Muster-Prüfprogramm

SAP-Berechtigungen

13 Prüfschritte · BSI, ISO 27001, GoBD

13 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 8 Unterlagen zur Anforderung und die typischen Feststellungen.

BSI APP.4.2 · ISO/IEC 27001:2022 Anhang A 5.15 · ISO/IEC 27001:2022 Anhang A 5.18 · ISO/IEC 27001:2022 Anhang A 5.3 · GoBD Rz. 100 · ISO/IEC 27001:2022 Anhang A 8.2 · ISO/IEC 27001:2022 Anhang A 8.2 und 8.15 · GoBD Rz. 107 · ISO/IEC 27001:2022 Anhang A 8.15 · ISO/IEC 27001:2022 Anhang A 8.31 und 8.32 · BSI ORP.4

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation Berechtigungen im ERP-System nach einem freigegebenen Konzept vergibt und regelmäßig überprüft, ob unvereinbare Funktionen getrennt sind und ob kritische Berechtigungen, Standard- und Notfallbenutzer sowie Änderungen am Produktivsystem kontrolliert und nachvollziehbar sind. Sie beurteilt außerdem, ob die Protokollierung die Nachvollziehbarkeit buchungsrelevanter Änderungen sichert.

GELTUNGSBEREICH

- Produktive SAP-Systeme und Mandanten mit buchungsrelevanten Prozessen
- Rollen, Benutzer, Antrags- und Genehmigungsprozess sowie Regelwerk zur Funktionstrennung
- Notfallbenutzer, Standardbenutzer, Schnittstellen- und Systembenutzer
- Nicht Gegenstand: Berechtigungen in Vorsystemen außerhalb von SAP, die eigene Prüfungen haben

Prüfschritte 1 bis 3

Schritt 01 — BSI APP.4.2; ISO/IEC 27001:2022 Anhang A 5.15

Ein Berechtigungskonzept beschreibt Rollenaufbau, Namenskonventionen, Vergabe, Überprüfung und Verantwortlichkeiten und ist freigegeben.

Prüfhandlung Konzept lesen, Freigabe prüfen und Namenskonventionen an zehn Rollen im System nachvollziehen.

Nachweise Berechtigungskonzept mit Freigabe, Rollenliste

Schritt 02 — BSI APP.4.2; ISO/IEC 27001:2022 Anhang A 5.18

Rollen sind fachlich zugeschnitten und haben verantwortliche Rolleneigentümer aus dem Fachbereich.

Prüfhandlung Für fünf Rollen Inhalt und Eigentümer prüfen und Eigentümer zur Kenntnis der Rolleninhalte befragen.

Nachweise Rollenbeschreibungen, Liste der Rolleneigentümer

Schritt 03 — ISO/IEC 27001:2022 Anhang A 5.18

Berechtigungen werden nur auf Antrag mit Genehmigung durch Vorgesetzte und Rolleneigentümer vergeben.

Prüfhandlung Zehn Rollenzuordnungen der letzten sechs Monate mit Anträgen und Genehmigungen abgleichen.

Nachweise Änderungsbelege der Benutzerstammsätze, Anträge, Genehmigungen

Prüfschritte 4 bis 6

Schritt 04

ISO/IEC 27001:2022 Anhang A 5.3; GoBD Rz. 100

Ein Regelwerk zur Funktionstrennung ist festgelegt; Konflikte werden erkannt, bewertet und durch Kontrollen ausgeglichen.

Prüfhandlung Regelwerk ansehen, aktuelle Konfliktauswertung abrufen und für drei Konflikte die ausgleichenden Kontrollen nachvollziehen.

Nachweise Regelwerk zur Funktionstrennung, Konfliktbericht, Kontrollnachweise

Schritt 05

ISO/IEC 27001:2022 Anhang A 8.2; BSI APP.4.2

Kritische Berechtigungen wie Vollzugriffsprofile, Debugging mit Änderungsrecht oder direkte Tabellenpflege sind auf wenige begründete Fälle beschränkt.

Prüfhandlung Benutzer mit kritischen Profilen und Berechtigungen auswerten und mit genehmigten Ausnahmen abgleichen.

Nachweise Auswertung kritischer Berechtigungen, Ausnahmegenehmigungen

Schritt 06

BSI APP.4.2

Standardbenutzer sind gesperrt oder mit geänderten Kennwörtern gesichert und in allen Mandanten überwacht.

Prüfhandlung Status und Kennwortänderung der Standardbenutzer in allen Mandanten auslesen.

Nachweise Auswertung der Standardbenutzer je Mandant

Prüfschritte 7 bis 9

Schritt 07 — ISO/IEC 27001:2022 Anhang A 8.2 und 8.15

Notfallbenutzer werden nur bei Bedarf freigeschaltet; ihre Tätigkeiten werden protokolliert und nachträglich kontrolliert.

Prüfhandlung Fünf Notfalleinsätze auswählen und Anlass, Freischaltung, Protokoll und Nachkontrolle nachvollziehen.

Nachweise Notfallprotokolle, Freigaben, Nachweise der Nachkontrolle

Schritt 08 — ISO/IEC 27001:2022 Anhang A 5.18

Berechtigungen werden regelmäßig durch Vorgesetzte und Rolleneigentümer rezertifiziert; Entzüge werden umgesetzt.

Prüfhandlung Letzte Rezertifizierung auf Vollständigkeit prüfen und für fünf Entzüge die Umsetzung im System nachvollziehen.

Nachweise Rezertifizierungsprotokoll, Änderungsbelege

Schritt 09 — GoBD Rz. 107; BSI APP.4.2

Produktivmandanten und Produktivsystem sind gegen direkte Änderungen gesperrt; Öffnungen sind genehmigt und protokolliert.

Prüfhandlung Einstellungen zur Änderbarkeit von System und Mandanten auslesen und Öffnungen der letzten zwölf Monate nachvollziehen.

Nachweise Systemeinstellungen, Protokoll der Systemänderbarkeit, Genehmigungen

Prüfschritte 10 bis 13

Schritt 10 GoBD Rz. 107; ISO/IEC 27001:2022 Anhang A 8.15

Tabellenprotokollierung und Änderungsbelege sind für buchungsrelevante Daten aktiv.

Prüfhandlung Systemparameter zur Tabellenprotokollierung prüfen und für drei relevante Tabellen die Protokollierung nachweisen lassen.

Nachweise Systemparameter, Auswertung der Tabellenprotokolle

Schritt 11 ISO/IEC 27001:2022 Anhang A 8.31 und 8.32

Entwicklung, Test und Produktion sind getrennt; Änderungen gelangen nur über das Transportwesen in die Produktion.

Prüfhandlung Transportwege ansehen und prüfen, ob im Produktivsystem Entwicklungsrechte vergeben sind.

Nachweise Transportlandschaft, Transportprotokolle, Auswertung der Entwicklungsrechte

Schritt 12 BSI APP.4.2; ISO/IEC 27001:2022 Anhang A 8.2

Schnittstellen- und Systembenutzer haben nur die für ihre Aufgabe nötigen Rechte und sind nicht für Dialoganmeldungen nutzbar.

Prüfhandlung Benutzer vom Typ System und Kommunikation auslesen und Rechte sowie Benutzertyp prüfen.

Nachweise Liste technischer Benutzer mit Rollen und Benutzertyp

Schritt 13 ISO/IEC 27001:2022 Anhang A 5.18; BSI ORP.4

Benutzer ausgeschiedener Mitarbeitender werden zeitnah gesperrt und Gültigkeiten werden gepflegt.

Prüfhandlung Austrittsliste der Personalabteilung mit aktiven SAP-Benutzern und letzten Anmeldungen abgleichen.

Nachweise Austrittsliste, Benutzerliste mit Status und letzter Anmeldung

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Berechtigungskonzept mit Freigabe
2. Rollenliste mit Rolleneigentümern
3. Regelwerk zur Funktionstrennung und aktuelle Konfliktauswertung
4. Auswertung kritischer Berechtigungen und Standardbenutzer
5. Protokolle der Notfallbenutzer mit Nachkontrolle
6. Protokoll der letzten Rezertifizierung
7. Einstellungen und Protokoll zur Systemänderbarkeit
8. Liste technischer Benutzer

TYPISCHE FESTSTELLUNGEN

- Mehrere Benutzer haben Vollzugriffsprofile im Produktivsystem.
- Konflikte der Funktionstrennung sind bekannt, ausgleichende Kontrollen fehlen.
- Notfallbenutzer werden genutzt, die Protokolle aber nie ausgewertet.
- Das Produktivsystem war über Wochen für direkte Änderungen geöffnet.
- Tabellenprotokollierung ist nicht aktiviert.
- Ausgeschiedene Mitarbeitende haben weiterhin gültige Benutzer.

Bibliothek Muster-Prüfprogramme

29 Muster-Prüfprogramme online

proauditmap.com/pruefprogramme/

Vollständiges Prüfpaket in ProAuditMap

proauditmap.com

ProAuditMap

Muster ohne Gewähr und keine Rechtsberatung. Gesetze, Verordnungen und Standards erscheinen nur als Fundstelle, Normtexte sind nicht abgedruckt. Passen Sie Umfang und Tiefe vor der Verwendung an Ihre Organisation, Ihre Risiken und die aktuelle Fassung der für Sie geltenden Vorschriften an. Stand: 13. Oktober 2026