollierungsfunktionen.*	○
Konsistenzprüfung: Customizing Buchungsbelegarten	*Risiko:* *Fehlerhafte Verarbeitung.*	●
Konsistenzprüfung: AA-Customizing	*Risiko:* *Fehlerhafte Verarbeitung.*	●
Konsistenzprüfung: SD-Customizing	*Risiko:* *Fehlerhafte Verarbeitung.*	●
Kontrolle: Ausprägung des Customizing betreffend die erforderliche Protokollierung von fiskalisch relevanten Tabellen	*Risiko:* *Gefährdung der Erfüllung der Anforderungen betreffend die Nachvollziehbarkeit (GoBD) durch unzureichendes Customizing bezüglich der Tabellenprotokollierung.*	●

Prüfbereich	**Bemerkungen**	
Dito (Kontrolle betreffend Veränderungen im Prüfungszeitraum)	Überprüfung der Wirksamkeit des internen Kontrollsystems.	❍
Kontrolle: Ausprägung des Customizing betreffend die Protokollierung der ggf. eigenentwickelten Tabellen im Kundennamensraum	*Risiko:* *Gefährdung der Erfüllung der Anforderungen betreffend die Nachvollziehbarkeit (GoBD) durch unzureichendes Customizing bezüglich der Tabellenprotokollierung.*	●
Kontrolle: Ausprägung des Customizing betreffend die Pufferungseinstellungen ausgewählter Belegobjekte mit fiskalischer Relevanz	*Risiko:* *Gefährdung der Erfüllung der Anforderungen betreffend die Vergabe einer fortlaufenden Belegnummer (siehe UStG §14 bzw. UStAE 14.5) durch ungewollte oder auch unberechtigte Veränderung des Customizing von fiskalisch relevanten Belegobjekten.*	●
Dito (Kontrolle betreffend Veränderungen im Prüfungszeitraum)	Überprüfung der Wirksamkeit des internen Kontrollsystems.	❍
Kontrolle: Ausprägung der Bewertungsbereiche für die Anlagenbuchhaltung	*Risiko:* *Fehlerhafte Verarbeitung.*	❍
Kontrolle: Ausprägung des Customizing betreffend die Kreditkontrollbereiche und deren Zuweisung zu den Buchungskreisen	*Risiko:* *Keine Kreditlimitprüfung.*	❍
Kontrolle: Ausprägung des Customizing betreffend die Belegänderungsregeln – Veränderungen im Prüfungszeitraum	*Risiko:* *Nicht autorisierte Veränderungen.*	❍

Prüfbereich	**Bemerkungen**	
Kontrolle: Ausprägung des Customizing betreffend die Definition eines automatisierten und protokollierten Vier-Augen-Prinzips bezüglich der Veränderung von Personenkontenstammdaten.	*Risiko:* *Nicht autorisierte Veränderungen von Stammdaten.*	❍
Kontrolle: Ausprägung des Customizing betreffend die Betragsgrenzen für die Ausbuchung von Kleindifferenzen	*Risiko:* *Fehlerhafte Buchungen.*	❍
Kontrolle: Ausprägung des Customizing betreffend die Betragsgrenzen für die systemseitige Eingabekontrolle der maximalen Kursabweichung	*Risiko:* *Fehlerhafte Buchungen.*	❍
Diverse Kontrollen betreffend des Customizing für die Materialwirtschaft	*Risiko:* *Fehlerhafte Materialbuchungen und hiermit verbunden Fehler bei der Bewertung.*	❍

- ● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
- ❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (In der Regel wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

2.13 PLAUSIBILISIERUNG DER DATENBESTÄNDE IM PRÜFUNGSZEITRAUM

Prüfbereich	**Bemerkungen**	
Kontrolle: Verbuchungsabbrüche	Risiko: *Gefährdung der Erfüllung der Anforderungen betreffend die Vollständigkeit.*	●
Kontrolle: Schnittstelle SD (Fakturen) / FI	Risiko: *Gefährdung der Erfüllung der Anforderungen betreffend die Vollständigkeit (Durch Fehler gesperrte Übergabedaten, noch nicht fakturierte Lieferungen, etc.)*	●
Konsistenzprüfung: Daten Modul Finanzbuchhaltung (FI)	Hinweis: Nur bei Einsatz von SAP ERP. Bei S/4 HANA, aufgrund der geänderten Strukturen der zugrunde liegenden Datenbank, nicht erforderlich!	●
Konsistenzprüfung: Daten Modul Materialwirtschaft (MM)	Risiko: *Fehlerhafter Werteausweis.*	●
Konsistenzprüfung: Daten Modul FI versus MM	Risiko: *Fehlerhafter Werteausweis.*	●
Analyse der SAP-Systemprotokollierung (Einsatz von Debugging oder der SE16-Emergency-Funktionalität zur Bearbeitung von fiskalisch relevanten Daten)	Risiko: *Verstoß Radierverbot (§ 239 HGB)*	●

● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (In der Regel wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

3. IHR KONTAKT

GERNE UNTERSTÜTZEN UND ÜBERZEUGEN WIR AUCH SIE MIT UNSEREN DIENSTLEISTUNGEN!

DORNBACH CONSULTING GMBH
Anton-Jordan-Straße 1
56070 Koblenz
www.dornbach-consulting.de

Ihr Ansprechpartner:

Herr Michael Küster
- Geschäftsführer -
Telefon: +49 (0) 261 94 31-441
E-Mail: mkuester@dornbach-consulting.de