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 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

DORNBACH Consulting GmbH
Anton-Jordan-Straße 1
56070 Koblenz

Inhaltsübersicht:

1. Vorwort (Gesellschaft, Dienstleistungsportfolio) 4
2. IT-Systemprüfung 6
2.1 Kurzbeschreibung der Anforderungen 6
2.2 Vorgehensmodell bei einer IT-Systemprüfung (systemunabhängige Darstellung) 7
2.3 Dokumentation des Customizings des zu prüfenden Systems (Standard bei allen Projekten) 8
2.4 SAP-Systemkonfiguration/-Organisation (Anforderungen der Ordnungsmässigkeit) 10
2.5 SAP-Systemkonfiguration/-Organisation (Anforderungen der Sicherheit) 12
2.6 Konzepte (Anforderungen der Ordnungsmäßigkeit sowie der Sicherheit) 13
2.7 SAP-Customizing 01 (Anmeldeverfahren/Berechtigungsvergabe) 16
2.8 SAP-Customizing 02 (Sonderbenutzer, Benutzerstamm Grundlagenprüfung) 20
2.9 SAP-Customizing 03 (Sonderbenutzer, Benutzerstamm erweiterte Prüfung) 22
2.10 SAP-Customizing 04 (Vergabe kritischer Berechtigungen) 24

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

2.11 SAP-Customizing 05 (Weiteres sicherheitsrelevantes Customizing) 28
2.12 SAP-Customizing 06 (fiskalisch relevantes Customizing - Basis/GoBD) 32
2.13 Plausibilisierung der Datenbestände im Prüfungszeitraum 35
3. Ihr Kontakt 36

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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 und GoBD-Beratung. Diese Broschüre beschreibt, ergänzend zu 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 zugrunde liegenden Datenbankprodukte und umfassendes Wissen, zu den Anforderungen an ein ordnungsgemäßes Rechnungswesen.

Unsere Prüfprojekte werden daher stets durch erfahrene Praktiker (Zertifizierungsbeispiele: SAP FI Berater, Bilanzbuchhalter, IT Auditor [IDW]) durchgeführt, die vor der Tätigkeit als Auditor, in verantwortlichen Positionen, 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 Fall der IT-Systemprüfung auftragsabhängig auch den Bereich Datenanalysen, so dass wir unsere Kunden, als Komplettdienstleister, mit skalierbaren Prüfungs- und Beratungsdienstleistungen, vollumfänglich unterstützen.

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Betreffend den Bereich Datenanalysen verweisen wir auf unsere separate Broschüre „Analytic Factory“, die 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, mit Hilfe von speziell für Belange einer IT-Systemprüfung im SAP-Umfeld entwickelter Datenabfragen, automatisiert aus dem SAP-System extrahiert, dies reduziert die Prüfungstätigkeiten am System und die hiermit verbundenen Kosten auf ein Minimum.

Die Basis für die vorbeschriebenen Tätigkeiten bilden die Software „CaseWare 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 Analyse-App „MK Solutions“ (Module: SAP-REVI / SAP-IKS), basierend auf der Entwicklungsumgebung der Software „Idea Smart Analyser“.

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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 der Abschlussprüfung. Es geht darum zu beurteilen, ob die rechtlichen Anforderungen (Ordnungsmäßigkeits- und Sicherheitsanforderungen) erfüllt werden und zu erkennen, ob Risiken durch wesentliche Fehler in der Rechnungslegung bestehen. In diesem Zusammenhang ist zu beachten, dass gemäß HGB §322 Abs. 3, der Wirtschaftsprüfer im Rahmen des Bestätigungsvermerks 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 über die Ordnungsmäßigkeit und die 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.

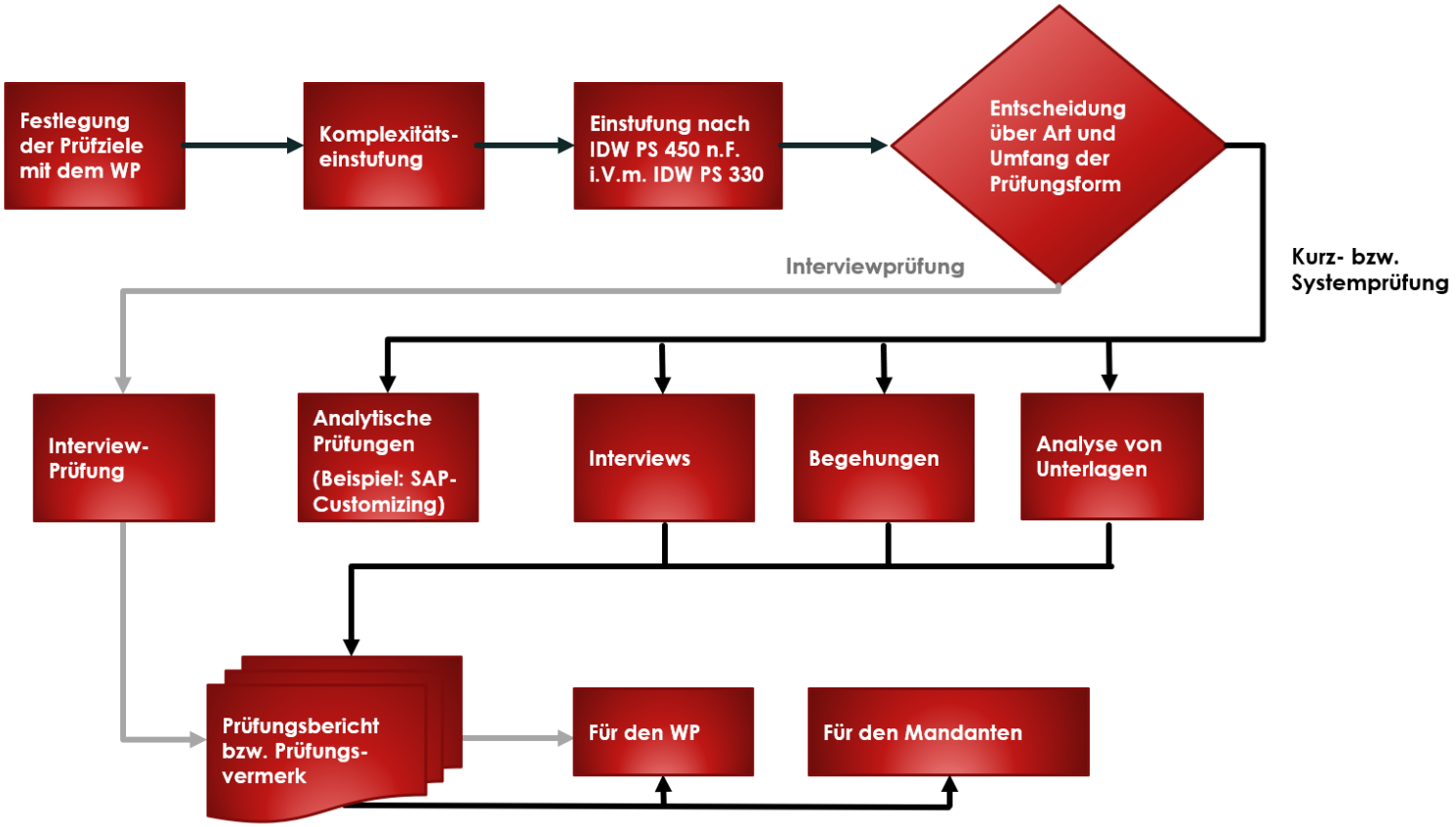
Eine Übersicht unserer Vorgehensweise, sowie detaillierte Informationen zu den Inhalten unseres skalierbaren Prüfungsmodells, finden Sie nachfolgend in den Punkten 2.2. bis 2.13. Letztere vermitteln eine Übersicht der nach unserem Ermessen wesentlichen Kontrollen, jedoch ohne Anspruch auf Vollständigkeit.

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

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

DORNBACH Consulting GmbH
Anton-Jordan-Straße 1
56070 Koblenz

2.2 VORGEHENSMODELL BEI EINER IT-SYSTEMPRÜFUNG (SYSTEMUNABHÄNGIGE DARSTELLUNG)



© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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

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

- 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

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

- 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 als Grundlage für die durchzuführenden Prüfungshandlungen!

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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 für die SAP-System-Administration	Kontrollen betreffend die Gewährleistung der Ordnungsmäßigkeitsanforderungen (Funktionstrennung, Vertretungsregelungen etc.).	●
Bestandsaufnahme des fiskalisch relevanten Customizings im Produktivsystem	1. Dokumentation des geprüften Systems (Nachvollziehbarkeit). 2. Schaffung erforderlicher Grundlagen für nachgelagerte Prüfungshandlungen.	●
Aktivierung der Tabellenprotokollierung (Transportsystem)	<u>Risiko:</u> *Gefährdung der Grundsätze der GoBD, keine Nachvollziehbarkeit von Updates („Change Managementprozess“ (Transporte von Programmen und Sonstigem)).*	●
Aktivierung der Tabellenprotokollierung (Produktivsystem)	<u>Risiko:</u> *Gefährdung der Grundsätze der GoBD, keine Nachvollziehbarkeit von Updates („Change Managementprozess“ (Transporte von Programmen und Sonstigem)).*	●
Dito (ergänzende Kontrolle in ggf. unterjährig durchgeführten Veränderungen)	<u>Risiko:</u> *Gefährdung der Grundsätze der GoBD, keine Nachvollziehbarkeit von Updates („Change Managementprozess“ (Transporte von Programmen und Sonstigem)).*	●

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
Aktivierung der Tabellenprotokollierung (Qualitätssicherungssystem; – Hinweis: abhängig von der Ausprägung der SAP-Systemlandschaft)	<u>Risiko:</u> *Gefährdung der Grundsätze der GoBD, keine Nachvollziehbarkeit von Updates („Change Managementprozess“ (Transporte von Programmen und Sonstigem)).*	●
Aktivierung der Tabellenprotokollierung (Entwicklungssystem)	<u>Risiko:</u> *Gefährdung der Grundsätze der GoBD, keine Nachvollziehbarkeit („Eigenentwickelte Programme“, „Change Managementprozess“ etc.).*	●
Aktivierung des SAP-Security Audit Log	1. Dokumentation des geprüften Systems (Nachvollziehbarkeit). 2. Schaffung erforderlicher Grundlagen für nachgelagerte Prüfungshandlungen. <u>Risiko:</u> *Gefährdung der Grundsätze der GoBD sowie DS-GVO.*	●
Konfiguration des SAP-Security Audit Logs und des organisatorischen Umfelds (Detailprüfung)	Gewährleistung der Ordnungsmäßigkeitsanforderungen, der Anforderungen der GoBD sowie der DS-GVO. <u>Risiko:</u> *Gefährdung der Grundsätze der GoBD sowie DS-GVO.*	❍

● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (i.d.R. wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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“ und „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“ und „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 und DS-GVO.*	●

● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (i.d.R. wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

2.6 KONZEPTE (ANFORDERUNGEN DER ORDNUNGSMÄßIGKEIT SOWIE DER SICHERHEIT)

Prüfbereich	**Bemerkungen**	
Datensicherung und Datenwiederherstellung (1)	Kontrolle der Gewährleistung der Anforderungen (Vollständigkeit der Inhalte, Regelungen zu den Verantwortlichkeiten, Regelungen bzgl. der Dokumentation (Bewertungsmaßstab: GoBD, DS-GVO etc.)). *Risiko:* *Es besteht die Gefahr, dass die Anforderungen aus den vorgenannten Regelwerken nicht erfüllt werden.*	●
Dito - Stichprobenprüfung der Wirksamkeit der diesbezüglich implementierten Kontrollmechanismen (Hinweis: dies ist sinnvoll und wichtig, sofern eine Bescheinigung ISAE 3402 oder Adäquates nicht vorliegt)	*Risiko:* *Es besteht die Gefahr, dass die Anforderungen aus den beim vorherigen Punkt beschriebenen Regelwerken, bedingt durch ein mangelhaftes internes Kontrollsystem nicht erfüllt werden.*	○
IT-Notfallkonzept (dito)	Kontrolle der Gewährleistung der Anforderungen (Vollständigkeit der Inhalte, Regelungen zu den Verantwortlichkeiten, Regelungen bzgl. der Dokumentation (Bewertungsmaßstab: GoBD, DS-GVO etc.)). *Risiko:* *Es besteht die Gefahr, dass die Anforderungen aus den vorgenannten Regelwerken nicht erfüllt werden.*	○
IT-Sicherheitskonzept (dito)	Kontrolle der Gewährleistung der Anforderungen (Vollständigkeit der Inhalte, Regelungen zu den Verantwortlichkeiten, Regelungen bzgl. der Dokumentation (Bewertungsmaßstab: GoBD, DS-GVO etc.)). *Risiko:* *Es besteht die Gefahr, dass die Anforderungen aus den vorgenannten Regelwerken nicht erfüllt werden.*	○

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
Betriebskonzept FireWall-Lösung (dito)	Kontrolle der Gewährleistung der Anforderungen (Vollständigkeit der Inhalte, Regelungen zu den Verantwortlichkeiten, Regelungen bzgl. der Dokumentation (Bewertungsmaßstab: GoBD, DS-GVO etc.)) *Risiko:* *Es besteht die Gefahr, dass die Anforderungen aus den vorgenannten Regelwerken nicht erfüllt werden.*	❍
Bestandsaufnahme und Bewertung der getroffenen Maßnahmen betreffend die IT-Betriebs- und IT-Funktionssicherung (dito)	Kontrolle der Gewährleistung der Anforderungen (Vollständigkeit der Inhalte, Regelungen zu den Verantwortlichkeiten, Regelungen bzgl. der Dokumentation (Bewertungsmaßstab: GoBD, DS-GVO etc.)) *Risiko:* *Es besteht die Gefahr, dass die Anforderungen aus den vorgenannten Regelwerken nicht erfüllt werden.*	❍
Stichprobenprüfung betreffend die Wirksamkeit des internen Kontrollsystems bezüglich der in den vorgenannten Konzepten definierten Prozesse und Kontrollmechanismen („Prüfungszeitraum“)	*Risiko:* *Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken, bedingt durch ein mangelhaftes internes Kontrollsystem nicht erfüllt werden.*	❍

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
Bestandsaufnahme der erforderlichen SAP-spezifischen Konzepte (Ausgewähltes, in Abstimmung zum Scope der Prüfung) Beispiele: - Konzept „SAP Notfallbenutzer“ - Konzept „SAP Sonderbenutzer“ - 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.	*Risiko:* *Es besteht die Gefahr, dass die Anforderungen an die Ordnungsmäßigkeit, die Sicherheit und insbesondere die Vollständigkeit, aufgrund fehlender Regelungen für ein adäquates internes Kontrollsystem (IKS) nicht erfüllt werden.*	❍
Detailprüfung ausgewählter Konzepte („Vollständigkeit“), nebst wahlweisen Kontrollen („Stichproben“) der Wirksamkeit der in den Prozessen implementierten Kontrollmechanismen.	*Risiko:* *Es besteht die Gefahr, dass die Anforderungen an die Ordnungsmäßigkeit, die Sicherheit und insbesondere die Vollständigkeit, aufgrund eines nicht wirksamen IKS nicht erfüllt werden.*	❍

- ● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
- ❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (i.d.R. wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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 Customizings betreffend die Verwendung von individuellen Anmeldepolicies („Produktivsystem“)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO etc.). *Risiko:* *Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.*	●
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.). *Risiko:* *Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.*	●

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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:* *Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden .*	●
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:* *Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.*	○
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:* *Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.*	○
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:* *Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.*	○

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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:* *Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.*	○
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:* *Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.*	●
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:* *Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.*	●
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:* *Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.*	●

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
Dito. (Systemkontrolle bezüglich deaktivierter Berechtigungsobjekte, sofern die vorbeschriebene Kontrolle zu Feststellungen führt)	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO etc.). *Risiko: Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.*	○

- ● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
- ○ Optionale Ergänzungen zu den Standardprüfungshandlungen (i.d.R. wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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: Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.	●
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.	●
Dito. (Stichproben bezüglich des Vergabeprozesses für SAP-Benutzer-IDs)	Kontrolle zur Wirksamkeit des IKS	○
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.).	●

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
	Risiko: Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.	
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: Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.	●

- ● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
- ❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (i.d.R. wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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: Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.	○
Referenzbenutzer	Kontrolle betreffend die Gewährleistung der Anforderungen an die Ordnungsmäßigkeit sowie die Sicherheit (Bewertungsmaßstab: GoBD, DS-GVO etc.). Risiko: Es besteht die Gefahr, dass die Anforderungen aus den vorbeschriebenen Regelwerken nicht erfüllt werden.	○
Verwendung von Sammelbenutzern (diverse 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.	●

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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 (i.d.R. wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

2.10 SAP-CUSTOMIZING 04 (VERGABE KRITISCHER BERECHTIGUNGEN)

Prüfbereich	Bemerkungen	
Zuweisung von kritischen Profilen (Kontrolle der 8 wesentlichen Profile)	*Risiko:* 1. *Gefahr, dass die Sicherheitsanforderungen nicht erfüllt werden (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. *Gefahr, dass die Sicherheitsanforderungen nicht erfüllt werden (GoBD, DS-GVO).* 2. *Gefahr, dass die Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit nicht erfüllt werden.* 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.*	•

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
Berechtigung zum Einsatz der SE16N-Emergency-Funktionalität	*<u>Risiko:</u>* 1. *Gefahr, dass die Sicherheitsanforderungen nicht erfüllt werden (GoBD, DS-GVO).* 2. *Gefahr, dass die Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit nicht erfüllt werden.* 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 Systemänderbarkeit	*<u>Risiko:</u>* 1. *Gefahr, dass die Sicherheitsanforderungen nicht erfüllt werden (GoBD, DS-GVO).* 2. *Gefahr, dass die Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit nicht erfüllt werden.* 3. *Gefährdung der Grundsätze der Unveränderlichkeit (Datenverlust oder auch Veränderung, bedingt durch manipulative oder auch ungewollte Veränderung des Customizings.).*	•
Berechtigung zur Änderung der Mandantenänderbarkeit	*<u>Risiko:</u>* 1. *Gefahr, dass die Sicherheitsanforderungen nicht erfüllt werden (GoBD, DS-GVO).* 2. *Gefahr, dass die Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit nicht erfüllt werden.* 3. *Gefährdung der Grundsätze der Unveränderlichkeit (Datenverlust oder auch Veränderung, bedingt durch manipulative oder auch ungewollte Veränderung des Customizings.).*	•

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
Berechtigung zur Pflege von Berechtigungen (Anlage neuer Benutzer-IDs, Berechtigungsänderungen für Benutzer-IDs, Löschung von Benutzer-IDs)	*<u>Risiko:</u>* 1. *Gefahr, dass die Sicherheitsanforderungen nicht erfüllt werden (GoBD, DS-GVO).* 2. *Gefahr, dass die Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit nicht erfüllt werden.* 3. *Gefährdung der Grundsätze der Unveränderlichkeit (Datenverlust oder auch Veränderung, bedingt durch manipulative oder auch ungewollte Veränderung des Customizings.).*	○
Berechtigung zur Pflege der Belegobjekte	*<u>Risiko:</u> Gefahr, dass die Anforderungen an die Vergabe einer fortlaufenden Belegnummer (siehe UStG §14 bzw. UStAE 14.5) durch ungewollte oder auch unberechtigte Veränderung des Customizings von fiskalisch relevanten Belegobjekten nicht erfüllt werden.*	○
Berechtigung zur Pflege der Nummernkreisintervalle	*<u>Risiko:</u> Gefahr, dass die Anforderungen an die Vergabe einer fortlaufenden Belegnummer (siehe UStG §14 bzw. UStAE 14.5) durch ungewollte oder auch unberechtigte Veränderung des Customizings von fiskalisch relevanten Belegobjekten nicht erfüllt werden.*	○
Berechtigung zur Änderung/Pflege der Buchungsperioden (Ebene: Applikation)	*<u>Risiko:</u> Werden die Buchungsperioden geändert und vor allem für die Vergangenheit geöffnet, kann in vergangene Perioden gebucht werden. Dieses gefährdet den Grundsatz der Zeitgerechtheit.*	○
Berechtigung zur Änderung/Pflege der Buchungsperioden (Ebene: Applikation oder mittels der Funktionen der Tabellenpflege)	*<u>Risiko:</u> Werden die Buchungsperioden geändert und vor allem für die Vergangenheit geöffnet, kann in vergangene Perioden gebucht werden. Dieses gefährdet den Grundsatz der Zeitgerechtheit.*	○

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
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)	*<u>Risiko:</u>* 1. *Gefahr, dass die Anforderungen an die Ordnungsmäßigkeit, die 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 nicht erfüllt werden.* 2. *Gefahr, dass die Anforderung der DS-GVO, bedingt durch unberechtigte Einsichtnahme in Daten auf der Ebene der Datenbank, nicht erfüllt werden.*	❍
Berechtigung zur Löschung der Änderungsbelege	*<u>Risiko:</u>* 1. *Gefahr, dass die Anforderungen der GoBD (Nachvollziehbarkeit), bedingt durch unbeabsichtigte oder auch manipulative Löschung von Änderungsbelegen nicht erfüllt werden.* 2. *Verstoß gegen das Radierverbot, bedingt durch unbeabsichtigte oder auch manipulative Löschung von Änderungsbelegen.*	❍
Berechtigung zur Löschung der Änderungsbelege sowie die Pflege der Änderungsbelegobjekte	*<u>Risiko:</u>* 1. *Gefahr, dass die Anforderungen der GoBD (Nachvollziehbarkeit), bedingt durch unbeabsichtigte oder auch manipulative Löschung von Änderungsbelegen nicht erfüllt wird.* 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 Veränderungen der SAP-Standard-Belegobjekte.*	❍

- ● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
- ❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (i.d.R. wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

2.11 SAP-CUSTOMIZING 05 (WEITERES SICHERHEITSRELEVANTES CUSTOMIZING)

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

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
Status: Customizing der Mandantentabelle (Produktivsystem)	*<u>Risiko:</u> Gefahr, dass die Anforderungen an die Nachvollziehbarkeit (GoBD) nicht erfüllt werden.*	●
Dito (Kontrolle betreffend Veränderungen im Prüfungszeitraum)	Überprüfung der Wirksamkeit des internen Kontrollsystems.	○
Status Customizing: Absicherung der SAP Auslieferungs- und Sondermandanten (Produktivsystem)	*<u>Risiko:</u>* *1. Gefahr, dass die Sicherheitsanforderungen (GoBD, DS-GVO) nicht erfüllt werden.* *2. Gefahr, dass die 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) nicht erfüllt werden.*	●
Vergabe von Entwickler- und Objektschlüsseln (Produktivsystem im Umfeld SAP-ERP) bzw. Vergabe von Entwicklerberechtigungen (Produktivsystem im Umfeld SAP S/4 HANA)	*<u>Risiko:</u>* *1. Gefahr, dass die Sicherheitsanforderungen (GoBD, DS-GVO) nicht erfüllt werden.* *2. Gefahr, dass die Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit, bedingt durch den Einsatz nicht autorisierter Programme, nicht erfüllt werden* *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.*	●

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
Customizing der Tabelle Entwicklerschlüssel (Produktivsystem im Umfeld SAP-ERP)	<u>Risiko:</u> *Gefahr, dass die Anforderungen an die Nachvollziehbarkeit (GoBD) nicht erfüllt werden.*	
Vergabe von Entwickler- und Objektschlüsseln (Qualitätssicherungssystem - Hinweis: Abhängig von der Ausprägung der SAP-Systemlandschaft der zu prüfenden Gesellschaft) bei SAP-ERP-Systemen	<u>Risiko:</u> *Manipulation von neuen Quellcodes auf dem vordefinierten Transportweg und hiermit verbunden:* 1. *Gefahr, dass die Sicherheitsanforderungen (GoBD, DS-GVO) nicht erfüllt werden.* 2. *Gefahr, dass die Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit, bedingt durch den Einsatz nicht autorisierter Programme nicht erfüllt werden.* 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) bei SAP-ERP-Systemen	<u>Risiko:</u> *Gefahr, dass die Anforderungen an die Nachvollziehbarkeit (GoBD) nicht erfüllt werden.*	●
Vergabe von Entwicklerberechtigungen (Qualitätssicherungssystem bei SAP S/4 HANA-Systemen)	<u>Risiko:</u> *Manipulation von neuen Quellcodes auf dem vordefinierten Transportweg und hiermit verbunden:* 1. *Gefahr, dass die Sicherheitsanforderungen (GoBD, DS-GVO) nicht erfüllt werden.*	●

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	Bemerkungen	
	2. *Gefahr, dass die Anforderungen an die Ordnungsmäßigkeit und insbesondere die Vollständigkeit und Nachvollziehbarkeit, bedingt durch den Einsatz nicht autorisierter Programme, nicht erfüllt werden.* 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 (Entwicklungssystem bei SAP-ERP-Systemen)	*Risiko:* *Gefahr, dass die Anforderungen an die Nachvollziehbarkeit (GoBD) nicht erfüllt werden.*	●

- ● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
- ❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (i.d.R. wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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. *Gefahr, dass die Anforderungen der GoBD nicht erfüllt werden.* 2. *Verstoß gegen das Radierverbot durch Veränderungen 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 Customizings betreffend die erforderliche Protokollierung von fiskalisch relevanten Tabellen	*Risiko:* *Gefahr, dass die Anforderungen an die Nachvollziehbarkeit (GoBD) durch unzureichendes Customizing bezüglich der Tabellenprotokollierung nicht erfüllt werden.*	●

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
Dito (Kontrolle betreffend Veränderungen im Prüfungszeitraum)	Überprüfung der Wirksamkeit des internen Kontrollsystems.	❍
Kontrolle: Ausprägung des Customizings betreffend die Protokollierung der ggf. eigenentwickelten Tabellen im Kundennamensraum	*Risiko:* *Gefahr, dass die Anforderungen an die Nachvollziehbarkeit (GoBD) durch unzureichendes Customizing bezüglich der Tabellenprotokollierung nicht erfüllt werden.*	●
Kontrolle: Ausprägung des Customizings betreffend die Pufferungseinstellungen ausgewählter Belegobjekte mit fiskalischer Relevanz	*Risiko:* *Gefahr, dass die Vergabeanforderungen an eine fortlaufende Belegnummer (siehe UStG §14 bzw. UStAE 14.5) durch ungewollte oder auch unberechtigte Veränderung des Customizings von fiskalisch relevanten Belegobjekten nicht erfüllt werden.*	●
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 Customizings betreffend die Kreditkontrollbereiche und deren Zuweisung zu den Buchungskreisen	*Risiko:* *Keine Kreditlimitprüfung*	❍
Kontrolle: Ausprägung des Customizings betreffend die Belegänderungsregeln – Veränderungen im Prüfungszeitraum	*Risiko:* *Nicht autorisierte Veränderungen*	❍
Kontrolle: Ausprägung des Customizings betreffend die Definition eines automatisierten und protokollierten Vier-Augen-Prinzips bezüglich der Veränderung von Personenkontenstammdaten.	*Risiko:* *Nicht autorisierte Veränderungen von Stammdaten*	●

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

Prüfbereich	**Bemerkungen**	
Kontrolle: Ausprägung des Customizings betreffend die Betragsgrenzen für die Ausbuchung von Kleindifferenzen	*Risiko:* *Fehlerhafte Buchungen*	❍
Kontrolle: Ausprägung des Customizings betreffend die Betragsgrenzen für die systemseitige Eingabekontrolle der maximalen Kursabweichung	*Risiko:* *Fehlerhafte Buchungen*	❍
Diverse Kontrollen betreffend des Customizings für die Materialwirtschaft	*Risiko:* *Fehlerhafte Materialbuchungen und hiermit verbunden Fehler bei der Bewertung.*	❍

- ● Unser Vorschlag für eine Standardprüfungshandlung („Dauerprüfung“)
- ❍ Optionale Ergänzungen zu den Standardprüfungshandlungen (i.d.R. wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

2.13 PLAUSIBILISIERUNG DER DATENBESTÄNDE IM PRÜFUNGSZEITRAUM

Prüfbereich	**Bemerkungen**	
Kontrolle: Verbuchungsabbrüche	*Risiko:* *Gefahr, dass die Anforderungen an die Vollständigkeit nicht erfüllt werden.*	●
Kontrolle: Schnittstelle SD (Fakturen) / FI	*Risiko:* *Gefahr, dass die Anforderungen an die Vollständigkeit (durch Fehler gesperrte Übergabedaten, noch nicht fakturierte Lieferungen etc.) nicht erfüllt werden.*	●
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 (i.d.R. wechselnd, im Rahmen eines mehrjährigen Prüfungsplans)

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.

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

© DORNBACH 2025. All rights reserved.
Der Umwelt zuliebe ist dieses Dokument nicht druckbar.