SAP

Best-Practice-Empfehlungen des
DSAG-Arbeitskreises Revision und Risikomanagement
Deutschsprachige SAP-Anwendergruppe e. V.

SAP S/4HANA Prüfleitfaden

Stand: Dezember 2022

DSAG

Autor:innen

Tabelle 1 Autor:innen nach Namen

Name	E-Mail	Unternehmen	Kürzel
Andreas Fritz	andreas.fritz@adesso-orange.com	adesso orange AG	AF
Björn Brencher	bjoern.brencher@sap.com	SAP SE	BB
Christina Köhler	ckoehler@deloitte.de	Deloitte GmbH Wirtschaftsprüfungsgesellschaft	CK
Christian Rinner	christian.rinner@sva.de	SVA System Vertrieb Alexander GmbH	CR
Georg Hohnhorst	georghohnhorst@kpmg.com	KPMG AG Wirtschaftsprüfungsgesellschaft	GH
Hendrik Müller	hendrik.mueller@sap.com	SAP SE	HM
Johannes Liffers	johannes.liffers@pwc.com	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft	JL
Andrea Kristina Buick-Feltes	andrea.buick-feltes@deu.kyocera.com	KYOCERA Document Solutions Europe B.V.	KB
Luisa Dechant	luisa.dechant@pwc.com	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft	LD
Martin Krause	martin.krause@pwc.com	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft	MK
Maren Sonnenschein	msonnenschein@rwe.com	RWE AG	MS
Nils Greßler	nils.gressler@pwc.com	PricewaterhouseCoopers GmbH WPG	NG
Peter Hamm	peter.hamm@pwc.com	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft	PH
Ralf Köhler	ralf.koehler@sap.com	SAP Deutschland SE & Co. KG	RK
Thomas Glauch	tglauch62@gmail.com	KPMG AG Wirtschaftsprüfungsgesellschaft	TG
Timm Schwarz	timm.schwarz@pwc.com	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft	TS

Tabelle 2 Autor:innen nach Kapiteln

Kapitel	Autor:innen	Stand
Einleitung	Thomas Glauch	Dez 2022
1 S/4HANA – die vierte Generation	Ralf Köhler / Thomas Glauch / Luisa Dechant	Dez 2022
2 Prüfenden-Rolle, SAP-Systemlandschaft und Richtlinien des Unternehmens	Peter Hamm / Thomas Glauch	Dez 2022
3 Authentifizierung	Christian Rinner / Ralf Köhler	Dez 2022
4 Autorisierung	Johannes Liffers / Martin Krause / Andrea Kristina Buick-Feltes / Timm Schwarz	Dez 2022
5 Change-Management – SAP Application Lifecycle Management / Solution Manager	Georg Hohnhorst	Dez 2022
6 SAP S/4HANA OnPremise	Christian Rinner / Johannes Liffers / Ralf Köhler	Dez 2022
7 SAP S/4HANA Cloud, public edition	Christina Köhler / Björn Brencher / Luisa Dechant / Christian Rinner / Nils Greßler / Martin Krause	Dez 2022
8 SAP HANA Datenbank	Hendrik Müller / Andrea Kristina Buick-Feltes / Christian Rinner / Johannes Liffers	Dez 2022
9 Betriebssysteme – Linux/Unix/Windows	Maren Sonnenschein / Björn Brencher/ Christina Köhler	Dez 2022
10 Risiken aus dem Einsatz von SAP GRC	Andreas Fritz	Dez 2022

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Einleitung

Der vorliegende Prüfleitfaden des Arbeitskreises Revision und Risikomanagement nimmt neue Entwicklungen der SAP im Hinblick auf die bestehende ERP-Software-Produktlinie in den Fokus und zielt auf die SAP-S/4HANA-Umgebung ab. Der Kern des Prüfleitfadens bezieht sich dabei auf die Systemstände S/4HANA (OnPremise) (Release-Stand S/4HANA 2021) sowie S/4HANA Public Cloud (Release-Stand S/4HANA Cloud 2208). Der Arbeitskreis Revision und Risikomanagement ist Teil der Deutschsprachigen SAP-Anwendergruppe e. V. (DSAG) mit Sitz in Walldorf.

Zielsetzung des Leitfadens ist es, Best-Practice-Empfehlungen für die Prüfungen der genannten SAP-Umgebungen und dabei vor allem prüferische Themenstellungen in den Vordergrund zu stellen. Er aktualisiert und erweitert den im Jahr 2015 in der Version 2.0 herausgegebenen Prüfleitfaden zu SAP ERP 6.0.

Die Prüfhinweise in diesem Leitfaden sind als Hinweise für mit SAP vertraute Prüfende und als eine Richtschnur für die mit der Erstellung und Wartung von Berechtigungskonzepten betrauten Administrator:innen und Consultants gedacht.

Sie sind keine verbindliche Richtlinie oder Norm. Jegliche Verantwortung für Art, Umfang und Ergebnis externer und interner Prüfungen verbleibt beim Prüfenden selbst. Grundsätzlich gilt, dass einschlägige rechtliche Rahmenbedingungen bzw. Anforderungen zu berücksichtigen sind, die sich zum Beispiel aus dem HGB (Vorschriften des Handels- und Steuerrechts [§§ 238 ff. HGB sowie §§ 140–148 AO]) oder den GoBD (dem Schreiben des Bundesfinanzministers [BMF] vom 28. November 2019 „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff) ergeben. Weiterhin sind unter anderem die Anforderungen zu beachten, die sich aus der EU-Datenschutz-Grundverordnung (DSGVO) sowie den Stellungnahmen des Fachausschusses IT (FAIT) des Instituts der Wirtschaftsprüfer (IDW) ergeben.

Zudem liegt in der Verantwortung des Prüfenden auch die Zuordnung der ausgewählten Prüfungsschwerpunkte zu einschlägigen ISO-Normen, z. B. für IT-Sicherheit ISO/IEC 27001, zu Rahmenwerken für die Prüfung, z. B. COSO/COBIT, oder zu berufsständischen Prüfungsstandards z. B. des Instituts der Wirtschaftsprüfer (IDW).

Weitere notwendige Voraussetzungen sind Erfahrungen mit S/4HANA (OnPremise) oder S/4HANA Cloud sowie Kenntnisse der gesetzlichen Vorschriften für die Rechnungslegung. Zur detaillierten Auseinandersetzung mit der SAP-Architektur verweist das Autorenteam auf die SAP-Online-Dokumentation, auf entsprechende Literatur und auf Schulungskurse.

Die aufgeführten Prüfprogramme stellen Handlungsempfehlungen dar.

Der notwendige Prüfungsumfang muss den Kund:innen-spezifischen organisatorischen Prozessen jeweils individuell angepasst werden.

Gender-Hinweis:
In diesem Leitfaden wird gegendert. Bewusst auf das Gendern des Begriffs „Benutzer“ wird jedoch verzichtet, da es sich dabei auch um die Bezeichnung im SAP-System handelt. Daher gilt die männliche Form für alle Fälle, in denen dies nicht explizit ausgeschlossen ist, für alle Geschlechter.

1 S/4HANA – die vierte Generation

SAP S/4HANA ist die neue Generation der Enterprise-Resource-Planning(ERP)-Systeme der SAP SE. Als Nachfolger der Produkte SAP R/3 und SAP ERP wurde das ERP-System im Jahr 2015 veröffentlicht und wird seither in jährlichen Release-Zyklen um neue Funktionen und Technologien wie Analytics und Artificial Intelligence erweitert. Der Name „S/4HANA“ leitet sich aus dem Begriff Simple (S), der 4. Softwaregeneration von SAP-ERP-Systemen sowie der zugrunde liegenden Datenbanktechnologie SAP HANA ab.

Mit der Einführung der SAP-HANA-Datenbank erfolgte eine Änderung und Vereinfachung des zugrunde liegenden Datenmodells bzw. der Tabellenstrukturen des ERP-Systems. Dies ermöglicht die Zusammenführung der Belege aus den Bereichen Finanzwesen, Anlagenbuchhaltung, Controlling, Material-Ledger und Ergebnisrechnung im Belegjournal „Universal Journal“ und damit die Schaffung einer „single source of truth“. Durch den Umstieg von einer zeilen- zu einer spalten-orientierten Speicherung von Daten und das Zusammenführen von Online-Analytical-Processing (OLAP) und Online-Transactional-Processing (OLTP) sind ein schneller Zugriff auf Transaktionen und umfassende Analysen für die operative und strategische Arbeit in Echtzeit realisierbar. Zusätzlich bietet SAP HANA erweiterte Such-, Analyse- und Datenintegrationsfunktionen sowohl für strukturierte als auch für unstrukturierte Daten.

Bei SAP HANA handelt es sich um eine sogenannte In-Memory-Datenbank (IMDB). Dies ist ein Datenbanktyp, der Daten im Arbeitsspeicher (RAM) eines Computers statt auf herkömmlichen Festplatten oder Solid-State-Laufwerken (SSD) speichert. Andere Datenbanken verfügen mittlerweile zwar ebenfalls über In-Memory-Funktionen, sind aber dennoch festplattenbasiert aufgebaut. Im Gegensatz dazu wurde SAP HANA so konzipiert, dass zunächst In-Memory-Daten verwendet werden, bei Bedarf aber andere Speichermechanismen genutzt werden können. Da Daten wesentlich schneller aus dem Arbeitsspeicher als von einer Festplatte oder SSD abgerufen werden können, verkürzen sich Reaktionszeiten somit im Vergleich zu herkömmlichen Datenbanken. SAP S/4HANA kann ausschließlich mit der SAP-HANA-Datenbank verwendet werden; die Nutzung einer anderen Datenbanktechnologie ist nicht möglich.

Mit der Einführung von S/4HANA wurde ebenfalls die neue Bedienoberfläche „Fiori Launchpad“ in Ergänzung zu SAP GUI pilotiert. Über die kachelbasierte, personalisierte, rollenbezogene Oberfläche „Fiori Launchpad“ bietet sie Anwendenden die Möglichkeit, Geschäftsprozesse, Analysen und operative Arbeiten in intuitiveren und simplifizierten Fiori Apps auf verschiedensten Endgeräten abzubilden.

Im Rahmen der Transformation von bisherigen ERP-Systemen (SAP und Non-SAP) zu SAP S/4HANA kann die Software in verschiedenen OnPremise- und Cloud-Optionen sowie Hybrid-Ansätzen betrieben werden. Die Entscheidung für eines der Betriebsmodelle kann dabei von verschiedenen Faktoren abhängig sein wie der IT-Strategie von Unternehmen, funktionalen und gesetzlichen Anforderungen, Innovationsbedürfnissen sowie Überlegungen zur Harmonisierung und Standardisierung von Prozessen.

Für die Lösung SAP S/4HANA bietet SAP im Wesentlichen drei Betriebsmodelle an:

- SAP S/4HANA (OnPremise) – bei dieser Deployment-Form kauft der Kunde/die Kundin Software-Lizenzen von SAP und ist für den Betrieb des Systems (Applikation, Datenbank, Infrastruktur) vollständig selbst verantwortlich (bspw. Betrieb im eigenen Rechenzentrum oder beim IT-Dienstleister)
- SAP S/4HANA Cloud, Private Edition – SAP übernimmt den Betrieb der für die Lösung notwendigen Infrastruktur; die Verantwortung für den Betrieb der eigentlichen Anwendung liegt bei dem/der Kund:in
- SAP S/4HANA Cloud – Software-as-a-Service-Lösung (SaaS), bei der SAP sowohl die Infrastruktur als auch die Anwendung betreibt

Alle S/4HANA-Deployment-Formen bauen auf dem gleichen Datenmodell und der SAP-HANA-Datenbank auf und beinhalten die angepasste moderne Bedienoberfläche. Die verschiedenen Lösungen unterscheiden sich unter anderem in den Standardisierungs- und Flexibilisierungsmöglichkeiten. Während die SaaS-Lösung S/4HANA Cloud ein hohes Maß an Standardisierung entlang den S/4HANA-Cloud-Best-Practices ermöglicht und teilweise unumgänglich macht, bieten die Deployment-Formen S/4HANA Cloud, Private Edition und S/4HANA Möglichkeiten der flexibleren Ausgestaltung des ERP-Systems, die mit einem geringeren Grad an Standardisierung einhergehen und einen höheren Aufwand für Upgrade-Prozesse bedingen können. Neben den Unterschieden bez. der Standardisierung und Flexibilisierung der Softwarelösungen gibt es weitere Abweichungen, wie die Implementierungsstrategie, Release-Zyklen sowie die Bedienoberfläche. Ein Auszug der Unterschiede zwischen den verschiedenen Deployment-Formen kann Abbildung 1 entnommen werden.

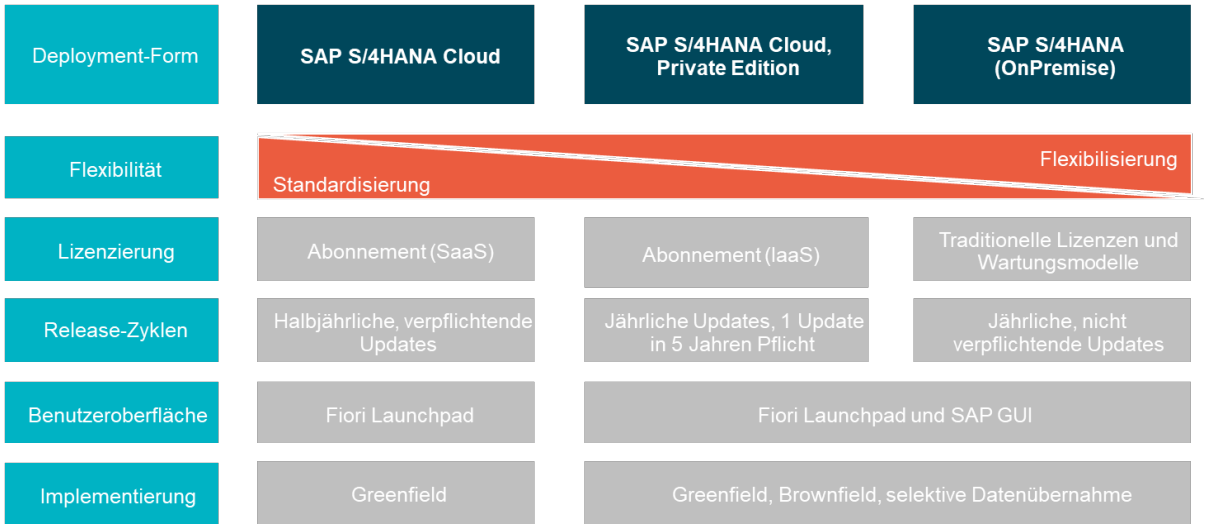

Abbildung 1 Übersicht SAP-S/4HANA-Deployment-Formen

Im Rahmen dieses Prüfleitfadens werden die folgenden Deployment-Formen betrachtet:

1. SAP S/4HANA (OnPremise)
2. SAP S/4HANA Cloud, Public Edition

Auf eine separate Erläuterung von Prüfstrategien für die Deployment-Form SAP S/4HANA Cloud, Private Edition oder weiterer Modelle wie bspw. HANA Enterprise Cloud (HEC) wird verzichtet, da die Prüfungsstrategien der beiden beschriebenen Modelle auf die weiteren Deployment-Formen unter Beachtung der Besonderheiten des jeweiligen Betriebsmodells entsprechend übertragen werden können.

Zu beachten ist, dass SAP Security Notes nur für SAP Support Package Stacks (SPS) der letzten 24 Monate geliefert werden. Wenn die SPS nicht regelmäßig eingespielt werden, erhält man auch entsprechend keine Security-Korrekturen von SAP mehr!

2 Prüfenden-Rolle, SAP-Systemlandschaft und Richtlinien des Unternehmens

Grundlagen zur Erstellung einer Prüfenden-Rolle

Im Rahmen einer Prüfung müssen neben den für das Unternehmen geltenden gesetzlichen Vorgaben auch die „internen“ Compliance-Vorgaben berücksichtigt werden, wobei den gesetzlichen Vorgaben Vorrang zu gewähren ist.

Zur Durchführung einer SAP-Systemprüfung benötigt der/die interne bzw. externe Prüfende generell alle Anzeigeberechtigungen, die das Prüfungsgebiet umfassen. Insofern ist die Einrichtung von Prüfenden-Rollen im Vorfeld anstehender Prüfungen empfehlenswert, damit bei Prüfungsbeginn nicht unnötige Zeit auf Anwendenden- und Prüfenden-Seite vertan wird. Die Prüfenden-Rollen sind in der Form aufzubauen, dass nur die Inhalte der zum Prüfungsumfang gehörenden Bereiche angezeigt werden dürfen. Dies gilt insbesondere dann, wenn gesetzliche Vorgaben im Kontext des Datenschutzes oder einer Steuerprüfung (DART-Zugriffe) zu erfüllen sind.

Benötigt eine/ein Prüfende:r Berechtigungen (z. B. Zugriff auf Eigenentwicklungen), die denen eines Notfall-Benutzers entsprechen, ist gemäß dem vorliegenden Notfall-Benutzer-Konzept zu verfahren.

Tabelle 3 Bestandsaufnahme der SAP-Systemlandschaft

Nr.	Bestandsaufnahme SAP-Systemlandschaft
1.	Gibt es einen – z. B. grafischen – Gesamtüberblick der SAP-Systemlandschaft?
2.	Gibt es eine Übersicht über alle eingesetzten SAP-Systeme, SAP-Anwendungen und deren Release-Stand?
3.	Auf welchen Betriebssystemen laufen die SAP-Systeme?
4.	Welche Datenbanken unterstützen die SAP-Anwendungen? SAP S/4HANA nutzt immer eine HANA-Datenbank.
5.	Gibt es ein detailliertes Diagramm der SAP-Systemarchitektur, das die Verbindungen der SAP-Systeme untereinander sowie zu den SAP-Clients und die Netzverbindung in das Internet darstellt?
6.	Welche Instanzen sind für den SAP-Betrieb eingerichtet? Es ist wichtig, dass jede Instanz einer Prüfung unterzogen wird.
7.	Welche SAP-Produkte und -Module sind implementiert (Bestandsverzeichnis)?
8.	Gibt es eine Übersicht über verschlüsselte Netzverbindungen?

Bestandsaufnahme der Richtlinien des Unternehmens

Die Unternehmen sind in der Vorgabe und der Gestaltung von internen Richtlinien frei. Allerdings üben gesetzliche Vorgaben und IT-Standards einen Normierungsdruck auf Inhalte und Ausprägung IT-bezogener Richtlinien aus.

Hier sind lediglich diejenigen Vorgaben aufgeführt, die für die Prüfung von SAP-Systemen relevant sind. Sind sie vorhanden, unterstützt das die Prüfung.

Tabelle 4 Unternehmensinterne Richtlinien und IT-Prozessdokumentation

Nr.	Unternehmensinterne Richtlinien und IT-Prozessdokumentation
1.	IT-Sicherheitsrichtlinie
2.	Aktuelles, gültiges Berechtigungskonzept
2.1.	› Identifikation von Benutzern
2.2.	› Vorgaben zum Passwortschutz
2.3.	› Festgelegte Zuständigkeiten und Rollen bei der Berechtigungsvergabe
2.4.	› Zuständigkeiten und Aufgaben der Dateneigentümer:innen sowie der Systembetreiber:innen
3.	Ist die IT-Sicherheit von spezifischen Systemplattformen geregelt und dokumentiert? Zum Beispiel für:
3.1.	› SAP-Client am Arbeitsplatz (PC, Notebook)
3.2.	› Netzverbindungen
3.3.	› MS-Windows-Server
3.4.	› UNIX-Server
3.5.	› Datenbank
4.	Projektrichtlinie
5.	Vorgaben für das Software-Development-Life-Cycle(SDLC)-Management
6.	Prozessdokumentationen für die SAP-Anwendungs- und -Systemlandschaft
6.1.	› Customizing
6.2.	› Betrieb und Überwachung
6.3.	› Change- und Konfigurationsmanagement
6.4.	› Release-Management

Nr.	Unternehmensinterne Richtlinien und IT-Prozessdokumentation
6.5.	› Zugangs- und Berechtigungsverwaltung
6.6.	› IT-Sicherheits-Management
6.7.	› Business-Continuity-Management
7.	Service-Level-Agreements zwischen den Betreibern der SAP-Systemlandschaft und den Geschäftseinheiten, die die SAP-Anwendungen für ihre Geschäftsprozesse nutzen
8.	User-Help-Desk

3 Authentifizierung

3.1 Einleitung

Was ist der Unterschied zwischen Authentifizierung und Autorisierung?
Die Autorisierung ist die Gewährung von Zugriffen auf Ressourcen mittels Rechten, die eine bestimmte Identität zugewiesen bekommen hat. Im Rahmen von SAP entspricht dies den Rollen mit den darin enthaltenen Rechten, die dem Benutzer zugewiesen wurden.

Die Authentifizierung ist die Sicherung der Identität eines Anfragenden gegenüber der liefernden Instanz. Hier auf SAP übertragen entspricht dies im einfachsten Fall dem Umstand, dass ein Benutzer seinen Anmeldenamen und das zugehörige Passwort eingibt. Sofern das Passwort korrekt ist, wird hiermit die Identität des Benutzers bestätigt.

Authentifizierung bezeichnet die Prüfung dieses Identitätsnachweises auf seine Authentizität.

Im weitesten Sinne ist der Mechanismus immer derselbe – ein Nutzender fragt virtuell nach Zugriff auf eine bestimmte Ressource, das System muss nun die beiden folgenden Punkte klären:

1. Wer fragt an? (Authentifizierung)
2. Darf derjenige/diejenige die Informationen bekommen? (Autorisierung)

Die Integrität des SAP-Systems ist nur gegeben, wenn hier nicht punktuell, sondern ganzheitlich geprüft wird.

Dies ist natürlich auch die Grundlage vieler Angriffe auf IT-Systeme: Entweder versucht der Angreifende, sich als jemand anderes auszugeben und umgeht hier die Mechanismen der Authentifizierung, oder er versucht, höhere Rechte zu bekommen (Autorisierung).

Leider ist die Beachtung der beiden Bereiche im SAP-System nicht immer ausgeglichen. Es wird intensiv an den Rechten der Nutzenden gearbeitet, allerdings gerät die Authentifizierung hier manchmal aufgrund der Zusammenhänge ins Hintertreffen.

Anmeldeverfahren auf ABAP-Systemen

Es gibt verschiedene Arten der Authentifizierung der Benutzer

SAP GUI (DIAG/RFC)

- mittels Kennwort (konventionelle Anmeldung)
- durch ein externes Sicherheitsprodukt (SNC)
- aufgrund X.509-Browser-Zertifikat (Intranet/Internet)
- Kerberos
- mittels Workplace-Single-Sign-On(SSO)-Ticket

Zusätzlich für Browser-basierten Zugriff (HTTP/TLS)

- Kerberos/SPNego
- Security Assertion Markup Language
- OAuth 2.0 / OpenID Connect

Die kennwortbasierte Authentifizierung der Benutzer wird standardmäßig verwendet.

Bei Einsatz anderer Authentifizierungsmethoden (siehe oben) kann es gewünscht sein, die Option der kennwortbasierten Anmeldung zu deaktivieren (login/disable_password_logon).

Die kennwortbasierte Anmeldung sollte nur dann deaktiviert werden, wenn sichergestellt ist, dass sich alle Benutzer auf andere Weise (per SNC / X.509 / SSO-Ticket) an diesem System anmelden können!

Generelle Hinweise zum Absichern der Authentifizierung gegenüber der Datenbank

Die Passwörter von Datenbankbenutzern, die für die Authentifizierung des SAP-Systems gegenüber der Datenbank oder für die Authentifizierung mit Datenbankwerkzeugen benötigt werden, müssen regelmäßig geändert werden. Ebenso sollten direkte Zugriffe auf die Datenbank stärker gesichert sein als ein Standardzugriff vom Fachbereich.

Um den Authentifizierungsprozess und die Kommunikation zu sichern, gibt es die folgenden Methoden:

- Verwendung des Verschlüsselungsmechanismus, der vom proprietären Datenbanktreiber bereitgestellt wird, falls verfügbar (dies hängt vom Datenbankhersteller ab)
- Verwendung von Betriebssystemmethoden oder Methoden auf Anwendungsebene (z. B. SSH- oder SSL-Tunnel)
- Platzieren Sie die Anwendungsserver und den Datenbankserver in einem separaten Hochsicherheits-Netzsegment, das über Sicherheitsmaßnahmen verfügt, die eine Überwachung des Netzverkehrs weniger möglich machen.
- Die Verschlüsselung in solchen Netzwerksegmenten ist nicht obligatorisch, wird aber empfohlen.
- Verwenden Sie den Secure-Store-and-Forward-Mechanismus (SSF) für die ABAP-Technologie.
- Die Verwendung einer Zwei-Faktor- oder Multi-Faktor-Authentifizierung.

SSF-Mechanismen sind in Anwendungsgebieten nützlich, in denen ein erhöhtes Maß an Sicherheit besteht für:

- die spezifische und eindeutige Identifizierung von Personen oder Komponenten (z. B. bei Workflow-Prozessen)
- Unleugbarkeit oder Verbindlichkeit (z. B. beim Unterzeichnen nicht in gedruckter Form vorliegender Verträge)
- Authentizität und Integrität der Daten (z. B. Sichern der Audit-Logs)
- Senden und Ablegen vertraulicher Daten

Durch den Einsatz der SSF-Mechanismen in SAP-Anwendungen können Sie gedruckte Dokumente und handschriftliche Unterschriften durch automatisierte Workflow-Prozesse und digitale Dokumente ersetzen, die mittels digitaler Signaturen und digitaler Umschläge gesichert sind.

Allerdings ist in einigen Ländern die Verwendung der Kryptografie und digitaler Signaturen gesetzlich geregelt. Diese Gesetze können sich ändern. Sie sollten sich

regelmäßig über die Auswirkungen dieser Gesetze auf Ihre Anwendungen informieren und sicherstellen, dass Ihnen alle weiteren Entwicklungen bekannt sind.

3.2 Risiken

Das größte Risiko im Bereich Authentifizierung ist, dass Dritte an Information gelangen, um sich gegenüber dem SAP-System als Berechtigte Benutzer auszugeben. Dies kann die Grundlage für zahlreiche Gefährdungen des Systems nach sich ziehen: Freigaben von Buchungen, Einsicht in vertrauliche Vorgänge, Störung des Systembetriebs bzw. von Unternehmensprozessen.

Ebenso müssen nicht nur Benutzer, sondern auch Systeme authentisiert werden, da gerade bei einer erhöhten Vernetzung auch jeder externe Server mit Zugriff auf Informationen vertrauenswürdig sein muss.

3.3 Kontrollziele

- Die Systemparameter für die Anmeldekontrollen sind so gesetzt, dass diese einen angemessenen Zugriffsschutz gewährleisten.
- Die Security Policies / Audit Logs sind so eingestellt, dass eine Systemmanipulation erkannt wird.
- Die Kommunikation zwischen Client und Server ist nach einem aktuellen Verfahren verschlüsselt.
- Die Gateway-Kommunikation wird mithilfe von Access Control Listen (ACL) geschützt.
- Mehrfachanmeldungen werden verhindert.
- Gültigkeitszeiträume für Benutzerkennungen sind definiert.
- Die Sonderbenutzer sind sicher konfiguriert.
- Sicherheitsmechanismen für die Verwaltung von Gruppen von Benutzern und für besondere Typen von Benutzern sind aktiviert.
- Die Wirksamkeit der Anmeldekontrollen wird überwacht.
- Serverzertifikate sind installiert und gültig.
- Es existieren Prozesse für den Notfallzugriff und eine Auditierung der durchgeführten Systemvorgänge.
- Es wird auf Endbenutzer-Seite ein aktueller Client zum Zugriff verwendet.
- Es existiert eine Dokumentation der eingesetzten Schnittstellen (RFC, SICF). Nicht mehr benötigte sind deaktiviert.
- Single-Sign-on (SSO) wird verwendet.

4 Autorisierung

4.1 Einleitung

Das Benutzer- und Berechtigungskonzept (die Autorisierungen) einer SAP-S/4HANA-Umgebung muss dazu geeignet sein, die unternehmensspezifischen Anforderungen der Ablauforganisation (Abbildung einzelner Prozessschritte/Aufgaben und Arbeitsplätze durch Berechtigungen in Rollen) und der Aufbauorganisation (organisatorischer/rechtlicher Aufbau des Unternehmens) abbilden zu können.

In Bezug auf die aktuelle technische Architektur der SAP-S/4HANA-Systemlandschaft gilt es dabei, unterschiedliche Technische Benutzer- und Berechtigungskonzepte in den verschiedenen System-Schichten S/4HANA (On-Premise), S/4HANA Cloud, SAP HANA, Fiori) zu beachten. Dabei können die Benutzer und die Berechtigungen fast in allen betrachteten Schichten nach wiederkehrenden Dimensionen gestaltet und beurteilt werden.

Insofern werden in diesem Kapitel die Prüfungshandlungen zum Prüfungsbereich Autorisierung generisch und unabhängig von den technischen Besonderheiten der S/4HANA-Schichten beschrieben. Die technischen Spezifika werden dann erst in den späteren schichtspezifischen Kapiteln in einem jeweiligen Unterkapitel für Autorisierung beschrieben.

Soweit Aspekte von Benutzern und Berechtigungen im Unternehmen bereits systemübergreifend geregelt werden und dokumentiert sind, kann eine Prüfung dieser Aspekte unter Nutzung der Prüfungshandlungen dieses Kapitels 4 bereits auf einer schichtenübergreifenden Ebene erfolgen. Wann immer Aspekte zu Benutzern und Berechtigungen schichtenspezifisch geregelt und dokumentiert sind, sind die Prüfungshandlungen aus Kapitel 4 mit in die Prüfprogramme für Autorisierungen der einzelnen Schichten zu übernehmen – dies nur in dem Maße, in dem die Prüfungshandlungen auf die jeweilige Anwendungsschicht anwendbar sind.

Je nach Unternehmensanforderung existieren verschiedene Differenzierungsmodelle für Berechtigungskonzepte. Dabei kann der Zugriff auf Sichten und Funktionen für Daten entweder rollenbasiert (RBAC – Role-based Access-Control) oder attributbasiert (ABAC – Attribute-based Access-Control) erfolgen. Im Rahmen von SAP-Systemen werden standardmäßig rollenbasierte Berechtigungskonzepte systemseitig unterstützt.

Mit der schon vorher existierenden, aber mit S/4HANA stärker integrierten Verteilung auf mindestens drei Schichten und insbesondere mit der vermehrten oder ausschließlichen Nutzung des Fiori Launchpads für die Navigation muss auch die Rollenmodellierung dem aus einer schichtübergreifenden Architektur Rechnung tragen. Dies bezieht sich sowohl auf die Gestaltung der Rollen in den jeweiligen

Schichten/Systemen als auch auf die Gestaltung von arbeitsplatzorientierten Rollen über die Systemschichten hinweg.

Um ein ordnungsgemäßes Berechtigungskonzept zu erstellen, sind insofern bereits am Anfang entsprechende ablauf- und aufbauorganisatorische Anforderungen zu identifizieren und ein entsprechend geeignetes Rollenmodell zu wählen.

4.2 Risiken

Die Risiken für Autorisierungen beziehen sich auf die Fehlsteuerung des Zugriffs von Anwendenden auf Funktionen und Daten von IT-Anwendungen mit dem Ergebnis einer Beeinträchtigung der Daten- und/oder Systemintegrität. Dabei beziehen sich die Risiken im Wesentlichen auf die beiden folgenden grundlegenden Autorisierungsaspekte:

Minimalprinzip: Grundsätzlich sollen Benutzer nur Berechtigungen mit dem Zugriff auf Sichten und Funktionen für die Daten erhalten, die sich aus ihrem Verhältnis zum Unternehmen ergeben. Dies wird als das Minimalprinzip, oder im englischen Sprachgebrauch als „Least-Privilege“-Prinzip, bezeichnet. Je mehr Anwendende Zugriff auf Funktionen und Daten erhalten, ohne dass dies ihrem definierten Aufgabenbereich entspricht, desto höher ist das Risiko einer Verfälschung oder eines Missbrauchs von Daten oder einer Gefährdung der Systemintegrität. Dabei sind die Zugriffe je Funktion/Daten auch im Zusammenhang mit den Instanzen der IT-Anwendungen zu betrachten.

Funktionstrennungsprinzip: Ergänzend zum Minimalprinzip sind Kombinationen einzelner Funktionen zu identifizieren und deren Vergabe an Anwendende zu vermeiden, die in ihrer kombinierten Vergabe an Benutzer zu einem im Vergleich zum Risiko der Einzelfunktionen erhöhten Risiko führen. Dies wird als Funktionstrennungsprinzip, oder im Englischen als „Segregation-of-Duties“(SoD)-Prinzip, bezeichnet. Mit jeder Vergabe von Zugriff auf Funktionen erhöht sich das Risiko, dass Anwendende aus diesen kombinierten Berechtigungen aufeinander bezogene Geschäftsvorfälle erfassen, um sich allein oder in Abstimmung mit fremden Personen zu bereichern oder allgemein dem Unternehmen Schaden zuzufügen.

Im Sinne einer angemessenen Fokussierung der Maßnahmen zur Adressierung dieser Aspekte ist es sinnvoll, eine risikoorientierte Einschätzung der Funktionen/Daten und der damit verbundenen Berechtigungen und Funktionstrennungskombinationen in IT-Anwendungen vorzunehmen. Dies sollte in Abstimmung mit der Risikoeinschätzung/Schutzbedarfsermittlung der IT-Anwendungen als Ganzes erfolgen.

In Abhängigkeit der Risiko-Levels der Funktionen/Rollen und Funktionstrennungen ist ein entsprechendes Maß an Aufmerksamkeit im Rahmen der Kontrollen und Prozesse

erforderlich. Dementsprechend können aber auch bei geringerem Risiko-Level Vereinfachungen ermöglicht werden.

Aus den oben geschilderten Hauptaspekten für Risiken im Bereich Autorisierungen ergeben sich eine Reihe weiterer daraus abgeleiteter Risiken und damit korrespondierende Kontrollziele und Prüfungshandlungen. Die folgenden Aspekte seien beispielhaft genannt:

- Die Strukturen (Benutzer, Rollen und Berechtigungen), die Prozesse, die Organisation und die Kontrollen sind für einen sachkundigen Dritten / eine an den Autorisierungsverfahren beteiligte Person aus den verfügbaren Dokumentationen und Standards nicht oder nur eingeschränkt verständlich. Hieraus ergeben sich unvermeidlich zunehmende Verschlechterungen im Rollenzustand, in der Vergabe der Rollen an Benutzer und damit in Bezug auf Minimal- und Funktionstrennungsprinzipien.
- Die Rollen & Berechtigungen folgen keiner einheitlichen Architektur / keinem einheitlichen Rollenschnitt; es gibt keine standardisierten Konventionen für die äußere Rollendeklaration (Name, Text, Beschreibung). In der Konsequenz können bei der Beantragung aufgrund des fehlenden Verständnisses der Beteiligten zu den Rolleninhalten nicht die richtigen Rollen für einen/eine Anwendende ausgewählt und von den Genehmigenden geprüft werden. Es ergibt sich die Gefahr der Überberechtigung und daraus folgend von Funktionstrennungsverletzungen.
- Universelle Berechtigungen und sicherheitskritische Systemeinstellungen werden nach dem Produktiveinsatz im System nicht geändert, obwohl diese nur für die Phase der Implementierung oder des Release-Wechsels vorgesehen sind. Im Produktivsystem gefährden diese aber die Systemintegrität und den ordnungsgemäßen Betrieb.
- Für Benutzer liegen keine Vorgaben für eine angemessene Einordnung nach Typen/Gruppen von Benutzern, Tätigkeit, Abteilung, Kostenstelle etc. vor, über die eine Beurteilung des Verhältnisses des Benutzers zum Unternehmen und daraus folgend der für den Benutzer erforderlichen Berechtigungen abgeleitet/beurteilt werden könnte.
- Die Prozesse zur Pflege von Rollen weisen keine geeigneten Vorgaben für die Prüfung und Genehmigung durch Rollen-Eigner:innen und -Koordinator:innen vor. Darunter leiden die Rollenarchitektur / der Rollenschnitt, die Rollendeklaration und die Übereinstimmung zwischen äußerer Deklaration und den Rolleninhalten (technischen Berechtigungen). Die Rollen verlieren an Transparenz. Durch Unterschiede zwischen äußerer Deklaration und abweichenden enthaltenen Berechtigungen werden bei der Vergabe mehr Berechtigungen zugeordnet als erkennbar und beabsichtigt.

- Die Prozesse zur Beantragung, Genehmigung und Vergabe von Rollen an Benutzer weisen keine geeigneten Vorgaben für Antragstellung sowie Prüfung und Genehmigung durch Manager:innen und Rollen-Genehmigende auf. Es werden Rollen vergeben, die nicht zur Ausübung der Tätigkeit der Benutzer, insbesondere in prozessfremden Bereichen, erforderlich sind.
- Eine Organisation und insbesondere eine Definition der Aufgaben/ Verantwortlichkeiten der Beteiligten in allen Autorisierungsprozessen ist nicht oder unzureichend definiert. Hierdurch ist nicht klar, wer beteiligt und betroffen ist. Aufgaben werden nicht wahrgenommen. Die Übereinstimmung der Rollenpflege und -vergabe mit dokumentierten Standards bleibt unberücksichtigt.
- Die Betrachtung und Integration von Kontrollen in die Prozesse für Benutzer und Berechtigungen sind nicht hinreichend definiert und etabliert. Dies betrifft insbesondere die Identifikation sensitiver Funktionen und Funktionstrennungen – bevorzugt präventiv als Bestandteil der Rollenpflege und -vergabe-Prozesse oder aber nachgelagert z. B. im Rahmen von Rezertifizierungsmaßnahmen für Benutzer und Rollen. Hieraus können sich Verstöße gegen das Minimal- und SoD-Prinzip ergeben.
- Vorgaben für autorisierungsrelevante Parameter fehlen oder sind unvollständig; sensible Geschäftsvorfälle/Transaktionen, die nur restriktiv oder nicht vergeben werden sollen, werden nicht über geeignete Protokolle aufgezeichnet. Dies führt zu einer erhöhten Gefährdung durch fehlenden Autorisierungsschutz oder durch fehlende Nachvollziehbarkeit und damit fehlende Kontrolle sensibler Transaktionen.

4.3 Kontrollziele

Die Kontrollziele beziehen sich insbesondere auf die effektive und effiziente Gestaltung der Strukturen, der Prozesse und der Organisation der Zugangs- und Berechtigungsverwaltung.

Dabei sind die oben genannten Risiken für Autorisierung ein Bestandteil des Risikomanagements des Unternehmens. Die Kontrollen und Kontrollziele für Autorisierungen stellen einen Ausschnitt der Anforderungen an ein internes Kontrollsystem sowie ein Informationssicherheitsmanagement-System (ISMS) dar, das Unternehmen einrichten, warten, überwachen und kontinuierlich optimieren müssen.

- Ein dokumentiertes Berechtigungskonzept der für Autorisierung relevanten Strukturen, Prozesse, Organisation und Kontrollen (im Regelbetrieb oder vor dem Projektstart) liegt vor, das die gesetzlichen und unternehmensinternen Anforderungen erfüllt.
- Ein transparentes Konzept mit Vorgaben für die Rollenarchitektur, den Rollenschnitt und die Rollendeklaration für Rollen und Berechtigungen ist für die risikorelevanten IT-Anwendungen und Anwendungsbereiche definiert und umgesetzt. Regeln mit Vorgaben für Standardrollen und -berechtigungen sind vorhanden.
- Vorgaben für Benutzer mit einer Klassifizierung in Typen von Benutzern sowie einer angemessenen organisatorischen, tätigkeitsbezogenen Einordnung der Benutzer sind definiert und werden u. a. über eine Integration mit den Identity-Repositories und HR-Systemen aktuell gehalten. Regeln mit Vorgaben für Standardbenutzer sind vorhanden.
- Die Prozesse, insbesondere des Managements von Benutzern oder auch User-Lifecycles (Joiner, Mover, Leaver), der Rollen- und Berechtigungspflege, der Rollenbeantragung, -genehmigung und -provisionierung, der Analyse und Lösung von Regelverstößen für Funktionstrennungen und sensitive Funktionen, der Rezertifizierung von Benutzern und Rollenzuordnungen sowie des Managements privilegierter Benutzer, sind geregelt und etabliert.
- Sensitive/kritische Berechtigungen und Berechtigungskombination sind im Rahmen eines Regelwerks auf einer sowohl generischen, systemübergreifenden als auch einer technischen systemspezifischen Ebene identifiziert. Die Regeln werden präventiv als Bestandteil der obigen Prozesse oder nachgelagert im Rahmen von Rezertifizierungen analysiert, und Verstöße werden analysiert und bereinigt.
- Parametrisierungen und Protokollierungen mit Autorisierungsrelevanz sind identifiziert und in den betroffenen IT-Anwendungen eingerichtet. Einstellungen sowie relevante protokollierte Vorgänge werden regelmäßig kontrolliert und notwendige Maßnahmen abgeleitet, deren Umsetzung überwacht wird.

4.4 Prüfprogramm: Dokumentation und Standards

Tabelle 5 Prüfprogramm: Dokumentation und Standards

Nr.	PRÜFPROGRAMM: DOKUMENTATION UND STANDARDS
1.	Kontrollziel und Risiko
1.1	**Kontrollziel:** Die für Benutzer und Berechtigungen vorliegenden Dokumentationen und Standards ermöglichen es den am Prozess Beteiligten, die korrespondierenden Strukturen und Prozesse, die Organisation und die hierbei zu beachtenden Vorgaben in angemessener Zeit nachzuvollziehen. **Risiko:** Durch fehlende, unvollständige oder unverständliche Dokumentation können die Beteiligten die Benutzer und Berechtigungen und ihre eigenen Aufgaben im Prozess nicht verstehen. Daraus ergeben sich Risiken für eine unsachgemäße Pflege und Vergabe der Rollen.
2.	Dokumentationsstandards
2.1.	**Nachvollziehbarkeit:** *Ist einem sachkundigen Dritten ein angemessener Einstieg in die Dokumentation des Benutzers- und Berechtigungskonzepts möglich, indem in der Einleitung die Schilderung des Inhalts und Gegenstands des Dokuments dargelegt wird?* Um für einen sachkundigen Dritten nachvollziehbar zu sein, muss eine Benutzer- und Berechtigungsdokumentation klar gegliedert sein und die Einleitung einen intuitiven Einstieg in das Dokument ermöglichen. Prüfung der Einleitung darauf hin, ob speziell die Einführung, aber auch damit verbunden die generelle Struktur und Inhalt der Dokumentation nachvollziehbar sind.
2.2.	**Identifikation Adressaten:** *Sind die Adressat:innen des Dokuments und insbesondere die aus Compliance-Gesichtspunkten relevanten Beteiligten ausreichend erläutert?* Hierbei sollten die genannten und erläuterten Personenkreise mit den aus Compliance-Gründen üblicherweise mit dem Benutzer- und Berechtigungskonzept befassten Personen korrespondieren. Prüfung des Dokuments auf eine angemessene Erläuterung der Adressat:innen und der mit dem Benutzer- und Berechtigungskonzept direkt oder indirekt befassten Personen.

Nr.	PRÜFPROGRAMM: DOKUMENTATION UND STANDARDS
2.3.	**Gültigkeit:** *Ist die thematische und zeitliche Gültigkeit des Dokuments definiert?* Der Benutzer- und Berechtigungsdokumentation sollte im Detail der Geltungsbereich der Dokumentation insbesondere in Bezug auf die betroffenen Systeme/ Instanzen/Mandant:innen sowie Funktionen/Module/ Prozesse sowie die betroffenen organisatorischen Einheiten identifiziert werden. Prüfung des Dokuments nach einer nachvollziehbaren und abgrenzungsscharfen Identifizierung des Geltungsbereichs der Dokumentation.
2.4.	**Externe und interne Anforderungen:** *Sind im Dokument externe und interne Anforderungen ausreichend identifiziert und berücksichtigt?* In Abhängigkeit von der geografischen und branchenspezifischen Ausrichtung eines Unternehmens sind in unterschiedlichem Maße regulatorische Anforderungen oder sonstige Standards von Belang. Diese müssen in einer Benutzer- und Berechtigungsdokumentation identifiziert und bei der Gestaltung der Dokumentationen und Konzepte berücksichtigt werden. Prüfung des Dokuments auf eine Identifikation und Berücksichtigung der im Rahmen des Benutzer- und Berechtigungskonzepts zu beachtenden externen Anforderungen (Compliance-Vorgaben) und internen Regelungen.
2.5.	**Dokumenteneigner und -pfleger:** *Ist im Dokument festgelegt, wer für die Pflege des Dokuments verantwortlich ist und wer insgesamt für Inhalt, Vollständigkeit und Richtigkeit des Dokuments verantwortlich ist?* Damit Benutzer- und Berechtigungsdokumente sowohl initial als insbesondere auch dauerhaft in Umfang und Inhalt den allgemein geltenden Anforderungen sowie den konkreten Umständen entsprechen, muss eine nachvollziehbare Dokumenteneignerschaft (Owner/Ownership) geregelt sein. Prüfung des Dokuments auf die Benennung von Dokumentenverantwortlichen und ob diese tatsächlich mit den aktuellen Verantwortlichen übereinstimmen sowie die Erläuterung und Einhaltung des Abnahmeverfahrens des Dokuments.

Nr.	PRÜFPROGRAMM: DOKUMENTATION UND STANDARDS
2.6.	**Publikation und Abnahme:** *Ist das Verfahren zur Änderung, Abnahme und Publikation/Inkraftsetzung beschrieben und eingehalten?* Zu den Benutzer- und Berechtigungsdokumenten ist nicht nur deren Existenz, Vollständigkeit und Richtigkeit von Belang, sondern dass diese auch tatsächlich in Kraft gesetzt und kommuniziert sind, damit sie Wirkung für ein Unternehmen entfalten können. Ist dies nicht der Fall, kann davon ausgegangen werden, dass die in der Dokumentation enthaltenen Anforderungen nicht in der Realität des Unternehmens angekommen sind. Prüfung der Dokumentation des Dokumentenänderungsverfahrens, der angemessenen Dokumentation von Änderungen und ihren Abnahmen sowie der Publikation der letzten abgenommenen Version des Dokuments.
3.	Rollen und Berechtigungen
3.1.	**Rollengestaltung und -konventionen:** *Sind angemessene Vorgaben zur Prozess- und Organisationseinordnung, zu Namenskonventionen und zur Rollengestaltung dokumentiert?* In einer Benutzer- und Berechtigungsdokumentation sind Vorgaben für die Rollengestaltung und für Namenskonventionen sowie eine Zuordnung von Rollen in die Prozess- und Organisationsstruktur des Unternehmens aufzunehmen. Prüfung auf angemessene Dokumentation von Vorgaben zur Prozess- und Organisationseinordnung, zu Namenskonventionen und zur Rollengestaltung.
3.2.	**Ausnahmeregelungen:** *Sind Vorgaben speziell für Kund:innen-eigene Berechtigungen dokumentiert?* Soweit in Anwendungen Kund:innen-eigene Berechtigungsstrukturen relevant sind, müssen geeignete Vorgaben hierfür in die Benutzer- und Berechtigungsdokumentation aufgenommen werden.

Nr.	PRÜFPROGRAMM: DOKUMENTATION UND STANDARDS
	Prüfung auf angemessene Dokumentation von Vorgaben für Kund:innen-eigene Berechtigungen.
3.3.	**Verantwortlichkeiten:** *Sind transparente Verfahren zur eindeutigen Identifikation eines Rollenverantwortlichen für jede Rolle dokumentiert?* Die Benutzer- und Berechtigungsdokumentation einer Anwendung muss ein Verfahren und Verweise auf Zuordnungen enthalten, mit denen für jede Rolle ein Rollenverantwortlicher identifiziert werden kann – dies mindestens für Rollen, die aktiv einem Benutzer zugeordnet sind. Prüfung auf angemessene Dokumentation von Verfahren zur eindeutigen Identifikation eines Rollenverantwortlichen und eines Vertreters für jede Rolle.
3.4.	**Standardrollen:** *Sind die in den betrachteten Systemen vorkommenden Standardrollen und die Verfahren zum Schutz vor deren Missbrauch dokumentiert?* Soweit für eine Anwendung Standardrollen mit der Anwendung ausgeliefert werden, sind hierfür in der Benutzer- und Berechtigungsdokumentation angemessene Erläuterungen der Rollen, ihres Verwendungszwecks und der Verfahren für ihren Schutz und Einsatz aufzunehmen. Prüfung auf angemessene Dokumentation von Standardrollen und Verfahren zum Schutz vor deren Missbrauch.
4.	Benutzer und Rechte
4.1.	**Klassifizierung, Konventionen und Einordnung der Benutzer:** *Sind angemessene Vorgaben zur Prozess- und Organisationseinordnung, zur Benutzerklassifizierung und zu Konventionen der Attribuierung dokumentiert?* In einer Benutzer- und Berechtigungsdokumentation sind Vorgaben für eine transparente Klassifizierung von Benutzern, Konventionen für die Attribuierung und eine Einordnung in die Prozess- und Organisationsstruktur

Nr.	PRÜFPROGRAMM: DOKUMENTATION UND STANDARDS
	des Unternehmens aufzunehmen. Prüfung auf angemessene Dokumentation von Vorgaben zur Prozess- und Organisationseinordnung, zu Namenskonventionen und zur Rollengestaltung.
4.2.	**Verantwortlichkeiten:** *Sind transparente Verfahren zur eindeutigen Identifikation eines Benutzerverantwortlichen für jeden Benutzer dokumentiert?* Die Benutzer- und Berechtigungs-Dokumentation einer Anwendung muss ein Verfahren und Verweise auf Zuordnungen enthalten, mit denen für jeden Benutzer ein Benutzer-Verantwortlicher identifiziert werden kann – dies mindestens für aktive Benutzer-Konten. Dabei können/müssen die Identifikationsverfahren den unterschiedlichen Benutzer-Klassifizierungen angepasst werden (z. B. Manager:in des HR-Systems für interne Mitarbeitende). Prüfung auf angemessene Dokumentation von Verfahren zur eindeutigen Identifikation eines Benutzer-Verantwortlichen für jeden Benutzer.
4.3.	**Standard- und Notfallbenutzer:** *Sind die in den betrachteten Systemen relevanten Standardbenutzer und die Verfahren für deren Nutzung/Schutz dokumentiert?* Soweit für eine Anwendung Standardbenutzer mit der Anwendung ausgeliefert werden, ist hierfür in der Benutzer- und Berechtigungsdokumentation eine angemessene Erläuterung der Benutzer, ihres Verwendungszwecks und der Verfahren für ihren Schutz und Einsatz aufzunehmen. Prüfung auf angemessene Dokumentation von Standardbenutzern und der Verfahren zum Einsatz und Schutz vor Missbrauch.
5.	Sensitive Funktionen und Funktionstrennung
5.1.	**Sensitive Funktionen:** *Sind Verfahren zur Identifikation und Analyse von sensitiven Funktionsregeln definiert und liegen konkrete sensitive Funktionsregeln vor?* Sensitive Funktionen beziehen sich auf Berechtigungen, die aus

Nr.	PRÜFPROGRAMM: DOKUMENTATION UND STANDARDS
	unterschiedlichen Perspektiven (z. B. finanziell, strategisch, datenschutzrechtlich) ein erhöhtes Risiko für ein Unternehmen darstellen und insofern einer erhöhten Aufmerksamkeit und Kontrolle unterliegen sollten. Prüfung auf dokumentierte Verfahren zur Festlegung und Prüfung von sensitiven Funktionen und auf das Vorhandensein angemessener und vollständiger sensitiver Funktionsregeln.
5.2.	**Funktionstrennung:** *Sind Verfahren zur Identifikation und Analyse von Funktionstrennungsregeln definiert und liegen konkrete Funktionstrennungsregeln vor?* Funktionstrennungsregeln beziehen sich auf Berechtigungen, bei denen sich aus der Kombination zweier sensitiver Funktionen ein gegenüber den Risiken der Einzelfunktionen erhöhtes Risiko für ein Unternehmen ergibt. Prüfung auf dokumentierte Verfahren zur Festlegung und Analyse von Funktionstrennungen und auf das Vorhandensein angemessener und vollständiger Funktionstrennungsregeln.
6.	Prozesse und Organisation
6.1.	**Prozesse:** *Sind alle im Kontext der Benutzer und Berechtigungen relevanten Prozesse angemessen festgelegt und dokumentiert?* Hierbei handelt es sich insbesondere um den User-Lifecycle, die Rollenpflege, die Rollenvergabe, die Funktionstrennungsanalyse, die Rezertifizierung und das Privileged-Identity-Management. Prüfung auf nachvollziehbare Dokumentation aller erforderlichen Prozesse mit den hierfür anzuwendenden Minimalanforderungen.
6.2.	**Organisation:** *Sind alle an den Verfahren für Benutzer und Berechtigungen beteiligten Personen (organisatorischen Rollen) mit ihren konkreten Verantwortlichkeiten hinreichend dokumentiert?* Hierbei handelt es sich insbesondere um organisatorische Rollen wie

Nr.	PRÜFPROGRAMM: DOKUMENTATION UND STANDARDS
	Rolleneigner:innen und -koordinator:innen, Rollenentwickler:innen, Benutzer-Koordinator:innen, Regel- und Kontroll-Eigner:innen und -Koordinator:innen. Prüfung auf nachvollziehbare Dokumentation aller beteiligten organisatorischen Rollen mit den für diese geltenden Verantwortlichkeiten.
7.	Protokollierung und Parameter
7.1.	**Protokollierung:** *Sind die Verfahren und der Umfang der Protokollierung (Umfang Benutzer und Umfang der aufgezeichneten Vorgänge) nachvollziehbar dokumentiert?* In Abhängigkeit der Anwendung stehen unterschiedliche Verfahren zur Protokollierung zur Verfügung: Die zwei Dimensionen Benutzer bzw. Benutzer-Klassen und Umfang der aufgezeichneten Vorgänge. Prüfung auf Angemessenheit der Dokumentation der Protokollierungskonfiguration und des Protokollierungsumfangs.
7.2.	**Parametrisierung:** *Sind die in den Anwendungen verfügbaren Parameter mit Relevanz für Benutzer und Berechtigungen und deren angestrebte Konfiguration nachvollziehbar beschrieben?* In Abhängigkeit von der Anwendung stehen in der Regel Möglichkeiten der Beeinflussung/Konfiguration der Authentifizierungs- und Autorisierungsverfahren zur Verfügung. Diese werden meist über Parametereinstellungen beeinflusst. Prüfung der nachvollziehbaren Dokumentation der Konfigurationsmöglichkeiten für Benutzer und Berechtigungen und der konkreten angemessenen Anwendung für das Unternehmen.

4.5 Prüfprogramm: Rollen und Berechtigungen

Tabelle 6 Prüfprogramm: Rollen und Berechtigungen

Nr.	PRÜFPROGRAMM: ROLLEN UND BERECHTIGUNGEN
	Kontrollziel: Die Vorgaben für Rollen und technische Berechtigungen und deren Umsetzung sorgen für eine vollständige Nachvollziehbarkeit von den technischen Berechtigungen auf der untersten Ebene bis hin zu den Rollen als Zwischenebene. **Risiko:** Bei fehlender Nachvollziehbarkeit auf einer oder mehreren Ebenen eines Benutzer- und Berechtigungskonzepts ergeben sich automatisch Mängel im Minimal- und Funktionstrennungsprinzip und damit eine Gefährdung der Integrität, Verfügbarkeit und Vertraulichkeit von Daten.
1.	Prozess- und Organisationseinordnung
1.1.	**Prozessdimension:** *Ist für alle Prozessbereiche des Unternehmens, die durch die betrachtete Anwendung und damit durch das Rollenkonzept unterstützt werden, eine vollständige und angemessen strukturierte Übersicht der Prozessbereiche (Prozessmodell/-hierarchie) vorhanden?* Eine der Organisation eines Unternehmens angemessene Gliederung der Prozesse/Prozessbereiche ist eine Voraussetzung für die Standardisierung von Prozess- und damit verbundenen Rollenstrukturen. Prüfung Angemessenheit, Vollständigkeit und Aktualität der Dokumentation der für das Unternehmen und die Anwendung relevanten Prozessbereiche.
1.2.	**Organisationsdimensionen:** *Ist je Prozessbereich dargestellt, welche Organisationsdimensionen jeweils relevant sind (rechtliche Einheit, Werk, Kostenrechnungskreis etc.)?* Eine angemessene Klärung der je Prozessbereich möglichen, sinnvollen und notwendigen Kriterien für eine organisatorische Differenzierung legt die Grundlage für eine angemessene Umsetzung in den Rollenkonzepten der jeweiligen Anwendungen. Prüfung des Dokuments auf Auflistung der für das Unternehmen relevanten Organisationsdimensionen pro Prozessbereich.

Nr.	PRÜFPROGRAMM: ROLLEN UND BERECHTIGUNGEN
1.3.	**Organisationswerte:** *Sind für jede Organisationsdimension die vorhandenen Ausprägungen aufgeführt und erläutert?* Eine angemessene Klärung der je Prozessbereich für die oben definierten organisatorischen Kriterien relevanten Ausprägungen ist erforderlich für eine Identifikation lokaler Verantwortlicher für die Zuordnung der lokal relevanten Rollen. Prüfung der Vollständigkeit und der Richtigkeit der in den Dokumentationen vorhandenen Aufstellungen zur Ausprägung der Organisationsdimensionen. Hinweis: Dies kann auch mit Verweis auf andere Dokumentationen oder direkt auf das System erfolgen. Insbesondere sollte der für die Organisationsdimensionen strukturgebende Grundgedanke erkennbar werden.
2.	Namenskonventionen
2.1.	**Konvention Name:** *Ist eine eindeutige Festlegung von Namenskonventionen für Berechtigungen dokumentiert?* Konventionen für die technischen Namen/IDs von Rollen sind das zentrale Hilfsmittel für die regelmäßig mit der Rollenpflege und -vergabe befassten Personen zur Einordnung und Filterung der Rollen. Prüfung des Vorhandenseins, der Vollständigkeit und der Nachvollziehbarkeit der Dokumentation der Namenskonvention. Hinweis: Zu konkreten Anforderungen an die Namenskonvention siehe die Vorgaben im Kapitel Benutzer und Berechtigung – Transparenz.
2.2.	**Konvention Text und Beschreibung:** *Ist neben der Konvention für die technischen Namen ebenfalls eine Minimalkonvention für den Langtext und die Beschreibung von Rollen dokumentiert, soweit diese Rollenelemente in einer Anwendung verfügbar sind?* Im Vergleich zum technischen Namen von Rollen richten sich die Texte und Beschreibungen vornehmlich an die weniger oft mit Rollen befassten fachlichen Prozessbeteiligten. Insofern kommt insbesondere den Texten, die auch häufig in IT-Lösungen für Rollenbeantragungen das zentrale Anzeige-Element sind, eine hohe Bedeutung bei der Auswahl und Genehmigung der richtigen Rollen zu. Prüfung, ob ebenfalls eine angemessene Namenskonvention für den Text und für die Beschreibung von Rollen vorhanden ist.

Nr.	PRÜFPROGRAMM: ROLLEN UND BERECHTIGUNGEN
3.	Rollengestaltung
3.1.	**Rollenklarheit:** *Sind für die mit den Rollen befassten Personen aus der Gesamtheit der Rollendeklaration alle wesentlichen Elemente zum Verständnis einer Rolle ableitbar?* Zu den wesentlichen Elementen gehören die Prozessdimension (der Prozessbereich, zu dem die Rolle gehört, der Rollentyp [Einzelrolle oder Sammelrolle]), die Organisationsdimension (die organisatorische Dimension, nach der die Rolle differenziert wird [Buchungskreis, Werk usw.]) sowie die Funktion (üblicherweise eine Kombination aus betriebswirtschaftlichem Objekt und Aktivität [z. B. Kreditorenstammdaten anzeigen, Materialbelege buchen usw.]). Prüfung der Namenskonventionen für Rollen auf Mindestbestandteile. Prüfung in Stichproben auf Anwendung der Namenskonvention.
3.2.	**Rollentransparenz:** *Sind die im System ausgeprägten Rollen für einen sachkundigen Dritten innerhalb angemessener Zeit nachvollziehbar?* Je weniger der Zusammenhang einer Sammelrolle mit einer Einzelrolle und der Einzelrolle mit den enthaltenen Berechtigungen erkennbar ist, desto weniger nachvollziehbar ist das Rollenkonzept. Die Berechtigungen sind so in Rollen zu gruppieren, dass bei prozessualen Reorganisationsmaßnahmen keine erhöhten Anpassungen am Rollenkonzept notwendig sind. Dies setzt voraus, dass auf Ebene von Applikationsrollen (SAP-Einzelrollen) möglichst Aufgaben („Kreditorenstammdaten ändern“) abgebildet werden. Verfügt ein Unternehmen über eine angemessene Standardisierung von Arbeitsplätzen und Aufgaben, sollten Arbeitsplätze auf der Ebene von Businessrollen oder SAP-Sammelrollen abgebildet werden. Prüfung einer klaren Vorgabe zum Rollenschnitt von Applikationsrollen (SAP-Einzelrollen) nach Prozessschritten/Aufgaben/Funktionen und von Businessrollen (SAP-Sammelrollen) nach Arbeitsplätzen. Prüfung in Stichproben auf Anwendung der Vorgabe.

Nr.	PRÜFPROGRAMM: ROLLEN UND BERECHTIGUNGEN
3.3.	**Rollenkongruenz:** *Entsprechen die technischen Berechtigungen der Rollen den im Rollennamen, im Rollentext und in der Rollenbeschreibung beschriebenen/kodierten Inhalten?* Die Deklaration einer Rolle muss mit den Rolleninhalten übereinstimmen. Dies bezieht sich sowohl auf die in den Rollen enthaltenen ausführbaren Programme (Transaktionen, WebDynpros, Fiori Apps) als auch auf die weitergehenden Berechtigungen einschließlich der organisatorischen Abgrenzungen. Prüfung in Stichproben für Rollen auf Übereinstimmung, insbesondere der Berechtigungselemente ausführbare Programme, Aktivitäten und organisatorische Abgrenzung.
3.4.	**Regelkonformität:** *Werden bei der Gestaltung (Mandant:innen-spezifische) Regelwerke für Funktionstrennungskonflikte und sensitive Funktionen beachtet? Sind Einzelrollen frei von inhärenten Regelverstößen?* Grundsätzlich sollten Rollen frei sein von inhärenten Funktionstrennungskonflikten und weder kritische, unzulässige Funktionen noch sensitive Funktionen enthalten, die nicht explizit aus der Rollendeklaration erkennbar sind. Prüfung in Stichproben für Rollen, dass entsprechende Regeln eingehalten sind.
4.	Verantwortlichkeiten
4.1.	**Rolleneigner:in:** *Ist jede Rolle in einem System oder einer Dokumentation eindeutig einem/einer Datenverantwortlichen zugeordnet?* Der Rolleneigner / Die Rolleneignerin ist für Einrichtung und Änderung der Rollen sowie für die Genehmigung der Vergabe der Rollen verantwortlich. Insofern sollte eine Zuordnung von Rollen zu Rolleneigner:innen, im Idealfall über eine Zuordnung der Rollen zu einem Prozessbereich / einer Organisationseinheit und einer Zuordnung der Prozessbereiche/Organisationseinheiten zu Rolleneigner:innen erfolgen. Prüfung in Stichproben, ob ein Verfahren zur eindeutigen Zuordnung jeder Rolle zu einem Rolleneigner / einer Rolleneignerin entweder über eine Zuordnung über Attribute der Rolle oder über eine direkte Mapping-Tabelle beschrieben und gegeben ist.

Nr.	PRÜFPROGRAMM: ROLLEN UND BERECHTIGUNGEN
4.2.	**Rollenkoordinator:in:** *Ist jede Rolle (wenn möglich über die Zuordnung zu einem Prozessbereich und einer Organisationseinheit) in einem System oder einer Dokumentation eindeutig einem Key-Benutzer zugeordnet?* Der/Die Rollenkoordinator:in unterstützt fachlich den IT-Bereich und die/den Datenverantwortliche:n in Fragen der Pflege und Vergabe von Rollen. Prüfung in Stichproben, ob ein Verfahren zur eindeutigen Zuordnung jeder Rolle zu einem Rollenkoordinator / einer Rollenkoordinatorin entweder über eine Zuordnung über Attribute der Rolle (insbesondere Name und Text) oder über eine direkte Mapping-Tabelle beschrieben und gegeben ist.
5.	Kund:innen-eigene Strukturen
5.1.	**Eigenentwickelte Berechtigungsobjekte:** *Werden eigenentwickelte Berechtigungsobjekte verwendet, wird die hierfür geltende Namenskonvention eingehalten und sind diese angemessen dokumentiert und integriert?* Dabei sollte die Dokumentation die durch die Berechtigungsobjekte geschützten betriebswirtschaftlichen oder technischen Objekte sowie die Kriterien, über die der Zugriff gesteuert wird, beschreiben. Prüfung der Kund:innen-eigenen Berechtigungsobjekte auf angemessene Dokumentation entweder (soweit möglich) im System, in der Berechtigungsdokumentation oder außerhalb.
6.	Standardrollen
6.1.	**Standardrollen:** *Wird die Zuordnung von Standardrollen entweder gänzlich vermieden oder mit klarer Eingrenzung auf Sonderbenutzer eingesetzt?* Standardrollen werden mit einer SAP-Anwendung oder über Lösungen auf der SAP-Plattform durch Drittanbieter ausgeliefert und zeichnen sich in der Regel durch weitreichende, für den Regelbetrieb unzulässige Berechtigungen aus. Insofern ist der Einsatz solcher Rollen zu vermeiden oder nur auf ausgewählte Sonderbenutzer zu begrenzen. Prüfung der Vorgaben zur Vermeidung der Vergabe von Standardrollen und zur Eingrenzung der Vergabe an Sonderbenutzer. Prüfung in Stichproben für Standardrollen der Zuordnungen zu Benutzern im Jahresverlauf und Nachverfolgung der korrespondierenden Dokumentation.

4.6 Prüfprogramm: Benutzer und Rechte

Tabelle 7 Prüfprogramm: Benutzer und Rechte

Nr.	PRÜFPROGRAMM: BENUTZER UND RECHTE
	Kontrollziel: Die Vorgaben für Benutzer und die Zuordnung von Rollen und Berechtigungen und deren Umsetzung sorgen für eine vollständige Nachvollziehbarkeit der Rollen und ggf. Berechtigungen und deren Zuordnung zu Benutzern und Identitäten. **Risiko:** Bei fehlender Nachvollziehbarkeit auf einer oder mehreren Ebenen eines Benutzer- und Berechtigungskonzepts ergeben sich automatisch Mängel im Minimal- und Funktionstrennungsprinzip und damit eine Gefährdung der Integrität, Verfügbarkeit und Vertraulichkeit von Daten.
1.	Prozess- und Organisationseinordnung
1.1.	**Organisationsstruktur:** *Ist eine angemessene Organisationsstruktur vorhanden, die eine Identifikation der Manager:innen/Vorgesetzten eines internen Mitarbeitenden und seiner Benutzer ermöglicht?* Im Idealfall ist es für jeden Mitarbeitenden möglich, eine Zuordnung über eine Planstelle auf die Organisationshierarchie und über die Hierarchieknoten zu einem Vorgesetzten herzustellen. Prüfung der Unterlagen oder Exporte aus dem HR- und/oder IAM-Kontext auf die Möglichkeit einer eindeutigen Zuordnung von Benutzern über die Organisationsstruktur zu Vorgesetzten.
1.2.	**Korrelation Organisation und Prozesse:** *Ist es möglich, sinnvolle Zusammenhänge zwischen den Organisationsbereichen der Benutzer und den Prozessbereichen der Rollen herzustellen?* Hierdurch kann die Angemessenheit von Rollen für Benutzer im Kontext von Rezertifizierungen oder Prüfungen beurteilt werden. Dies kann sowohl über die Benutzer-ID als auch über weitere Attribute des Benutzers wie Abteilung, Kostenstelle, Planstelle oder Organisationshierarchie erfolgen. Prüfung, ob eine Zuordnung von Prozessbereichen und Organisationsbereichen möglich ist und vorgenommen wird.

Nr.	PRÜFPROGRAMM: BENUTZER UND RECHTE
2.	Benutzer-Klassifizierung
2.1.	**Benutzer-Klassifizierung:** *Liegt eine Einteilung/Klassifizierung von Benutzern vor, die angemessen zur Ableitung und Prüfung von Eigenschaften wie Funktionstrennung genutzt werden kann?* Dabei sollte für eine angemessene Differenzierung zumindest eine Unterteilung in Interne, Externe, Technische Benutzer erfolgen. Ergänzend sind weitere Benutzer-Klassen wie Praktikant:innen, RPA-Benutzer, Privilegierte Benutzer zu empfehlen. Dabei dient die Klassifizierung der Einordnung und Prüfung korrespondierender Benutzer-Eigenschaften, zulässiger Zugriffsrechte und zu beachtender Funktionstrennungen zwischen Benutzer-Klassen. Prüfung einer angemessenen Benutzer-Klassifizierung und zumindest in Stichproben deren Anwendung auf Benutzer.
3.	Namenskonventionen
3.1.	**Eindeutigkeit:** *Existieren geeignete Verfahren, je Benutzer pro Anwendung/Instanz nur eine eindeutige ID zu vergeben und, soweit möglich, eine anwendungsübergreifend einheitliche ID?* Eine Person sollte, soweit möglich, dieselbe Benutzer-ID in allen Systemen haben und nur einen Benutzerstamm je System. Dies lässt sich am besten über ein zentrales Identity-Management-System und über ein Verfahren absichern, bei dem die Anlage verpflichtend zentral erfolgt und die Benutzerkonten erst nachgelagert in den verteilten Anwendungen oder einem vergleichbaren organisatorischen Verfahren erstellt werden. Prüfung auf geeignete Verfahren und Konventionen für die Anlage von Anwendenden mit eindeutiger Benutzer-ID. Prüfung in Stichproben auf Einhaltung und Referenzierbarkeit zum zentralen Identity-Repository.

Nr.	PRÜFPROGRAMM: BENUTZER UND RECHTE
3.2.	**Pflichtfelder:** *Sind angemessene Mindestinformationen für die Pflege des Benutzerstamms festgelegt? Wird systemseitig die Eingabe der Mindestinformationen erzwungen?* Zu den Mindestinformationen gehören u. a. bei allen Benutzern eine ID und Klassifizierung, für interne Mitarbeitende der Organisationsbereich, für interne und externe Benutzer der Vor- und Nachname, für Technische Benutzer eine Beschreibung der Funktion. Prüfung auf eine angemessene Vorgabe und auf angemessene Verfahren zur Erfassung von Mindestbenutzerinformationen. Prüfung in Stichproben für Benutzer unterschiedlicher Benutzerklassen auf Einhaltung der Standards.
4.	Verantwortlichkeiten
4.1.	**Für Benutzer Verantwortliche:** *Ist für jeden Benutzer (intern, extern, nicht personalisiert) die Identifizierung eines Benutzer-Verantwortlichen möglich?* Ein Benutzer-Verantwortlicher ist für interne Mitarbeitende der i. d. R. über das HR-System ermittelte disziplinarische oder fachliche Vorgesetzte. Für externe und nicht personalisierte Benutzer ist davon abweichend ein Benutzer-Verantwortliche:r festzulegen, wenn möglich ebenfalls über die Organisationshierarchie oder andere Zwischengruppierungen. Diese/Dieser ist vollumfänglich für den Benutzer, ihre/seine Daten, ihre/seine Berechtigungen und die Verwendung der Benutzer verantwortlich. Prüfung auf eine angemessene Vorgabe und auf angemessene Verfahren zur vollständigen Identifizierung einer/eines Benutzer-Verantwortlichen für jeden Benutzer. Prüfung in Stichproben für Benutzer unterschiedlicher Benutzer-Klassen auf die konkrete Identifizierung der/des Benutzer-Verantwortlichen.
5.	Standard- und Notfallbenutzer

Nr.	PRÜFPROGRAMM: BENUTZER UND RECHTE
5.1.	**Standardbenutzer:** *Wird die Verwendung von Standardbenutzern entweder gänzlich vermieden oder auf klar abgegrenzte Nutzungszwecke beschränkt und angemessen abgesichert?* Standardbenutzer werden mit einer SAP-Anwendung oder für Dritt-Lösungen auf der SAP-Plattform ausgeliefert und zeichnen sich in der Regel durch weitreichende, für den Regelbetrieb unzulässige Berechtigungen aus. Insofern ist der Einsatz solcher Benutzer zu vermeiden oder im Rahmen differenzierter Einsatzzwecke und kontrollierter Verfahren zu beschränken. Prüfung der Vorgaben zur Vermeidung der Nutzung von Standardbenutzern und der kontrollierten Nutzung von Sonderbenutzern. Prüfung in Stichproben für Standardbenutzer, der Freigabe und Nutzung von Benutzern im Jahresverlauf und Nachverfolgung der korrespondierenden Dokumentation.
5.2	**Privilegierte Benutzer:** *Sind geeignete Regelungen für die eindeutige Identifizierung von Notfallbenutzern getroffen?* Privilegierte Benutzer (auch Notfallbenutzer) verfügen über die den Anwendenden im Tagesbetrieb zugänglichen Berechtigungen hinausgehende Zugriffsrechte. Insofern müssen für Notfallverfahren verwendete Benutzer eindeutig als solche identifizierbar sein. Dies kann über den Anmeldenamen oder weitere Attribute in einer Applikation oder in Benutzermanagement-Lösungen erfolgen. Prüfung, ob nicht personalisierte Dialogbenutzer über den Anmeldenamen oder über Attribute eindeutig als Shared oder Privilegierte Benutzer erkennbar sind und nicht zweckentfremdet werden.

4.7 Prüfprogramm: Sensitive Funktionen

Tabelle 8 Prüfprogramm: Sensitive Funktionen

Nr.	PRÜFPROGRAMM: SENSITIVE FUNKTIONEN
	Kontrollziel: Für Anwendungen und die in den Anwendungen unterstützten Prozesse und Objekte liegt ein Regelwerk mit sensitiven Funktionen vor. Sensitive Funktionen werden ausschließlich über Rollen vergeben, deren Deklaration die beinhalteten sensitiven Funktionen eindeutig erkennbar machen. Für Rollen mit sensitiven Funktionen ist ausgewiesen, für welche Instanzen und an welche Benutzergruppen eine Vergabe zulässig ist.

Nr.	PRÜFPROGRAMM: SENSITIVE FUNKTIONEN
	Benutzer erhalten Berechtigungen für sensitive Funktionen unter strenger Beachtung des Minimalprinzips. **Risiko:** Die Nutzung von Rollen mit nicht nachvollziehbaren sensitiven Berechtigungen und die Vergabe sensitiver Berechtigungen an Benutzer unter Verstoß gegen Minimalprinzip und Funktionstrennungsregeln gefährden die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen.
1.1.	**Generelle Risikobewertung:** *Sind die Anwendungen und die von diesen unterstützten Prozesse nach den inhärenten Risiken in Bezug auf den Jahresabschluss, aber auch ggf. auf anderweitig relevante Risiken bewertet?* Zur Risikobewertung der Anwendungen und Prozesse kann auf bereits vorhandene Verfahren wie auf das Risikomanagement, auf die Informationssicherheit oder auf Interne Kontrollsysteme zurückgegriffen werden. Soweit Anwendungen und Prozesse Risiken aufweisen, sind eine Aufnahme sensitiver Funktionen und Funktionstrennungsregeln zur Minderung der Risiken und die Etablierung von Prozessen zur Überwachung sensitiver Funktionen und Funktionstrennungen für die betrachteten Systeme und Prozesse durchzuführen. Prüfung, ob eine Aufnahme von Risiken für die betrachteten Anwendungen und Prozesse vorliegt und sich hieraus eine Notwendigkeit für die Aufnahme und Kontrolle sensitiver Funktionen und Funktionstrennungen ergibt.
1.2.	**Sensitive generische Funktionen:** *Sind für als risikorelevant identifizierte Prozessbereiche Funktionen, die einen erkennbaren Einfluss auf die Daten- und/oder Systemintegrität haben, im Rahmen eines Regelwerks für sensitive Funktionen erfasst?* Dabei sollte sich der beurteilte Einfluss primär auf Daten des Jahresabschlusses, aber auch auf weitere Risikobereiche wie Datenschutz, operative und strategische Risiken oder andere regulatorische Anforderungen beziehen. Die Regeln sind mit einer insbesondere für Fachbereiche nachvollziehbaren Risikobeschreibung zu versehen.

Nr.	PRÜFPROGRAMM: SENSITIVE FUNKTIONEN
	Prüfung der für risikorelevante Prozessbereiche definierten Regeln für sensitive Funktionen auf Vollständigkeit, Richtigkeit und Nachvollziehbarkeit.
1.3.	**Technische Regelausprägung:** *Sind für die sensitiven Funktionsregeln die zugehörigen technischen Berechtigungen identifiziert, die zur Ausführung der Funktion erforderlich sind?* Bei der technischen Ausprägung handelt es sich vornehmlich um die beiden Dimensionen ausführbare Programme und weitere technische Berechtigungen. Die technische Ausdifferenzierung ist die Grundlage für eine nachfolgende Auswertung auf Benutzer- und Rollenebene. Prüfung, ob je sensitiver Funktion die dazu korrespondierenden technischen Berechtigungen identifiziert sind.
1.4.	**Risikoeinstufung:** *Existiert eine nachvollziehbare Skala zur Risikoeinstufung der sensitiven Funktionen und sind die Funktionen zutreffend gemäß der Skala eingeordnet?* Um eine gezielte Einordnung sensitiver Funktionen und der jeweils korrespondierenden Maßnahmen und Kontrollen zu unterstützen, ist eine Einordnung der sensitiven Funktion in eine standardisierte Skala vorzunehmen. Dabei ist neben der eigentlichen Skala (oftmals kritisch, hoch, mittel, gering) eine Übersetzung der Bedeutung der Einstufung und der hieraus resultierenden Wirkungen notwendig. Prüfung auf das Vorhandensein einer angemessenen Skala mit Erläuterung und Wirkungsbeschreibung sowie der Anwendung auf alle vorhandenen sensitiven Funktionen des Regelwerks.
1.5.	**Fokus Entwicklung und Customizing:** *Sind im Regelwerk sensitiver Funktionen alle wesentlichen IT-Funktionen der Entwicklung und des Customizing repräsentiert?* Funktionen des Repository-Bereichs sind deswegen besonders relevant, weil sie nur im Entwicklungssystem zugänglich sein sollten und daher auch nur in für die Entwicklung zulässigen Rollen enthalten und nur Benutzern in Entwicklungssystemen zugeordnet sein sollten. In der Produktion ist die Berechtigung von Repository-Funktionen unzulässig; diese Funktionen sind

Nr.	PRÜFPROGRAMM: SENSITIVE FUNKTIONEN
	deswegen grundsätzlich als kritisch einzuordnen. Prüfung der Vollständigkeit des Regelwerks auf Entwicklungs- und Customizing-Funktionen. Prüfung von Benutzern und Rollen auf ausgewählte Repository-Funktionen.
1.6.	**Fokus Administration:** *Sind im Regelwerk sensitiver Funktionen alle sensiblen Administrations-Funktionen repräsentiert?* Funktionen der Administration sind deswegen relevant, weil sie häufig zum Zugriff auf Funktionen mit anwendungsübergreifender Wirkung berechtigen. Die Vergabe ist in der Regel nur an autorisierte und berechtigte Personen des IT-Bereichs zulässig. Die Funktionen sind deswegen in der Regel als solche mit hohem oder mittlerem Risikogehalt einzuordnen. Prüfung der Vollständigkeit des Regelwerks auf Administrations-Funktionen. Prüfung von Benutzern und Rollen auf ausgewählte Administrations-Funktionen.
1.7.	**Fokus Stammdaten und Bewegungsdaten:** *Sind im Regelwerk sensitiver Funktionen sensible Stamm- und Bewegungsdaten-Pflege-Funktionen repräsentiert?* Funktionen der Stamm- und Bewegungsdatenpflege sind dann relevant, wenn sie direkte oder indirekte Wirkung auf Daten mit Relevanz für regulatorische, operative oder strategische Anforderungen haben. Die Vergabe ist in der Regel nur an autorisierte und berechtigte Personen des Fachbereichs zulässig. Die Funktionen sind deswegen in der Regel als solche mit mittlerem bis hohem Risikogehalt einzuordnen. Prüfung der Vollständigkeit des Regelwerks auf sensible Stamm- und Bewegungsdaten-Funktionen. Prüfung von Benutzern und Rollen auf ausgewählte Fachbereichs-Funktionen.
1.8.	**Fokus Datenschutz:** *Sind im Regelwerk sensitive Funktionen der Anzeige personenrelevanter Daten berücksichtigt?* Bereits mit dem Bundesdatenschutzgesetz, aber vermehrt mit der DSGVO, sind auch Anzeigefunktionen für personenrelevante Daten von erhöhter regulatorischer Relevanz. Dabei ist zu beachten, dass nicht alle personenrelevanten Daten gleich sensibel sind. So ist generell zwischen allgemeinen und besonders geschützten Daten zu unterscheiden. Prüfung der Vollständigkeit des Regelwerks auf sensible Anzeige-

Nr.	PRÜFPROGRAMM: SENSITIVE FUNKTIONEN
	Funktionen. Prüfung von Benutzern und Rollen auf ausgewählte Anzeige-Funktionen.
1.9.	**Prozesszuordnung:** *Ist in der Namenskonvention einer Regel oder einer Kontrolle der Prozessbereich kodiert, auf den sich die jeweilige Regel auswirkt? Ist ebenso durch die Namenskonvention vorgegeben, ob es sich bei einer Regel um eine Regel zur Überwachung einer sensitiven Funktion oder um eine Funktionstrennungsregel handelt?* Die Namens-Kodierung der Rollen und Kontrollen sollte eine eindeutige Zuordnung zum Prozessbereich unterstützen. Dabei sollten sich die Prozessbereiche aller drei Elemente Rollen, Regeln und Kontrollen an derselben Prozessstruktur orientieren. Prüfung, ob die Namenskonvention eine durchgängige Kodierung des einheitlich definierten Prozessbereichs sowie eine Abgrenzung der Regel-Typen berücksichtigt.
1.10.	**Regel-/Kontrolleigner:in:** *Kann jede Regel und Kontrolle über die Zuordnung zu einem Prozessbereich eindeutig einer/einem Regel-/Kontrollverantwortlichen / einer/einem Regel-Genehmigenden zugeordnet werden?* Der/Die identifizierte Regel-/Kontrollverantwortliche ist für die Einrichtung und Änderung der Regeln und Kontrollen sowie für die Interpretation der Regelauswertungen und die Ableitung von Maßnahmen verantwortlich. Prüfung, ob eine eindeutige Zuordnung jeder Regel und Kontrolle zu einer/einem eindeutigen Datenverantwortlichen möglich ist.

4.8 Prüfprogramm: Funktionstrennung

Tabelle 9 Prüfprogramm: Funktionstrennung

Nr.	PRÜFPROGRAMM: FUNKTIONSTRENNUNG
	Kontrollziel: Für Anwendungen und die in den Anwendungen unterstützten Prozesse und Objekte liegt ein Regelwerk mit Funktionstrennungen sowie mit korrespondierenden mitigierenden Kontrollen vor. Das Regelwerk bezieht sich auf einzelne sensitive Funktionen, die in Kombination ein höheres Risiko aufweisen, als es sich aus den jeweils einzelnen Risiken ergibt. Rollen und Berechtigungen werden unter Vermeidung von

Nr.	PRÜFPROGRAMM: FUNKTIONSTRENNUNG
	Funktionstrennungen erstellt. Funktionstrennungsverletzungen aus der Vergabe von Rollen und Berechtigungen an Benutzer werden vermieden oder durch Zuordnung mitigierender Kontrollen kompensiert. **Risiko:** Durch das Auftreten von Funktionstrennungsverletzungen in Benutzern ergeben sich Risiken für die Integrität und Verfügbarkeit von Daten.
1.1.	**Funktionstrennung:** *Sind für als risikorelevant identifizierte Prozessbereiche Funktionstrennungsregeln berücksichtigt?* Sensitive Funktionen, deren kombinierte Vergabe an Anwendende zu einem im Vergleich zu den isoliert vergebenen Funktionen erhöhten Risiko führen, sind als Funktionstrennungsregeln aufzunehmen und regelmäßig zu überwachen. Dabei sind in der Regel Funktionstrennungsregeln überwiegend für jahresabschlussrechtliche und operative Risiken von Relevanz. Prüfung, ob für die als risikorelevant eingestuften Prozessbereiche Regeln für Funktionstrennungen definiert sind und ob diese als vollständig einzuschätzen sind.
1.2.	**Risikoeinstufung:** *Existiert eine nachvollziehbare Skala zur Risikoeinstufung der Funktionstrennungsregeln und sind die Regeln zutreffend gemäß der Skala eingeordnet?* Um eine gezielte Einordnung von Funktionstrennungen und der jeweils korrespondierenden Maßnahmen und Kontrollen zu unterstützen, ist eine Einordnung der sensitiven Funktion in eine standardisierte Skala vorzunehmen. Dabei ist neben der eigentlichen Skala (oftmals kritisch, hoch, mittel, gering) eine Übersetzung der Bedeutung der Einstufung und der hieraus resultierenden Wirkungen notwendig. Die Skala ist in der Regel individuell abweichend für sensitive Funktionen und Funktionstrennungen.

Nr.	PRÜFPROGRAMM: FUNKTIONSTRENNUNG
	Prüfung auf das Vorhandensein einer angemessenen Skala mit Erläuterung und Wirkungsbeschreibung sowie der Anwendung auf alle vorhandenen Funktionstrennungsregeln des Regelwerks.
2.3.	**Kompensierende Kontrollen:** *Sind geeignete Kontrollen definiert, um das Risiko aus vorliegenden Funktionstrennungsverletzungen zu kompensieren?* Kompensierende Kontrollen sind dann von Bedeutung, wenn aufgrund geringer Kapazitäten, Urlaubsregelungen oder Ähnlichem eine Funktionstrennung oder restriktive Handhabung sensitiver Funktionen nicht möglich ist. Dabei sind geeignete Kontrollen mit spezifischer Wirkung für das Risiko korrespondierender Funktionstrennungsrisiken zu identifizieren, um sich als kompensierende Kontrolle zu qualifizieren. Prüfung auf Vorhandensein und Effektivität eines Katalogs mit Kontrollen als Vorschlagswerte für die Kompensation von Risiken aus Funktionstrennungsregelverstößen.
2.4.	**Trennung IT- und Fachbereichsfunktionen:** *Sind im Funktionstrennungs-Regelwerk Verfahren zur Prüfung von IT-Benutzern mit sensiblen Fachbereichsfunktionen und von IT-Mitarbeitenden mit sensiblen Fachbereichsfunktionen berücksichtigt?* Aufgrund der hohen Risikosteigerung der Kombination von sensiblen IT- und Fachbereichsfunktionen ist eine Trennung der beiden Domänen eine der grundlegenden Funktionstrennungsregeln, die zu überwachen sind. Dabei ist für eine Prüfung eine besondere Form der Auswertung erforderlich. Prüfung auf eine wirksame Kontrolle zur Prüfung von IT-Benutzern mit sensiblen Fachbereichsfunktionen und Fachbereichs-Benutzern mit sensiblen IT-Funktionen.
2.5.	**Trennung Benutzerpflege und Rollenpflege:** *Sind im Funktionstrennungs-Regelwerk Regeln zur Trennung der Pflege von Benutzerkonten, insbesondere die Zuordnung von Rollen, und deren Pflege von Rollen berücksichtigt?* Die kombinierte Berechtigung zur Pflege und Zuordnung von Rollen erhöht das Risiko der Umgehung vorgegebener Autorisierungs-Verfahren. Ist eine personelle Trennung aus Kapazitätsgründen nicht möglich, sollten regelmäßig kompensierende Kontrollen durchgeführt werden. Prüfung des Regelwerks auf eine Regel zur Trennung der Rollenpflege und Rollenvergabe. Prüfung der Bestandbenutzer auf Kombinationen der

Nr.	PRÜFPROGRAMM: FUNKTIONSTRENNUNG
	Rollenpflege im Entwicklungssystem und der Rollenvergabe insbesondere im Produktivsystem.
2.6.	**Vermeidung Eigenpflege:** *Wird die Pflege des eigenen Accounts von Benutzern bei Benutzer-Administrator:innen wirksam vermieden?* Benutzer-Administrator:innen sollten nicht in der Lage sein, das eigene Konto der Benutzer zu pflegen. Dies insbesondere, weil die Vergabe von Rollen an den eigenen Account vermieden werden soll. Prüfung auf geeignete präventive Maßnahmen, die Pflege des eigenen Kontos der Benutzer durch Benutzer-Administrator:innen zu unterbinden, oder nachgelagerte Kontrollen zur Aufdeckung von Eigenpflegen.
2.7.	**Prozesszuordnung:** *Ist in der Namenskonvention einer Regel oder einer Kontrolle der Prozessbereich kodiert, auf den sich die jeweilige Regel auswirkt? Ist ebenso durch die Namenskonvention vorgegeben, ob es sich bei einer Regel um eine Regel zur Überwachung einer sensitiven Funktion oder um eine Funktionstrennungsregel handelt?* Die Namens-Kodierung der Rollen und Kontrollen sollte eine eindeutige Zuordnung zum Prozessbereich ermöglichen. Dabei sollten sich die Prozessbereiche aller drei Elemente Rollen, Regeln und Kontrollen an derselben Prozessstruktur orientieren. Prüfung, ob die Namenskonvention eine durchgängige Kodierung des einheitlich definierten Prozessbereichs sowie eine Abgrenzung der Regel-Typen berücksichtigt.
2.8.	**Regel-/Kontrolleigner:in:** *Kann jede Regel und Kontrolle über die Zuordnung zu einem Prozessbereich eindeutig einer/einem Regel-/ Kontrollverantwortlichen zugeordnet werden?* Der/Die Regel-/Kontrollverantwortliche ist für die Einrichtung und Änderung der Regeln und Kontrollen sowie für die Interpretation der Regelauswertungen und die Ableitung von Maßnahmen verantwortlich. Prüfung, ob eine eindeutige Zuordnung jeder Regel und Kontrolle zu einem eindeutigen Datenverantwortlichen möglich ist.

4.9 Prüfprogramm: Prozesse und Organisation

Tabelle 10 Prüfprogramm: Prozesse und Organisation

Nr.	PRÜFPROGRAMM: PROZESSE UND ORGANISATION
	Kontrollziel: Die für Benutzer und Berechtigungen etablierten Prozesse und organisatorischen Rollen gewährleisten, dass der Zustand der Vergabekette zwischen Benutzern, Rollen und technischen Berechtigungen auf einem angemessenen Niveau unter Beachtung der regulatorischen Anforderungen verbleibt. **Risiko:** Bei fehlenden Vorgaben oder unzureichender Anwendung der Vorgaben für Prozesse und organisatorische Rollen ergibt sich eine Verschlechterung der Benutzer- und Berechtigungsstrukturen mit der Folge der Verletzungen des Minimalprinzips und den sich ergebenden Gefährdungen der Integrität, Verfügbarkeit und Vertraulichkeit von Daten.
1.	Role-Lifecycle-Management (Berechtigungsadministration)
1.1.	**Prozess:** *Ist das Verfahren für Berechtigungsadministration (Role-Lifecycle-Management) angemessen geregelt, dokumentiert, in Kraft gesetzt und publiziert?* Ein angemessener Prozess beinhaltet Vorgaben für die Anlage, Änderung, Ableitung / organisatorische Differenzierung und Löschung von Rollen einschließlich der Pflege der technischen Berechtigungen und präventiver Kontrollen. Die Verfahren beziehen sich auf Rollen der Kombination von Berechtigungen innerhalb von Systemen (z. B. Einzel- und Sammelrollen in S/4HANA [On-Premise], aber auch übergreifend über Systemgrenzen hinweg [z. B. Businessrollen]). Prüfung auf ordnungsgemäße Verfahren der Berechtigungsadministration.

Nr.	PRÜFPROGRAMM: PROZESSE UND ORGANISATION
1.2.	**Rollenänderungs-Beantragung:** *Werden Berechtigungsänderungen mit einem angemessenen Standardformular mit Mindestinformationen und durch qualifizierte Mitarbeitende (Key-Benutzer) beantragt?* Minimalinformationen sind alle Elemente der Namenskonvention für Name, Text und Beschreibung, Rolleneigner:in, Grund der Änderung sowie fachliche Konkretisierung der Anlage/Änderung auf Ebene der ausführbaren Programme und weiterer funktionaler und organisatorischer Differenzierungen. Beantragung sollte nur durch Personen erfolgen, die sowohl fachliche als auch technische Aspekte der Änderung beurteilen können. Prüfung in Stichproben auf ordnungsgemäße, vollständige und nachvollziehbare Befüllung der Rollenänderungsanträge.
1.3.	**Rollenänderungs-Genehmigung:** *Werden Änderungen an Berechtigungen von der/dem zuständigen Daten-/Rollenverantwortlichen genehmigt?* Werden Rollenänderungen, die nicht mit dem Prozessbereich oder der Organisationseinheit einer Rolle korrespondieren, von der/dem Daten-/ Rollenverantwortlichen dieses fremden Datenbereichs geprüft und genehmigt? Der/Die Rollenverantwortliche ist hierbei für die Beurteilung der Notwendigkeit einer Rollenanlage oder -änderung in Übereinstimmung mit der Deklaration (Name, Text, Beschreibung) der Rolle verantwortlich. Dabei sollten, wenn möglich, die Beantragung und die Genehmigung durch eine übergeordnete, von der Beantragung abweichende Instanz/Person erfolgen. Prüfung in Stichproben für Rollenänderungen, ob entsprechende Freigaben durch die/den Datenverantwortliche:n mit direktem Bezug zu vollständigen Anträgen vorliegen.
1.4.	**Rollenänderungs-Einrichtung, -Test, -Freigabe:** *Werden Rollenänderungen über ein angemessenes Transport-, Test- und Freigabeverfahren aus der Entwicklungs- über die Test- in die Produktivumgebung verbracht?* Rollenänderungen sind im Entwicklungssystem von einer Rollenentwicklerin / einem Rollenentwickler einzurichten, über ein Standardtransportverfahren in die Testumgebung zu transportieren, von qualifizierten Key-Benutzern der antragstellenden Fachabteilung zu testen und nach Freigabe in die Produktion zu transportieren. Prüfung in Stichproben für Rollenänderungen auf Einhaltung der Einrichtungs-, Test- und Freigabestufen.

Nr.	PRÜFPROGRAMM: PROZESSE UND ORGANISATION
1.5.	**Rollenänderungs-Prüfung:** *Werden im Rahmen der Rollenänderung Prüfungen auf inkongruente sensitive Funktionen und Berechtigungen sowie Funktionstrennungskonflikte analysiert und bereinigt?* Bei jeglichen Rollenänderungen sollte nach der Änderung im Entwicklungssystem eine Analyse auf Verunreinigungen durch falsche sensitive Funktionen und Berechtigungen sowie auf SoD-Konflikte erfolgen. Die Verfälschungen sind direkt durch die Rollenentwicklerin / den Rollenentwickler in Absprache mit dem Fachbereich zu bereinigen. Prüfung in Stichproben für Rollenänderungen auf dokumentierte Analyse von Berechtigungs-, Funktions- und SoD-Regeln und Bereinigung von festgestellten Abweichungen.
2.	User-Lifecycle-Management (Benutzeradministration)
2.1.	**Prozess:** *Ist das Verfahren für Benutzeränderungen (User-Lifecycle-Management) und Rollenzuordnungen angemessen geregelt, dokumentiert, in Kraft gesetzt und publiziert?* Ein angemessener Prozess beinhaltet Vorgaben für Benutzeranlagen und Änderungen bei Einstellungen, Personalbereichswechseln, Entlassungen sowie die hiermit verbundenen Rollenbeantragungen und -entziehungen einschließlich präventiver Kontrollen. Prüfung auf ordnungsgemäße Verfahren der Benutzeranlage/-änderungs- und Rollenzuordnungsanträge.
2.2.	**Antrag Benutzeranlagen/-änderungen und Rollenzuordnungen:** *Werden Benutzeranlagen/-änderungen und Rollenzuordnungen mit einem angemessenen Standardformular mit qualifizierten Mindestinformationen beantragt?* Minimalinformationen sind die Identifikation der betroffenen Benutzer, bei Anlage Minimalattribute zur Anlage der Benutzer (soweit nicht automatisiert aus zentralem Identity-Repository), vorzunehmende Änderungen, bei Rollenzuordnungsänderungen die konkreten Rollen sowie Benutzer- und Rollenverantwortliche:r (soweit nicht automatisch aus Workflow-Funktionen ermittelt). Prüfung in Stichproben auf Vollständigkeit und Qualifizierung der Antragstellung nach Mindestanforderungen aus der Verfahrensbeschreibung.

Nr.	PRÜFPROGRAMM: PROZESSE UND ORGANISATION
2.3.	**Genehmigung Vorgesetzte:r/Benutzerverantwortliche:r:** *Werden Benutzeränderungen durch die/den Vorgesetzte:n bzw. durch die/den Benutzerverantwortliche:n (bei externen und nicht personalisierten Benutzern) genehmigt?* Die Genehmigung schließt die Beurteilung ein, dass der/die Mitarbeitende die Berechtigungen benötigt und für deren Anwendung qualifiziert ist. Prüfung in Stichproben auf Vorliegen einer Genehmigung durch eine/einen Vorgesetzte:n oder andere:n Benutzerverantwortliche:n.
2.4.	**Genehmigung Rollenverantwortliche:r:** *Werden Rollenzuordnungen durch die/den Rollenverantwortliche:n der beantragten Rollen genehmigt?* Dies gilt insbesondere für Benutzeranträge, bei denen der/die Manager:in nicht gleichzeitig verantwortlich ist für die für den Benutzer beantragten Rollen und für Rollen mit höherem Risiko-Level. Prüfung in Stichproben für Rollenzuordnungsanträge auf Genehmigung durch Rollenverantwortliche der beantragten Rollen.
2.5.	**Rollenvergabe-Prüfung:** *Werden im Rahmen der Beantragung von Rollenzuordnungen Prüfungen auf Funktionstrennungskonflikte durchgeführt und aufgezeigte Konflikte bereinigt oder kompensiert?* Bei der Beantragung von Rollenzuordnungen muss eine Prüfung auf Funktionstrennungskonflikte unter Beachtung der neu beantragten und vergebenen Rollen erfolgen. Dies sollte durch Analysen auf technischer Berechtigungsebene erfolgen. Bei auftretenden Konflikten sind diese durch Rücknahme einer beantragten oder bestehenden Rolle zu vermeiden oder durch Zuordnung einer wirksamen Kontrolle zu kompensieren. Prüfung in Stichproben für Rollenzuordnungen auf dokumentierte Analyse von Funktionstrennungs-Regeln und Vermeidung oder Kompensation festgestellter Abweichungen.

Nr.	PRÜFPROGRAMM: PROZESSE UND ORGANISATION
2.6.	**Sperrung und Löschung:** *Sind für die Sperrung, das Ungültig-Setzen und die Löschung von Benutzern spezifische Regelungen getroffen worden?* Es ist zu prüfen, ob der/die Vorgesetzte diesen Vorgängen immer zustimmen muss. Aus Sicherheitsgründen muss eine Sperrung oder ein Ungültig-Setzen schnellstmöglich erfolgen. Die Zustimmung kann deswegen auch nachgelagert erfolgen, dies auch, wenn die Sperrung durch automatisierte Verfahren z. B. aufgrund von Triggern aus dem HR-System oder aufgrund von Automatismen bei Fehlanmeldungen resultiert. Prüfung, ob die speziellen Anforderungen an die Sperrung und Löschung von Benutzern gesondert geregelt sind. Prüfung in Stichproben, dass diese Anforderungen auch angewendet wurden.
2.7.	**Entsperrung und Initialisierung:** *Wurden für die Entsperrung und Initialisierung von Benutzern spezifische Regelungen getroffen, die insbesondere die Genehmigung dieser Vorgänge einschließen?* Erfolgte die Sperrung gezielt aufgrund von Fehlanmeldungen oder eines Antrags durch Vorgesetzte, ist immer der/die Vorgesetzte in die Entscheidung einzubeziehen. Prüfung, ob die speziellen Anforderungen an die Sperrung, Entsperrung und Initialisierung von Benutzern gesondert geregelt sind. Prüfung in Stichproben, dass diese Verfahren auch angewendet wurden.
3.	Privileged-Access-Management (Notfallbenutzer)
3.1.	**Prozess:** *Ist das Verfahren für die Zuordnung und Nutzung Privilegierter Benutzer (Privileged-Identity-Management – PIM) angemessen geregelt, dokumentiert, in Kraft gesetzt und publiziert?* Ein angemessener Prozess beinhaltet Vorgaben für die Architektur der verfügbaren Privilegierten Benutzer, die Zuordnung von Privilegierten Benutzern zu Anwendenden sowie die Aktivierung, Dokumentation, Protokollierung und regelmäßige Kontrolle der Nutzung der Privilegierten Benutzer. Prüfung auf ordnungsgemäße Verfahren der Zuordnung und Nutzung Privilegierter Benutzer.

Nr.	PRÜFPROGRAMM: PROZESSE UND ORGANISATION
3.2.	**Benutzer-Architektur:** *Liegen für Privilegierte Benutzer angemessene Abstufungen von Benutzern mit unterschiedlicher Funktion und Risiko-Stufe zur Eingrenzung des mit der Nutzung verbundenen Risikos und Kontrollmaßnahmen vor?* Hierbei kann und sollte eine Unterscheidung zwischen einem Benutzer mit allumfassenden Berechtigungen auf dem höchsten Level, gefolgt von Entwicklungs-/Customizing-Benutzern bis hin zu reinen Stamm- und Bewegungsdaten-Benutzern vorliegen. Auf den beiden letzteren Ebenen sollte eine Abgrenzung nach Prozessbereichen erwogen werden. Prüfung auf Nutzung einer differenzierten Privilegierten-Benutzer-Architektur.
3.3.	**Benutzer-Zuordnung:** *Erfolgt eine Freigabe zur potenziellen Nutzung von Privilegierten Benutzern an bestimmte Anwendende?* Ein Zugriff auf Privilegierte Benutzer sollte nur ausgewählten, qualifizierten Anwendenden und mit Bezug zu ausgewählten Privilegierten Benutzern ermöglicht werden. Hierzu ist ein Antrags- und Genehmigungsprozess festzulegen und zu dokumentieren. Prüfung in Stichproben auf vorherige Genehmigung der Zuordnung von Privilegierten Benutzern zu Anwendenden durch eine unabhängige Instanz.
3.4.	**Nutzungs-Protokollierung:** *Werden für alle Privilegierten Benutzer durchgängig die hiermit ausgeführten Tätigkeiten, soweit mit einer Applikation möglich, protokolliert?* Hierfür ist üblicherweise eine Aktivierung der im System vorhandenen Konfiguration sowohl insgesamt der in die Protokollierung aufzunehmenden Benutzer als auch des je Benutzer oder Benutzergruppe aufzunehmenden Umfangs der zu protokollierenden Aktivitäten erforderlich. Prüfung auf eine so weit als mögliche Aktivierung der Protokollierungsfunktionen für alle Privilegierten Benutzer.

Nr.	PRÜFPROGRAMM: PROZESSE UND ORGANISATION
3.5.	**Nutzungs-Dokumentation:** *Erfolgt für jede Nutzung eine vollständige und nachvollziehbare Dokumentation?* Eine vollständige Dokumentation beinhaltet den Grund für die Nutzung (das zugrunde liegende zu lösende Problem), die Notwendigkeit der Nutzung eines und speziell des/der ausgewählten PIM-Nutzenden sowie die Beschreibung des Lösungsvorgehens inkl. Änderungen im Nutzungsprozess. Prüfung in Stichproben auf vollständige und nachvollziehbare Dokumentation der Nutzung eines Privilegierten Benutzers.
3.6.	**Nutzungs-Kontrolle:** *Werden die Angemessenheit der Nutzungen von Privilegierten Benutzern und deren Dokumentation im Rahmen einer Prüfung durch eine unabhängige Instanz kontrolliert?* Nach Abschluss einer Nutzung eines Privilegierten Benutzers müssen von einer/einem unabhängigen Dritten die Vollständigkeit der Dokumentation, die Notwendigkeit der Nutzung und des ausgewählten Benutzers im Speziellen und die Übereinstimmung des Lösungswegs mit den protokollierten Aktivitäten geprüft werden. Im Falle von Feststellungen sind geeignete Gegenmaßnahmen abzuleiten. Prüfung in Stichproben auf Durchführung und Dokumentation einer Kontrolle der Nutzungen durch eine/einen fachlich qualifizierte:n, unabhängige:n Dritte:n.
3.7.	**Benutzer-Limitierung und -Initialisierung:** *Werden Privilegierte Benutzer mit einer zeitlichen Begrenzung zur Verfügung gestellt und nach einer Nutzung mit einer Anpassung des Passworts, Sperrung und Befristung angemessen vor personenorientierten Cyber-Angriffen geschützt?* Eine Aushändigung eines Privilegierten Benutzers über ID und Passwort an eine:n berechtigte:n Anwendende:n hat mit einer Befristung der Benutzer zu erfolgen. Nach Ablauf der Nutzung ist der Benutzer zu sperren. Das Passwort ist zu verändern. Prüfung auf Befristung des Nutzungszeitraums sowie Sperrung und Passwortrücksetzung nach Beendigung der Nutzung.

Nr.	PRÜFPROGRAMM: PROZESSE UND ORGANISATION
4.	Access-Compliance-Management
4.1.	**Sensitive Funktionsprüfung:** *Sind angemessene Verfahren für die Definition und Prüfung sensitiver Funktionen geregelt, dokumentiert, in Kraft gesetzt und publiziert?* Ein angemessener Prozess beinhaltet Vorgaben für die Identifizierung sensitiver Funktionen, die technische Spezifizierung der für die Berechtigung der Funktionen erforderlichen technischen Berechtigungen sowie der Prüfung auf sensitive Funktionen in der Rollenpflege und -vergabe sowie nachgelagerten Analysen und Rezertifizierungen. Prüfung auf ordnungsgemäße Verfahren der Definition und Prüfung sensitiver Funktionen.
4.2.	**SoD-Prüfung:** *Sind angemessene Verfahren für die Definition und Prüfung von Funktionstrennungen geregelt, dokumentiert, in Kraft gesetzt und publiziert?* Ein angemessener Prozess beinhaltet Vorgaben für die Identifizierung von Funktionstrennungsregeln als Kombination sensitiver Funktionen sowie der Prüfung auf Funktionstrennungsverletzungen in der Rollenpflege und -vergabe sowie nachgelagerten Analysen und Rezertifizierungen einschließlich der Ableitung von Bereinigungs- oder Kompensationsmaßnahmen. Prüfung auf ordnungsgemäße Verfahren der Definition und Prüfung von Funktionstrennungen.
4.3.	**Rezertifizierung:** *Sind angemessene Verfahren für die Durchführung von regelmäßigen nachgelagerten Rezertifizierungen geregelt, dokumentiert, in Kraft gesetzt und publiziert?* Ein angemessener Prozess beinhaltet Vorgaben für die regelmäßigen, in der Regel jährlichen Bestätigungsaktionen für Benutzer, Rollenzuordnungen, Funktionstrennungen und sensitive Funktionen. Die Bestätigung erfolgt durch Vorgesetzte und/oder Rollenverantwortliche. Die Aktionshäufigkeit kann den Risiko-Leveln der Benutzer, Rollen und Regeln angepasst werden – üblicherweise sechs Monate für hohe und kritische Risiken und jährlich für Elemente mit geringerem Risiko. Prüfung auf ordnungsgemäße Verfahren der Rezertifizierung.

4.10 Prüfprogramm: Protokolle und Parameter

Tabelle 11 Prüfprogramm: Protokolle und Parameter

Nr.	PRÜFPROGRAMM: PROTOKOLLE UND PARAMETER
	Kontrollziel: Eine angemessene Konfiguration der Protokollierung und der Parameter hat Einfluss auf die ordnungsgemäße Nachverfolgbarkeit von Geschäftsvorfällen sowie auf einen angemessenen Schutz von Systemen und Daten insbesondere über Einstellungen zur Autorisierung über Benutzer und Berechtigungen. **Risiko:** Bei unzureichender Parametrisierung und Protokollierung können risiko- und rechtslegungsrelevante Sachverhalte nicht mehr zum Urhebenden zurückverfolgt werden und werden Systeme und Daten durch unzureichenden Berechtigungsschutz nicht vor unautorisierten Zugriffen geschützt.
	Protokollierung: *Sind die in den Anwendungen verfügbaren risiko- und ordnungsmäßigkeitsrelevanten Protokollierungen in Übereinstimmung mit den dokumentierten Vorgaben der Benutzer- und Berechtigungsdokumentation eingerichtet?* Dabei muss in der Regel eine Prüfung in zwei Dimensionen erfolgen: a) Umfang der in die Protokollierung aufgenommenen Benutzer und b) Umfang der für die Benutzer aufgezeichneten Geschäftsvorfälle/Transaktionen. Prüfung der einschlägigen Einstellungen der Protokollierung auf Übereinstimmung mit den Vorgaben der Benutzer- und Berechtigungsdokumentation.
	Parametrisierung: *Sind die in den Anwendungen verfügbaren berechtigungsrelevanten generellen Konfigurations-/ Parametrisierungsmöglichkeiten in Übereinstimmung mit den dokumentierten Vorgaben der Benutzer- und Berechtigungsdokumentation eingerichtet?* Die meisten der betrachteten SAP-S/4-relevanten Anwendungen bieten die Möglichkeit einer Beeinflussung autorisierungsrelevanter Parameter. Für diese Parameter sollte eine revisionskonforme Entscheidung zur Ausgestaltung der Parameter getroffen, dokumentiert und regelmäßig gegen die im System vorgenommenen Einstellungen geprüft werden. Prüfung der einschlägigen Einstellungen der Parametrisierung für Berechtigungen auf Übereinstimmung mit den Vorgaben der Benutzer- und Berechtigungsdokumentation.

5 Change-Management – SAP Application Lifecycle Management / Solution Manager

5.1 Einleitung

Ein SAP-System dient im Regelfall der Unterstützung von Geschäftsprozessen. Veränderungen dieser Geschäftsprozesse, aber auch eine Weiterentwicklung der genutzten SAP-Programmfunktionen führen zwangsläufig zu der Notwendigkeit, ein Veränderungs- bzw. Change-Management für die genutzten SAP-Systeme zu etablieren, welches allen internen und externen Anforderungen gerecht wird und hilft, die Risiken im Hinblick auf Programmänderungen zu kontrollieren.

Der Begriff „Programmänderungen“ wird hier weit gefasst. Er beinhaltet das Erstellen, Ändern und Löschen von ABAP-Programmen, von FIORI-Programmen unter S/4HANA, z. B. native Anwendungen unter JavaScript, Java oder Python, und jede Art von Änderungen am Customizing. Die organisatorischen Kontrollen zum Change-Management sind weitgehend unabhängig vom eingesetzten SAP-System. Sie betreffen z. B. Kontrollen zu der Fragestellung: Werden neu entwickelte Programme vor deren produktivem Einsatz hinreichend getestet? Die technischen Kontrollen unterscheiden sich stark in Abhängigkeit von dem eingesetzten SAP-System.

In diesem Abschnitt 5.1 werden neben den grundsätzlichen organisatorischen Kontrollen die technischen Kontrollen für SAP-Betriebsmodelle unter Einsatz klassischer SAP-ERP-Systeme sowie S/4HANA (OnPremise) behandelt. Die Spezifika unter Einsatz des SAP Solution Manager im Rahmen des Change-Managements werden in Abschnitt 5.2 dargestellt. Der Abschnitt 5.3 geht auf Kontrollen ein, wenn SAP S/4HANA Cloud genutzt wird.

„Programmänderungskontrollen“ umfassen nicht die Maßnahmen, wie sie im Rahmen einer kompletten Neueinführung von SAP-Systemen, der Transformation auf SAP-Systeme oder der Datenmigration auf SAP-Systeme geboten sind.

5.2 Risiken

Die Risiken in Bezug auf Programmänderungen bestehen in der mangelhaften Umsetzung des geforderten internen Kontrollsystems, das unternehmensindividuell und risikoorientiert zum Change-Management zu realisieren ist. Insbesondere bestehen die übergeordneten Risiken, dass geschäftskritische Daten fehlerhaft verarbeitet werden und dass das SAP-System nicht für die Geschäftsprozesse zur Verfügung steht. Fehler in der Buchführung, Vermögensschäden oder Reputationsverlust können die Folge sein.

Weitere Risiken ergeben sich für das Unternehmen aus einer möglichen Nichteinhaltung gesetzlicher Anforderungen, wenn beispielsweise Programmänderungen nicht nachvollziehbar dokumentiert wurden und Informationen, die Eingang in die Rechnungslegung des Unternehmens gefunden haben, nicht mehr belegbar sind.

Beispiele für Risiken sind:

- Änderungen an Programmen und Einstellungen des Produktivsystems werden nicht sach- bzw. anforderungsgerecht umgesetzt.
- Änderungen des eingesetzten Verfahrens erfolgen unautorisiert.
- Nicht ausreichend durchgeführte Programmtests führen dazu, dass Fehler zu spät oder gar nicht entdeckt werden.
- Die Datenkonsistenz der Produktivdaten geht verloren.
- Eine Änderungsdokumentation wird nicht erstellt, und dieser Sachverhalt gefährdet die Nachvollziehbarkeit des eingesetzten Verfahrens.
- Sicherheitsrelevante SAP-Meldungen (SAP Security Notes) werden nicht zeitnah umgesetzt. Dies führt als Folge zu Daten-Leaks, Systemstillständen oder unautorisierten Manipulationen der gesamten IT-Landschaft.

5.3 Kontrollziele

Die mittels Kontrollen zu begrenzenden Risiken ergeben sich im Bereich des Change-Managements aus dem Spannungsfeld zwischen den verschiedenen Prozess- und Kontrollzielen, welche sich zum einen aus Effizienzgesichtspunkten und zum anderen auch aus den Grundsätzen ordnungsmäßiger Buchführung (GoBD) ableiten.

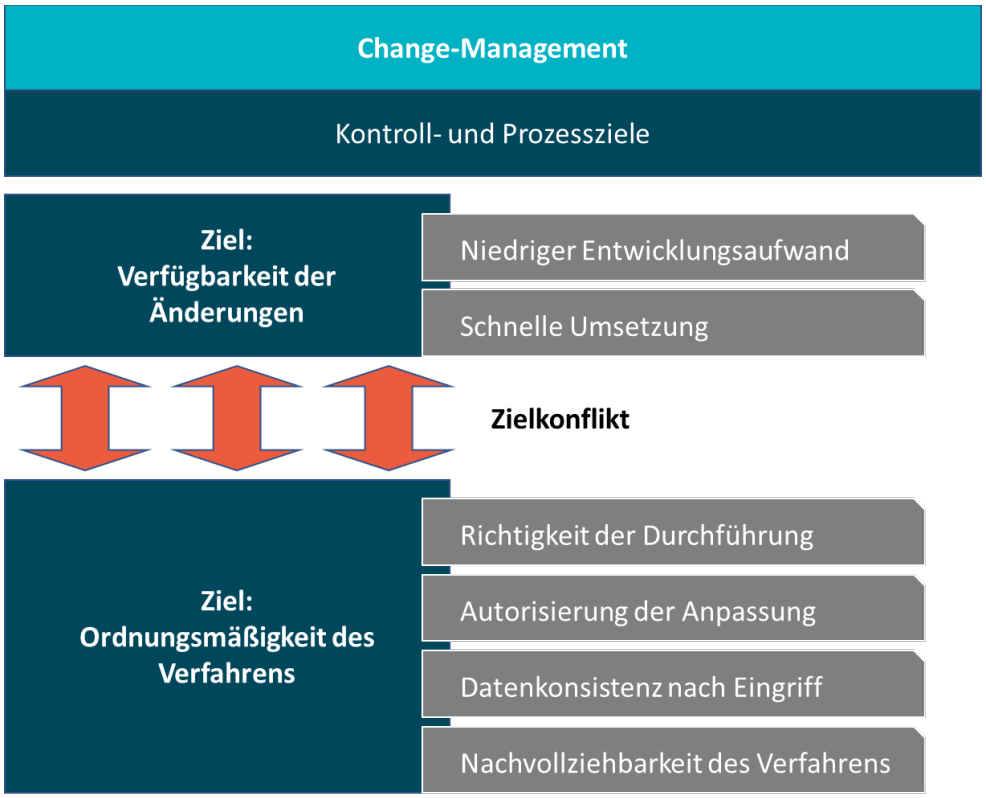

Abbildung 2 Zielkonflikte im Change-Management

Das sich an der Effizienz des Change-Managements orientierende Ziel ist, Geschäftsprozesse anforderungsgerecht und möglichst kostengünstig umzusetzen. Dabei sollen Änderungen an Programmen und Daten möglichst zeitnah bereitstehen, um die Vorteile des IT-gestützten Verfahrens voll auszuschöpfen. Das bedeutet, dass sich die IT-Verfahren in einem SAP-System einfach und schnell ändern lassen müssen, ohne dass die zu unterstützenden Prozesse gestört werden. Die Beachtung der Grundsätze ordnungsmäßiger Buchführung gemäß § 239 Abs. 4 HGB und die Berücksichtigung der damit verbundenen Anforderungen an die Sicherheit IT-gestützter Rechnungslegungssysteme stellen ein weiteres Prozessziel dar. Dieses Ziel kann zu einem Zielkonflikt mit dem erstgenannten Ziel führen, da die regulatorischen Anforderungen einen nicht zu vernachlässigenden Kontroll- und Dokumentationsaufwand erfordern, welcher den Prozess insgesamt verlangsamen und die Kosten einer jeden Programmänderung steigern kann.

Aus den beschriebenen Risiken leiten sich die Kontrollziele für den Change-Management-Prozess ab.

Beispiele für Kontrollziele sind:

- Nur autorisierte und ausreichend getestete Änderungen werden in ein produktives SAP-System übernommen.
- Für die Entwicklung sowie den Test von Programmänderungen stehen gesonderte SAP-Systeme und geeignete Testdaten zur Verfügung.
- Änderungen sind nachvollziehbar, sodass das Management das eingesetzte Verfahren steuern kann.
- Sicherheitsrelevante Änderungen erfolgen zeitnah, um die Sicherheit des SAP-Systems und der damit verarbeiteten Daten zu gewährleisten.
- Restriktive Vergabe von Berechtigungen zur Durchführung von Änderungen an Programmen und Customizing-Einstellungen sowie zum Schutz der Programme und Einstellungen des Produktivsystems.
- Entwicklungsdaten und Produktivdaten sind strikt voneinander getrennt und befinden sich in voneinander unabhängigen Systemen.
- Test- und Freigabeverfahren einschließlich Maßnahmen unter Anwendung des Vier-Augen-Prinzips werden durch die SAP-Systemlandschaft und das Transportmanagement festgelegt.
- Notfalländerungen werden durch ein geordnetes und nachvollziehbares Verfahren kontrolliert, welches durch Funktionstrennung und Überwachungstätigkeiten die richtige Umsetzung von Änderungen sicherstellt.
- Systemeinstellungen bez. der Protokollierung von Änderungen stellen sicher, dass die Änderungsdokumentationserstellung durch das SAP-System unterstützt wird.
- Änderungen werden nachvollziehbar dokumentiert, sodass die Anforderungen an eine transparente Verfahrensdokumentation gemäß den GoBD, den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff, erfüllt werden.

5.4 Prüfprogramm: Grundsätzliches Change-Management

Tabelle 12 Prüfprogramm: Grundsätzliches Change-Management

NR.	Prüfprogramm: Grundsätzliches Change-Management
	Die Durchführung der Tests und die Produktivsetzung von Programmänderungen erfolgt in SAP-Systemen in Abhängigkeit von der SAP-Systemlandschaft, den organisatorischen Regelungen und den technischen Einstellungen insbesondere zum Transportwesen.
1.	**Kontrollziel:** Die SAP-Systemlandschaft ist so ausgestaltet, dass ein geordnetes Change-Management unterstützt wird. Im Regelfall wird mindestens eine Drei-System-Landschaft mit getrenntem Entwicklungs-, Test-/Qualitätssicherungs- und Produktivsystem eingesetzt. **Risiko:** Programmänderungen erfolgen ungetestet unmittelbar im Produktivsystem und führen zu Fehlern.
1.1 H	Die SAP-Systemlandschaft besteht aus getrennten Entwicklungs-, Test-/ Qualitätssicherungs- und Produktivsystemen. Vorgehen zur Prüfung der Einstellungen zum Transport Management System (TMS): Transaktion: STMS_PATH Programm: RSTMS_TRANSPORT_PATH
1.2 H	Die Transportwege und -schichten sind so eingerichtet, dass Transporte durch das TMS vom Entwicklungs- zum Test- sowie zum Produktivsystem erfolgen. Vorgehen zur Prüfung der Einstellungen der Transportwege: Transaktion: STMS Transaktion: STMS_DOM
1.3 H	Die Einstellung der globalen Systemänderbarkeit unterbindet unmittelbare Programmänderungen im produktiven SAP-System. Vorgehen zur Prüfung der globalen Systemänderbarkeit: Transaktion: SE06 Programm: RSWBO004 Vorschlagswerte: Für produktive SAP-Systeme ist die globale Einstellung „nicht änderbar“. Auf Ebene der einzelnen Softwarekomponenten und der Namensräume werden unmittelbare Änderungen unterbunden.
1.4 H	Änderungen zur globalen Systemänderbarkeit erfolgten im Prüfungszeitraum sachgerecht. Vorgehen zur Prüfung der Historie zur globalen Systemänderbarkeit: Transaktion: SE06, Klick auf das Dokumenten-Icon zum Aufruf des Logs.

NR.	Prüfprogramm: Grundsätzliches Change-Management
1.5 H	Die Einstellung der Änderbarkeit auf Mandanten-Ebene unterbindet unmittelbare Programmänderungen im produktiven SAP-System. Vorgehen zur Prüfung der Mandanten-Änderbarkeit: Transaktion: SCC4 Tabelle: T000 Vorschlagswerte: Für Mandanten der Rolle P (produktive SAP-Mandanten) sind keine Änderungen zugelassen.
1.6 H	Änderungen zur Änderbarkeit auf Mandanten-Ebene erfolgten im Prüfungszeitraum sachgerecht. Vorgehen zur Prüfung der Historie zur Mandanten-Änderbarkeit: Transaktion: SCU3 Programm: RSTBHIST Klick auf „Protokolle auswerten“, Selektion im nachfolgenden Screen auf „Customizing-Objekt/Tabelle“ = „T000“, den Prüfungszeitraum und „Auswertung bezüglich“ mit der Radiobox „Tabellen“
1.7 H	Die produktiv verwendeten Buchungskreise sind als solche eingestellt. Vorgehen zur Prüfung der Buchungskreise: Tabelle: T001, Feld XPROD
2.	**Kontrollziel:** Änderungen an Customizing-Tabellen im Produktivsystem können anhand von Protokollen nachvollzogen werden. **Risiko:** Programmänderungen, die durch Änderungen an Tabellendaten vorgenommen werden, sind nicht nachvollziehbar.
2.1 H	Die grundlegende Tabellenänderungsprotokollierung ist in den Systemprofilparametern richtig eingestellt. Vorgehen zur Prüfung der grundlegenden Tabellenänderungsprotokollierung: Programm: RSPARAM, Parameter rec/client Tabelle: PAHI Vorschlagswerte: Die produktiv genutzten SAP-Mandanten sind eingestellt oder der Eintrag lautet auf „all“.
2.2 H	Die Tabellenänderungsprotokollierung ist je relevanter Tabelle richtig eingestellt. Dabei sollten mindestens die rechnungslegungsrelevanten Customizing-Tabellen im Produktivsystem das Protokollkennzeichen besitzen. Hilfestellung bietet der SAP-Hinweis 112388. Vorgehen zur Prüfung der Tabellenänderungsprotokollierung: Programm: RSPARAM, Parameter rec/client Tabelle: DD09L Feld PROTOKOLL Vorschlagswerte: Wert „X“ im Feld PROTOKOLL.

NR.	Prüfprogramm: Grundsätzliches Change-Management
2.3 H	Die Tabellenänderungsprotokollierung ist so eingestellt, dass auch bei Transporten eine Protokollierung erfolgt. Vorgehen zur Prüfung der Tabellenänderungsprotokollierung bei Transporten: Programm: RSTMSTPP, Parameter recclient Vorschlagswerte: Die produktiv genutzten SAP-Mandanten sind eingestellt oder der Eintrag lautet auf „all“. Ab S/4HANA 2021 kann der Parameter im Default durch einen Eintrag in der Tabelle TPSYSTEMDEFAULTS geändert werden.
3.	**Kontrollziel:** Programmänderungen werden nach revisionssicheren Verfahren vorgenommen. **Risiko:** Programmänderungen erfolgen unautorisiert, ungetestet oder unsachgemäß und führen zu Fehlern.
3.1 H	Für Programmänderungen bestehen Richtlinien, die insbesondere die Aktivitäten und Kontrollen im Rahmen des gesamten Change-Management-Prozesses festlegen. Vorgehen zur Prüfung der Change-Management-Richtlinien: Durchsicht von Richtlinien insbesondere im Hinblick darauf, ob sachgerechte Vorgaben im Hinblick auf folgende Punkte bestehen: - Anforderungen zu Programmänderungen sind nachvollziehbar dokumentiert. - Anforderungen werden klassifiziert und priorisiert und unterliegen einer fachlichen Freigabe vor deren Freigabe. - Sicherheitsrelevante Änderungen werden bei den Anforderungen mit berücksichtigt. Diese umfassen auch SAP Security Notes und Hinweise aus dem SAP-Patch-Tag. - Bei der Umsetzung von Programmänderungen wird ein Vier-Augen-Prinzip bez. Anforderndem/Anfordernder und Änderndem/Ändernder eingehalten. - Programmänderungen werden hinreichend getestet. - Programmänderungen werden unter Einhaltung der Funktionstrennung und mittels TMS in das Produktivsystem überführt. Das Vier-Augen-Prinzip bezieht sich auf die/den Freigebende:n der Änderung und den/die Administrator:in, der/die den Transport durchführt. - Für Programmänderungen, die nicht dem regulären Change-Management unterliegen, z. B. Notfall-Änderungen unmittelbar im Produktivsystem, bestehen gesonderte Notfall-Change-Management-Verfahren. - Programmänderungen werden nachvollziehbar im Rahmen der Verfahrensdokumentation nach Maßgabe der GoBD dokumentiert.

NR.	Prüfprogramm: Grundsätzliches Change-Management
3.2 H	Eine Funktionstrennung zwischen den Aktivitäten im Entwicklungs- und Produktivsystem wird eingehalten. Transport-Owner, die den Transportauftrag im Regelfall im Entwicklungssystem anlegen, sind nicht identisch mit dem/der Administrator:in, der/die den Transport in das Produktivsystem durchführt. Vorgehen zur Prüfung der Funktionstrennung: Tabelle: TPALOG, Felder - TRUSER (Transport-Owner) - ADMIN (Administrator:in)
3.3 H	Das Verfahren zum Change-Management wurde für den Prüfungszeitraum entsprechend den Vorgaben und revisionssicher eingehalten. Vorgehen zur Stichproben-basierten Prüfung von Transporten im Produktivsystem: Tabelle: TPALOG, Felder - TRTIME = Prüfungszeitraum - TRSTEP = „I“ (Importe als Haupttransporte) - TARSYSTEM = Produktivsystem als Zielsystem
3.4 H	Das Verfahren zum Change-Management wurde für den Prüfungszeitraum entsprechend den Vorgaben und revisionssicher eingehalten. Vorgehen zur Stichproben-basierten Prüfung der direkten Änderung von Objekten im SAP-System: Tabelle: OBJH, relevante Felder: OBJTRANSP = „leer“ oder „3“ LUSER ungleich „SAP“
3.5 H	Im Transportwesen wurde das normale Verfahren nicht unter Einsatz der Funktion „Repair“ umgangen. Vorgehen zur Stichproben-basierten Prüfung bei Einsatz der „Repair“-Funktion: Tabelle: E070, Felder - TRFUNCTION = „R“ - AS4DATE = Prüfungszeitraum

NR.	Prüfprogramm: Grundsätzliches Change-Management
3.6 H	Änderungen, die mithilfe der Transaktion SE16N unmittelbar im Produktivsystem erfolgten, wurden unter Anwendung von Kontrollen des Change-Management-Verfahrens durchgeführt. Vorgehen zur Ermittlung der Fälle von Änderungen über die Transaktion SE16N: Programm: RKSE16N_CD_DISPLAY Tabellen als Alternative zu dem Programm: SE16N_CD_KEY und SE16N_CD_DATA Verbinden der Tabellen SE16N_CD_KEY und SE16N_CD_DATA über das Feld ID Selektion auf das Feld SDATE = Prüfungszeitraum

5.5 Prüfprogramm: Authentifizierung und Autorisierung im Change-Management

Für die Durchführung jeglicher Programmänderungen, deren Test und die Produktivsetzung sind im SAP-System Benutzer erforderlich, für die Kontrollen und Einstellungen zur Authentifizierung und Autorisierung greifen. Für die Prüfprogramme wird verwiesen auf die Kapitel 3 zur Authentifizierung und 4 zur Autorisierung sowie die spezifischen Prüfprogramme in den Kapiteln 4.4 bis 4.10.

5.6 Change-Management bei Einsatz von S/4HANA Cloud, public edition

In der S/4HANA Cloud sind große Teile des Change-Managements in der Verantwortung der SAP. Hierdurch ergeben sich verschiedene Änderungen im Prüfungsvorgehen. Beispielsweise erfolgt die Aktualisierung der S/4HANA Cloud global und zeitgleich für alle Kunden-Systeme, beginnend mit den nicht produktiven Systemen gefolgt von den produktiven Kunden-Systemen mit einem zeitlichen Versatz von mehreren Wochen.

Details des S/4HANA-Cloud-Change-Managements werden im entsprechenden Kapitel beschrieben.

6 SAP S/4HANA OnPremise

6.1 Einleitung

S/4HANA (OnPremise) ist der direkte Nachfolger der SAP-R/3-ERP-Lösung und wird wie der Vorgänger, und wie auch das zusätzliche Wort OnPremise verspricht, in einem eigenen oder dem Rechenzentrum eines Dienstleisters gehostet. Die OnPremise-Version kann wie der Vorgänger vollumfänglich angepasst, erweitert und modifiziert werden – dies im Gegensatz zur neuen Alternative S/4HANA Cloud, die hier später in einem eigenen Schicht-Kapitel beschrieben ist. Im Vergleich mit dem R/3-Vorgänger bleibt es auch beim S/4HANA-OnPremise bei der Nutzung des SAP-NetWeaver-Application-Servers mit dem klassischen ABAP-Stack. Damit bleiben den Anwendenden die meisten der altbekannten und lieb gewonnenen ABAP-Platform-Funktionen erhalten.

Die zwei für Prüfungshandlungen wesentlichen Unterschiede beziehen sich auf die HANA-Datenbank und die Fiori Apps. Mit dem Wechsel nach S/4HANA OnPremise gibt es keine Wahlfreiheit mehr in der der Anwendungsschicht unterlegten Datenbanklösung. Dem S/4 unterliegt nun die verpflichtende In-Memory-basierte SAP-HANA-Datenbanklösung, deren Prüfungsaspekte unten in einem eigenen Kapitel beschrieben sind. Ebenfalls kommt mit S/4 der bereits vorher verfügbaren SAP-Fiori-Lösung und dem Fiori Launchpad erheblich stärkere Bedeutung für die Benutzernavigation und für die Benutzeroberflächen zu. Der Java-Stack ist nur noch für wenige Funktionalitäten und die korrespondierenden WebDynpros im S/4HANA-Kontext nötig und wird daher in diesem Prüfleitfaden nicht mehr betrachtet.

Mit der bleibenden Relevanz der ABAP Platform ist auch weiterhin die überwiegende Mehrzahl der bereits aus dem alten Prüfleitfaden bekannten Prüfungshandlungen nach wie vor gültig. Dies betrifft insbesondere die wie bisher gültigen Berechtigungsstrukturen mit Berechtigungen für Berechtigungsobjekte mit Feldern und Feldwerten, die direkt über Einzelrollen oder indirekt über Sammelrollen an Benutzerkonten vergeben werden. Auch an den bekannten Transaktionen und Funktionen wie dem Profilgenerator mit den OrgEbenen- und Ableitungsfunktionen sowie an der Benutzerpflege hat sich nichts Prüfungsrelevantes verändert.

Nur in einzelnen Fällen haben sich Veränderungen der für die Prüfungshandlungen relevanten Transaktionen und Reports ergeben (z. B. beim Security Audit Log). Die Prüfungshandlungen in diesem Kapitel betreffen nur die S/4HANA-OnPremise-Spezifika, die nicht bereits im generischen Kapitel 4 Autorisierung behandelt worden sind. Einige sehr ausführlich im alten Prüfleitfaden behandelte Themen haben wir hier lediglich stark verkürzt aufgenommen, verweisen aber auf die alten Passagen (z. B. Funktionstrennungs-Szenarien in der Benutzer- und Berechtigungsverwaltung).

Auch haben sich mit der Umstellung auf die neue HANA-Datenbank Möglichkeiten der Überarbeitung der Tabellenstrukturen ergeben, die auch zu Veränderungen von Funktionen, Transaktionen und Fiori Apps geführt haben. Insbesondere in Bezug auf eine Migration von Bestandsrollenkonzepten, aber auch von Regeln für Funktionstrennungen und sensitive Funktionen muss insofern eine Anpassung der hierfür relevanten Berechtigungen erfolgen. Zwei besonders prominente Beispiele sind hier die Anpassungen im Kontext des neuen Universal-Journals für die Kombination der Finanzbuchhaltung und der Kostenrechnung und die Transformation der Geschäftspartnerpflege mit einer Konsolidierung der Pflege von Kund:innen und Lieferant:innen mit der alten Geschäftspartnerpflege.

Ebenfalls sind neue Prüfungshandlungen zum Thema Berechtigungen für ausführbare Programme über Fiori Apps hinzugefügt worden. Im Gegensatz zu den klassischen ABAP-Transaktionen sind für die Ausführung von Fiori Apps insbesondere Berechtigungen für OData-Services erforderlich sowie neue Fiori-spezifische Strukturen, Fiori-Kataloge und Gruppen oder Spaces/Pages/Sections mit den Fiori Apps anzulegen und über die bekannten Einzelrollen an Benutzer zu erteilen. Aus prüferischer Sicht sind hierbei nur die ODS-Berechtigungen und die Kataloge zur Ausführung von Fiori Apps zwingend; die folgenden Prüfungshandlungen beschränken sich insofern auf genau diese beiden Elemente.

6.2 Risiken

Mit den im Vergleich sehr ausgereiften und differenzierten Rollenstrukturen in anderen Berechtigungskonzepten im SAP S/4HANA OnPremise sind alle in Kapitel 4 Autorisierung enthaltenen Risiken ohne Abstriche anwendbar.

Im Bereich Authentifizierung ist das größte Risiko, dass Dritte an Informationen gelangen, um sich gegenüber dem SAP-System als Berechtigte Benutzer auszugeben. Dies kann die Grundlage für zahlreiche Gefährdungen des Systems nach sich ziehen: Freigaben von Buchungen, Einsicht in vertrauliche Vorgänge, Störung des Systembetriebs bzw. von Unternehmensprozessen.

Ebenso müssen nicht nur Benutzer, sondern auch Systeme authentisiert werden, da gerade bei einer erhöhten Vernetzung auch jeder externe Server mit Zugriff auf Informationen vertrauenswürdig sein muss.

Im Bereich Change-Management bestehen die in Kapitel 5 aufgezeigten Risiken. Wird im Rahmen des Change-Managements der SAP Solution Manager (SolMan) eingesetzt, bieten dessen Funktionen Kontrollmöglichkeiten, bei denen spezifische Risiken berücksichtigt werden sollten. Ein wesentliches Risiko besteht darin, dass neue oder geänderte Programme ohne ausreichende Tests und Freigaben in die S/4HANA-OnPremise-Umgebung produktiv genommen werden und damit zu falschen

Verarbeitungsergebnissen führen. Um derartige Risiken und die korrespondierenden Kontrollen beurteilen zu können, dient das Prüfprogramm zum Change-Management in Kapitel 6.7.

6.3 Kontrollziele

Im Rahmen von SAP S/4HANA OnPremise sind einige Aspekte besonders hervorzuheben, die in den nachfolgenden Prüfungshandlungen in Ergänzung der generischen Prüfungshandlungen aus Kapitel 4 Autorisierung ergänzt werden:

Im Kontrollbereich Benutzer und Rechte verfügt OnPremise über eine Reihe guter Klassifizierungsmöglichkeiten wie insbesondere die Gruppen/Typen von Benutzern sowie eine Vielzahl weiterer Attribute, die eine Einordnung unterstützen können. Ebenso liefern SAP und weitere Drittanbieter von OnPremise-basierten Programmen Standardbenutzer aus, die einen angemessenen Schutz / angemessene Kontrollen erfordern.

Im Kontrollbereich Rollen und Berechtigungen zeichnet sich OnPremise durch die Möglichkeit einer zweistufigen Schichtung von technischen Berechtigungen auf Einzel- und Sammelrollenebene aus. Ergänzend ist es möglich, Einzel- und Sammelrollen zusätzlich über Referenzbenutzer an Benutzer zu vergeben. Während diese Funktionen bereits aus dem R/3-Kontext bekannt sind, kommen mit S/4 nun die Fiori-Kataloge und Berechtigungen für OData-Services als berechtigungsrelevante Aspekte bei der Rollenpflege hinzu, die in den Prüfungshandlungen als getrenntes Kapitel berücksichtigt worden sind.

Im Kontrollbereich Protokolle und Parameter verfügt OnPremise über eine Reihe von für die Autorisierung relevanten Parameter-Einstellungen und ebenso über Protokollierungsfunktionen, die in Ergänzung von Berechtigungen zu aktivieren und einzurichten sind.

Im Kontrollbereich Change-Management können über den SAP SolMan sämtliche Prozesse des Software-Lifecycle-Managements systemseitig unterstützt und abgebildet werden. Das Prüfprogramm zum Change-Management in Kapitel 6.7 zeigt Prüfungshandlungen auf, um diese spezifischen Kontrollen zu beurteilen.

6.4 Prüfprogramm: Authentifizierung

Tabelle 13 Prüfprogramm: Authentifizierung

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
1.	**Authentifizierungsmethoden**
	Kontrollziel: Verwendete Authentifizierungsmethoden sollen dokumentiert und durch technische und organisatorische Maßnahmen abgesichert sein; ihre Verwendung soll klar gegeneinander abgegrenzt sein. Nicht verwendete Authentifizierungsmethoden und Authentication-Provider sind aus dem System zu entfernen. **Risiko:** Konkurrierende Authentifizierungsverfahren können Sicherheitskonzepte aushebeln, indem bei der Kontrolle nur Teilaspekte von Angriffsszenarien im Blick sind. Obsolete Authentifizierungsverfahren oder Authentication-Provider können für unberechtigten Zugriff auf das System verwendet werden, wenn eine effektive Überwachung fehlt.
1.1.	**Allgemeine Authentifizierungs-Parameter:** *Sind die Parameter für die Authentifizierung gemäß den Vorgaben für angemessene Passwort-Sicherheit eingerichtet?* Die Systemparameter für die Anmeldekontrollen sind so zu pflegen, dass sie einen angemessenen Zugriffsschutz gewährleisten. Als Anhalt kann hierfür die unten beigefügte separate Tabelle mit Richtwerten genutzt werden. Eine Prüfung der konfigurierten Parameterwerte kann über die Transaktionen RZ10/RZ11 oder über die Reporttransaktion RSPARAM erfolgen. Prüfung auf Übereinstimmung der für die Kennwort-Authentifizierung eingerichteten Parameter mit den definierten Richtwerten.
1.2.	**SSO-Authentifizierung:** *Wird, soweit möglich, für die Anmeldung am System die Single-Sign-on(SSO)-Authentifizierung genutzt?* SSO reduziert das Risiko, dass Passwörter erraten werden. Über den Report (Transaktion SA38/SE38) SSF02 mit der Variante Version ermitteln kann geprüft werden, ob die verwendete SAPCRYPTOLIB der aktuellen aus dem SAP Marketplace entspricht. Weiter kann mit der Transaktion SSO2 geprüft werden, ob Anmeldetickets akzeptiert werden und somit eine Anmeldung via SSO möglich ist. Prüfung auf Nutzung der SSO-Authentifizierung zur Systemanmeldung.

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
1.3.	**Aussteuerung Authentifizierungsmethoden:** *Wird sichergestellt, dass bei genereller SSO-Anmeldung eine Passwort-Anmeldung nur noch für Ausnahme-Benutzer erlaubt wird?* Wenn SSO im Unternehmen eingesetzt wird, sollte eine einfache Anmeldung über Passwort nur noch Sondernutzenden erlaubt sein. Dies kann über einen Systemparameter (login/disable_password_logon) und eine entsprechende benutzerindividuelle Security-Policy realisiert und über die Transaktion SECPOL geprüft werden. Ebenso sollte mittels der Transaktion RZ10 der Parameter login/accept_sso2_ticket geprüft werden; falls eine SSO-Anmeldung nur über ein X509-Client-Zertifikat erfolgen soll, muss dieser den Wert 0 haben. Prüfung auf Begrenzung der Passwort-Authentifizierung bei genereller SSO-Anmeldung auf spezifische Ausnahme-Benutzer – beispielsweise SAP-Basis-Administrator:innen oder Schnittstellen-Nutzenden, bei denen es keine technische Alternative gibt.
1.4.	**Prüfung der Sicherheitsattribute der jeweiligen Sicherheitsrichtlinien.** Überprüfung, ob die Sicherheitsrichtlinienattribute mit den Compliance-Anforderungen der jeweiligen Benutzergruppe übereinstimmen. Über die Transaktion SECPOL können die Einstellungen der Sicherheitsrichtlinienattribute überprüft werden.
1.5.	**Sicherheitsrichtlinien (Security-Policies):** Welcher Benutzer hat einen Eintrag für die Sicherheitsrichtlinien? Jeder Benutzer im System muss mittels Systemparameter Einstellung oder Sicherheitsrichtlinien geschützt sein. Es muss geprüft werden, welche Benutzer im System eine Sicherheitsrichtlinie zugeordnet haben; dies kann über das Benutzerinformationssystem (SUIM) mittels der Transaktion S_BCE_68001400 ermittelt werden.
1.6.	**Prüfung der Sicherheitsrichtlinien-Änderungsbelege** Mittels der Transaktion SECPOL_DISPLAY_CHANGEDOCUMENTS kann geprüft werden, von wem und zu welchem Zeitpunkt die letzte Anpassung der Sicherheitsrichtlinien durchgeführt wurde.

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
2.	**Verschlüsselte Kommunikation**
	Kontrollziel: Die Kommunikation zwischen Client und Server einerseits und zum Gateway-Server andererseits ist nach einem aktuellen Verfahren verschlüsselt. **Risiko:** Ohne eine verschlüsselte Kommunikation im Netzwerk ist es möglich, den Datenverkehr der Netzwerkprotokolle auszulesen und Nutzenden-Namen sowie Passwörter in lesbarer Form als Angreifenden zu erlangen.
2.1.	**Verschlüsselung Kommunikation Client und Server:** *Ist die Kommunikation zwischen Client und Server nach einem aktuellen Verfahren verschlüsselt?* Die Verschlüsselung kann über den T-Code SM51 mit dem Icon SNC-Status (STRG + F10) geprüft werden. SNC sollte hierbei den Status Grün haben. Weiter sollte geprüft werden, ob die Kommunikation für weitere relevante Komponenten ebenso verschlüsselt ist. Weiter sollte man den aktuellen Stand der Kryptografie-Bibliothek prüfen (siehe OSS-Note 1848999). Prüfung auf angemessene Verschlüsselung der Client-Server-Kommunikation.
2.2.	**Schutz der Kommunikation RFC Gateway:** *Sind die ACLs (Zugriffssteuerungslisten) für die Gateway-Kommunikation vorhanden und angemessen gepflegt (secinfo, reginfo)?* Das Vorhandensein und die Werte der ACL-Liste können über die Menüleiste Springen → Expert:innen-Funktion → Externe Sicherheit → Pflege ACL-Dateien oder die Transaktion SMGW geprüft werden. Die Dateien Secinfo und Reginfo sollten vorhanden sein und mit den Werten P (erlauben) und D (verweigern) entsprechend der vorgesehenen Kommunikation ausgeprägt sein. Prüfung auf Vorhandensein und angemessene Einrichtung der ACL-Dateien für die Gateway-Kommunikation.

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
2.3.	**Absicherung Schnittstellen-Verbindungen:** *Sind alle eingerichteten Schnittstellen erforderlich und angemessen abgesichert?* Prüfen über die SM59 oder die Transaktion SE16 die Tabelle RFCDES, dass die vorhandenen RFC-Verbindungen dokumentiert sind; im Speziellen ist hier auf die Trusted-Verbindungen zu achten. Ebenso sind die aktiven Dienste in der SICF zu prüfen, und nicht benötigte Dienste sind zu deaktivieren. Prüfung auf angemessene Absicherung genutzter und Bereinigung ungenutzter Schnittstellen.
3.	**Zertifikate**
	Kontrollziel: Sind Zertifikate im Einsatz? Sind diese durch eine Zertifizierungsstelle (Certificate Authority, CA) verifiziert? Sind diese Zertifikate nicht zu lange gültig (< = 365 Tage)? **Risiko:** Ein ungültiges Zertifikat führt zu Störungen im Betriebsablauf; ebenso kann ein Angreifender mit einem geklauten Zertifikat eine „Man in the middle"-Attacke durch Vorspiegelung einer falschen Identität durchführen.
3.1.	**Serverzertifikate:** *Sind die Serverzertifikate installiert und gültig?* Eine Prüfung auf gültige Zertifikate kann über die Transaktion STRUST für die Ordner SNC SAPCryptolib, SSL-Server Standard, erfolgen. Die Zertifikate sollten einen grünen Status haben. Ebenso muss geprüft werden, ob die ungültigen Zertifikate aus der Zertifikatsliste zu entfernen und eventuell nicht vertrauenswürdige darin enthalten sind. Je nach eingesetzten Modulen kann es nötig sein, weitere Ordner zu prüfen. Die PSE-Dateien sollten vor Änderung geschützt sein; dies kann aus der Transaktion STRUST mittels der Tastenkombination Umschalten + F7 geprüft werden. Prüfung auf angemessene Einrichtung der Serverzertifikate.
4.	**Client-Software**
	Kontrollziel: Wird ein aktueller, sicherer Client beim Zugriff auf das SAP-System verwendet? **Risiko:** Alte SAP-GUI-Clients und veraltete Browser können Sicherheitslücken enthalten, die weitreichend bekannt und einfach auszunutzen sind. Somit reduziert sich der Aufwand eines Angriffs und erhöht sich das Risiko für das System.

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
4.1.	**Aktuelle Client-Software:** *Gibt es angemessene Vorgaben zur Verteilung/Aktualisierung der Client-Software?* Die Nutzung veralteter Clients erleichtert es Angreifenden, bekannte Sicherheitslücken auszunutzen. Dies kann durch angemessene Vorgabe für die verwendeten Clients und einen definierten Release-Zyklus erschwert werden (z. B. SAPGUI und Webbrowser auf Chromium-Basis). Prüfung, dass die Client-Software SAP GUI / Webbrowser und das verwendete Betriebssystem einen aktuellen Sicherheitsstand haben.

6.5 Systemparametereinstellungen und Sicherheitsrichtlinien

In SAP-Systemen werden mithilfe von Systemparametern Grundeinstellungen zur Benutzer- und Berechtigungsadministration eingestellt. Diese Parameter werden im Folgenden erläutert. Die Werte der Parameter können mithilfe des Reports RSPARAM oder der Transaktion RSPFPAR kontrolliert werden. Für die Verwaltung der Parameter stehen die Transaktionen RZ10 (Verwaltung von Instanzenprofilen) und RZ11 (Pflege von Systemparametern) zur Verfügung. Die Pflege der Parameter erfolgt ausschließlich durch den Fachbereich Basis.

Mit Basis-Release 7.31 hat SAP die Sicherheitsrichtlinien (Transaktion SECPOL) eingeführt. Im Gegensatz zu den Systemparametern, die Benutzer- und Mandant:innen-übergreifend gelten, werden Sicherheitsrichtlinien via Transaktion SU01 den Benutzerstammsätzen direkt zugeordnet. Somit ist nun ein individuelles Einstellen der Parameter möglich. Die meisten Systemparameter, die die Kennwortregelungen und das Verhalten bei der Anmeldung steuern, werden durch die Sicherheitsrichtlinien ersetzt. Nur bei Benutzerstammsätzen, denen keine Sicherheitsrichtlinie zugeordnet worden ist, bleiben die bisherigen Systemparameter wirksam.

Tabelle 14 Systemparameter

Parameter-Name	Begründung	Vorschlag	Default
login/disable_multi_gui_login	Der Parameter steuert, ob sich ein Benutzer mehrfach am SAP-System anmelden darf. Im Standard ist die Mehrfachanmeldung am System gestattet (Wert = 0). Es wird empfohlen, die Mehrfachanmeldung zu untersagen (Wert = 1). Die Mehrfachanmeldung eines Benutzers an unterschiedlichen Geräten wird unterbunden. Dies reduziert die Möglichkeit, dass Änderungen am System durch einen nicht eindeutig identifizierten Benutzer möglich sind. Ebenso wird so eine vergessene Anmeldung bei Anmeldung an einem anderen Arbeitsplatz automatisch beendet und kann nicht mehr missbräuchlich verwendet werden.	1	0
login/multi_login_users	Wenn der Parameter Mehrfachanmeldung auf den Wert 1 gesetzt wurde und damit allgemein die Mehrfachanmeldung deaktiviert wurde, kann man über diesen Parameter Benutzer (z. B. Administrator:innen) benennen, die sich mehrfach am System anmelden können. Die Anmeldenamen sind durch Komma („,“) getrennt aufzulisten.	„BASISADMIN“	

Parameter-Name	Begründung	Vorschlag	Default
login/failed_user_auto_unlock	Mithilfe dieses Parameters wird gesteuert, ob die Kennwortsperre nur am gleichen Tag, an dem sie gesetzt wurde, gültig sein soll (damit begrenzt man die Sperrung auf maximal 24 Stunden). Ein automatisches Entsperren von Benutzern ohne aktiven Eingriff durch eine Administratorin / einen Administrator kann einen Brute-Force-Angriff möglich machen.	0	0
login/fails_to_session_end	Anzahl der Falschanmeldungen, die mit einem Benutzerstamm gemacht werden können, bis das Anmeldeverfahren abgebrochen wird. Verhinderung eines Brute-Force-Angriffs.	3	3
login/fails_to_user_lock	Anzahl der Falschanmeldungen, die mit einem Benutzerstamm gemacht werden können, bis der Benutzer gesperrt wird. Dies dient der Verhinderung eines Brute-Force-Angriffs.	3	3
login/min_password_diff	Mit diesem Parameter kann die Administratorin / der Administrator festlegen, in wie vielen Zeichen sich ein neues Passwort vom alten mindestens unterscheiden muss, wenn der Benutzer sein Passwort ändert. Das Passwort sollte sich mindestens in drei Stellen unterscheiden, um die Ähnlichkeit zu vorherigen Passwörtern zu verringern.	3	1
login/min_password_digits	Dieser Parameter bestimmt die minimale Anzahl von Ziffern (0–9). Es sollte mindestens eine Zahl im Passwort verwendet werden.	1	1
login/min_password_letters	Dieser Parameter bestimmt die minimale Anzahl von Buchstaben (a–z, A–Z). Es sollten mindestens zwei Buchstaben im Passwort verwendet werden.	2	1
login/min_password_lng	Passwortlänge sollte mindestens zehn Zeichen betragen.	10	10
login/min_password_lowercase	Mit diesem Parameter wird festgelegt, wie groß die minimale Anzahl von Kleinbuchstaben (a–z) im Kennwort sein muss. Es sollte mindestens ein Kleinbuchstabe enthalten sein.	1	1

Parameter-Name	Begründung	Vorschlag	Default
login/min_password_specials	Dieser Parameter bestimmt die minimale Anzahl von Sonderzeichen, die im Passwort enthalten sein müssen. Als Sonderzeichen werden alle Zeichen betrachtet, die - weder Ziffern (0–9) - noch die ASCII-Buchstaben A–Z bzw. a–z sind. Hierzu gehören nationale Sonderzeichen und Unicode-Zeichen (sofern es sich um ein Unicode-System handelt) ebenso wie die ASCII-Zeichen: !"@ $%&/()=?`*+~#-_.,;:{[]}\<> Die möglichen Sonderzeichen sind auch abhängig von den Parametereinstellungen des folgenden Parameter: login/password_charset und login/password_downwards_compatibility Es sollte mindestens ein Sonderzeichen verwendet werden.	1	0
login/min_password_uppercase	Mit diesem Parameter wird festgelegt, wie groß die minimale Anzahl von Großbuchstaben (A–Z) im Kennwort sein muss. Es sollte mindestens ein Großbuchstabe verwendet werden.	1	1
login/password_change_waittime	Mit diesem Parameter kann festgelegt werden, nach welcher Zeitspanne (gemessen in Tagen) ein Benutzer sein Produktivkennwort erneut ändern kann.	1	1
login/password_charset	Vorausetzung: Prüfung auf den Parameter erfolgt nur unter der Voraussetzung, dass der Systemparameter login/password_downwards_compatibility auf den Wert 5 gesetzt ist. Andernfalls verhält sich das System so, als würde der Parameter auf dem Wert 2 stehen. Dieser Parameter bestimmt die Zeichenmenge, aus deren Zeichen sich ein Kennwort zusammensetzen darf: Wert 0: Das Kennwort darf nur aus Ziffern, Buchstaben und den folgenden 32 (ASCII-)Sonderzeichen bestehen: !"@ $%&/()=?`*+~#-_.,;:{[]}\<>| Wert 1: Das Kennwort darf aus beliebigen Zeichen einschließlich nationaler Sonderzeichen (z. B. aus ISO Latin-1, 8859-1) bestehen; allerdings werden alle Zeichen, die nicht in der oben (bei login/password_charset = 0) genannten Menge enthalten sind, auf das gleiche (Sonder-) Zeichen abgebildet und werden daher nicht unterschieden. Dieser Wert ist der Vorgabewert (abwärtskompatibel). Wert 2: Das Kennwort darf aus beliebigen Zeichen bestehen; es wird intern in das Unicode-Format UTF-8 konvertiert. Sofern Sie kein Unicode-taugliches System einsetzen, sollten Sie aber beachten, dass u. U. nicht alle Zeichen auf dem Anmeldebild eingegeben werden können (Restriktion aufgrund der durch die Systemsprache vorgegebenen Codepage => siehe Hinweis 735356). Der Systemparameter sollte daher nur dann auf den Wert 2 gesetzt werden, wenn sichergestellt werden kann, dass alle beteiligten Systeme die neue Kennwortkodierung unterstützen.	2	1

Parameter-Name	Begründung	Vorschlag	Default
login/password_ compliance_to_current_ policy	Bei einer kennwortbasierten Anmeldung wird geprüft, ob das verwendete Kennwort den aktuellen Kennwortregeln genügt und ob, falls erforderlich, der Benutzer zur Änderung des Kennworts aufgefordert werden soll.	1	1
login/password_ downwards_compatibility	Abwärtskompatibilität von Kennwörtern	0	0
login/password_ expiration_time	Gültigkeitsdauer von Kennwörtern (in Tagen). Da immer wieder Passwortlisten veröffentlicht werden und die Nutzenden häufig dieselben Passwörter verwenden, ist die regelmäßige Änderung erforderlich. Das SAP-System ist eine Einzelanwendung; generell sollte man sich hier an die Vorgaben der Betriebssystemanmeldung (Domänen-Passwort) orientieren. Eine zu strenge Passwort-Politik mit zu häufigen Passwort-Änderungen führt bei den Nutzenden zu trivialen Passwörtern und reduziert die Sicherheit, statt sie zu erhöhen. Aufgrund der Nutzung von Single-Sign-On (SSO) kann es möglich sein, dass der Parameter keinen praktischen Nutzen hat.	90	0
login/password_hash_ algorithm	Bei der Berechnung neuer Kennwort-Hash-Werte wird dieser Profilparameter ausgewertet, um das Hash-Verfahren und das Kodierungsformat zu bestimmen. Hierzu ist die SAP Note https://launchpad.support.sap.com/#/notes/991968 zu beachten, da hier durch den technologischen Fortschritt Hashwerte, die durch ein schwaches Verfahren generiert wurden, zurückgerechnet werden können.	encoding=RFC2307, algorithm=iSSHA-1, iterations=1024, saltsize=96	encoding=RFC2307, algorithm=iSSHA-1, iterations=1024, saltsize=96
login/password_history_ size	Dieser Parameter regelt die Größe der Kennworthistorie. In dieser wird eine durch den Parameterwert festgelegte Anzahl von Kennwörtern gespeichert. Die Kennworthistorie sollte mindestens 15 Kennwörter betragen (bei einem Wechsel, der alle 90 Tage erzwungen wird).	15	5
login/password_max_ idle_initial	Wenn die Benutzeradministratorin / der Benutzeradministrator ein neues Benutzerkonto einrichtet oder das Kennwort eines bestehenden Benutzerkontos auf einen neuen Wert setzt, muss der Benutzer dieses sogenannte Initialkennwort bei der nächsten Anmeldung ändern (um sicherzustellen, dass das Kennwort nur dem Benutzer selbst bekannt ist). Mit diesem Parameter kann die maximale Zeitspanne zwischen dem Zeitpunkt der Kennwortsetzung bzw. der Kennwortrücksetzung und der ersten Anmeldung festgelegt werden. Nach Ablauf dieser Frist wird die Meldung „Das Initialpasswort ist abgelaufen“ ausgegeben und die Anmeldung abgelehnt. Nach dem initialen Zuweisen sollte maximal nach drei Tagen eine Änderung erfolgt sein.	3	0

Parameter-Name	Begründung	Vorschlag	Default
login/password_max_idle_productive	Bei einer Kennwortänderung durch den Benutzer entsteht ein sogenanntes Produktivkennwort. Mit diesem Parameter kann die maximale Zeitspanne eingestellt werden, in der sich ein Benutzer mit ihrem/seinem Produktivkennwort manuell anmelden muss. Eine Anmeldung mittels Single-Sign-on wird vom System nicht als manuelle Anmeldung mithilfe des Produktivkennworts gewertet und setzt den Zähler dementsprechend nicht zurück. Nach Ablauf dieser Frist wird die Meldung „Das Initialkennwort ist abgelaufen“ ausgegeben, und die Anmeldung wird abgelehnt. Die Gültigkeitsdauer der von dem Benutzer verwendeten Kennwörter sollte +1 Tag vor dem geforderten Kennwortwechsel sein.	91	0
login/show_detailed_errors	Der Parameter steuert, ob der Benutzer nach einer gescheiterten Anmeldung bei seiner nächsten Anmeldung eine detaillierte Fehlermeldung angezeigt bekommt. Diese detaillierten Informationen kann ein potenzieller Angreifer verwenden. Aus diesem Grund wird empfohlen, den Parameterwert auf 0 zu setzen = nur allgemeine Fehlermeldung.	0	1
login/system_client	Mit diesem Systemparameter wird festgelegt, welche Mandant:in / welcher Mandant bei der Anmeldung als Systemstandardmandant:in vorgeschlagen wird. Der/Die vorgeschlagene Systemstandardmandant:in kann durch den Benutzer überschrieben werden und sollte auf den aktuellen bzw. meist genutzten Mandanten / die aktuelle bzw. meist genutzte Mandantin eingestellt sein, um unnötige Falschanmeldungen zu verhindern.	Kund:innen-Wert	000
login/update_logon_timestamp	Bei jeder Anmeldung kann ein Zeitstempel (Datum/Uhrzeit) erzeugt werden, wobei im Standard nur die Anmeldezeit minutengenau erfasst wird. Bei besonders kritischen Systemen und der nötigen Performance sollte man den Wert s einstellen (sekundengenaue Erfassung).	m	m
login/password_change_for_SSO	Bei nicht kennwortbasierten Anmeldevarianten (SSO: SNC, X.509, PAS, Anmeldeticket) wurde bislang nicht überprüft, ob der Benutzer ein Kennwort besitzt, welches geändert werden müsste (mögliche Gründe: Kennwort ist initial oder abgelaufen). Mit diesem Parameter lässt sich das gewünschte Systemverhalten wie folgt festlegen: Wert 0: Kennwortänderungspflicht wird ignoriert (=> abwärtskompatibel) Wert 1: Pop-up mit Auswahl 2 oder 3 (Benutzer entscheidet, Default) Wert 2: nur Kennwortänderungsdialog (Eingabe: altes und neues Kennwort) Wert 3: Deaktivierung des Kennworts (automatisch, kein Pop-up)	1	1

Parameter-Name	Begründung	Vorschlag	Default
login/server_logon_ restriction	Der Parameter ermöglicht es, die Anmeldung von Benutzern am Applikations-Server zu verhindern. Der/Die Benutzer-Administrator:in legt fest, ob alle Benutzer blockiert werden sollen oder nur einer bestimmten Benutzergruppe die Anmeldung erlaubt ist. Es besteht zudem die Möglichkeit, nur den Benutzern die Anmeldung zu erlauben, die eine bestimmte Sicherheitsrichtlinieneinstellung haben. Bereits angemeldete Benutzer sind davon nicht betroffen. Die eingeschränkte Anmeldung ist hilfreich, wenn Benutzer während einer Systemwartung ausgesperrt werden sollen. Wert=0 Alle Benutzer können sich am System anmelden (default). Wert=1 Nur bestimmte Benutzer sollen auf das System zugreifen. Wert=2 Es soll kein Benutzer auf das System zugreifen. Wert=3 Der externe Zugriff von Benutzern auf das System soll eingeschränkt werden. Wert=4 Der externe Zugriff von Benutzern auf das System soll unterbunden werden. Beim Wert 1 und 3 ist den jeweiligen Benutzern das Sicherheitsattribut server_logon_privilege mit dem Wert =1 über eine entsprechende Sicherheits-Policy zuzuordnen, um eine Anmeldung zu gewährleisten.	0	0
rdisp/gui_auto_logout	Mit diesem Parameter kann die automatische Abmeldung eines Benutzers ausgelöst werden, wenn diese/dieser für einen längeren Zeitraum keine Aktivitäten am System durchgeführt hat. Allerdings werden damit alle laufenden Arbeiten des Benutzers abgebrochen. Dadurch können unter anderem erfasste und noch nicht gesicherte Daten verloren gehen. Der Parameter ist mit einem Wert in Sekunden zu füllen, wobei der Wert 0 für eine Deaktivierung des automatischen Ausloggens steht. Es wird eine Aktivierungszeit von 8 Stunden (Wert 28800) empfohlen, wobei in diesem Fall darauf zu achten ist, dass bei einer Inaktivität von max. 15 Minuten der Desktop automatisch gesperrt wird.	28800	0
login/no_automatic_user _sapstar	Mithilfe dieses Parameters können die Eigenschaften des Standardbenutzers SAP* definiert werden. Ist für diesen Parameter der Wert „0“ gesetzt, ist es möglich, wenn der Benutzerstammsatz des Benutzers SAP* gelöscht wird, eine Neuanmeldung mit SAP* und Initialpasswort PASS durchzuführen. SAP* hat dann folgende Eigenschaften: - Der Benutzer verfügt über sämtliche Berechtigungen, da keine Berechtigungsprüfungen durchgeführt werden. - Das Standardpasswort PASS kann nicht geändert werden. Es wird empfohlen, dem Standardbenutzer die Sonderrechte zu entziehen (Wert=1) und das Standardpasswort zu ändern.	1	0

Parameter-Name	Begründung	Vorschlag	Default
rsau/enable	Mit diesem Parameter kann das Security Audit Log aktiviert werden (Wert=1). Im Standard ist das Security Audit Log deaktiviert (Wert=0). Aus Sicht der Revision sollte das Security Audit Log aktiv sein. In dem Auditprofil müssen die zu überwachenden Benutzer und die zu überwachenden Aktivitäten gepflegt werden (Transaktion RSAU_CONFIG). Die Auswertung des Security Audit Log erfolgt über die Transaktion RSAU_READ_LOG. Die maximale Größe des Security Audit Log erfolgt über den Parameter rsau/max_diskspace/local und sollte mindestens 1.000.000 Bytes betragen.	1	0
zcsa/installed_ languages	Der Parameter definiert die Sprachen, für die eine Anmeldung auf dem Applikations-Server erlaubt ist. Damit sich Benutzer zum Beispiel in deutscher und französischer Sprache anmelden können, ist die Parametereinstellung DF notwendig. Mögliche Parameterwerte sind sämtliche Sprachkürzel. Standard: Anmeldesprache: Deutsch und Englisch	DE	DE
zcsa/system_language	Der Parameter definiert die Standard-Anmeldesprache für einen Applikations-Server. Mit dieser Parametereinstellung wird auch die Sprache des Log-on-Screen festgelegt. Die Standard-Anmeldesprache muss im Parameter „Mögliche Anmeldesprachen“ zcsa/installed_languages enthalten sein.	D	D

Sicherheitsrichtlinien und Sicherheitsattribute (SECPOL)

Sicherheitsrichtlinie

Eine Sicherheitsrichtlinie ist eine Sammlung von Sicherheitsrichtlinienattributen und deren Werten.

Dieses Verfahren löst die Verhaltensdefinition mittels Systemparametern ab, sobald dem Benutzerstammsatz eine Sicherheitsrichtlinie zugeordnet worden ist. Ab diesem Zeitpunkt bestimmen die Sicherheitsrichtlinienattribute das gewünschte Verhalten. Systemparameterwerte sind somit nur noch für jene Benutzerstammsätze von Relevanz, denen keine Sicherheitsrichtlinie zugeordnet worden ist.

Systemparameter, die nicht durch ein Sicherheitsrichtlinienattribut ersetzt werden, behalten weiter ihre Funktion.

Sicherheitsrichtlinienattribute

Zu jeder Sicherheitsrichtlinie gehört eine Anzahl von Sicherheitsrichtlinienattributen; über sie lässt sich folgendes Verhalten steuern:

- Kennwortregeln
- Kennwortänderungen
- Anmelderestriktionen

Eine Beschreibung der einzelnen Sicherheitsattribute kann auch durch das Auswählen eines Attributs und den anschließenden Aufruf der Wertehilfe im System direkt erfolgen.

Definition der Sicherheitsattribute für Sicherheitsrichtlinien:

Tabelle 15 Sicherheitsattribute

Sicherheitsattribute	Beschreibung	Vorschlag	Default
CHECK_PASSWORD_ BLACKLIST	**Prüfung auf die Verwendung „verbotener Kennwörter“** Einen Bestandteil der Kennwortregeln stellt die Prüfung dar, ob das Kennwort in einer Negativliste („verbotene Kennwörter“) vorhanden ist. Über dieses Sicherheitsrichtlinienattribut lässt sich festlegen, ob eine solche Prüfung erfolgen soll. Wert = 0, es findet keine Auswertung der Negativliste statt. Wert = 1, Tabelle USR40, „verbotene Kennwörter“ wird ausgewertet.	1	1
MIN_PASSWORD_ LENGTH	**Mindest-Passwort Gesamtlänge** Dieses Sicherheitsrichtlinienattribut bestimmt die minimale Länge eines Kennworts. Es wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen bestehender Kennwörter. Dieses Sicherheitsattribut ersetzt den Systemparameter: login/min_password_lng	10	10
MIN_PASSWORD_ DIGITS	**Mindestanzahl von Ziffern im Passwort** Dieses Sicherheitsrichtlinienattribut bestimmt die minimale Anzahl von Ziffern (0–9), die in einem Kennwort enthalten sein müssen. Es wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen bestehender Kennwörter. Dieses Sicherheitsattribut ersetzt den Systemparameter: login/min_password_digits	1	1
MIN_PASSWORD_ LETTERS	**Mindestanzahl von Buchstaben im Passwort** Dieses Sicherheitsrichtlinienattribut bestimmt die minimale Anzahl von ASCII-Buchstaben (A–Z und a–z), die in einem Kennwort enthalten sein müssen. Es wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen bestehender Kennwörter. Dieses Sicherheitsattribut ersetzt den Systemparameter: login/min_password_letters	1	1
MIN_PASSWORD_ LOWERCASE	**Mindestanzahl von Kleinbuchstaben im Passwort** Dieses Sicherheitsrichtlinienattribut bestimmt die minimale Anzahl von ASCII-Kleinbuchstaben (a–z), die in einem Kennwort enthalten sein müssen. Es wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen bestehender Kennwörter.	1	1

Sicherheitsattribute	Beschreibung	Vorschlag	Default
	Dieses Sicherheitsattribut ersetzt den Systemparameter: login/min_password_lowercase		
MIN_PASSWORD_ UPPERCASE	**Mindestanzahl von Großbuchstaben im Passwort** Dieses Sicherheitsrichtlinienattribut bestimmt die minimale Anzahl von ASCII-Großbuchstaben (A–Z), die in einem Kennwort enthalten sein müssen. Es wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen bestehender Kennwörter. Dieses Sicherheitsattribut ersetzt den Systemparameter: login/min_password_uppercase	1	1
MIN_PASSWORD_ SPECIALS	**Mindestanzahl von Sonderzeichen im Passwort** Dieses Sicherheitsrichtlinienattribut bestimmt die minimale Anzahl von Sonderzeichen, die in einem Kennwort enthalten sein müssen. Es wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen bestehender Kennwörter. Dieses Sicherheitsattribut ersetzt den Systemparameter: login/min_password_specials	1	0
MIN_PASSWORD_ DIFFERENCE	**Mindestanzahl unterschiedlicher Zeichen bei einem neuen Passwort** Dieses Sicherheitsrichtlinienattribut bestimmt die minimale Anzahl an Zeichenunterschieden zum vorherigen Passwort. Dieses Sicherheitsrichtlinienattribut ersetzt den Systemparameter: login/min_password_diff	3	3
PASSWORD_HISTORY_ SIZE	**Vorhalten vorangegangener Passwörter** Dieses Sicherheitsrichtlinienattribut legt die Größe der Kennworthistorie fest. Die Kennworthistorie wird ausgewertet, wenn ein Benutzer ein neues Kennwort wählt. Von der Administratorin / Vom Administrator vergebene Kennwörter werden nicht in der Kennworthistorie gespeichert. Dieses Sicherheitsrichtlinienattribut ersetzt den Systemparameter: login/password_history_size	15	15
PASSWORD_ COMPLIANCE_TO_ CURRENT_POLICY	**Kennwortänderung nach Regelanpassung** Dieses Sicherheitsrichtlinienattribut steuert, ob das System bei einer kennwortbasierten Anmeldung prüfen soll, ob das verwendete Kennwort den aktuellen Kennwortregeln genügt und ob der Benutzer zur Änderung des Kennworts aufgefordert werden soll. Benutzer vom Typ „SERVICE“ und „SYSTEM“ sind prinzipiell von der Kennwortänderungspflicht ausgenommen und daher nicht von dieser Regelung betroffen. 0 = Keine Prüfung. 1 = Prüfung, ob das aktuelle Kennwort den neuen Regeln	1	0

Sicherheitsattribute	Beschreibung	Vorschlag	Default
	entspricht. Dieses Sicherheitsrichtlinienattribut ersetzt den Systemparameter: login/password_compliance_to_current_policy		
PASSWORD_CHANGE_FOR_SSO	**Kennwortänderungspflicht bei Single-Sign-on-Anmeldungen** Bei nicht kennwortbasierten Anmeldeverfahren wurde bislang nicht überprüft, ob der Benutzer ein Kennwort besitzt, welches sie/er ändern müsste. Mit diesem Sicherheitsrichtlinienattribut lässt sich das gewünschte Systemverhalten festlegen. 0 = Kennwortänderungspflicht wird ignoriert (abwärtskompatibel) 1 = Benutzer entscheidet: Ändern oder Löschen (Standardeinstellung) 2 = Benutzer muss das Kennwort ändern 3 = Das Kennwort wird automatisch gelöscht Dieses Sicherheitsrichtlinienattribut ersetzt den Systemparameter: login/password_change_for_SSO	1	1
PASSWORD_CHANGE_INTERVAL	**Intervall regelmäßig. Kennwortänderungen** Dieses Sicherheitsrichtlinienattribut legt fest, ob bzw. nach wie vielen Tagen (seit der letzten Kennwortänderung) Benutzer aufgefordert werden sollen, erneut ihr Kennwort zu ändern. Bei der Vergabe des Wertes 0 läuft das Kennwort nicht ab und der/die Anwendende wird entsprechend nicht zur Änderung des Produktivkennworts aufgefordert. Dieses Sicherheitsrichtlinienattribut ersetzt den Systemparameter: login/password_expiration_time	90	0
MIN_PASSWORD_CHANGE_WAITTIME	**Minimale Wartezeit bei Kennwortänderung** Dieses Sicherheitsrichtlinienattribut legt fest, nach welcher Zeitspanne (gemessen in Tagen) ein Benutzer sein Kennwort erneut ändern kann. Nur Kennwortänderungen, die der Benutzer veranlasst hat, werden in Betracht gezogen. Dieses Sicherheitsattribut ersetzt den Systemparameter: login/password_change_waittime	1	1
MAX_PASSWORD_IDLE_INITIAL	**Maximale Gültigkeit für Initialkennwörter** Dieses Sicherheitsrichtlinienattribut kann die maximale Zeitspanne (gemessen in Tagen) zwischen dem Zeitpunkt der Kennwortrücksetzung und der nächsten Anmeldung mit dem Initialkennwort festlegen. Wenn die Benutzeradministratorin / der Benutzeradministrator ein neues Benutzerkonto einrichtet oder das Kennwort eines bestehenden Benutzerkontos auf einen neuen Wert setzt, so muss der Benutzer dieses sogenannte Initialkennwort bei der nächsten interaktiven Anmeldung ändern. Nach Ablauf dieser Frist wird die Meldung „Das Initialkennwort ist abgelaufen“ ausgegeben und die Anmeldung abgelehnt. 0 = Initialkennwörter sind unbegrenzt gültig	3	0

Sicherheitsattribute	Beschreibung	Vorschlag	Default
	Dieses Sicherheitsrichtlinienattribut ersetzt den Systemparameter: login/password_max_idle_initial		
MAX_PASSWORD_IDLE_PRODUCTIVE	**Gültigkeit ungenutzter Produktivkennwörter** Mit diesem Sicherheitsrichtlinienattribut kann die maximale Zeitspanne zwischen dem Zeitpunkt der letzten Kennwortänderung und der nächsten Anmeldung mit diesem Kennwort festgelegt werden. Nur Kennwortänderungen, die der Benutzer veranlasst hat, werden in Betracht gezogen (nicht durch den Administrator / die Administratorin). Nach Ablauf dieser Frist wird die Meldung „Kennwort wurde längere Zeit nicht verwendet und daher deaktiviert“ ausgegeben, und die Anmeldung wird abgelehnt. 0 = Produktivkennwort ist unbegrenzt gültig Dieses Sicherheitsrichtlinienattribut ersetzt den Systemparameter: login/password_max_idle_productive	30	0
MAX_FAILED_PASSWORD_LOGON_ATTEMPTS	**Maximale Anzahl von fehlgeschlagenen Anmeldeversuchen** Dieses Sicherheitsrichtlinienattribut setzt die festgelegte Obergrenze an maximalen Anmeldeversuchen. Nach dem Überschreiten wird eine Kennwortsperre gesetzt. Dieses Sicherheitsrichtlinienattribut ersetzt den Systemparameter: login/fails_to_user_lock	5	5
PASSWORD_LOCK_EXPIRATION	**Automatische Entsperrung von Benutzern** Dieses Sicherheitsrichtlinienattribut legt die maximale Gültigkeitsdauer für Kennwortsperren fest. Normalerweise bleibt eine Kennwortsperre unbegrenzt lange bestehen und muss manuell aufgehoben werden. Es ist aber auch möglich, eine automatische Entsperrung des Benutzerkontos festzulegen. 0 = Kennwortsperre muss explizit aufgehoben werden 1 = Kennwortsperre gilt maximal 24 Stunden (automatische Entsperrung) Dieses Sicherheitsrichtlinienattribut ersetzt den Systemparameter: login/failed_user_auto_unlock	0	0
DISABLE_PASSWORD_LOGON	**Kennwortanmeldung unterbinden** Dieses Sicherheitsrichtlinienattribut verhindert eine Anmeldung am System via Passwort. 0 = Kennwortanmeldung ist zulässig (sofern möglich) 1 = Kennwortanmeldung wird unterbunden (d. h. ist nicht möglich) Dieses Sicherheitsrichtlinienattribut ersetzt die Systemparameter login/disable_password_logon und login/password_logon_usergroup	0	0
DISABLE_TICKET_LOGON	**Ticketanmeldung unterbinden** Dieses Sicherheitsrichtlinienattribut unterbindet, dass sich ein Benutzer mittels Anmeldeticket bzw. Zusicherungsticket am System anmelden kann.	0	0

Sicherheitsattribute	Beschreibung	Vorschlag	Default
	0 = Ticketanmeldung ist zulässig (sofern möglich) 1 = Anmeldetickets werden abgelehnt (Zusicherungstickets sind nicht betroffen) 2 = Sowohl Anmelde- als auch Zusicherungstickets werden abgelehnt Abhängigkeiten Ob sich ein Benutzer mittels Anmeldeticket bzw. Zusicherungsticket am System anmelden kann, hängt von weiteren Faktoren ab: – Der Parameter login/accept_sso2_ticket muss auf den Wert 1 gesetzt sein – Vertrauensbeziehung zum ticketausstellenden System muss etabliert sein – Das Ticket muss innerhalb der Gültigkeitsdauer empfangen worden sein		
SERVER_LOGON_ PRIVILEGE	**Eingeschränkte Anmeldung an den SAP NetWeaver Application Server** Dieses Sicherheitsrichtlinienattribut ist nur relevant, wenn der Wert des dazugehörigen Systemparameters (SERVER_LOGON_RESTRICTION) auf 1 oder 3 steht. In diesen Fällen haben nur Benutzer Zugriff auf das System, die dieses Attribut mit dem Wert 1 zugeordnet haben. Standardmäßig ist kein Privileg vergeben (also: Wert = 0).	0	0
MIN_TOTP_ PASSPHRASE_LENGHT	**Mindestlänge des TOTP-Geheimnisses** Legt die Mindestlänge der Kennphrase fest, die zum Personalisieren des Geräts verwendet wird, die Benutzer zum Generieren von TOTP verwenden.	10	4
SESSION_MEMORY_ LIMIT_EXEMPTION	**Nutzende Speicherzuweisung** Über den Profilparameter em/sessionmem_ext wird der Prozentsatz eines Speicherzuschlags festgelegt, den ein Benutzer erhalten kann. Durch Zuweisung einer Sicherheitsrichtlinie wird einem Benutzer dieser Speicherzuschlag erteilt. Wertebereich des Attributs SESSION_MEMORY_LIMIT_EXEMPTION: 0 = Kein Speicherzuschlag (em/sessionmem_ext hat keinen Effekt) 1 = Sonderrecht: Speicherzuschlag (em/sessionmem_ext) wird erteilt	0	0
TENANT_RUNLEVEL_ LOGON_PRIVILEG	**Anmeldung bei jedem Tenant-Runlevel** Die Mehr-Mandant:innen-Fähigkeit (Multi-Tenancy) ermöglicht die gemeinsame Nutzung eines einzelnen SAP-Systems durch verschiedene Kund:innen (organisatorisch eigenständige Einheiten). Das Runlevel-Konzept erlaubt es, einzelne Tenants stufenweise zu starten und anzuhalten, um sie beispielsweise auf andere Systeme verschieben zu können. 0 = keine Sonderbehandlung bez. des Tenant-Runlevels 1 = Sonderrecht: Anmeldung bei jedem Tenant-Runlevel > 0	0	0

6.6 Prüfprogramm: Autorisierung

Tabelle 16 Prüfprogramm: Autorisierung

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
1.	**Dokumentation und Standards**
	Kontrollziel: Die für Benutzer und Berechtigungen vorliegenden Dokumentationen und Standards ermöglichen es den am Prozess Beteiligten, die korrespondierenden Strukturen, die Prozesse und die Organisation sowie die hierbei zu beachtenden Vorgaben in angemessener Zeit nachzuvollziehen. **Risiko:** Durch fehlende, unvollständige oder unverständliche Dokumentation können die Beteiligten die Benutzer und Berechtigungen und ihre eigenen Aufgaben im Prozess nicht verstehen. Daraus ergeben sich Risiken für eine unsachgemäße Pflege und Vergabe der Rollen.
1.1.	**Platzhalter Dokumentation und Standards:** *Sind alle im Prüfprogramm in Kapitel 4.5 Dokumentation und Standards enthaltenen, im S/4HANA-*OnPremise*-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Dokumentation und Standards vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das S/4HANA-OnPremise-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag. Berücksichtigung der nachfolgenden Hinweise zu Rollen und Berechtigungen und Benutzer und Rechte.
1.2.	**Rollen und Berechtigungen:** Hinweis: Die dokumentierten Standards für Rollen und Berechtigungen müssen mindestens die an Anwendende vergebenen Kund:innen-eigenen SAP-Einzel- und Sammelrollen sowie Berechtigungsobjekte in Kombination mit den im System verfügbaren Informationen nachvollziehbar machen. Sammel- und Einzelrollen finden sich über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Rollen > Rollen nach komplexen Selektionskriterien > Rollen nach komplexen Selektionskriterien oder die Tabellen AGR_DEFINE, ggf. ergänzt um Texte aus der AGR_TEXTS, Berechtigungsobjekte über Werkzeuge > Administration >

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Benutzerpflege > Infosystem > Berechtigungsobjekte > Berechtigungsobjekte nach komplexen Selektionskriterien oder Tabelle TOBJ, ggf. ergänzt um Texte aus der TOBJT.
1.3.	**Benutzer und Rechte:** Hinweis: Auch hier ist es sinnvoll, sich einen Überblick über die Benutzer und deren organisatorische Einordnung und ihre Klassifizierungen zu verschaffen. Eine Aufstellung der Benutzer mit allen Attributen findet sich über Werkzeuge > Administration > Benutzerpflege > Infosystem > Benutzer > Benutzer nach komplexen Selektionskriterien > Benutzer nach komplexen Selektionskriterien. Eine Liste der Benutzergruppen findet sich über Transaktion SUGR oder die Tabelle USGRP. Interessante Felder sind insbesondere Typ von Benutzern, Gruppe von Benutzern, Abteilung, Kostenstelle, Firma.
1.4.	**Protokollierung:** Hinweis: Die Vorgaben zur Protokollierung beziehen sich im Kontext eines S/4-Systems zu Benutzern und Berechtigungen überwiegend auf die Einrichtung und Überwachung des Security Audit Logs (SAL). Insofern müssen die dokumentierten Standards Hinweise auf die Vorgaben und Prozesse zur Einrichtung des SAL über die Transaktion RSAU_CONFIG_SHOW (alter T-Code SM19) und die Auswertung und Nachverfolgung der protokollierten Ereignisse über die Transaktion RSAU_READ_LOG (alter T-Code SM20) geben; sollte es sich um archivierte Elemente handeln, kann dies über RSAU_READ_ARC erfolgen. Ebenso ist es möglich, das aktuelle Profil über die Transaktion RSAU_TRANSFER als Datei zu sichern.
2.	**Benutzer und Rechte**
	Kontrollziel: Die Vorgaben für Benutzer und die Zuordnung von Rollen und Berechtigungen und deren Umsetzung sorgen für eine vollständige Nachvollziehbarkeit der Rollen und ggf. Berechtigungen und deren Zuordnung zu Benutzern und Identitäten. **Risiko:** Bei fehlender Nachvollziehbarkeit auf einer oder mehreren Ebenen eines Benutzer- und Berechtigungskonzepts ergeben sich automatisch

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Mängel im Minimal- und Funktionstrennungsprinzip und damit eine Gefährdung der Integrität, Verfügbarkeit und Vertraulichkeit von Daten.
2.1.	**Platzhalter Benutzer und Rechte:** *Sind alle im Prüfprogramm in Kapitel 4.5 Dokumentation und Standards enthaltenen, im S/4HANA-OnPremise-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Benutzer und Rechte vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das S/4HANA-OnPremise-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag. Berücksichtigung der nachfolgenden Hinweise zu Benutzern und Rechten.
a)	Benutzerklassifizierung
2.2.	**Typen von Benutzern:** *Liegt eine strukturierte und vollständige Definition aller in den SAP-Systemen eines Unternehmens relevanten Typen von Benutzern vor?* In SAP S/4HANA OnPremise werden Benutzer bei der Anlage einem der standardmäßig verfügbaren Typen von Benutzern über den Pfad Werkzeuge > Administration > Benutzerpflege > Transaktion SU01 Benutzer im Reiter Logondaten im Feld Benutzertyp (Dialog, System, Kommunikation, Service, Referenz) zugeordnet. Eine Übersicht der Typen aller Benutzer findet sich über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Benutzer > Transaktion S_BCE_68001400 Benutzer nach komplexen Selektionskriterien entweder über einen Filter im Reiter Logondaten > Benutzertyp oder in der Ergebnisliste in der Spalte Typ > Benutzertyp. Prüfung, ob die zumindest aktiven Benutzer zutreffend dem richtigen Benutzertyp gem. der Definition in der Berechtigungsdokumentation zugeordnet sind.
2.3.	**Gruppe von Benutzern allgemein:** *Werden Benutzer vollständig Benutzergruppen zugeordnet, die eine angemessene Differenzierung nach unterschiedlichen Vertragsverhältnissen der Benutzer und damit eine Beurteilung ihrer zugeordneten Berechtigungen unterstützen?* In SAP S/4HANA OnPremise können Gruppen von Benutzern frei über den Pfad Werkzeuge > Administration > Benutzerpflege > Transaktion SUGR > Benutzergruppen gepflegt werden (Tabelle USGRP) und über den Pfad

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Werkzeuge > Administration > Benutzerpflege > SU01 > Benutzer im Reiter Logondaten im Feld Benutzergruppen einer Benutzergruppe (Tabelle USR02 Feld CLASS) oder im Reiter Gruppen mehreren weiteren Benutzergruppen (Tabelle USGRP_USER Feld USERGROUP) zugeordnet werden. Nur das Feld im Reiter Logondaten beeinflusst die Berechtigungsprüfung für die Administration von Benutzern über Gruppen von Benutzern. Eine Übersicht der Gruppen aller Benutzer findet sich über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Benutzer > Transaktion S_BCE_68001400 Benutzer nach komplexen Selektionskriterien über die Filter „Gruppe für Berechtigung“ oder „Benutzergruppe (allgemein)“. Prüfung, ob die zumindest aktiven Benutzer zutreffend einer zutreffenden Gruppe von Benutzern gem. der Definition in der Berechtigungsdokumentation zugeordnet sind.
2.4	**Benutzergruppen Berechtigungen:** *Werden Benutzergruppen für die Berechtigungsprüfung verwendet, die angemessen zur Funktionstrennung genutzt werden können?* Die Benutzergruppen für die Differenzierung des Zugriffs für die Benutzeradministration werden nur über das Feld Benutzergruppen im Reiter Logondaten gepflegt. Hierbei sollte zumindest eine Administration der eigenen Benutzer der Benutzeradministrator:innen über zwei Administrator:innen-Gruppen sowie zusätzlich eine Differenzierung in normale Dialogbenutzer und Sonderbenutzer erfolgen. Die Transaktionen und Tabellen können, wie bei Benutzergruppen, allgemein aber mit Einschränkung auf die berechtigungsrelevanten Benutzergruppen verwendet werden. Prüfung auf Pflege angemessener berechtigungsrelevanter Benutzergruppen und der vollständigen Zuordnung der Benutzer zu diesen Gruppen.
b)	Standardbenutzer
2.5.	**SAP-Standardbenutzer/Standardkennwörter:** *Sind in jeder/jedem Mandant:in die Standardkennwörter aller SAP-Standardbenutzer geändert?* SA38 mit Report RSUSR003. Wenn die Rolle der/des Prüfenden diesen Report nicht zulässt, muss der/die Prüfende einen/eine der zugelassenen

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Systemadministrator:innen in seinem/ihrem Beisein den Report ausführen lassen und das Ergebnis sofort prüfen.
2.6.	**SAP*/Grundschutz:** *Ist der Benutzer SAP* gegen unbefugte Nutzung geschützt?* Der Benutzer SAP* ist ein von SAP ausgelieferter Standardbenutzer, der über vollumfängliche Berechtigungen der Sammelprofile SAP_ALL und SAP_NEW verfügt. Insofern sollte dieser Benutzer umfassend durch die folgenden Maßnahmen entschärft werden: a) sämtliche Berechtigungen im Benutzerstammsatz SAP* werden entzogen, b) der Benutzerstammsatz SAP* wird gesperrt, c) Der Benutzerstammsatz SAP* wird der Gruppe SUPER zugeordnet, d) Es wird über die Setzung des Systemparameters login/ no_automatic_user_sapstar auf den Wert 1 verhindert, dass nach Löschung des Benutzers SAP* (mit Benutzerstammsatz) der systeminterne Benutzer SAP* mit dem unveränderbaren Standardkennwort PASS aufgerufen werden kann, e) für die Systemadministration wird ein Notfallbenutzer mit umfassenden Berechtigungen angelegt. Identifikation des Status über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Benutzer > Transaktion S_BCE_68001400 Benutzer nach komplexen Selektionskriterien, Selektion nach Benutzer SAP*. Prüfung auf angemessene Entschärfung des Standardbenutzers SAP* über die oben dargestellten Maßnahmen.
2.7.	**DDIC/Grundschutz:** *Ist der Benutzer DDIC gegen unbefugte Nutzung geschützt?* *Der Benutzer DDIC ist mit den vollständigen Rechten zur Verwaltung des Repository von R/3 ausgestattet. Mit diesen Rechten können mit dem Benutzer während Installations- und Release-Wechselarbeiten Änderungen am Data-Dictionary vorgenommen werden. Im Gegensatz zum SAP* hat der Benutzer DDIC währen dieser ausgewählten Phasen auch dauerhaft Relevanz. Er sollte jedoch über die folgenden Maßnahmen angemessen*

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	geschützt werden: a) der Benutzer DDIC wird in allen Systemen gesperrt, b) der Benutzer wird der Benutzergruppe SUPER zugeordnet, c) das Standardpasswort wird geändert, d) der Benutzer wird lediglich im Bedarfsfall durch die/den Benutzeradministrator:in entsperrt Identifikation des Status über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Benutzer > Transaktion S_BCE_68001400 Benutzer nach komplexen Selektionskriterien, Selektion nach den Benutzern SAP* und DDIC. Da DDIC bereits initial im SAP-System vorhanden ist, werden von Unternehmen unter diesem Anmeldenamen regelmäßig auch dauerhaft Jobs eingeplant. Dies sollte durch dafür explizit eingerichtete Technische Benutzer mit darauf zugeschnittenen Berechtigungen übernommen werden. Prüfung auf angemessenen Schutz des Standardbenutzers DDIC über die oben dargestellten Maßnahmen. Vorhergehende Prüfung auf Nutzung des DDIC für die Einplanung von Jobs.
2.8.	**SAP* und DDIC / Benutzergruppe SUPER Administration:** *Ist die Pflege der sensiblen Benutzer (insb. SUPER) nur wenigen qualifizierten Benutzer-Administrator:innen erlaubt?* Eine Prüfung auf Berechtigungen für die Benutzeradministration für Benutzer der Benutzergruppe SUPER erfolgt über die Transaktion RSUSR002 mit den Eingaben S_TCODE = SU01, S_USER_GRP (Benutzerverwaltung) mit Aktivität 01 (Anlegen), 02 (Ändern) oder „*“ und Gruppe = „*“ oder = „SUPER“. Prüfung auf restriktive Vergabe der Berechtigungen für die Benutzeradministration für die Benutzergruppe SUPER.
2.9.	**Sonstige SAP-Standardbenutzer:** Sind alle übrigen SAP-Standardbenutzer, soweit anwendbar, analog geschützt? Auch für alle übrigen von SAP und anderen Dritt-Anbietern ausgelieferten Standardbenutzern sollten dieselben Schutzmaßnahmen ergriffen werden: a) sämtliche Berechtigungen im Benutzerstammsatz werden entzogen, b) der Benutzerstammsatz wird gesperrt und, soweit anwendbar, das Standard-Passwort angepasst, c) Der Benutzerstammsatz SAP* wird der Gruppe SUPER zugeordnet.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Prüfung auf Anwendung der oben genannten Maßnahmen, soweit möglich, für alle sonstigen Standard-SAP- und Drittanbieter-Benutzer.
c)	Referenzbenutzer
2.10.	**Referenzbenutzer/Vorkommen:** *Werden Referenzbenutzer nur in begründeten Ausnahmefällen eingesetzt?* Neben der Vergabe von Berechtigungen an Benutzer über Einzel- oder Sammelrollen gibt es eine weitere Möglichkeit, Sammel- und Einzelrollen an Benutzer zu vergeben und dann wiederum diese Benutzer an weitere Benutzer zu vergeben. Dies erfolgt über den Pfad Werkzeuge > Administration > Benutzerpflege > Transaktion SU01 Benutzer im Reiter Rollen im Feld Referenzbenutzer. Hiermit wird noch zusätzlich zu den bereits bestehenden zwei Rollenebenen eine weitere Schicht eingeführt, die der Nachvollziehbarkeit der Berechtigungsvergabe abträglich ist. Insofern sollte die Nutzung von Referenzbenutzern auf begründete Ausnahmefälle beschränkt werden. Eine Auswertung, ob Benutzer Referenzbenutzer zugeordnet sind, kann über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Benutzer > Transaktion S_BCE_68001400 Benutzer nach komplexen Selektionskriterien erfolgen. Ob einem Benutzer Referenzbenutzer zugeordnet sind, findet sich im Ergebnis in der Spalte Referenzbenutzer. Prüfung, dass Benutzer grundsätzlich keine Referenzbenutzer zugeordnet sind.
2.11.	**Referenzbenutzer/Ausnahmen:** *Wird die Nutzung von Referenzbenutzern als Ausnahme angemessen dokumentiert und passen die Berechtigungen der Referenzbenutzer zur Ausnahmenutzung?* Sollte abweichend von der Vorgabe oben eine Nutzung von Referenzbenutzern erfolgen (Ergebnisliste kann aus der vorherigen Prüfungshandlung übernommen werden), sind für die Benutzer mit Referenzbenutzern Dokumentationen zu identifizieren, die die Nutzung begründen. Ebenso sind die Berechtigungen der vergebenen Referenzbenutzer zu identifizieren, und es ist zu prüfen, ob deren Umfang

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	mit dem Nutzungszweck übereinstimmt. Prüfung im Falle der Vergabe von Referenzbenutzern auf angemessene Dokumentation, Sinnhaftigkeit des Einsatzes und angemessene Vergabe von Berechtigungen in Übereinstimmung mit dem Nutzungszweck.
d)	Standardbenutzertypen
2.12.	**Servicebenutzer/Rechte:** *Werden Benutzer vom Typ Service nur in Ausnahmefällen und mit stark eingeschränkten, nicht sensiblen Berechtigungen eingesetzt?* Servicebenutzer sind Dialogbenutzer, die als geteilte Benutzer von einer höheren Anzahl an Anwendenden genutzt werden können (shared user). Um das zu gewährleisten, sind für die Servicenutzenden die Standardparameter zur Erzwingung und zum Ablauf der Passwortänderung außer Kraft gesetzt. Aufgrund des damit verbundenen höheren Risikos sind Service-Benutzer nur für besondere Einsatzzwecke zu verwenden und nur mit nicht sensiblen Berechtigungen auszustatten. Prüfung auf Vermeidung oder nur sehr eingeschränkte, dokumentierte Nutzung in Ausnahmefällen mit Berechtigungen mit nicht sensiblen Berechtigungen.
2.13	**Systembenutzer/Grundschutz:** *Werden Benutzer vom Typ System nur in den hierfür vorgesehenen Nutzungsfällen eingesetzt?* System-Benutzer werden für die dialogfreie Kommunikation innerhalb eines Systems (für RFC- bzw. CPIC-Service-Benutzer) bzw. für die Hintergrundverarbeitung innerhalb eines Systems verwendet. Eine Dialoganmeldung ist nicht möglich. Ein Benutzer dieses Typs ist von den allgemeinen Einstellungen zur Gültigkeitsdauer eines Passworts ausgeschlossen. Das Passwort kann nur durch Benutzer-Administrator:innen über die Transaktion SU01 geändert werden. Die System-Benutzer sollten einer eigenen Benutzergruppe zugewiesen

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	werden. Prüfung auf Verwendung des Typs von Benutzern in den hierfür vorgesehenen Nutzungsfällen unter Anwendung der oben genannten Bedingungen.
2.14	**Kommunikationsbenutzer/Grundschutz:** *Wird die Verwendung von Benutzern vom Typ Kommunikation vermieden?* Kommunikationsbenutzer (z. B. RFC, ALE-Benutzer) werden für die dialogfreie Kommunikation zwischen Systemen (für verschiedene Anwendungen wie z. B. ALE, Workflow, TMS, ZBV) genutzt. Eine Dialoganmeldung ist nicht möglich. Der einzige Unterschied zwischen den Benutzertypen Kommunikation und System ist, dass bei der Anmeldung mit einem Kommunikationsbenutzer eine Prüfung auf abgelaufene/initiale Passwörter erfolgt und somit die Gültigkeit des Passworts auch abläuft. Aus diesem Grund sollte von einer Verwendung des Benutzertyps Kommunikation komplett Abstand genommen werden und nur der Benutzertyp System zum Einsatz kommen (siehe auch OSS Hinweis 622464). Prüfung auf vollständige Vermeidung der Nutzung von Benutzern mit dem Benutzertyp Kommunikation.
e)	Notfallbenutzer
2.15.	**Notfallbenutzer-Kennung:** *Sind für die Notfallverfahren spezifische Notfallbenutzer eingerichtet und angemessen geschützt?* Bei der Anlage und Pflege von Notfallbenutzern ist ähnlich den Standardbenutzern eine Reihe von Maßnahmen zu beachten: a) es sind nur in Ausnahmefüllen die Berechtigungen SAP_ALL und SAP_NEW zu verwenden, b) Notfallbenutzer sind der Benutzergruppe SUPER

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	zuzuordnen, c) Notfallbenutzer sollten darüber hinaus über die allgemeinen Benutzergruppen und/oder die Namenskonvention als Notfallbenutzer erkennbar sein. Prüfung von Benutzern für Notfallzwecke auf Einhaltung angemessener Schutzmaßnahmen.
3.	**Rollen und Berechtigungen**
	Kontrollziel: Die Vorgaben für Rollen und technische Berechtigungen und deren Umsetzung sorgen für eine vollständige Nachvollziehbarkeit der technischen Berechtigungen auf der untersten Ebene bis zu den Rollen als Zwischenebene. **Risiko:** Bei fehlender Nachvollziehbarkeit auf einer oder mehreren Ebenen eines Benutzer- und Berechtigungskonzepts ergeben sich automatisch Mängel im Minimal- und Funktionstrennungsprinzip und damit eine Gefährdung der Integrität, Verfügbarkeit und Vertraulichkeit von Daten.
3.1.	**Platzhalter Rollen und Berechtigungen:** *Sind alle im Prüfprogramm in Kapitel 4.6 Rollen und Berechtigungen enthaltenen, im S/4HANA-OnPremise-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Prozesse und Organisation vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das S/4HANA-OnPremise-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag. Berücksichtigung der nachfolgenden Hinweise zu Rollen und Berechtigungen.
3.2.	**Namenskonventionen/Rollengestaltung/Verantwortlichkeiten:** Hinweis: Eine Auswahl aller an Benutzer vergebenen und damit für die Prüfung in diesem Abschnitt relevanten Einzel- und Sammelrollen kann über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Rollen > Rollen nach komplexen Selektionskriterien > Transaktion S_BCE_68001425 und Selektion „Mit gültiger Zuordnung von“ im Reiter

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	„Selektion nach Benutzerzuordnung“ oder über eine Verknüpfung der Tabellen AGR_DEFINE und AGR_USERS ermittelt werden.
a)	Rollengestaltung
3.3.	**Rollenkongruenz – sensitive Funktionen:** *Enthalten Rollen nur die sensitiven Funktionen, die mit der äußeren Deklaration der Rollen übereinstimmen?* Insofern sich Einzelrollen für Pflegetätigkeiten an den Rollenschnitt nach Aufgaben wie oben beschrieben halten, dürften Rollen nur eine sensitive Funktion beinhalten, und die äußere Beschreibung der Rolle müsste mit der Beschreibung der sensitiven Funktion übereinstimmen (z. B. dürfte die Funktion zur Pflege von Bestellungen nur in einer Rolle für die Pflege von Bestellungen vorkommen). Prüfung von Rollen gegen sensitive Funktionen mit dem Ergebnis, dass bei Rollen mit Treffern für sensitive Funktionen i. d. R. nur eine sensitive Funktion enthalten sollte und die Deklaration der Funktion mit der Deklaration der Rolle übereinstimmen sollte.
3.4.	**Rollenkongruenz – Berechtigungsobjekte:** *Enthalten Rollen nur die sensitiven Berechtigungsobjekte, die mit der äußeren Deklaration der Rollen übereinstimmen?* Einzelrollen sollten nur die Berechtigungsobjekte enthalten, die sich aus ihrer äußeren Beschreibung ergeben (z. B. sollten Berechtigungen für Objekte für Buchhaltungsbelege zumindest mit pflegenden Rechten nur in Rollen des Rechnungswesens vorkommen). Hierbei ist eine Expert:innen-Tabelle mit sensitiven Berechtigungsobjekten (und ggf. Feldwerten) und

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	einer Zuordnung zu bestimmten Prozessbereichen (und ggf. semantischen Objekten) erforderlich. Prüfung von Rollen gegen sensitive Berechtigungen für Berechtigungsobjekte, die mit der äußeren Deklaration der Rollen übereinstimmen.
3.5.	**Rollenkongruenz – Aktivitätswerte:** *Sind bei Anzeigerollen die Aktivitäten in den Berechtigungen auf reine Anzeige eingeschränkt?* In einer Vielzahl von Fällen werden die Berechtigungen nicht oder nicht nur über Anzeige-beschränkte Transaktionen, sondern auch durch Aktivitäts-Felder in Berechtigungsobjekten auf reine Anzeige-Berechtigungen eingeschränkt. Insofern sollten bei Rollen, die als reine Anzeigerollen ausgewiesen sind, die in den Rollen vorhandenen Anzeige-Felder durchgängig auf reine Anzeige-Aktivitätswerte wie insbesondere 03 – Anzeige beschränkt sein. Aktivitätsfelder werden überwiegend mit dem Feldnamen ACTVT ausgewiesen. Prüfung von Anzeigerollen auf Ausprägung der Aktivitäts-Felder nur auf Anzeige-Feldwerte.
3.6.	**Regelkonformität:** Hinweis: Soweit bei der Prüfung kein Zugang zu einer der einschlägigen SAP-Analyselösungen für kritische Berechtigungen und Funktionstrennungen vorliegt, kann eine Auswertung über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Benutzer > mit kritischen Berechtigungen oder Transaktion S_BCE_68002111 und Auswahl „Rolle“ unter Selektionskriterien eine Analyse der Rollen auf Funktionen, Funktionstrennungen und kritische Berechtigungen erfolgen.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Dabei ist zu beachten, dass die Transaktion nur das Analysewerkzeug für Prüfungen zur Verfügung stellt, nicht jedoch die Regeln.
b)	Ausnahmeregelungen
3.7.	**Eigenentwickelte Berechtigungsobjekte:** Hinweis: Eine Auswahl der in einem S/4HANA OnPremise vorhandenen Kund:innen-eigenen Berechtigungsobjekte ist über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Berechtigungsobjekte > Transaktion S_BCE_68001413 – Berechtigungsobjekte nach komplexen Selektionskriterien und Auswahl über das Berechtigungsobjekt-Feld für Objekte beginnend mit X*, Y* oder Z* zu erreichen, da Berechtigungsobjekte als Repository-Objekte in diesen Namensräumen oder Kund:innen-eigenen Namensräumen angelegt werden müssen. Um rein auf genutzte Objekte zu fokussieren, kann mit etwas Aufwand eine Verknüpfung Objekte zu Rollen (Transaktion S_BCE_68001422 – Rollen nach Berechtigungsobjekt) und Rollen zu Benutzern (Transaktion S_BIE_59000199 – Benutzer nach Rollen) hergestellt werden.
c)	Standardrollen (SAP-Standard-Rollen und -Profile)
3.8.	**Standard-Sammelprofil SAP_ALL:** *Sind Maßnahmen getroffen, die Nutzung des Standard-Profils SAP_ALL weitestmöglich einzuschränken?* Das Profil SAP_ALL verfügt über Berechtigungen aller Berechtigungsobjekte in SAP S/4 inklusiver einer Vielzahl kritischer Berechtigungen. Insofern sollte SAP_ALL in produktiven Systemen nicht oder nur für SAP-Wartungseinsätze vergeben werden. Für Notfallverfahren sollte maximal eine um kritische Berechtigungen angepasste Rolle Anwendung finden. Es sollte ebenfalls vermieden werden, dass SAP_ALL-

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Derivate unter anderem Namen, aber mit gleichem oder vergleichbarem Inhalt genutzt werden. Werden Benutzer gleichwohl mit dem Profil SAP_ALL oder vergleichbaren Varianten ausgestattet, sind diese nach dem Verfahren für privilegierte Benutzer zu behandeln (siehe Kapitel Prozesse und Organisation – Privileged-Access-Management). Prüfung auf die Vergabe des Profils SAP_ALL im betrachteten Prüfzeitraum über die Transaktion S_BCE_68002311 – für Benutzer über den Reiter Rollen > Profile > Profilname. Prüfung von Rollen/Profilen auf kritische Berechtigungen zur Identifizierung von mit SAP_ALL vergleichbaren umfangreichen Rollen/Profilen über Transaktion RSUSRAUTH – Suche nach Einzelrollen mit Berechtigungsdaten und S_BCE_68001409 – Profile nach komplexen Selektionskriterien.
3.9.	**Standard-Sammelprofil SAP_NEW:** *Sind Maßnahmen getroffen, die Nutzung des Standard-Profils SAP_NEW weitestmöglich einzuschränken?* Das Standard-Profil SAP_NEW enthält alle Berechtigungen für Berechtigungsobjekte, die mit einem Release neu hinzugekommen sind. Nach jedem Release-Wechsel benötigt man dieses Profil, damit bestimmte Aufgaben problemlos ablaufen können. Die Berechtigungen sollten geprüft und ggf. in Bestandsrollen übernommen werden. Danach sollte das SAP_NEW bereinigt werden. SAP_NEW sollte maximal an Notfallbenutzer vergeben werden. Werden Benutzer gleichwohl mit dem Profil SAP_NEW oder vergleichbaren Varianten ausgestattet, sind diese nach dem Verfahren für privilegierte Benutzer zu behandeln (siehe Kapitel Prozesse und Organisation – Privileged-Access-Management). Prüfung auf die Vergabe des Profils SAP_NEW im betrachteten Prüfzeitraum über die Transaktion S_BCE_68002311 – für Benutzer über den Reiter Rollen > Profile > Profilname. Prüfung auf ein angemessenes Verfahren zur Validierung, Übernahme von SAP_NEW-Berechtigungen und Bereinigung des SAP_NEW-Profils.
3.10.	**Sonstige kritische Standardprofile/-rollen:** *Sind Maßnahmen getroffen, die Nutzung weiterer kritischer Standard-Profile/-Rollen einzuschränken?* Neben den beiden oben genannten Profilen existiert eine Reihe weiterer sensibler Standard-Rollen/-Profile wie S_A.SYSTEM, S_A.ADMIN, S_A.CUSTOMIZ, S_A.DEVELOP, S_CTS_ALL, S_CTS_PROJECT, S_DATASET_AL, S_C_FUNCT_AL, S_TCD_ALL, S_TSKH_ALL, F_BUCH_ALL, Z_ANWEND. Eine Verwendung sollte maximal im Rahmen von Notfallverfahren erfolgen, insbesondere jedoch nicht zur Vergabe an

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Benutzer in produktiven Systemen. Werden Benutzer gleichwohl mit Standardprofilen/-rollen ausgestattet, sind diese nach dem Verfahren für privilegierte Benutzer zu behandeln (siehe Kapitel Prozesse und Organisation – Privileged-Access-Management). Prüfung auf Vergabe der oben genannten kritischen Standard-Rollen/ -Profile im betrachteten Prüfzeitraum über die Transaktion S_BCE_68002311 – für Benutzer über den Reiter Rollen > Profile > Profilname.
d)	Fiori-Frontend- und S/4HANA-Backend-Rollen
3.11.	**Fiori-Kataloge:** *Sind die Zugriffe auf Fiori Apps angemessen über einheitliche Kataloge in Front- und Backend-Rollen geschützt?* Bei Nutzung von Fiori Apps ist die Anlage von Katalogen erforderlich, die die zur Ausführung vorgesehenen Fiori Apps beinhalten. Ein Katalog mit den Fiori Apps muss der Frontend-Rolle zugeordnet sein, um Fiori Apps über das Fiori Launchpad ausführen zu können. Derselbe Katalog sollte bei getrennten Front- und Backend-Rollen auch der Backend-Rolle zugeordnet werden, um die automatische Vorschlagsfunktion für Berechtigungen für die Backendrolle nutzen zu können. Es ist zu empfehlen, genau einen Katalog je Front- und Backendrolle in Abbildung von eindeutigen Tasks (siehe Rollengestaltung) zu implementieren und zuzuordnen. Die den Frontend-Rollen zugeordneten Kataloge finden sich über den Pfad Werkzeuge > Administration > Rollenverwaltung > Rollen Transaktion PFCG, und hier als Eintrag im Reiter Menü mit dem Symbol Launchpad-Katalog. Der Inhalt des Katalogs wird zum einen direkt unterhalb des PFCG-Katalog-Eintrags und alternativ im Fiori Launchpad über den Pfad UI2/FLPD_CUST Launchpad Designer (Client-Specific) > Reiter Catalogs > Eingabe des relevanten Katalogs im Suchfeld > Selektion des Katalogs > die enthaltenen Fiori Apps werden im Detailbereich angezeigt. Prüfung auf Pflege einheitlicher Fiori-Kataloge mit einer 1:1-Beziehung zwischen Katalog, Frontend- und Backend-Rolle.
3.12.	**Fiori-OData-Service-Berechtigungen:** *Erfolgt eine angemessene Pflege der S_SERVICE-Berechtigungen über Kataloge?* Für die Ausführung von Fiori Apps ist neben der Zuordnung der Fiori Apps über Kataloge in der Frontend-Rolle eine Berechtigung für das

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Berechtigungsobjekt S_SERVICE mit dem Hash-Wert des externen Service erforderlich. Bei angemessener Zuordnung der Kataloge sowohl zu den Frontend- als auch zu den Backend-Rollen werden diese Hashwerte automatisch vom System angelegt und bei Änderungen auf Fiori-App-Ebene ebenso aktualisiert. Eine direkte Pflege der Hash-Werte sollte insofern unterbleiben. Dies lässt sich über den Pfad Werkzeuge > Administration > Rollenverwaltung > Rollen Transaktion PFCG und hier als Eintrag im Reiter Berechtigungen > Button Anzeige Berechtigungsdaten > Selektion Berechtigung zu Objekt S_SERVICE prüfen. Der Pflege-Status der Berechtigungen muss „Standard“ sein. Prüfung, ob die Hashwerte der Berechtigungen für das Objekt S_SERVICE in Front- und Backend-Rollen rein automatisch befüllt sind.
4.	**Sensitive Funktionen**
	Kontrollziel: Für SAP HANA liegt ein Regelwerk mit sensitiven Funktionen vor. Sensitive Funktionen werden ausschließlich über Rollen vergeben, deren Deklaration die beinhalteten sensitiven Funktionen eindeutig erkennbar machen. Für Rollen mit sensitiven Funktionen ist ausgewiesen, für welche Instanzen und an welche Benutzergruppen eine Vergabe zulässig ist. Benutzer erhalten Berechtigungen für sensitive Funktionen unter strenger Beachtung des Minimalprinzips. **Risiko:** Die Nutzung von Rollen mit nicht nachvollziehbaren sensitiven Berechtigungen und die Vergabe sensitiver Berechtigungen an Benutzer unter Verstoß gegen Minimalprinzip und Funktionstrennungsregeln gefährden die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen.
4.1.	**Platzhalter Sensitive Funktionen:** *Sind alle im Prüfprogramm in Kapitel 4.8 Sensitive Funktionen und Funktionstrennung enthaltenen, im S/4HANA-OnPremise-Kontext anwendbaren Prüfungshandlungen für sensitive Funktionen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Sensitive Funktionen und Funktionstrennung vorgegebenen und anwendbaren Prüfungshandlungen für sensitive Funktionen an dieser Stelle in das S/4HANA-OnPremise-Prüfprogramm als Ersatz für diesen Platzhalter-

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Eintrag. Berücksichtigung der nachfolgenden Hinweise zu sensitiven Funktionen.
4.2.	**Sensitive Funktionen:** Hinweis 1: Soweit für die Auswertungen auf sensitive Funktionen keine dedizierten IT-Lösungen eingesetzt werden, kann, wenn auch mit funktionalen Einschränkungen, eine Analyse über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Benutzer > Benutzer nach komplexen Selektionskriterien > Benutzer nach komplexen Selektionskriterien oder Transaktion S_BCE_68001400 und für Rollen der Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Rollen > Rollen nach komplexen Selektionskriterien > Rollen nach komplexen Selektionskriterien oder Transaktion S_BCE_68001425 vorgenommen werden.
4.3.	**Sensitive Funktionen:** Hinweis 2: Bei den im Folgenden aufgeführten spezifischen sensitiven Funktionen handelt es sich um ausgewählte Beispiele. Ein vollständiges und unternehmensindividuelles Regelwerk geht im Umfang weit darüber hinaus. Auch haben wir in Bezug auf die technische Spezifizierung auf Transaktions-/Fiori-App- und Objekt-Ebene lediglich ausgesuchte Beispiele gegeben. Auch hier sind weitere Transaktionen und Objekte/Feldwerte hinzuzufügen, um vollständige und richtige Ergebnisse zu erzielen.
4.4.	**Sensitive Funktionen:** Hinweis: Im Rahmen des SAP S/4HANA OnPremise erfordert eine Prüfung von Benutzern und Rollen die Analyse auf eine Kombination aus Berechtigungen für a) den Start von Transaktionen über das Berechtigungsobjekt S_TCODE (TCode-Check) und b) für weitere in den betroffenen Programmen verankerte Berechtigungsobjekte (Authority-Checks). Bei Nutzung von für sensitive Funktionen und Funktionstrennungen relevante Fiori Apps anstelle von Transaktionen

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	ersetzt das Berechtigungsobjekt S_SERVICE das Objekt S_TCODE mit Hash-Werten für die Fiori Apps statt Transaktionscodes für Transaktionen.
a)	Entwicklung und Customizing
4.5.	**Systemeinstellungen ändern:** *Sind die Berechtigungen zur Änderung von Systemeinstellungen nur einem eingeschränkten Kreis von Basis-Administrator:innen zugänglich?* Anwendende mit diesen Berechtigungen können Systemeinstellungen bez. Repository- bzw. Mandant:innen-übergreifender Customizing-Objekte ändern. Das Risiko von ungenehmigten Änderungen dieser Systemeinstellungen führt u. U. zu Fehlern bzw. Instabilitäten oder zu fehlerhaften Sicherheitseinstellungen der Produktivumgebung. Hierzu sind beispielsweise die Transaktionen SCTS_RSWBO004, SE03 und SE06 in Kombination mit den korrespondierenden Berechtigungen für Berechtigungsobjekte erforderlich. Prüfung auf Vergabe der obigen Transaktions-/Berechtigungskombinationen nur an einen restriktiven Kreis von Basis-Administrator:innen.
4.6.	**Debug-Funktionalität im Änderungsmodus ausführen:** *Wird die Vergabe von Berechtigungen zur Durchführung von Debugging im Änderungsmodus in der Produktion unterbunden?* Benutzer können nicht nachvollziehbare direkte Änderungen an rechnungslegungsrelevanten Daten im Hauptspeicher des Rechners vornehmen. Somit läge ein Verstoß gegen die Unveränderlichkeit und die Nachvollziehbarkeit von rechnungslegungsrelevanten Daten vor. Hierzu sind Berechtigungen für das Berechtigungsobjekt S_DEVELOP insbesondere mit den Feldern/Feldwerten ACTVT / 02 oder 03 und OBJTYPE / DEBUG erforderlich.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Prüfung auf fehlendes Vorkommen von Benutzern in der Produktion mit der obigen Berechtigungskombination.
b)	Administration
4.7.	**Rollen, Profile und Berechtigungen pflegen:** *Wird die Pflege von Rollen und Berechtigungen in der Produktion unterbunden?* Benutzer können unangemessene oder nicht freigegebene Berechtigungen in bestehende oder neue Rollen einbauen. Dadurch besteht das Risiko, dass unkontrolliert und undokumentiert sensitive Berechtigungen an Anwendende verteilt werden. Hierzu sind Berechtigungen beispielsweise für die Transaktion PFCG in Kombination insbesondere mit einer Berechtigung für das Berechtigungsobjekt S_USER_AGR und den Feldern/Feldwerten ACTVT / 01, 02 oder 64 erforderlich. Prüfung auf fehlendes Vorkommen von Benutzern in der Produktion mit der obigen Transaktions-/Berechtigungskombination.
4.8.	**Rollen und Profile zuweisen:** *Sind die Berechtigungen zur Zuweisung von Rollen und Profilen nur einem eingeschränkten Kreis von Benutzer-Administrator:innen zugänglich?* Benutzer können anderen Benutzern unautorisierten Zugriff gewähren. Dieses könnte eine unvollständige und unrichtige Erfassung von Geschäftsvorfällen zur Folge haben. Zudem werden allgemeine Sicherheitsanforderungen als Voraussetzung für die Ordnungsmäßigkeit der IT-gestützten Rechnungslegung nicht erfüllt. Hierzu sind Berechtigungen beispielsweise für die Transaktion SU01 in Kombination insbesondere mit einer Berechtigung für das Berechtigungsobjekt S_USER_SAS und den Feldern/Feldwerten ACTVT / 22 und für das Berechtigungsobjekt

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	S_USER_GRP mit den Feldern/Feldwerten ACTVT / 02 erforderlich. Prüfung auf Vergabe der obigen Transaktions-/Berechtigungskombinationen nur an einen restriktiven Kreis von Benutzer-Administrator:innen.
4.9.	**Änderungshistorie und Änderungsprotokolle löschen:** *Wird die Löschung von Änderungshistorie und -protokollen in der Produktion und Entwicklung unterbunden?* Benutzer können Belegänderungen und deren Protokolle sowie Änderungsprotokolle hinsichtlich Systemeinstellungen und Customizing-Änderungen löschen. Dadurch ist die Nachvollziehbarkeit nicht mehr gewährleistet, ein Verstoß gegen das Radierverbot möglich. Für die Beleghistorie sind Berechtigungen beispielsweise für die Transaktion SCU3 in Kombination insbesondere mit einer Berechtigung für das Berechtigungsobjekt S_TABU_CLI und den Feldern/Feldwerten CLIIDMAINT / X sowie S_TABU_DIS und ACTVT / 02 und DICBERCLS / SA erforderlich. Für die Systemprotokolle sind Berechtigungen für die Transaktion SCDO in Kombination insbesondere mit einer Berechtigung für das Berechtigungsobjekt S_SCD0 und den Feldern/Feldwerten ACTVT / 06 oder 08 erforderlich. Prüfung auf fehlendes Vorkommen von Benutzern in der Produktion mit den obigen Transaktions-/Berechtigungskombinationen.
4.10.	**Datenbankänderung mit DBA-Cockpit:** *Wird bei Nutzung des DBA-Cockpits die Möglichkeit des direkten Überschreibens von Daten in der HANA DB unterbunden?* Über die Transaktion DBACOCKPIT ist es möglich. aus der S/4HANA Anwendungsschicht heraus direkt auf die HANA-DB-Daten zuzugreifen. Dabei sind sowohl Änderungen an der Datenbankkonfiguration als auch an den Benutzer sowie an einzelnen Datensätzen möglich. Prüfung, dass die Transaktion nur einem eingeschränkten Personenkreis zugänglich ist. Prüfung auf Einschränkung der Berechtigungen auf reine Anzeigefunktionen.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
c)	Stammdaten und Bewegungsdaten
4.11.	**Buchungsperioden pflegen:** *Sind die Berechtigungen zum Öffnen und Schließen der Buchungsperioden nur einem eingeschränkten Kreis von Fach-Administrator:innen zugänglich?* Benutzer könnten Buchungsperioden in der Vergangenheit und in der Zukunft öffnen. Hieraus würde sich das Risiko von nicht periodengerechten Buchungen ergeben. Hierzu sind Berechtigungen beispielsweise für die Transaktion OB52 in Kombination mit einer Berechtigung für das Berechtigungsobjekt S_TABU_DIS und den Feldern/Feldwerten ACTVT / 02 und DICBERCLS / FC31 erforderlich. Prüfung auf Vergabe der obigen Transaktions-/Berechtigungskombinationen nur an einen restriktiven Kreis von Fach-Administrator:innen.
4.12.	**Beleg buchen (Hauptbuch):** *Sind die Berechtigungen zum Buchen von Belegen im Hauptbuch nur einem eingeschränkten Kreis von Sachbearbeitenden im Rechnungswesen zugänglich?* Benutzer könnten manuell fiktive oder fehlerhafte FI-Buchungen auf Sachkonten buchen. Hieraus würden sich falsche Buchungen im Hauptbuch ergeben, was zu einer fehlerhaften Darstellung von Geschäftsvorfällen in Bilanz oder GuV führt. Hierzu sind Berechtigungen beispielsweise für die Transaktion FB50 in Kombination mit Berechtigungen für die Berechtigungsobjekte F_BKPF_BES, F_BKPF_BLA, F_BKPF_BUK, F_BKPF_GSB, F_FAGL_SEG und den Feldern/Feldwerten ACTVT / 01 erforderlich. Prüfung auf Vergabe der obigen Transaktions-/Berechtigungskombinationen nur an einen restriktiven Kreis von Sachbearbeitenden im Rechnungswesen.
d)	Datenschutz
4.13.	**Tabellen anzeigen (alle):** *Wird die uneingeschränkte Anzeige von Tabellen in der Produktion insbesondere aus der Perspektive personenorientierter Daten unterbunden?* Benutzer können mit dem lesenden Zugriff auf Tabellen uneingeschränkt deren Inhalt einsehen. Damit besteht das Risiko, dass nicht autorisierte Benutzer Einsicht in sensible Daten, wie insbesondere DSGVO-relevante

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Daten, erhalten. Hierzu sind Berechtigungen beispielsweise für die Transaktion SE16 in Kombination mit einer Berechtigung für das Berechtigungsobjekt S_TABU_DIS und den Feldern/Feldwerten ACTVT / 03 und DICBERCLS / „*“ erforderlich. Prüfung auf fehlendes Vorkommen von Benutzern in der Produktion mit der obigen Transaktions-/Berechtigungskombination.
5.	**Funktionstrennung**
	Kontrollziel: Für SAP S/4HANA liegt ein Regelwerk mit Funktionstrennungen sowie mit korrespondierenden mitigierenden Kontrollen vor. Das Regelwerk bezieht sich auf einzelne sensitive Funktionen, die in Kombination ein höheres Risiko aufweisen, als sich aus den jeweils einzelnen Risiken ergibt. Rollen und Berechtigungen werden unter Vermeidung von Funktionstrennungen erstellt. Funktionstrennungsverletzungen aus der Vergabe von Rollen und Berechtigungen an Benutzer werden vermieden oder durch Zuordnung mitigierender Kontrollen kompensiert. **Risiko:** Durch das Auftreten von Funktionstrennungsverletzungen in Benutzern ergeben sich Risiken für die Integrität und Verfügbarkeit von Daten.
5.1.	**Platzhalter Funktionstrennungen:** *Sind alle im Prüfprogramm in Kapitel 4.8 Sensitive Funktionen und Funktionstrennung enthaltenen, im S/4HANA-OnPremise-Kontext anwendbaren Prüfungshandlungen für Funktionstrennungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Sensitive Funktionen und Funktionstrennung vorgegebenen und für Funktionstrennungen anwendbaren Prüfungshandlungen an dieser Stelle in das S/4HANA-OnPremise-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag. Berücksichtigung der nachfolgenden Hinweise zu Funktionstrennungen.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
5.2.	**Funktionstrennungen:** Hinweis 1: Soweit für die Auswertungen auf Funktionstrennungen keine dedizierten IT-Lösungen eingesetzt werden, kann, wenn auch mit funktionalen Einschränkungen, über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Benutzer > mit kritischen Berechtigungen oder Transaktion S_BCE_68002111 eine Analyse von Benutzern und Rollen auf Funktionen, Funktionstrennungen und kritische Berechtigungen erfolgen.
5.3.	**Funktionstrennungen:** Hinweis 2: Bei den im Folgenden aufgeführten spezifischen Funktionstrennungen handelt es sich um ausgewählte Beispiele. Ein vollständiges und unternehmensindividuelles Regelwerk geht im Umfang weit darüber hinaus. Bei den Kombinationen der in den Funktionstrennungsregeln enthaltenen Funktionen verweisen wir insbesondere auch in Bezug auf die technische Spezifizierung auf die Informationen in Kapitel 4 Sensitive Funktionen.
5.4.	**Funktionstrennungen:** Hinweis: Die Einzelfunktionen der folgenden Funktionstrennungsregeln sind im Kapitel Sensitive Funktionen bereits erläutert, sodass hier nur noch ein Verweis auf die in den Funktionstrennungen relevanten Funktionen enthalten ist.
5.5.	**Funktionstrennung Periodenpflege und Beleg buchen (Hauptbuch):** *Wird die Vergabe von Berechtigungen für die Öffnung von Buchungsperioden und für die Bebuchung von Sachkonten durch angemessene Verfahren unterbunden?* Benutzer könnten sowohl Buchungsperioden der Vergangenheit oder der Zukunft öffnen als auch Geschäftsvorfälle auf Sachkonten buchen. Hieraus würde sich das Risiko von nicht periodengerechten Buchungen auf Sachkonten durch einen Benutzer ergeben. Zur Feststellung von SoD-Verletzungen ist eine Auswertung von Benutzern auf die beiden oben eingeführten sensitiven Funktionen erforderlich und eine Verknüpfung über die Benutzer-ID. Benutzer mit Treffern für beide Funktionen haben einen Funktionstrennungskonflikt.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Prüfung auf Vergabe von Berechtigungen sowohl für Periodenpflege als auch für Sachkontenbuchungen. Bei vorliegenden Konflikten auf Benutzer-Ebene Prüfung auf angemessene Kompensation der Risiken durch korrespondierende dokumentierte und ausgeführte Kontrollmaßnahmen.
5.6.	**Funktionstrennung Rollenpflege und Rollenzuweisung:** *Werden die Vergabe von Rollenpflegeberechtigungen in der Entwicklung und Rollenzuweisungsberechtigungen in der Produktion durch angemessene Verfahren unterbunden?* Kombinationen von Berechtigungen in der Benutzer- und Berechtigungspflege führen zu erhöhten Risiken der Vergabe unangemessener und unautorisierter Berechtigungen an Benutzer. Dies gilt auch und insbesondere für die Kombination der unangemessenen Anlage oder Erweiterung von Rollen und der unberechtigten Vergabe dieser erweiterten Rollen an Benutzer. Zur Feststellung von SoD-Verletzungen ist eine Auswertung von Benutzern auf die beiden oben eingeführten sensitiven Funktionen erforderlich und eine Verknüpfung über die Benutzer-ID. Benutzer mit Treffern für beide Funktionen haben einen Funktionstrennungskonflikt. Prüfung auf Vergabe von Berechtigungen sowohl für Rollenpflege in der Entwicklung als auch Rollenzuordnung in der Produktion. Bei vorliegenden Konflikten auf Benutzer-Ebene Prüfung auf angemessene Kompensation der Risiken durch korrespondierende dokumentierte und ausgeführte Kontrollmaßnahmen.
5.7.	**Vermeidung Pflege eigener Benutzer:** *Wird über geeignete Benutzergruppen und Berechtigungen die Pflege der eigenen Benutzer durch Benutzer-Administrator:innen vermieden?* Die Pflege der Benutzer von Benutzer-Administrator:innen sollte nicht durch diese Administrator:innen selber erfolgen. Hierzu sollten die Administrator:innen einer eigenen Gruppe von Benutzern (z. B. Admin) zugeordnet werden. Die Benutzer-Administrator:innen sollten nur berechtigt sein, die Benutzer anderer Benutzergruppen zu pflegen. Im Zweifelsfall können auch zwei Benutzer-Administrator:innen nur auf jeweils den Benutzern des anderen Administrators / der anderen Administratorin und aller übrigen Benutzer berechtigt werden unter Verwendung von zwei Admin-Gruppen von Benutzern (z. B. Admin1 und Admin2). Detailliertere Anleitungen finden sich im DSAG-Best-Practice-Prüfleitfaden ERP 6.0. Die

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Zuordnung der Administrator:innen zur Benutzergruppe findet sich über die Transaktion SU01 im Reiter Logondaten, Feld Benutzergruppe. Die Berechtigungen der Administrator:innen können über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Benutzer > Benutzer nach komplexen Selektionskriterien > Benutzer nach komplexen Selektionskriterien oder Transaktion S_BCE_68001400 auf Berechtigungen für das Berechtigungsobjekt S_USER_GRP ausgewertet werden. Das Objekt sollte im Feld CLASS keinen Feldwert mit der eigenen Benutzergruppe der Administrator:innen oder eine gesternte Berechtigung in Kombination mit den Aktivitäten 01 oder 02 für das Feld ACTVT enthalten. Prüfung auf Vermeidung der Vergabe von Berechtigungen zur Pflege des eigenen Benutzers an Benutzeradministrator:innen.
6.	**Prozesse und Organisation**
	Kontrollziel: Die für Benutzer und Berechtigungen etablierten Prozesse und organisatorischen Rollen gewährleisten, dass der Zustand der Vergabekette zwischen Benutzern, Rollen und technischen Berechtigungen auf einem angemessenen Niveau unter Beachtung der regulatorischen Anforderungen verbleibt. **Risiko:** Aus fehlenden Vorgaben oder unzureichender Anwendung der Vorgaben für Prozesse und organisatorische Rollen folgt eine Verschlechterung der Benutzer und Berechtigungsstrukturen mit der Folge von Verletzungen des Minimalprinzips und den sich ergebenden Gefährdungen der Integrität, Verfügbarkeit und Vertraulichkeit von Daten.
6.1.	**Platzhalter Prozesse und Organisation:** *Sind alle im Prüfprogramm in Kapitel 4.9 Prozesse und Organisation enthaltenen, im S/4HANA-OnPremise-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Prozesse und Organisation vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das S/4HANA-OnPremise-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag. Berücksichtigung der nachfolgenden Hinweise zur Berechtigungs- und Benutzeradministration.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
a)	Role-Lifecycle-Management (Berechtigungsadministration)
6.2.	**Role-Lifecycle-Management (Berechtigungsadministration):** Hinweis: Für die Prüfung der angemessenen Verfahren für die Berechtigungsadministration können die Stichproben für Rollenänderungen über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Änderungsbelege > Benutzer > für Rollen oder Transaktion RSSCD100_PFCG ermittelt werden. Der Status der Rollen aus den Stichproben kann zum Zeitpunkt der Prüfung über den Pfad Werkzeuge > Administration > Rollenverwaltung > Rollen oder die Transaktion PFCG angezeigt werden.
b)	User-Lifecycle-Management (Benutzeradministration)
6.3.	**User-Lifecycle-Management (Benutzeradministration):** Hinweis: Für die Prüfung der angemessenen Verfahren für die Berechtigungsadministration können die Stichproben für Rollenänderungen über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Änderungsbelege > Benutzer > für Benutzer oder für Rollenzuordnungen oder Transaktion S_BCE_68002311 bzw. RSSCD100_PFCG_USER ermittelt werden. Bei den Stichproben sollten alle Prozessvarianten wie z. B. auch Sperrung und Löschung sowie Entsperrung und Initialisierung einbezogen werden.
c)	Privileged-Access-Management (Notfallbenutzer)
6.4.	**Nutzungs-Protokollierung:** *Werden die Aktivitäten aller Privilegierten Benutzer über das Security Audit Log (SAL) umfassend protokolliert?* Für eine Protokollierung der Privilegierten Benutzer ist a) eine Aktivierung des Security Audit Log über den Parameter in der Transaktion RSAU_CONFIG > Security-Audit-Log-Konfiguration > Parameter hier „Statistisches Security Audit Log aktiv“ und b) eine Einrichtung der Filter für alle Privilegierten Benutzer ebenfalls über die Transaktion RSAU_CONFIG > Security-Audit-Log-Konfiguration > Dynamische oder Statische Konfiguration nötig. Soweit die Benutzer-IDs aller Privilegierten Benutzer mit derselben Zeichenfolge beginnen oder derselben Benutzergruppe zugeordnet sind, muss nur ein Filter mit dem Namen oder der

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Benutzergruppe eingerichtet sein. Der Filter muss zur Aufzeichnung für alle Audit-Klassen eingerichtet sein. Prüfung auf Aktivierung des SAL und Einrichtung der Filterung für alle Privilegierten Benutzer mit allen Audit-Klassen.
6.5.	**Nutzungs-Dokumentation und -Kontrolle:** Hinweis: Die Auswahl der Stichproben für die Nutzungs-Dokumentation und -Kontrolle kann a) generell mit dem Report über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Änderungsbelege > Benutzer > für Benutzer, Filterung über die Namenskonvention oder Benutzergruppe für Privilegierte Benutzer und Auswahl von Entsperrungen/Password-Initialisierungen oder b) bei vollständiger Protokollierung über das Security Audit Log über die Transaktion RSAU_READ_LOG und Filterung über die Namenskonvention oder Benutzergruppe für Privilegierte Benutzer getroffen werden.
6.6.	**Nutzungs-Kontrolle:** Hinweis: Für die Prüfung der Stichproben auf Übereinstimmung des Lösungswegs mit den protokollierten Aktivitäten sollten die originalen Protokolldaten aus dem SAL über die Transaktion RSAU_READ_LOG mit Filterung auf den ausgewählten Privilegierten Benutzer und den betrachteten Nutzungszeitraum ausgelesen und mit den im Kontext der Nutzungsdokumentation abgelegten Daten verglichen werden.
6.7.	**Benutzer-Limitierung und -Initialisierung:** Hinweis: Die Kontrolle der Benutzersperrung und der Anpassung des Passworts nach Abschluss der Nutzung ist über den Pfad Werkzeuge > Administration > Benutzerpflege > Infosystem > Änderungsbelege > Benutzer > für Benutzer oder Transaktion S_BCE_68002311 mit Filterung auf den Privilegierten Benutzer und den Zeitraum der Nutzung oder genauer des Abschlusses der Nutzung durchzuführen.
d)	Access-Compliance-Management
6.8.	**Sensitive Funktionsprüfung und SoD-Prüfung:** Hinweis: Soweit für die SoD- und sensitiven Funktionsanalysen keine dedizierten IT-Lösungen eingesetzt werden, kann, wenn auch mit funktionalen Einschränkungen, über den Pfad Werkzeuge > Administration

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	> Benutzerpflege > Infosystem > Benutzer > mit kritischen Berechtigungen oder Transaktion S_BCE_68002111 eine Analyse auf Funktionen, Funktionstrennungen und kritische Berechtigungen erfolgen.
7.	**Protokoll und Parameter**
	Kontrollziel: Ein angemessenes Sicherheitskonzept einer Anwendung muss eine Protokollierung aller Aktivitäten im Bereich der Berechtigungsverwaltung umfassen sowie angemessene Einstellungen der verfügbaren Systemparameter mit Wirkung auf den Authentifizierungs- und Autorisierungsprozess regeln. **Risiko:** Eine unzureichende Regelung und Anwendung von Standards für Protokolle und Parameter kann zu Beeinträchtigungen der Nachvollziehbarkeit rechnungslegungsrelevanter Vorgänge durch fehlende Zuordnungsmöglichkeit von Vorgängen zu den verursachenden Benutzern oder sogar zu unautorisierten Geschäftsvorfällen durch unautorisierte Zugriffe führen.
a)	Security Audit Log
7.1.	**Security-Audit-Log-Einrichtung:** *Umfassen die Filter des Security Audit Log (SAL) kritische Ereignisse aller Benutzer und alle Ereignisse von Super- und Privilegierten Benutzern?* Für eine Protokollierung ist a) eine Aktivierung des SAL über den Parameter in der Transaktion RSAU_CONFIG > Security-Audit-Log-Konfiguration > Parameter hier „Statistisches Security Audit Log aktiv“ und b) eine Einrichtung der Filter der Benutzer über die Transaktion RSAU_CONFIG > Security Audit Log Konfiguration > Dynamische oder Statische Konfiguration nötig. Der Filter muss zur Aufzeichnung für alle Audit-Klassen oder bei allen Dialog-Benutzern lediglich für kritische Audit-Klassen eingerichtet sein.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Prüfung auf Aktivierung des SAL und Einrichtung der Filterung für alle Super- und Privilegierten Benutzer mit allen Audit-Klassen und alle Dialog-Benutzer mit kritischen Audit-Klassen.
b)	Berechtigungsparameter
7.2.	**Parameter Deaktivierung Berechtigungsobjekte:** *Wird eine globale/lokale Deaktivierung von Berechtigungsprüfungen über die korrespondierenden Parameter verhindert?* Es ist möglich, eine Kund:innen-individuelle Deaktivierung von Berechtigungsprüfungen entweder global (für alle Transaktionsausführungen) oder lokal (nur für bestimmte Transaktionen) vorzunehmen. Dafür muss der Parameter auth/object_disabling_active für globale und auth/no_check_in_some_cases für lokale Deaktivierungen auf „Y“ stehen. Zumindest der globale Parameter sollte auf „N“ stehen. Prüfung auf Einstellung der Deaktivierungsparameter und bei Öffnung für Deaktivierung auf angemessene Dokumentation und Nachvollziehbarkeit der Öffnung und der hierüber ermöglichten Deaktivierungen.
7.3.	**Konkrete Deaktivierung Berechtigungsobjekte:** *Sind erfolgte Deaktivierungen von Berechtigungsprüfungen nachvollziehbar dokumentiert?* Eine Deaktivierung von Berechtigungsprüfungen ist bei entsprechender Parametrisierung (siehe oben) sowohl global über die Transaktion SU25 oder in Abhängigkeit individueller Transaktionen lokal über die Transaktion SU24 möglich. Deaktivierungen sind alternativ über Tabelle USOBX_C Feld OKFLAG mit Feldwert „N“ und Feld MODIFIED mit Feldwert „X“ für lokale Deaktivierungen und über Tabelle TOBJ_OFF auswertbar. Prüfung, ob Berechtigungsprüfungen lokal oder global deaktiviert sind, und wenn, ob diese dokumentiert und sinnvoll begründet sind.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
7.4.	**Parameter Deaktivierung Transaktionsprüfung:** *Wird eine Deaktivierung der Transaktionsprüfung über die korrespondierenden Parameter verhindert?* Über den Parameter auth/no_check_on_tcode ist es möglich, den Transaktions-Check bei Start einer Transaktion vollständig mit dem Wert „N“ zu deaktivieren. Der Parameter sollte es Unternehmen mit Berechtigungskonzepten aus Vor-S_TCODE-Zeiten ermöglichen, ihre Bestandsrollen ohne eine Erweiterung um Berechtigungen für S_TCODE zumindest für eine vorübergehende Zeit zu nutzen. Aktuelle Rollenkonzepte sollten immer über S_TCODE Berechtigungen verfügen. Insofern sollte der Parameter immer auf „N“ eingerichtet sein. Prüfung auf Einstellung der Deaktivierungsparameter für die Transaktionsprüfung.

Tabelle 17 Deaktivierungsparameter

Parameter-Name	Begründung	Vorschlag	Default
auth/no_check_in_some_cases	Auch wenn der Parameter-Name es aus Revisionsgründen nahezulegen scheint, mit einem „N“ eine Deaktivierung von Berechtigungsprüfungen grundsätzlich zu vermeiden, setzt die Nutzung des Profilgenerators die Einstellung mit „Y“ voraus und ist also „alternativlos“.	Y	Y
auth/object_disabling_active	Wird der Parameter auth/object_disabling_active auf „Y“ gesetzt, kann über die Transaktion AUTH_SWITCH_OBJECTS ein beliebiges Berechtigungsobjekt bei der Berechtigungsprüfung aller Transaktionen, in denen es verwendet wird, vollständig deaktiviert werden. Insofern sollte der Parameter auf „N“ eingestellt sein.	N	N
auth/no_check_on_tcode	Der Parameter ermöglicht es, die Prüfung der Ausführung von Transaktionen über das Berechtigungsobjekt S_TCODE vollständig zu deaktivieren. Insofern sollte der Parameter immer mit „N“ eingerichtet sein.	N	N
auth/rfc_authority_check	Der Profilparameter auth/rfc_authority_check definiert, in welchen Fällen eine S_RFC-Berechtigungsprüfung stattfindet. Während der Parameter im Default auf 1 eingerichtet ist, sollte eine Anpassung auf 6 (Anmeldung und Berechtigungsprüfung erforderlich, aber nicht für den Funktionsbaustein RFC_PING) vorgenommen werden.	6	1

6.7 Change-Management bei Verwendung des SolMan

6.7.1 Application Lifecycle Management (ALM) mit dem SAP Solution Manager

Der SAP Solution Manager (SolMan) ist eine auf ABAP und Java basierte Plattform für das Application Lifecycle Management (ALM). Die Web-basierte Plattform unterstützt somit die Planung, Steuerung und Kontrolle von Software über ihren gesamten Lebenszyklus hinweg – beginnend bei der Konzeption über die Entwicklung und den Einsatz bis hin zur Stilllegung. Die Implementierungs- und Betriebsphasen im ALM werden unter dem SolMan 7.2 durch folgende Anwendungsfälle, auch nach einem agilen ALM, unterstützt:

- Application-Operations
- Business-Process-Operations
- Data-Volume-Management
- Change-Control-Management
- Custom-Code-Management
- IT-Service-Management
- Landscape-Management
- Process-Management
- Project-Management
- Test-Suite
- Cross-opics
- Focused Build and Focused Insights

6.7.2 Risiken

- Anforderungen zu Änderungen von Programmen und Konfigurationen in den an einen SAP SolMan angeschlossenen IT-Systemen werden nicht präzise definiert, nicht richtig priorisiert oder unkontrolliert freigegeben.
- Änderungen an Programmen und Einstellungen des Produktivsystems werden nicht sach- bzw. anforderungsgerecht umgesetzt.
- Änderungen des eingesetzten Verfahrens erfolgen unautorisiert.
- Nicht ausreichend durchgeführte Programmtests führen dazu, dass Fehler zu spät oder gar nicht entdeckt werden.
- Die Datenkonsistenz der Produktivdaten geht verloren.
- Eine Änderungsdokumentation wird nicht erstellt, und dieser Sachverhalt gefährdet die Nachvollziehbarkeit des eingesetzten Verfahrens.
- Sicherheitsrelevante SAP-Meldungen werden nicht zeitnah umgesetzt. Dies führt als Folge zu Daten-Leaks, Systemstillständen oder unautorisierten Manipulationen der gesamten IT-Landschaft.

6.7.3 Kontrollziele

- Nur autorisierte und ausreichend getestete Änderungen werden über den SAP SolMan an ein produktives IT-System zur Implementierung weitergegeben.
- Änderungen sind nachvollziehbar, sodass das Management das eingesetzte Verfahren steuern kann.
- Sicherheitsrelevante Änderungen erfolgen zeitnah, um die Sicherheit des SAP-Systems und der damit verarbeiteten Daten zu gewährleisten.
- Die Vergabe von Berechtigungen zum ALM im SAP SolMan erfolgt nach dem Prinzip der Vergabe geringstmöglicher Rechte und unter Wahrung von Funktionstrennungen.
- Test- und Freigabeverfahren einschließlich von Maßnahmen unter Anwendung des Vier-Augen-Prinzips sind im SolMan implementiert und nachvollziehbar.
- Systemeinstellungen bez. der Protokollierung von Änderung stellen im SolMan sicher, dass die Änderungsdokumentationserstellung durch das SAP-System unterstützt wird.
- Änderungen für die an den SolMan angeschlossenen IT-Systeme werden über den SolMan nachvollziehbar dokumentiert, sodass die Anforderungen an eine transparente Verfahrensdokumentation gemäß den GoBD, den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff, erfüllt werden.

6.7.4 Prüfprogramm: SolMan

Tabelle 18 Prüfprogramm: SolMan

NR.	Prüfprogramm: SolMan
	Bei Einsatz des SolMan kann bereits in der Planungsphase zur Implementierung der SolMan mit der Applikation „Projektmanagement und Lösungsdefinition“ eingesetzt werden. Die Lösungsdefinition führt in der Regel die fachlichen Anforderungen und die SAP-Lösung zusammen, um diese Anforderungen zu implementieren.
1.	**Kontrollziel:** Lösungsdokumentationen erfolgen strukturiert und kontrollwirksam nach „Geschäftsprozessen“ bzw. „Bibliotheken“. **Risiko:** Das Anlegen und Managen der Lösungsdokumentationen erfolgen unstrukturiert. Damit besteht das Risiko, dass Dokumentationen gar nicht, falsch oder durch unautorisierte Anwendende bearbeitet werden mit der Folge einer nicht zielgerichteten Implementierung.

NR.	Prüfprogramm: SolMan
1.1 H	Lösungsdokumentationen erfolgen strukturiert in den Rubriken „Geschäftsprozesse“ bzw. „Bibliotheken“. Vorgehen zur Prüfung: - App. Projektmanagement und Lösungsdokumentation - App. Lösungsdokumentation - Lösung > Geschäftsprozesse bzw. Bibliotheken
1.2 H	Die Zugriffsrechte zum Management der Lösungsdokumentationen sind nach dem Prinzip der Vergabe geringstmöglicher Rechte und unter Wahrung der Funktionstrennung vergeben. Im SAP-Backend-System erfolgt die Vergabe von Rollen und Berechtigungen unter Bezugnahme auf das Berechtigungsobjekt SM_SDOC, Lösungsdokumentation. Für dessen Feld ACTVT, Aktivität, stehen folgende Berechtigungsausprägungen zur Verfügung: • 01 - Hinzufügen • 02 - Ändern • 03 - Anzeigen • 06 - Löschen • 07 - Aktivieren • 43 - Freigeben • 50 - Verschieben • 68 - Modellieren • 69 - Verwerfen • 94 - Übersteuern • D1 – Kopieren Vorgehen zur Prüfung der vergebenen Berechtigungen: Transaktion: SUIM Programm: RSUSR002

NR.	Prüfprogramm: SolMan
1.3 H	Die Zugriffsrechte zum Management der Lösungsdokumentationen sind in Bezug auf die Projekte und die „Geschäftsprozesse“ bzw. „Bibliotheken“ im SolMan nach dem Prinzip der Vergabe geringstmöglicher Rechte vergeben. Im SAP-Backend-System erfolgt die Vergabe von Rollen und Berechtigungen unter Bezugnahme auf das Berechtigungsobjekt SM_SDOC, Lösungsdokumentation, Feld SMUDAAREA, Berechtigungsbereich, und Feld SMUDAUTHGR, Berechtigungsgruppe. Berechtigungsbereiche und Berechtigungsgruppen können über das Viewcluster SMUD_AUTHG geprüft werden. Vorgehen zur Prüfung der vergebenen Berechtigungen: Transaktion: SUIM Programm: RSUSR002 Transaktion zur Anzeige des Viewclusters SMUD_AUTHG: SM34
2.	**Kontrollziel:** Der SolMan unterstützt über die Testsuite ein ordnungsgemäßes Testmanagement. Programmänderungen an IT-Systemen, die an den SolMan angeschlossen sind, werden vor der Produktivsetzung angemessen getestet. **Risiko:** Nicht hinreichend getestete Änderungen führen zu fehlerhaften Verarbeitungen und Daten in den SAP-Systemen.
2.1 H	Die Zugriffsrechte zur Testplanverwaltung sind nach dem Prinzip der Vergabe geringstmöglicher Rechte und unter Wahrung der Funktionstrennung vergeben. Die Apps „Testplanverwaltung“ und „Testplanauswahl“ sind für die testenden Anwendenden sachgerecht autorisiert. Die Berechtigungen sind differenziert nach den Tests zu den relevanten „Geschäftsprozessen“ bzw. „Bibliotheken“. Im SAP-Backend-System erfolgt die Vergabe von Rollen und Berechtigungen unter Bezugnahme auf das Berechtigungsobjekt SM_SDOC, Lösungsdokumentation. Für die Differenzierung der Zugriffsrechte bez. Tests zu den relevanten „Geschäftsprozessen“ bzw. „Bibliotheken“ stehen folgende Felder zur Verfügung: • SMUDAAREA, Berechtigungsbereich • Feld SMUDAUTHGR, Berechtigungsgruppe.

NR.	Prüfprogramm: SolMan
	Berechtigungsbereiche und Berechtigungsgruppen können über das Viewcluster SMUD_AUTHG geprüft werden. Vorgehen zur Prüfung der vergebenen Berechtigungen: Transaktion: SUIM Programm: RSUSR002 Transaktion zur Anzeige des Viewclusters SMUD_AUTHG: SM34 Vorgehen zur Prüfung der vergebenen Berechtigungen: Transaktion: SUIM Programm: RSUSR002
2.2 H	Sicherheitskritische Berechtigungen zur Testplanverwaltung sind eingeschränkt bzw. gar nicht vergeben. Die Testsuite insbesondere mit den Apps „Testplanverwaltung“ und „Testplanauswahl“ ist für die testenden Anwendenden sachgerecht autorisiert. Das relevante Berechtigungsobjekt lautet S_DEVELOP, ABAP Workbench. Für das Testmanagement sind folgende Ausprägungen zu dem Feld OBJTYPE, Objekttyp, relevant: • ECAT, Testskripte • ECSC, Testskripte • ECSD, Systemdatencontainer • ECTC, Testkonfigurationen • ECTD, Testkonfigurationen • SCAT, Testfälle Vorgehen zur Prüfung der vergebenen Berechtigungen: Transaktion: SUIM Programm: RSUSR002
3.	**Kontrollziel:** Änderungen an der SolMan-Systemkonfiguration über die Apps der „System- und Anwendungsüberwachung“ erfolgen kontrollwirksam und sind nachvollziehbar. **Risiko:** Die Konfiguration des SolMan und die Aktivitäten zur SolMan-Systemadministration und -überwachung bestimmen maßgeblich das ordnungsgemäße Change-Management der an den SolMan angeschlossenen IT-Systeme. Unsachgemäße Einstellungen können zu Fehlern in den angeschlossenen IT-Systemen führen.

NR.	Prüfprogramm: SolMan
3.1 H	Die Zugriffsrechte zur Systemadministration im SolMan sind nach dem Prinzip der Vergabe geringstmöglicher Rechte vergeben. Im SAP-Backend-System erfolgt die Vergabe von Rollen und Berechtigungen über Berechtigungsobjekte in der Objektklasse SM, Solution Manager. Um in der App „Alert-Eingang“ im SolMan eine Änderung der Konfiguration über einen Alert auszuschließen, sind lesende Berechtigungen zu folgendem Berechtigungsobjekt zu vergeben: Berechtigungsobjekt: SM_MOAL_TC, Zugriff auf Monitoring and Alerting Feld: Monitor, Monitore in Monitore and Alerting, Wert: CONFIG Feld: Aktivität in Monitoring and Alerting: 03 Vorgehen zur Prüfung der vergebenen Berechtigungen: Transaktion: SUIM Programm: RSUSR002

7 SAP S/4HANA Cloud, public edition

Die Beschreibung der Risiken, Kontrollen und Prüfungshandlungen basiert auf dem S/4HANA Cloud, public edition Release 2208.

7.1 Einleitung

Die Software-as-a-Service-Lösung SAP S/4HANA Cloud, ehemals Multi-Tenant Edition, Essentials Edition oder Public Cloud genannt, ist eine der möglichen Deployment-Formen der SAP-S/4HANA-Technologie. Die Softwarelösung unterscheidet sich in technischer Hinsicht deutlich von den übrigen S/4HANA Betriebsmodellen sowie von den Vorgängerversionen SAP R/3 bzw. SAP ERP. Dies hat Einfluss auf die Entwicklung einer entsprechenden Prüfungsstrategie sowie auf die Durchführung von IT-System-Prüfungen für das S/4HANA-Cloud-System. Nachfolgend sind einzelne Charakteristika mit Auswirkung auf die Prüfungsstrategie aufgelistet:

- Bedienoberfläche: Der Zugriff zum SAP-S/4HANA-Cloud-System erfolgt ausschließlich über das im Rahmen der Entwicklung von SAP S/4HANA neu eingeführte Fiori Launchpad. Die Nutzung der SAP-GUI ist weder für IT- noch für Anwendungsbenutzer möglich.
- Release-Updates: Die SAP-S/4HANA-Cloud-Lösung wird im Rahmen verpflichtender Release-Updates kontinuierlich aktualisiert und durch neue Technologien und ergänzende Funktionalitäten erweitert. Informationen zu geplanten und erfolgten Änderungen im Rahmen der Release-Updates werden von SAP bereitgestellt und können auf verschiedenen Websites (bspw. SAP Road Map Explorer, What's New Viewer, Release Assessment and Scope Dependency) je Business-Area eingesehen und analysiert werden.
- Konfiguration: In der SAP S/4HANA Cloud ist eine individuelle Erstellung und Anpassung von Funktionalitäten, Anwendungsoberflächen, Logik etc. nur eingeschränkt bzw. teilweise gar nicht umsetzbar. Die Anpassung der Konfiguration (bspw. Definition von Belegarten, Einstellungen zur Kontenfindung) des SAP-Systems erfolgt mithilfe der Konfigurationselemente „Self Service Configuration User Interface“ (SSCUI) in der Fiori App „Lösung verwalten“ (App-ID F1241) bzw. via SAP Central Business Configuration. Der SAP-Customizing-Einführungsleitfaden (SAP IMG) steht in der SAP S/4HANA Cloud nicht zur Verfügung.

- Funktionsumfang: Die Softwarelösung ermöglicht durch eine starke Orientierung entlang der SAP S/4HANA Cloud Best-Practices und eingeschränkten individuellen Anpassungsmöglichkeiten ein hohes Maß an Standardisierung. Zur Abbildung der eigenen Prozesse erfolgt hierbei die Aktivierung von Funktionspaketen (Scope Items). Zusätzlich kann der vorausgelieferte Funktionsumfang mithilfe ausgewählter benutzerdefinierter Logiken (BAdIs), Reports, Objekte, Felder, analytischer Abfragen etc. erweitert werden. Einen Überblick über die SAP-S/4HANA-Cloud-Funktionsumfänge und Scope-Items kann im SAP Best Practice Explorer gewonnen werden (SAP Best Practice Explorer).
- Betrieb: Das SAP-S/4HANA-Cloud-System wird durch SAP betrieben und aus SAP-Rechenzentren oder ausgewählten Hyperscalern[1] zur Verfügung gestellt. SAP ist hierbei für die Datenbank und die Applikations-Plattform verantwortlich. Sofern das SAP-S/4HANA-Cloud-System im SAP-Rechenzentrum gehostet wird, liegt die Verantwortlichkeit für den Betrieb der Infrastruktur ebenfalls bei SAP. Wenn das S/4HANA-Cloud-System beim Hyperscaler läuft, werden Teile der grundlegenden Infrastruktur vom jeweiligen Hyperscaler betrieben. Auch die Prozesse und Aktivitäten im Bereich Software-Change-Management und Programmentwicklung liegen durch die Bereitstellung und verpflichtende Einspielung von Updates zu großen Teilen bei SAP.

Diese Charakteristika führen zu Änderungen bei der Kontrolldurchführung in den verschiedenen Prüfungsbereichen (Authentifizierung, Autorisierung, Change-Management, IT-Operations, Analyse SOC-Report). Während die Kontrolldurchführung bisher größtenteils bei dem/der Kund:in lag, erfolgt mit der Einführung der SAP S/4HANA Cloud ein Übergang der Kontrollhandlungen im Rahmen des internen Kontrollsystems von dem/der Kund:in hin zu SAP. Die Gesamtverantwortung für die Prozesse und betrieblichen Abläufe liegt hierbei weiterhin bei dem/der Kund:in.

Für die IT-System-Prüfung im Rahmen der Jahresabschlussprüfungen stellt SAP seinen Kund:innen über das SAP Trust Center Service Organization Control Reports (SOC-Reports) zur Verfügung:

- SOC 1: Prüfung nach SSAE-18- und ISAE-3402-Standards (Typ I und Typ II)
- SOC 2: Prüfung nach Prüfungsstandards ISAE 3000 und AT 101, basiert auf den AICPA-Grundsätzen für Vertrauensdienste

Die Reports beschreiben das durch SAP implementierte Kontrollsystem zur Sicherstellung der Verfügbarkeit, Vertraulichkeit, Integrität und zum Datenschutz der

[1] Überbegriff für Infrastructure-as-a-Service(IaaS)-Provider.

verarbeiteten Daten des/der Kund:in. Die Reports können durch die Kund:innen im SAP Trust Center angefordert werden (SAP Trust Center).

Rollen, Kataloge und Restriktionen

Hinweis: Im Gegensatz zu OnPremise ist es in S/4HANA Cloud nicht möglich, Anwendungsbenutzer direkt anzulegen, sondern es müssen zunächst sogenannte „Mitarbeitende“ angelegt werden. Auf Basis der Mitarbeitenden können dann Benutzer erstellt werden, denen wiederum Berechtigungen zugeordnet werden.

Bei erster Betrachtung der in der S/4HANA Cloud verfügbaren Apps für die Pflege von Benutzern und Berechtigungen entsteht beim Betrachter der Eindruck einer im Vergleich zum S/4HANA OnPremise eigenständigen Struktur.

Dies ist eine Konsequenz aus dem Angebot der SAP, den Anwendenden über die Fiori Apps zur Benutzer- und Berechtigungspflege die auch im S/4HANA Cloud nach wie vor vollumfänglich zugrunde liegende alte Berechtigungsarchitektur des S/4HANA OnPremise in einer möglichst einfachen Form der Pflege zur Verfügung zu stellen.

Die Fiori Apps werden über das Fiori Launchpad via Business-Kataloge (ähnlich zu S/4HANA-OnPremise-Einzelrollen) zur Verfügung gestellt und den Benutzern via Business-Rollen (ähnlich zu S/4HANA-OnPremise-Sammelrollen) zugeordnet. In den Business-Katalogen sind ein oder mehrere Fiori Apps zusammengefasst, die semantisch zusammengehören. Die Business-Kataloge werden von SAP vordefiniert ausgeliefert und lassen sich nicht in Bezug auf Namen oder Text und in Bezug auf eine Verringerung der zugeordneten Apps reduzieren. Die einzig mögliche Änderung ist eine Erweiterung um individuelle, benutzerdefinierte Apps.

Neben den Fiori Apps enthält ein Business-Katalog darüber hinaus sogenannte Zugriffseinschränkungen („Restriktionen“). Dabei handelt es sich um die Möglichkeit einer Differenzierung des Zugriffs über a) Aktivitäten, b) über organisatorische und c) weitere funktionale Kriterien. Im Gegensatz zu OnPremise gibt es in der S/4HANA Cloud zur Einschränkung der Aktivitäten ausschließlich drei Möglichkeiten:

- „Schreibend“ (alle Arten von Datenänderungen wie bspw. Erstellen, Ändern und Löschen)
- „Lesend“ (lesender Zugriff auf Daten)
- „Werte Hilfe“ (lesender Zugriff auf die Werte Hilfe).

Auch bei den Restriktionen handelt es sich technisch um von der SAP für die Pflege durch Anwendende selektiv ausgewählte Felder von Berechtigungsobjekten.

Ein oder mehrere Kataloge werden in S/4HANA Cloud einer Anwendungsrolle zugeordnet. SAP stellt hierfür auch Standard-Anwendungsrollen (Template Anwendungsrollen) zur Verfügung. Diese bilden typische Arbeitsplätze analog zur Activate-Methodik ab. Bei Nutzung dieser Standardrollen können bei Release-

Wechseln Change-Informationen nachvollzogen und die Kund:innen-individuellen Ableitungen abgeglichen und angepasst werden (siehe **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.**).

Das S/4HANA-Cloud-System enthält sogenannte „Business Role Templates“ (BRT), welche von der SAP vordefinierte Berechtigungen enthält. Diese BRTs werden von der SAP ausgeliefert, damit ein Kunde in nicht produktiven Systemen eine Möglichkeit hat, neue Funktionalitäten zu testen, ohne explizit neue Rollen dafür erstellen zu müssen; diese BRTs sind für die produktive Nutzung im SAP-System nicht geeignet. Die Verwendung von BRTs im Starter- und im Q-System ermöglicht einen schnelleren Start in das Projekt, sofern dies aus Risikoperspektive vertretbar ist und keine sensiblen Daten in den Vorsystemen vorhanden sind. Eine dauerhafte Zuordnung ist nicht empfehlenswert.

Im Produktivsystem müssen Kund:innen-eigene Business-Kataloge unter Berücksichtigung der Kund:innen-spezifischen Aufbauorganisation eingerichtet werden.

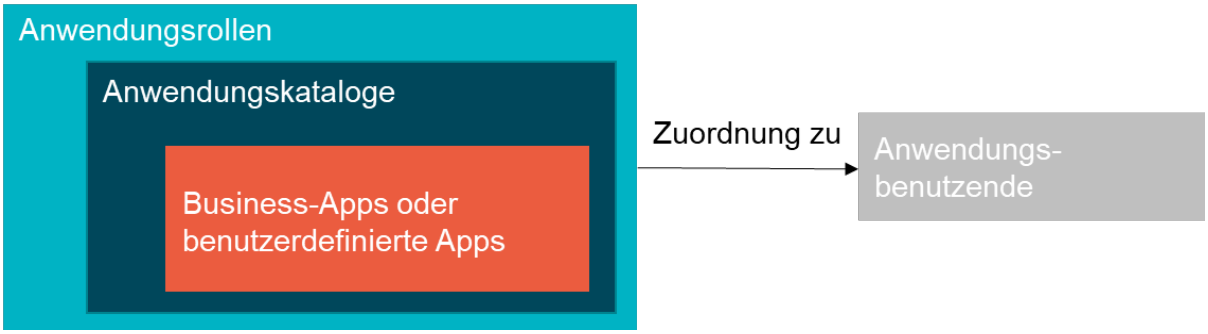

Abbildung 3 Elemente des SAP-S/4HANA-Cloud-Berechtigungskonzepts

Da die Kataloge von den Anwendenden verpflichtend verwendet werden müssen und keine Analysemöglichkeit auf Ebene der zugrunde liegenden technischen Berechtigungen möglich ist, werden die Kataloge regelmäßig durch einen externen / eine externe Prüfende analysiert, um sicherzustellen, dass diese frei von Segregation-of-Duty(SoD)-Konflikten sind. Die Prüfung erfolgt nach dem internationalen Prüfstandard ISAE 3000 (revised). Der jeweilige Assurance-Report der letzten Prüfung kann von SAP-Kund:innen im SAP Trust Center angefordert werden.

Dies kann jedoch nur für die Kataloge gelten. Anwendungsrollen als Kombination von Katalogen sind nicht zwangsläufig SoD-frei und sind insofern Gegenstand einer eigenen Prüfung des/der Kund:in gegen sensitive Funktionen und Funktionstrennungen.

Neben der reduzierten und vereinfachten Sicht und Pflege der Rollen und Berechtigungen sind auch in Bezug auf die Benutzerpflege einige Besonderheiten in S/4HANA Cloud zu beachten.

Typen von Benutzern

Eine/Ein AnwendungsBenutzer ist eine Person, die sich am SAP-S/4HANA-Cloud-System anmelden kann und die die relevanten Geschäftsaufgaben erledigen muss. Diese Person benötigt zum Erledigen ihrer Aufgaben Zugriff auf Daten, jedoch nur auf die für diese spezifischen Aufgaben erforderlichen Daten.

Unter den verschiedenen Arten von Anwendungsbenutzern gibt es zwei besondere:

Administrator-Anwendungsbenutzer: Der Administrator / Die Administratorin hat sehr technische Aufgaben im Zusammenhang mit der Einrichtung des Systems für alle anderen Benutzer. Zu den Aufgaben des Administrators / der Administratorin gehören zum Beispiel das Anlegen von Benutzern, die Zuweisung von Rollen und Berechtigungen an Benutzer, die Einrichtung von Verbindungen zwischen SAP S/4HANA Cloud und anderer Software usw.

Konfigurations-Expert:innen: Konfigurationsexpert:innen sind dafür verantwortlich, die S/4HANA-Cloud-Lösung auf die unternehmensspezifischen Anforderungen anzupassen. Dies erfolgt über die SAP Central Business Configuration oder den Solution Builder. Im Rahmen dessen werden spezifische Anwendungsrollen mit ausgeliefert, die diese Benutzer zugewiesen bekommen können. Bei der Zuordnung ist zu beachten, dass eine Aufteilung des/der Expert:in sinnvoll sein kann, wenn dies zum Minimalberechtigungsprinzip beiträgt. So kann es sein, dass zum Beispiel eine Aufteilung nach Modulen sinnvoll ist, wenn die Konfigurations-Expert:innen nicht modulübergreifend arbeiten.

Technische SAP-Benutzer: Diese Benutzer sind ein spezifischer Typ eines im SAP-S/4HANA-Cloud-System verfügbaren technischen Benutzer. Diese Benutzer wurden von SAP zum Ausführen operativer Aufgaben im SAP-S/4HANA-Cloud-System vordefiniert. Technische SAP-Benutzer werden außerdem für Kund:innen-spezifische Aufgaben wie das Ausführen und Einplanen von Jobs benötigt. Die erforderliche Jobvorlage enthält standardmäßig der für das Ausführen des Jobs benötigte technische SAP-Benutzer.

Kommunikationsbenutzer: In SAP S/4HANA Cloud sind Kommunikationsbenutzer Technische Benutzer, die für die Kommunikation zwischen dem SAP-S/4HANA-Cloud-System und einem beliebigen integrierten System erforderlich sind. Dabei kann zwischen von SAP vordefinierten SAP-Kommunikationsbenutzern und von Kund:innen angelegten Kommunikationsbenutzern unterschieden werden.

Benutzerdefinierte Kommunikationsbenutzer werden in der App „Kommunikationsbenutzer pflegen“ erstellt und den Systemen für die ein- und ausgehende Kommunikation zugewiesen. Diese technischen Benutzer verwenden entweder eine einfache Authentifizierung oder Zertifikate, um zwischen der SAP S/4HANA Cloud und dem integrierten System zu kommunizieren.

Für jedes Kommunikationsszenario und damit auch für jeden technischen User gibt es einen vordefinierten Business-Katalog der dem technischen User automatisch zugeordnet wird. Dieser Business-Katalog wird von der SAP definiert und kann von Kund:innen nicht verändert werden. Diese Vorgehensweise trifft auf sämtlichen technischen User zu, wie zum Beispiel auch auf Druck-User.

Support Benutzer: SAP verwendet Support-Benutzer, um Kund:innen bei Problemen mit dem SAP-S/4HANA-Cloud-System zu unterstützen. Für die Unterstützung ist ein Kund:innen-Ticket erforderlich. Die Einsätze können über die Apps „Technische Benutzer anzeigen“ und „Security Audit Log anzeigen“ nachvollzogen werden. Die Benutzer-ID ist für den/die Kund:in aus Gründen des Datenschutzes anonymisiert ersichtlich; der Bezug zu einer Person ist für SAP möglich.

Initiale Benutzer: In älteren S/4HANA-Cloud-Systemen wurde ein generischer Benutzer mit zufälligem Anmeldenamen und Passwort generiert, mit dessen Hilfe das initiale Anlegen der Geschäftsbenutzer mit Rollen für Administrator:innen in S/4HANA-Cloud-Systemen und das Anlegen weiterer Administrator:innen in den SAP Cloud Identity Services – Identity Authentication (IAS) durchgeführt werden konnte. Die nachgelagerte Benutzeradministration ist dann mit persönlichen Benutzern durchzuführen. Die initialen Anmeldedetails wurden mit zwei E-Mails an die IT-Kontaktperson des/der Kund:in verschickt.

In aktuellen S/4HANA-Cloud-Systemen wird direkt ein persönlicher Benutzer für die IT-Kontaktperson des/der Kund:in mit administrativen Berechtigungen generiert. Die initiale Anmeldung erfolgt hier durch einen Aktivierungslink für die SAP Cloud Identity Services Identity Authentication (IAS).

Standardbenutzer: Es gibt keine Standardbenutzer mit bekannten Passwörtern (z. B. DDIC, SAP*).

Ergänzende Hinweise: In S/4HANA Cloud sind folgende Themen im Vergleich zum S/4HANA OnPremise für den Kund:innen-Zugriff nicht mehr relevant/verfügbar:

- Es gibt keine weitreichenden SAP-Basis-Berechtigungen für Kund:innen-Benutzer (z. B. SAP_ALL, Löschen von Änderungsbelegen)
- Es gibt keine Referenzbenutzer als Typ von Benutzern.
- Es gibt keinen direkten Zugriff auf kritische Systemtabellen für Kund:innen-Geschäftsbenutzer.
- Das Security Audit Log ist von SAP im S/4HANA-Cloud-System aktiviert worden und kann von dem/der Kund:in nicht deaktiviert oder konfiguriert werden. Der aktivierte Status des Security Audit Logs ist in der Kachel „Statisches System-Audit anzeigen“ sichtbar.

Change-Management in der S/4HANA Cloud

Alle Änderungen an einem Produktivsystem, die sich auf die Funktionalität der Finanzbuchhaltung auswirken, müssen von den Kund:innen getestet werden. Das Ziel ist es, sicherzustellen, dass diese Änderungen keine negativen Auswirkungen auf die Vollständigkeit und Richtigkeit der Finanzbuchhaltung haben. Im Falle einer Jahresabschlussprüfung müssen die Kund:innen nachweisen, dass sie Änderungen („Changes“) an ihrem System regelmäßig testen und vor dem Transport in das Produktivsystem freigeben.

Es gibt mehrere Gründe für solche Systemänderungen:

- Eine neue Version des Softwareprodukts
- Änderungen an der Geschäftskonfiguration des Softwareprodukts
- Änderungen an den Geschäftsrollen des Softwareprodukts
- Änderungen an der Erweiterbarkeit

SAP S/4HANA Cloud bietet Kund:innen ein Testsystem (Q) und ein Produktivsystem (P). Im Q-System werden Änderungen durchgeführt und getestet. Wenn die Tests erfolgreich sind, werden diese Änderungen in das P-System übertragen. Weiterhin gibt es inzwischen auch die Möglichkeit, ein Entwicklungssystem (D) zu nutzen, um Kund:innen-spezifische Entwicklungen im Rahmen der Erweiterbarkeit zu entwickeln. Weitere Details in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.**.

7.2 Risiken

Generell gelten die generischen Risiken aus den Kapiteln 3.2, 4.2 und 5.1.2 auch für SAP S/4HANA Cloud. Es gibt jedoch verschiedene Risiken aus diesen Kapiteln, die nicht auf SAP S/4HANA Cloud zutreffen. Folgende Risiken sind beispielsweise obsolet:

- Sicherheitsanforderungen (bspw. Aktivierung des Security Audit Log, Aktivierung der Tabellenprotokollierung, Schließung des Systems gegen Änderungen) sind nicht ausreichend im SAP-ERP-System definiert und implementiert.
- Die Standardpasswörter für Standard-SAP-IDs wurden nicht in allen Mandant:innen geändert und sind nicht angemessen gesichert.
- Programmänderungen durch den/die Kund:in werden nicht angemessen getestet und genehmigt, bevor sie in die Produktionsumgebung übernommen werden.
- Weitreichende Profile (bspw. SAP_ALL, SAP_NEW, Änderungsbelege löschen) sind im Produktivsystem vergeben und werden nicht ausreichend überwacht.

- Die Möglichkeit zur Pflege der globalen Systemänderungsoption und der Mandant:innen-Wartungseinstellungen ist nicht (genügend) eingeschränkt.
- In der Produktionsumgebung wird Entwicklungszugang gewährt, der nicht (ausreichend) auf autorisierte Konten beschränkt ist (z. B. Notfallzugang), und die Nutzung wird nicht überwacht.

Zusätzlich kommen für SAP S/4HANA Cloud beispielsweise die folgenden Risiken hinzu:

- Rollen und Verantwortlichkeiten sind nicht explizit und ausführlich genug zwischen dem Dienstleister und dem auslagernden Unternehmen aufgeteilt beziehungsweise definiert.
- Dem auslagernden Unternehmen ist es nicht möglich, die Einhaltung regulatorischer Anforderungen zu überprüfen.
- Das interne Kontrollsystem des Dienstleisters ist nicht ausreichend, um den reibungslosen und ordnungsgemäßen Betrieb zu garantieren.
- Die Beteiligten haben keinen ausreichenden Überblick über die technischen und finanziellen Anforderungen, die eine Auslagerung mit sich bringt.
- Das auslagernde Unternehmen ist nicht imstande, die Resilienz der Cloud-Infrastruktur zu beurteilen; infolgedessen kommt es zu Systemausfällen.
- Das auslagernde Unternehmen ist nicht imstande, Daten zu löschen und wiederzuerlangen.
- Die physische Infrastruktur des Dienstleisters ist nicht ausreichend gegen unautorisierte Zugriffe gesichert.
- Aufgrund erhöhter Netzwerk- beziehungsweise Systemlatenz kommt es zu Beeinträchtigungen der Cloud-Services.
- Complementary-User-Entity-Controls werden vom Unternehmen nicht gekannt oder nicht durchgeführt.
- Die Auswirkungen von ineffektiven internen Kontrollen des Dienstleisters auf das eigene Unternehmen werden nicht oder nur unzureichend bewertet.

7.3 Kontrollziele

- Die jahresabschlussrelevanten, auszulagernden Dienste sind eindeutig definiert und festgehalten.
- Dienstleister, Zeitraum sowie die Form der Auslagerung sind genau definiert.
- Die Risiken der Auslagerung sowie die Voraussetzungen für selbige wurden im Vorfeld ausführlich evaluiert.
- Die Kontrollen, für deren Durchführung der Dienstleister verantwortlich ist, sind eindeutig definiert.
- Die Verantwortlichkeit für das IKS ist definiert.
- Das auslagernde Unternehmen überprüft regelmäßig die Eignung und Funktionalität des IKS.
- Jahresabschlussrelevante Daten werden über die gesetzlich vorgeschriebene Aufbewahrungszeit hinweg aufbewahrt.
- Rechnungslegungsrelevante Daten für die IT-Prüfung werden seitens des Dienstleisters gespeichert und stehen für den Jahresabschluss zur Verfügung.
- Das Ziel ist es, sicherzustellen, dass der Service-Provider (sprich SAP) keine unautorisierten Handlungen im Produktivsystem der Kund:innen durchführt. Der Fernzugriff von SAP zur Software-Wartung ist eingeschränkt, autorisiert und rechtzeitig entfernt. Der Zugriff auf die SAP-Support-Benutzer wird angemessen kontrolliert, wenn die IDs nicht in Gebrauch sind.

  Hinweis: Es ist nicht möglich, dass der Kunde auf SAP-Support-Benutzer zugreifen kann. Die Verwendung der SAP-Support-Benutzer kann im Security Audit Log nachvollzogen werden.
- Notfallzugriffe und Supportzugriffe der SAP erfolgen ausschließlich nach vorheriger Genehmigung durch den/die Kund:in, werden protokolliert, von einer anderen Person als dem Benutzer, der den Zugriff verwaltet, überwacht und zeitnah wieder entfernt.

7.4 Prüfprogramm: Authentifizierung

Tabelle 19 Prüfprogramm: Authentifizierung - Anwendungsbenutzer

NR.	Prüfprogramm: Authentifizierung – Anwendungsbenutzer
-	Die Authentifizierung von Anwendungsbenutzern erfolgt nicht im S/4HANA-Cloud-System, sondern in den angeschlossenen SAP Cloud Identity Services – Identity Authentication Service (IAS) Tenant (Identity-Provider). Da der Identity-Provider für unterschiedliche Systeme eingesetzt werden kann, ist in einem ersten Schritt die Applikation zu identifizieren, da diese definiert, welche Authentifizierungseinstellungen für das S/4HANA-Cloud-System angewendet werden. Hier angegeben sind die englischen Navigations-Pfade. IAS: Applications and Resources > Applications > Suche nach den S/4HANA-Cloud-Systems, z. B. my<ID>.s4hana.ondemand.com > Tab Authentication and Access. Relevante Einstellungen sind: • Password-Policy (z. B. Enterprise, Standard, benutzerdefiniert), • Risk-Based Authentication, • User-Application-Access Die Passwort-Regeln können anschließend angezeigt werden: IAS: Applications and Resources > Password Policies In Abhängigkeit von der Konfiguration der SAP Cloud Identity Services – Identity Authentication Tenants besteht die Möglichkeit, dass die Authentifizierung nochmals zu einem anderen Identity-Provider weitergeleitet werden kann. In diesem Fall ist die Authentifizierungskonfiguration dort zu prüfen. IAS: Applications and Resources > Applications > Suche nach den S/4HANA Cloud Systems, z. B. my<ID>.s4hana.ondemand.com > Tab Trust > Conditional Authentication > Default Authenticating Identity Provider Hinweise: • Ein Verhindern von Mehrfachanmeldungen ist technisch nicht möglich. • Die Passwörter für die Authentifizierung von Benutzern unterliegen bestimmten Regeln. Diese Regeln werden in der Kennwortrichtlinie definiert. Der Identity Authentication Service (IAS) bietet zwei vordefinierte und eine benutzerdefinierte Kennwortrichtlinie: ○ Standard: (vordefinierte) Standardeinstellung

NR.	Prüfprogramm: Authentifizierung – Anwendungsbenutzer
	○ Unternehmen: (vordefiniert) erweiterte Kennwortverwaltungsfunktionen, die stärker als der Standard sind ○ Benutzerdefiniert: (konfigurierbar) benutzerdefinierte Kennwortverwaltungsfunktionen, die es erlauben, für verschiedene Attribute stärkere Einstellungen vorzunehmen als in der Richtlinie Unternehmen. • Die Kennwortkomplexität ist standardmäßig im IAS festgelegt und muss mindestens drei der folgenden Klassen enthalten: Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen.
1.	**Kontrollziel:** Die Bildung des Kennworts unterliegt Komplexitätsregeln; die Gültigkeitsdauer eines Kennworts ist beschränkt; das Ausprobieren von Kennworten ist erschwert. **Risiko:** Bei Verwendung von schwachen Passwörtern können diese ggf. erraten, ausprobiert oder ausgespäht werden.
1.1 TOP	Die genutzte Passwort-Richtlinie ist hinsichtlich folgender Punkte zu überprüfen: - Kennwortlänge - Kennworthistorie - Maximale Kennwortgültigkeit - Minimale Kennwortgültigkeit - Maximale Anzahl der Falschanmeldungen bis zur Sperre der Passwortanmeldung - Zeit der Sperre für die Passwortanmeldung Sichere Passwörter können nach unterschiedlichen Kriterien gebildet werden, bspw. sehr lange Passwörter ohne Rotation vs. 8-stellige Passwörter mit regelmäßigem Wechsel (siehe BSI IT-Grundschutz ORP.4.A23).
2.	**Kontrollziel:** Verhinderung des Missbrauchs von gestohlenen Kennwörtern **Risiko:** Gestohlene Kennwörter können zur unautorisierten Anmeldung in S/4HANA-Cloud-Systemen verwendet werden.
2.1 TOP	Die Zwei-Faktor-Authentifizierung ist in der Risk-Based Authentication für kritische Benutzergruppen oder als Standard konfiguriert.

Tabelle 20 Prüfprogramm: Authentifizierung – Initiale/Initialer Benutzer

NR.	Prüfprogramm: Authentifizierung – Initiale/Initialer Benutzer
-	Fiori-Kachel: „Technische Benutzer anzeigen“
3.	**Kontrollziel:** Nutzung des initialen Benutzers verhindern **Risiko:** Der initiale Benutzer kann zur direkten Anmeldung am S/4HANA-Cloud-System verwendet werden ohne Nutzung des IAS.
3.1	Das Sperrkennzeichen für den initialen Benutzer (Anmeldename: <zufällig erzeugt>, Technische-Benutzer-ID: SAP_CUST_INI) ist gesetzt.

Tabelle 21 Prüfprogramm: Authentifizierung – Kommunikationsbenutzer

NR.	Prüfprogramm: Authentifizierung – Kommunikationsbenutzer
-	Die Authentifizierung von technischen Benutzern durch die/den Mandant:in, bspw. im Rahmen von technischen Integrationen, erfolgt direkt im S/4HANA-Cloud-System über eine gesonderte API-URL (Application Programming Interface), z. B. my312287my<ID>-api.s4hana.ondemand.com. Die Anmeldung bzw. Authentifizierung erfolgt für Kommunikationsbenutzer direkt an der S/4HANA Cloud und nicht über IAS. Ein Überblick der Kommunikationsbenutzer erfolgt über die Fiori-Kachel: „Kommunikationsbenutzer pflegen“. Hinweise: • Die minimale Kennwortlänge und -komplexität sind von SAP definiert und können von dem/der Kund:in nicht angepasst werden. Die vordefinierten Kennwortregeln sind in der Kachel „Statisches System-Audit anzeigen“ sichtbar.
1.	**Kontrollziel:** Inaktive, Technische Benutzer sind gesperrt. Nur autorisierte Mitarbeitende kennen das Passwort für den technischen Benutzer. **Risiko:** Unautorisierte Nutzung der Kommunikationskanäle, die dazu führt, dass Daten nicht vollständig und/oder fehlerhaft übertragen werden. **Hinweis:** Benutzer können die Kommunikationsszenarien nicht mehr anpassen; bspw. kann kein Benutzer des/der Kund:in mit dem Anwendungsbenutzer anpassen, wie Daten und welche Daten übertragen werden. Jedoch ist es möglich, mit einem technischen Benutzer die bestehenden Daten innerhalb der Schnittstelle zu verändern.

NR.	Prüfprogramm: Authentifizierung – Kommunikationsbenutzer
1.1 TOP	**Prozessschritte** **Inaktive Kommunikationsbenutzer** Eine Liste der Kommunikationsbenutzer mit dem Datum der letzten erfolgreichen Anmeldung erhält man über die Anwendung Kommunikationsbenutzer pflegen > Einblenden der Spalte „Letzte Anmeldung“ > Überprüfung, ob alle Kommunikationsbenutzer, die sich bspw. seit 90 Tagen nicht angemeldet haben, ein Sperrkennzeichen gesetzt haben. **Zugriff auf Passwörter der Kommunikationsbenutzer** Der Kunde muss prüfen, welche Mitarbeitenden Zugriff auf das Passwort / die Passwörter der Kommunikationsbenutzer haben. Zugriff sollten nur wenige, autorisierte Mitarbeitende aus der IT erhalten.

7.5 Prüfprogramm: Autorisierung

Tabelle 22 Prüfprogramm: Autorisierung

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
1.	**Dokumentation und Standards**
	Kontrollziel: Die für Benutzer und Berechtigungen vorliegenden Dokumentationen und Standards ermöglichen es den am Prozess Beteiligten, die korrespondierenden Strukturen, die Prozesse, die Organisation und die hierbei zu beachtenden Vorgaben in angemessener Zeit nachzuvollziehen. **Risiko:** Durch fehlende, unvollständige oder unverständliche Dokumentation können die Beteiligten die Benutzer und Berechtigungen und ihre eigenen Aufgaben im Prozess nicht verstehen. Daraus ergeben sich Risiken für eine unsachgemäße Pflege und Vergabe der Rollen.
1.1.	**Platzhalter Dokumentation und Standards:** *Sind alle im Prüfprogramm in Kapitel 4.5 Dokumentation und Standards enthaltenen, im S/4HANA-Cloud-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Dokumentation und Standards vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das S/4HANA-Cloud-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag. Berücksichtigung der nachfolgenden Hinweise zu Rollen und Berechtigungen und Benutzer und Rechte.
2.	**Benutzer und Rechte**
	Kontrollziel: Die Vorgaben für Benutzer und die Zuordnung von Rollen und Berechtigungen und deren Umsetzung sorgen für eine vollständige Nachvollziehbarkeit der Rollen und ggf. Berechtigungen und deren Zuordnung zu Benutzern und Identitäten. **Risiko:** Bei fehlender Nachvollziehbarkeit auf einer oder mehreren Ebenen eines Benutzer- und Berechtigungskonzepts ergeben sich automatisch Mängel im Minimal- und Funktionstrennungsprinzip und damit eine Gefährdung der Integrität, Verfügbarkeit und Vertraulichkeit von Daten.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
2.1.	**Platzhalter Benutzer und Rechte:** *Sind alle im Prüfprogramm in Kapitel 4.5 Dokumentation und Standards enthaltenen, im S/4HANA-Cloud-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Benutzer und Rechte vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das S/4HANA-Cloud-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag. Berücksichtigung der nachfolgenden Hinweise zu Benutzern und Rechten.
2.2.	**Benutzerkonventionen:** Hinweis: In S/4HANA Cloud werden diese Benutzerinformationen aus dem führenden Identity-Provider übernommen. Benutzer-IDs zu Benutzern können über den Pfad „Identitäts- und Zugriffsmanagement > Anwendungsbenutzer pflegen“ eingesehen werden.
2.3.	**Sonder- und Notfallbenutzer:** Im Vergleich zu OnPremise gibt es keine klassischen Sonder- oder Notfallbenutzer mehr (vgl. SAP_ALL etc. sind obsolet). Es gibt weiterhin Technische Benutzer, die in der App „Technische Benutzer anzeigen“ angezeigt werden können. Dies umfasst technische SAP-Benutzer (User ID SAP* und DDIC), Druckbenutzer (User ID CP*), SAP-Kommunikationsnutzende (User ID SAP_COM_*) wie auch eigens angelegte Kommunikationsnutzende (User ID CC*) sowie die/den initiale:n Nutzende:n (User ID SAP_CUST_INI). Zudem können alle SAP-Supportuser angezeigt werden (User ID _SAP*), sowie das SAP-Support-Benutzeranfragenprotokoll. Hinweis: Der/Die initiale Nutzende (User ID SAP_CUST_INI) sollte im Produktivbetrieb gesperrt sein.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
2.4.	**SAP-Support-Benutzer:** *Wird der Zugriff von SAP-Support-Benutzern angemessen überwacht?* Der Zugriff von SAP-Anwendungsbetreuern auf Funktionen des Cloud-Systems erfolgt über dedizierte technische SAP-Service- und Support-Benutzer. Die Beantragung eines Benutzers durch eine/einen SAP-Support-Mitarbeitende:n ist mittels der App „Technische Benutzer anzeigen“ sichtbar. Hier werden auch Details wie Vorfall-ID, Benutzer-ID, Zugriffskategoriebeschreibung, Kund:innen-Benutzer, Anforderungsdatum und Gültigkeitsdatum angezeigt. Sicherheitskritische Aktivitäten von SAP-Support-Mitarbeitenden werden im Security Audit Log protokolliert und können mit der App: „Security Audit Log anzeigen“ angezeigt werden. Prüfung auf Beantragung und Nutzung der SAP-Service- und -Support-Benutzer hinsichtlich folgender Aspekte: Passen die Vorfall-IDs zu den Beantragungen der SAP-Support-Benutzern (insb. bei Beantragung eines Kund:innen-Benutzers)? Wurden Debug-Aktivitäten durchgeführt? Wurde die Systemänderbarkeit verändert? Hinweis: Im Unterschied zu OnPremise können Kund:innen SAP-Support-Benutzer nicht selber erzeugen oder administrieren. Diese werden im Rahmen der Bearbeitung von SAP-Support-Tickets von der SAP verwaltet.
	Technische Benutzer: *Wird der Zugriff von sonstigen technischen Benutzern angemessen überwacht?* Neben den „normalen“ Dialogbenutzern stehen in der S/4HANA Cloud auch Technische Benutzer im System zur Verfügung. Diese können wie die SAP-Service-Benutzer über die App/Kachel „Technische Benutzer anzeigen“ angezeigt werden. Druckbenutzer und der initiale Benutzer können auch gesperrt oder entsperrt sowie das Passwort zurückgesetzt werden. Prüfung auf angemessene Überwachung und Administration von sonstigen technischen Benutzern.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
3.	**Rollen und Berechtigungen**
	Kontrollziel: Die Vorgaben für Rollen und technische Berechtigungen und deren Umsetzung sorgen für eine vollständige Nachvollziehbarkeit der technischen Berechtigungen auf der untersten Ebene bis zu den Rollen als Zwischenebene. **Risiko:** Bei fehlender Nachvollziehbarkeit auf einer oder mehreren Ebenen eines Benutzer- und Berechtigungskonzepts ergeben sich automatisch Mängel im Minimal- und Funktionstrennungsprinzip und damit eine Gefährdung der Integrität, Verfügbarkeit und Vertraulichkeit von Daten.
3.1.	**Platzhalter Rollen und Berechtigungen:** *Sind alle im Prüfprogramm in Kapitel 4.6 Rollen und Berechtigungen enthaltenen, im S/4HANA-Cloud-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Prozesse und Organisation vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das S/4HANA-Cloud-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag. Berücksichtigung der nachfolgenden Hinweise zu Rollen und Berechtigungen.
3.2.	**Namenskonvention und Rollengestaltung:** Hinweis: Die im SAP-System vorhandenen Rollen können über die Apps „Business-Rollen pflegen“ und „IAM-Informationssystem“ eingesehen werden.
3.3.	**Organisationsdimensionen:** Hinweis: Die aktuell verwendeten Organisationsdimensionen und Einschränkungstypen pro SAP-Rolle samt Ausprägungen können über die App „IAM-Informationssystem“ durch Auswahl der Hauptentität „Anwendungsrolle“ und Auswahl des Reiters „Anwendungsrolle – Einschränkung“ eingesehen werden.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
4.	**Sensitive Funktionen**
	Kontrollziel: Für die Anwendung liegt ein Regelwerk mit sensitiven Funktionen vor. Sensitive Funktionen werden ausschließlich über Rollen vergeben, deren Deklaration die beinhalteten sensitiven Funktionen eindeutig erkennbar machen. Für Rollen mit sensitiven Funktionen ist ausgewiesen, für welche Instanzen und an welche Benutzergruppen eine Vergabe zulässig ist. Benutzer erhalten Berechtigungen für sensitive Funktionen unter strenger Beachtung des Minimalprinzips. **Risiko:** Die Nutzung von Rollen mit nicht nachvollziehbaren sensitiven Berechtigungen und die Vergabe sensitiver Berechtigungen an Benutzer unter Verstoß gegen Minimalprinzip und Funktionstrennungsregeln gefährden die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen.
4.1.	**Platzhalter Sensitive Funktionen:** *Sind alle im Prüfprogramm in Kapitel 4.8 Sensitive Funktionen und Funktionstrennung enthaltenen, im S/4HANA-Cloud-Kontext anwendbaren Prüfungshandlungen für sensitive Funktionen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Sensitive Funktionen vorgegebenen und anwendbaren Prüfungshandlungen für sensitive Funktionen an dieser Stelle in das S/4HANA-Cloud-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag. Berücksichtigung der nachfolgenden Hinweise zu sensitiven Funktionen.
4.2.	**Sensitive Funktionen:** Hinweis 1: Bei den im Folgenden aufgeführten spezifischen sensitiven Funktionen handelt es sich um ausgewählte Beispiele. Ein vollständiges und unternehmensindividuelles Regelwerk geht im Umfang weit darüber hinaus.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
4.3.	**Sensitive Funktionen:** Hinweis 2: Eine Identifizierung von Anwendenden und Applikationsrollen mit sensitiven Funktionen erfolgt über die Identifizierung des für die Ausführung der Funktionen erforderlichen Katalogs in Kombination mit den korrespondierenden Einschränkungen zumindest für die Aktivität Schreiben. Hierzu werden die beiden folgenden Schritte ausgeführt: a) Navigieren Sie zur Anwendung IAM-Informationssystem > Anwendungsrolle – Applikation > Bericht herunterladen. Die weitere Analyse kann in einer Tabellenkalkulationsanwendung vorgenommen werden > Pivot-Tabelle mit Filter für kritische Anwendungen. b) Navigieren Sie zu den IAM-Informationen der Anwendung > Anwendungsrolle – Einschränkung > Wenden Sie die identifizierten Anwendungsrollen aus a) als Filter an > Generieren Sie einen Bericht > Wenden Sie „schreiben“ als Filter auf die Spalte „Kategorie“ an und identifizieren Sie Anwendungsrollen mit Schreibzugriff. Kombinieren Sie die Ergebnisse der Vorgänge a) und b) über die Anwendungsrolle. Nur Anwendungsrollen mit beiden Ergebnissen erfüllen die Voraussetzungen einer sensitiven Pflege-Aktivität. c) Navigieren Sie zur Anwendung IAM-Informationssystem > Anwendungsrolle – Anwendungsbenutzer > Werten Sie die identifizierten Anwendungsrollen mit Schreibzugriff aus b) an > Laden Sie den Bericht der Anwendenden mit den identifizierten Anwendungsrollen herunter. Hinweis: Via Applikation „IAM-Kennzahlen“ kann man diverse Prüfungshandlungen durchführen (zum Beispiel wie lange sich bestimmte Benutzer im System nicht mehr angemeldet haben oder wie viele Business-Rollen einem Benutzer zugewiesen sind). Bezüglich sensitiver Funktionen kann ein/eine Auditor:in via Report „Uneingeschränkte Business-Rollen“ sehen, wie viele Business-Rollen mit uneingeschränkten Aktivitäten „Schreibend“, „Lesend“ und „Wertehilfe“ im System vorhanden sind.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
a)	Administration
4.4.	**Benutzerverwaltung:** *Sind die Berechtigungen zur Pflege von Benutzern nur einem eingeschränkten Kreis von Benutzer-Administrator:innen zugänglich?* Die Prüfung kann über das oben beschriebene Verfahren unter Einschränkung auf die Anwendungskatalog-ID „SAP_CORE_BC_IAM_UM“ (Identitäts- und Zugriffsverwaltung – Benutzerverwaltung) erfolgen. Prüfung auf Vergabe des obigen Katalogs zur Benutzerverwaltung mit Schreibrechten nur an einen restriktiven Kreis von Benutzer-Administrator:innen.
4.5.	**Rollenzuordnung:** *Sind die Berechtigungen zur Zuordnung von Rollen nur einem eingeschränkten Kreis von Benutzer-Administrator:innen zugänglich?* Die Prüfung kann über das oben beschriebene Verfahren unter Einschränkung auf die Anwendungskatalog-ID „SAP_CORE_BC_IAM_RA“ (Identitäts- und Zugriffsverwaltung – Rollenzuordnung) erfolgen. Prüfung auf Vergabe des obigen Katalogs zur Zuordnung von Rollen mit Schreibrechten nur an einen restriktiven Kreis von Benutzer-Administrator:innen.
4.6.	**Rollenpflege:** *Sind die Berechtigungen zur Pflege von Rollen (auch im Rahmen von Upgrades) nur einem eingeschränkten Kreis von Rollen-Administrator:innen zugänglich?* Die Prüfung kann über das oben beschriebene Verfahren unter Einschränkung auf die Anwendungskatalog-ID „SAP_CORE_BC_IAM_RM“ (Identitäts- und Zugriffsverwaltung – Rollenverwaltung) und „SAP_CORE_BC_IAM_UPGRADE“ (Identitäts- und Zugriffsverwaltung – Upgrade) erfolgen. Prüfung auf Vergabe des obigen Katalogs zur Pflege von Rollen mit Schreibrechten nur an einen restriktiven Kreis von Rollen-Administrator:innen.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
4.7.	***Nachrichten-Monitoring:*** *Sind die Berechtigungen zum Überwachen von Nachrichten (Schnittstellen für Datentransfer) nur einem eingeschränkten Kreis von Administrator:innen zugänglich?* Die Prüfung kann über das oben beschriebene Verfahren unter Einschränkung auf die Anwendungskatalog-ID „SAP_CORE_BC_COM*“ (Nachrichtenmonitoring*) erfolgen. Prüfung auf Vergabe des obigen Katalogs zur Pflege von Rollen mit Schreibrechten nur an einen restriktiven Kreis von Rollen-Administrator:innen.
4.8.	**Job-Monitoring:** Berechtigungen für das Anlegen und Ausführen von Batch-Jobs *Sind die Berechtigungen zur Anlage und Verwaltung von Anwendungsjobs nur einem eingeschränkten Kreis von Administrator:innen zugänglich?* Die Prüfung kann über das oben beschriebene Verfahren unter Einschränkung auf die Anwendungskatalog-ID „SAP_CORE_BC_APJ_JCE“ (Anwendungsjobverwaltung – Anwendungsjobs) und „SAP_CORE_BC_APJ_TPL“ (Anwendungsjobverwaltung – Anwendungsjobvorlagen) erfolgen. Jobs können in dem hier beschriebenen Release-Stand nur unter dem eigenen Anmeldenamen angelegt werden. Eine Zuordnung zu einem anderen Benutzer kann mit der App „Pflege Job User“ (Anwendungskatalog-ID „SAP_CORE_BC_APJ_USR_PC“) durchgeführt werden. Prüfung auf Vergabe des obigen Katalogs zur Pflege von Anwendungsjobs nur an einen restriktiven Kreis von Administrator:innen.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
b)	Logs und Data Browser
4.9.	**Auswerten Security Audit Log:** *Sind die Berechtigungen zur Auswertung der Protokolldateien des Security Audit Log nur einem eingeschränkten Kreis von Systemadministrator:innen und weiteren explizit berechtigten Mitarbeitenden zugänglich?* Die Prüfung kann über das oben beschriebene Verfahren unter Einschränkung auf die Anwendungskatalog-ID „SAP_CORE_BC_SEC_SAL“ (Security-Audit-Log anzeigen) erfolgen. Prüfung auf Vergabe des obigen Katalogs zum Auslesen des Security Audit Log nur an einen restriktiven Kreis von Systemadministrator:innen und weiteren explizit berechtigten Mitarbeitenden.
4.10.	**Kund:innen-Daten-Browser:** *Sind die Berechtigungen zur Nutzung des Kund:innen-Daten-Browsers nur einem eingeschränkten Kreis zugänglich?* Die Nutzung des Kund:innen-Daten-Browsers erlaubt eine direkte Leseansicht von Tabelleninhalten und CDS-Sichten, die von der SAP freigegeben wurden. Die Prüfung kann über das oben beschriebene Verfahren unter Einschränkung auf die Anwendungskatalog-ID „SAP_CORE_BC_CDB_PC“ erfolgen. Prüfung auf Vergabe des obigen Katalogs Nutzung des Kund:innen-Daten-Browsers nur für ausgewählte Mitarbeitende und für ausgewählte Tabellen/CDS-Sichten.
c)	Business Configuration
4.11	**SAP Central Business Configuration (CBC):** *Sind die Berechtigungen zur Nutzung der SAP Central Business Configuration nur einem eingeschränkten Kreis von Mitarbeitenden zugänglich?* **Hinweis:** Diese Prüfungshandlung ist nur relevant für S/4HANA-Cloud-Systeme, die mit CBC provisioniert wurden. Systeme, die vorher erstellt wurden, verwenden für Scoping und Business Configuration die App

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	„Lösung verwalten“. Ob ein System CBC verwendet oder nicht, ist beim Öffnen der App „Lösung verwalten“ sichtbar. **Hinweis:** Die Berechtigungen in CBC steuern das sog. Scoping und die Konfiguration der organisatorischen Struktur (z. B. Erzeugung eines Company Code). Die S/4HANA-Cloud-bezogene Business Configuration erfolgt weiterhin im S/4HANA-Cloud-System und benötigt entsprechende Berechtigungen im S/4HANA-Cloud-System. Der Zugang zu CBC kann über folgende Gruppen im angeschlossenen IAS vergeben werden. Diese Berechtigungen steuern das sog. Scoping. • „SAP_CBC_CONSUMPTION_PROJECT_LEAD“ (alt: „SAP_CBC_CONSUMPTION_ACTIVITY_ALL“) (Project-Manager: Ausführen aller Project-Experience-Tätigkeiten), • „SAP_CBC_CONSUMPTION_KEY_BENUTZER (Key-Benutzer: Ausführen von Project-Experience-Tätigkeiten, mit Ausnahme kritischer Aktivitäten (wie Beantragen von Systemen) • „SAP_CBC_CONSUMPTION_DISPLAY_USER“ (Lesezugriff von Project-Experience-Tätigkeiten) Prüfung auf Vergabe der obigen IAS-Gruppen nur für ausgewählte Mitarbeitende.
4.12	**Business Configuration:** *Sind die Berechtigungen zur Änderung der Kund:innen-Konfiguration nur einem eingeschränkten Kreis zugänglich?* In der S/4HANA Cloud können Kund:innen nur in eingeschränktem Umfang Änderungen an der Systemkonfiguration vornehmen. Die Berechtigungen können über granulare Anwendungskataloge für die unterschiedlichen Konfigurationsbereiche vergeben werden. Die Navigation zur Business Configuration erfolgt entweder über die SAP Central Business Configuration oder die Vorgänger-App „Lösung verwalten“. Die Prüfung kann über das oben beschriebene Verfahren unter Einschränkung auf verschiedene Anwendungskatalog-IDs erfolgen, z. B. • „SAP_CA_BC_IC_LND_CBC_PC“ Central Business Configuration – General Configuration • „SAP_CA_BC_IC_LND_FIN_AP0_PC“ Kreditorenbuchhaltung – Konfiguration

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	• „SAP_CA_BC_IC_LND_FIN_AR0_PC“ Debitorenbuchhaltung – Konfiguration Eine vollständige Liste aller Anwendungskatalog-IDs können in dem Business-Role-Template „SAP_BR_BPC_EXPERT“ eingesehen werden. Weitere Informationen, zu welchem Anwendungskatalog eine Konfigurationsaktivität gehört, befinden sich im Dokument „Configuration Activity.xlsm (SAP Customer)“ im Schritt „Request Expert Configuration“ der „SAP Activate Methodology for SAP S/4HANA Cloud“. Prüfung auf angemessene und genehmigte Vergabe der Berechtigungen zur Konfiguration an berechtigte und qualifizierte Mitarbeitende.
5.	**Funktionstrennung**
	Kontrollziel: Für die Anwendung liegt ein Regelwerk mit Funktionstrennungen sowie mit korrespondierenden mitigierenden Kontrollen vor. Das Regelwerk bezieht sich auf einzelne sensitive Funktionen, die in Kombination ein höheres Risiko aufweisen, als sich aus den jeweils einzelnen Risiken ergibt. Rollen und Berechtigungen werden unter Vermeidung von Funktionstrennungen erstellt. Funktionstrennungsverletzungen aus der Vergabe von Rollen und Berechtigungen an Benutzer werden vermieden oder durch Zuordnung mitigierender Kontrollen kompensiert. **Risiko:** Durch das Auftreten von Funktionstrennungsverletzungen in Benutzern ergeben sich Risiken für die Integrität und Verfügbarkeit von Daten.
5.1.	**Platzhalter Funktionstrennungen:** *Sind alle im Prüfprogramm in Kapitel 4.8 Sensitive Funktionen und Funktionstrennung enthaltenen, im S/4HANA-Cloud-Kontext anwendbaren Prüfungshandlungen für Funktionstrennungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Funktionstrennung vorgegebenen und für Funktionstrennungen anwendbaren Prüfungshandlungen an dieser Stelle in das S/4HANA-Cloud-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag. Berücksichtigung der nachfolgenden Hinweise zu Funktionstrennungen.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
5.2.	**Funktionstrennung:** Hinweis: Zur Auswertung von Funktionstrennungen nutzen Sie die Ergebnisse der sensitiven Funktionen unter 4.3, die an den in Ihrem Unternehmen relevanten Funktionstrennungsregeln beteiligt sind. Analysieren Sie, ob risikorelevante Kombinationen a) auf Anwendungsrollen-Ebene sowie b) auf Benutzer-Ebene vorkommen.
5.3.	**Funktionstrennung Rollenpflege und Rollenzuweisung:** *Wird die Vergabe von Rollenpflegeberechtigungen in der Entwicklung und von Rollenzuweisungsberechtigungen in der Produktion durch angemessene Verfahren unterbunden?* Zur Feststellung von SoD-Verletzungen ist eine Auswertung auf eine Kombination von „Rollenzuordnung“-Anwendungsrollen mit Katalog „SAP_CORE_BC_SEC_RM“ und Schreib-Einschränkung in der Produktion und „Rollenpflege“-Anwendungsrollen mit Katalog „SAP_CORE_BC_SEC_RA“ und Schreib-Einschränkung in der Entwicklung andererseits durchzuführen (zum Risiko siehe vertiefte Erläuterungen in Kapitel 6.5). Prüfung auf Vergabe von Berechtigungen sowohl für Rollenpflege in der Entwicklung als auch für Rollenzuordnung in der Produktion. Bei vorliegenden Konflikten auf Benutzer-Ebene Prüfung auf angemessene Kompensation der Risiken durch korrespondierende dokumentierte und ausgeführte Kontrollmaßnahmen.
6.	**Prozesse und Organisation**
	Kontrollziel: Die für Benutzer und Berechtigungen etablierten Prozesse und organisatorischen Rollen gewährleisten, dass der Zustand der Vergabekette zwischen Benutzern, Rollen und technischen Berechtigungen auf einem angemessenen Niveau unter Beachtung der regulatorischen Anforderungen verbleibt. **Risiko:** Aus fehlenden Vorgaben oder unzureichender Anwendung der Vorgaben für Prozesse und organisatorische Rollen folgt eine Verschlechterung der Benutzer- und Berechtigungsstrukturen mit der Folge der Verletzung des Minimalprinzips und der sich ergebenden Gefährdung der Integrität, Verfügbarkeit und Vertraulichkeit von Daten.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
6.1.	**Platzhalter Prozesse und Organisation:** *Sind alle im Prüfprogramm in Kapitel 4.9 Prozesse und Organisation enthaltenen, im S/4HANA-Cloud-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Prozesse und Organisation vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das S/4HANA-Cloud-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag. Berücksichtigung der nachfolgenden Hinweise zur Berechtigungs- und Benutzeradministration.
6.2.	**User-Lifecycle-Management:** Hinweis: Eine Liste der aktiven Benutzer erhält man über folgende Anwendung: „Anwendungsbenutzer pflegen“ > Herunterladen > Benutzer herunterladen. Eine Liste der Benutzer und der diesen zugeordneten Berechtigungen findet sich über die Anwendung: „Anwendungsbenutzer pflegen“ > Herunterladen > Benutzer Rollenzuordnung herunterladen. Die Selektion von Benutzeränderungen und Rollenzuordnungen kann über die Anwendung „Anwendungsbenutzer pflegen“ > Änderungen anzeigen > Prüfungszeitraum und alle Filter anwenden > Herunterladen vorgenommen werden. Hierbei kann nach einem Änderungszeitraum, der Anwendungsbenutzer-ID ebenso wie nach durchgeführten Aktionen („Anwendungsrollen wurden geändert“) selektiert werden. Hinweis: Das Sperren inaktiver Anwendungsbenutzer nach einer definierten Anzahl von Tagen (bspw. 90 Tage) kann mit Anwendung „Sperre für nicht verwendete Anwendungsbenutzer einplanen“ und dem Anwendungsjob „Nicht verwendete Anwendungsbenutzer sperren“ automatisiert werden.
6.3.	**Role-Lifecycle-Management:** Hinweis: Um Stichproben zur Prüfung der angemessenen Dokumentation von Rollenanlagen und -änderungen zu erhalten, kann eine Liste der Rollenänderungen über die Applikation „Anwendungsrollen pflegen“ ermittelt werden im Menübereich „Anzeige der Änderungen“. In produktiven Umgebungen ist grundsätzlich davon auszugehen, dass Anwendungsrollen nicht direkt geändert werden.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Die Art von Änderungen an Anwendungsrollen, die über Transporte kommen, können über die App „Erweiterbarkeitsbestand“ im Katalog „SAP_CORE_BC_EXT_INVENTORY“ eingesehen werden. Die Änderungen für spezifische Anwendungsrollen können auch direkt über die Rolle eingesehen werden. In der Applikation ist dazu auf folgenden Menübereich abzuspringen: „Erweiterbarkeitsbestand“ durch Klicken auf folgendes Symbol: 
6.4.	**Privileged-Access-Management** Hinweis: Wie bei anderen technischen Layern, müssen auch bei S/4HANA Cloud privilegierte Benutzer eindeutig identifizierbar sein. Mit dieser Information können die Daten der privilegierten Benutzer und die diesen zugeordneten Berechtigungen über die oben unter User-Lifecycle-Management genannten ersten beiden Apps ermittelt werden. Die Selektion von Änderungsbelegen für Aktionen privilegierter Benutzer für Stichproben können über die App/Kachel „Security-Audit-Log anzeigen“ durch Einschränken des Zeitstempels und Selektion der relevanten Audit-Ereignisse ermittelt werden.
6.5.	**Access-Compliance-Management** Hinweis: Für den Fall, dass SAP Cloud Identity Access Governance (IAG) verwendet wird: Den Regelsatz erhält man, indem man im Administrations-Panel auf der Registerkarte Zugriffsanalyse > Anwendung Regel-Setup > den Produktionsregelsatz des Clients auswählt und dann „Datei herunterladen“. Die Benutzerzugriffsanalyse erhalten Sie durch Navigieren zu > „Benutzerzugriff analysieren“ auf der Registerkarte Zugriffsanalyse > Ausführen des Berichts für ALLE Benutzer > Herunterladen des Berichts. Wird IAG nicht verwendet: Hier müssen die Regeln manuell über die Relationen Benutzer und Rollen/Kataloge ausgewertet werden über Identity and Access Management > Anwendungsbenutzer pflegen > Benutzer Rollenzuordnung herunterladen.

7.6 Prüfprogramm: Change-Management

Tabelle 23 Prüfprogramm: Neue Software-Versionen

NR.	Prüfprogramm: Neue Software-Versionen
-	Neue Software-Versionen werden regelmäßig durch SAP eingespielt (Stand 2022 – alle 6 Monate); eine Beschreibung des relevanten Prozesses kann in den SOC-Berichten nachgelesen werden. Der Kunde muss sicherstellen, dass notwendige Tests/Berechtigungsanpassungen für das neue Release gemacht werden. Die neuen Software-Versionen werden zunächst in das Qualitätssystem eingespielt; zwei Wochen später erfolgt die Aktualisierung des Produktivsystems. Die Upgrade-Termine sind nicht flexibel, die Updates erfolgen für alle SAP-S/4HANA-Cloud-Systeme an denselben Wochenenden (Februar und August). Wenn während des Upgrade-Prozesses Probleme identifiziert werden, die mehrere Kund:innen betreffen, erfolgt die Erstellung eines Knowledge-Base-Artikels durch SAP sowie – sofern zur Lösung des Problems notwendig – die Einspielung von Hotfixes. Die durch den/die Kund:in im Rahmen der Upgrade-Prozesse durchzuführenden Aktivitäten können der Beschreibung der Phase „Run“ im SAP Roadmap Viewer für die SAP S/4HANA Cloud entnommen werden. Entsprechend der Komplexität der Prozesse und Schnittstellen sind ergänzende Kontrollen/Aktivitäten durch den/die Kund:in durchzuführen. Für die Analyse von Änderungen im Rahmen der Release-Upgrades stehen verschiedene durch SAP bereitgestellte Quellen zur Verfügung. Hierzu gehören bspw. • S/4HANA Cloud Release Assessment and Scope Dependency Tool (https://whats-new-generic.cfapps.us10.hana.ondemand.com) • SAP Road Map Explorer (https://roadmaps.sap.com/board?PRODUCT=67837800100800007389&range=CURRENT-LAST#Q4%202021) • Roadmap Viewer (https://go.support.sap.com/roadmapviewer/) • What’s new (https://help.sap.com/docs/SAP_S4HANA_CLOUD) • S/4 HANA Cloud IAM Release Activities (https://support.sap.com/content/dam/SAAP/SAP_Activate/S4H_701%20Identity%20and%20Access%20Management%20Quarterly%20Release%20Activities.pdf)

NR.	Prüfprogramm: Neue Software-Versionen

	Hinweise:
	• Folgende Themen aus S/4HANA OnPremise sind nicht mehr in Kund:innen-Verantwortung, sondern von SAP definiert.
	  ○ Es gibt keine Möglichkeit für die/den Kund:in, die Systemänderbarkeit/Mandant:innen-Änderbarkeit umzustellen.
	  ○ Es gibt keine Möglichkeit, den SAP-Quellcode zu verändern.
	  ○ Der/Die Kund:in muss keine SAP Security Notes einspielen.
	• Neue Releases werden automatisch von SAP nach dem definierten Release-Zyklus eingespielt.
	• Optional bietet SAP auch „CFD – Continous Feature Deliveries“ an.

1.	**Kontrollziel:** Neue Software-Versionen werden auf ihre Auswirkungen auf bestehende Prozesse, Berechtigungen und Schnittstellen hin überprüft. Betroffene Prozesse und Schnittstellen werden nach Einspielen des Release-Upgrades in das Qualitätssystem getestet (Durchführung von Regressionstests). Die Tests, ggf. aufgetretene Fehler sowie ggf. notwendige Anpassungen an Schnittstellen, Prozesse oder Konfiguration werden dokumentiert. **Risiko:** Auswirkungen auf bestehende Prozesse und Schnittstellen bei Einspielung neuer Software-Versionen werden nicht ausreichend analysiert. Beeinträchtigungen im Prozess sowie in den Schnittstellen werden nicht erkannt, was zu Fehlern in der Datenverarbeitung und zu manuellem Mehraufwand führen kann.
1.1 TOP	**Kontrollfragen zum Prozess:** • Gibt es einen definierten Prozess für die Analyse und Überwachung der eingespielten Release-Updates sowie Hotfixes? • Wie werden relevante Änderungen und Neuerungen in den Updates identifiziert und getestet? • Welche Prozesse sind für die Durchführung der Regressionstests implementiert? • Wie werden Änderungen an Anwendungsrollen nach Upgrades geprüft und ggf. notwendige Änderungen vorgenommen?

NR.	Prüfprogramm: Neue Software-Versionen
1.2 TOP	**Anwendungsrollen nach Upgrade pflegen** Navigieren Sie zur Fiori App „Anwendungsrollen nach Upgrade verwalten“ (App ID F1492) und prüfen Sie, ob in der Auflistung unbearbeitete Anwendungsrollenänderungen enthalten sind > Prüfen Sie die Listen Einschränkungstypen, Anwendungskatalogabhängigkeiten, Obsolete Anwendungskataloge, Anwendungsrollenvorlagen, Betroffene Anwendungsrollen Hinweis: Die Inhalte in der Fiori App „Anwendungsrollen nach Upgrade verwalten“ sollten nach Einspielung des Upgrades überprüft und angepasst werden. Sobald eine Anpassung vorgenommen wurde, verschwindet die Änderung aus der Auflistung in der Fiori App. Es ist somit ein Abarbeitungsstand in der Fiori App nachvollziehbar. https://support.sap.com/content/dam/SAAP/SAP_Activate/S4H_701%20Identity%20and%20Access%20Management%20Quarterly%20Release%20Activities.pdf
1.3 TOP	• Neuerungen (bspw. Release-Upgrades/Hotfixes) im System prüfen • a) Navigieren Sie im Fiori Launchpad zu Ihrem Namen/Namenskürzel oben rechts in der Anzeigeleiste > Wählen Sie „Über“ > Navigieren Sie zu „Produktname“ > Prüfen Sie die installierte Softwareversion • b) Navigieren Sie zum SAP Road Map Explorer (https://roadmaps.sap.com/board?PRODUCT=67837800100800007389&range=CURRENT-LAST#Q4%202021) > Prüfen Sie, welche Releases im Prüfungszeitraum eingespielt wurden • c) Navigieren Sie zur Fiori App „Neuerungen in Ihrem System“ (App-ID F5641) > Navigieren Sie zu „Releaseunabhängige Neuerungen“, prüfen Sie die Neuerungen und befragen Sie den/die Kund:in hinsichtlich der Berücksichtigung der aufgelisteten Neuerungen und Bewertung des (potenziellen) Einflusses auf die Prozesse und Kontrollen > Navigieren Sie zu „Dringende Neuerungen (aktuell)“, prüfen Sie die Neuerungen und befragen Sie den/die Kund:in hinsichtlich der Berücksichtigung der aufgelisteten Neuerungen.

NR.	Prüfprogramm: Neue Software-Versionen
	Weiterführender Link: • SAP S/4HANA Cloud Documentation https://help.sap.com/docs/SAP_S4HANA_CLOUD • SAP S/4HANA Cloud, 2-System Landscape and SAP Marketing Cloud – Upgrade and Maintenance Schedule • https://www.sap.com/documents/2017/01/867629d8-a27c-0010-82c7-eda71af511fa.html • SAP S/4HANA Cloud, 3-System Landscape – Upgrade and Maintenance Schedule • https://www.sap.com/documents/2021/09/58ffa59e-f97d-0010-bca6-c68f7e60039b.html
1.4	**Kontrollfragen zum Prozess der Notfall-Korrekturen** In Ausnahmefällen kann SAP Notfall-Änderungen auf das betroffene SAP-S/4HANA-Cloud-System verteilen. • War es notwendig, dass Probleme in Kund:innen-Meldungen durch Notfall-Änderungen von SAP korrigiert wurden? • Wenn ja, wie wurden diese Notfall-Änderungen von dem/der Kund:in getestet?

Tabelle 24 Prüfprogramm: Änderungen an der Konfiguration

NR.	Prüfprogramm: Änderungen an der Konfiguration
-	Der Kunde kann Änderungen an definierten Customizing-Einstellungen vornehmen. Diese werden von dem/der Kund:in durchgeführt und in Sprints eingeteilt, die in der Regel ein bis zwei Wochen dauern. Alle Änderungen werden in einem sogenannten Business-Change-Project (BCP) gesammelt, das auf zwei Arten in das Produktionssystem implementiert werden kann. Das BCP kann am Ende eines Sprints im Q-System in eine Warteschlange gestellt werden, damit es in das P-System transportiert werden kann. Der Import erfolgt dann automatisch. Wenn ein Änderungsprojekt zu einem früheren Zeitpunkt in das P-System transportiert werden muss, kann ein sofortiger Transport über die App „Import Collection“ im P-System durchgeführt werden. Es gibt aktuell zwei Möglichkeiten, wie Geschäftskonfigurationsänderungen durch den/die Kund:in durchgeführt werden können. Welche Möglichkeit im System aktiv ist, hängt vom Zeitpunkt der Systembereitstellung ab. • „Central Business Configuration“ (CBC) ist eine übergeordnete Anpassungsoption. Der Zweck von CBC ist es, ein zentrales Werkzeug für die Anpassung jeder Cloud-Lösung zu sein, die ein Kunde betreibt. CBC ist mit dem Qualitätssystem (Q-System) verbunden, das die Testumgebung von S/4HANA darstellt. Diese Verknüpfung impliziert, dass jede Änderung getestet wird, bevor sie in die Produktion überführt wird. • „Manage Your Solution“ (Vorgängerlösung) ist eine Customizing-Option zur Feinabstimmung, die Central-Self-Service-Benutzer-Interface (SSCUI) genannt wird, dem Customizing in älteren Versionen entspricht und nur innerhalb des Q-Systems durchgeführt werden kann. Hinweis: Einige SSCUIs (Self-Service Configuration User Interfaces) sind besonders gekennzeichnet („In P-System wiederholen“) und müssen sowohl im Q-System als auch im P-System durchgeführt werden (dies trifft auch auf Systeme mit angeschlossener CBC zu).
1.	**Kontrollziel:** Änderungen am Customizing werden angemessen getestet und genehmigt, bevor sie in die Produktionsumgebung übernommen werden. **Risiko:** Es werden unangemessene Änderungen an der S/4HANA Cloud vorgenommen, die relevante (automatische) Kontrollen und/oder Berichtslogik enthalten und /oder beeinflussen.

NR.	Prüfprogramm: Änderungen an der Konfiguration
TOP	**Kontrollfragen zum Prozess:** Gibt es einen definierten Prozess, um sicherzustellen, dass nur angemessen getestete und genehmigte Änderungen am Produktivsystem vorgenommen werden? (Hinweis: Relevante Kataloge zur Änderung an Konfigurationseinstellungen beinhalten das technische Kürzel *_LND_*).
1.1	Änderungsprotokolle für einige Web-GUI-SSCUIs, die manuell im P-System nachgearbeitet werden müssen, werden im P-System je SSCUI protokolliert.

Tabelle 25 Prüfprogramm: Erweiterbarkeit

NR.	Prüfprogramm: Erweiterbarkeit
-	S/4HANA Cloud bietet unterschiedliche Möglichkeit der Erweiterbarkeit an: - Erweiterbarkeit für Anwendungsexpert:innen - Erweiterbarkeit für Entwickler:innen - Side-by-Side-Erweiterbarkeit Die Erweiterbarkeit wird von der SAP aktuell noch verbessert. Aus diesem Grund können nur generische Empfehlungen zur Prüfung gegeben werden, da sich die technischen Aspekte noch ändern können. **Kontrollziel:** Erweiterungen werden zentral getestet und genehmigt, bevor sie im Produktivsystem genutzt werden. **Risiko:** Erweiterungen können den Ablauf der Geschäftsprozesse verändern und dazu führen, dass weitere/andere Kontrollen nötig sind, um die ordnungsgemäße Buchhaltung sicherzustellen.
	Nutzung von S/4HANA-Cloud-Erweiterbarkeit *Wird die S/4HANA-Cloud-Erweiterbarkeit genutzt?* Es können verschiedene Apps verwendet werden, um festzustellen, ob die Erweiterbarkeit von S/4HANA Cloud von dem/der Kund:in verwendet wird. - App „IAM Informationssystem“, Hauptentität Anwendung und Anwendungskategorie: Benutzerspezifische Anwendung - „Softwarekollektionen importieren“ - Apps im Bereich „Erweiterbarkeit“, z. B. Erweiterbarkeitsbestand

NR.	Prüfprogramm: Erweiterbarkeit
	Kontrollfragen zum Prozess: Gibt es einen definierten Prozess, um sicherzustellen, dass nur angemessen getestete und genehmigte Erweiterungen im Produktivsystem verwendet werden?
	In Abhängigkeit von der genutzten Erweiterbarkeit werden diese im Entwicklungssystem (3-System-Landschaft) oder im Testsystem (2-System-Landschaft) definiert und durch das Transportmanagement in die folgenden Systeme übertragen. Der Status der importieren Erweiterungen kann in der App „Kollektionen importieren“ angezeigt werden.
	Kontrollfragen zum Prozess: Werden die Erweiterungen in das existierende Berechtigungskonzept integriert?

7.7 Prüfprogramm: IT Operations

Tabelle 26 Prüfprogramm: Interface-/Nachrichten-Monitoring

NR.	Prüfprogramm: Interface-/Nachrichten-Monitoring
-	Es ist möglich, sowohl innerhalb der S/4HANA Cloud (zwischen den Geschäftsbereichen) als auch in Richtung ein- und ausgehender Systeme (SAP und Nicht-SAP) Schnittstellen zu überwachen. Das System bietet die Möglichkeit, den Zugriff auf das Interface-Monitoring einzuschränken. Dies bedeutet, dass ein Benutzer nur dann ein Monitoring durchführen kann, wenn die Berechtigung entsprechend vergeben ist. Innerhalb der S/4HANA Cloud bieten mehrere Anwendungen mit Prefix „Nachrichten-Monitoring“ Zugriff auf Nachrichten und deren Status.
1.	**Kontrollziel:** Die Nachrichten werden überwacht, und festgestellte Probleme werden zeitnah behoben. Der Zugang zu Änderungen an den Nachrichten wird auf der Grundlage der jeweiligen Zuständigkeiten angemessen gewährt. **Risiko:** Abgebrochene, fehlerhafte Nachrichten führen zu einer ungenauen, unvollständigen oder unzulässigen Verarbeitung von Daten.

NR.	Prüfprogramm: Interface-/Nachrichten-Monitoring
1.1	Kontrollfragen zum Prozess: Gibt es einen definierten Prozess, um ungenaue, unvollständige oder unzulässige Verarbeitungen von Nachrichten regelmäßig auszuwerten?
1.2	Innerhalb von Fiori kann die Liste der Nachrichten eingesehen werden, indem man zu Nachrichten-Monitoring > Message Change Log > Gewünschte Filterkriterien einstellen > den Prozess mit einem Klick auf „Go“ starten navigiert. Bspw.: Nachrichten-Monitoring für Administrator:innen mittels Anwendungskatalog „SAP_CA_BC_COM_OP_ERR_PC“. Mit diesem Anwendungskatalog bekommt man einen Überblick über alle systemübergreifenden Schnittstellen und ihre Datennachrichten. Man kann beispielsweise die Grundursachen von Fehlern analysieren und Datennachrichten neu starten oder abbrechen.

Tabelle 27 Prüfprogramm: Job-Monitoring

NR.	Prüfprogramm: Job-Monitoring (z. B. Jobs and Batch-Jobs)
-	In der SAP S/4HANA Cloud kann die Liste der Jobabbrüche durch Aufrufen der Fiori-App „Anwendungsjobs“ eingesehen werden. Die App bietet einen Überblick über die vom Endbenutzer ausgeführten Jobs. Zudem gibt die App „Workflow System Jobs“ einen Überblick über die vom Systembenutzer ausgeführten Jobs. Hinweis: Es können Tools von Drittanbietern zur Planung und Überwachung von Jobs verwendet werden; diese sollten bei diesem Test berücksichtigt werden. Das System bietet die Möglichkeit, zu definieren, welche Berechtigungen das Anlegen und Ausführen von (Batch-)Jobs ermöglichen, um den Zugriff zu beschränken. Dies bedeutet, dass ein Benutzer nur dann einen (Batch-)Job anlegen/ausführen kann, wenn die Berechtigung entsprechend vergeben ist.
1.	**Kontrollziel:** Kritische/rechnungslegungsrelevante (Batch-)Jobs werden überwacht und Verarbeitungsfehler werden korrigiert, um eine vollständige, richtige und periodengerechte Verbuchung zu gewährleisten.

NR.	Prüfprogramm: Job-Monitoring (z. B. Jobs and Batch-Jobs)
	Risiko: Verarbeitungsfehler kritischer/rechnungslegungsrelevanter (Batch-) Jobs werden nicht korrigiert, sodass eine vollständige, richtige und periodengerechte Verbuchung nicht gewährleistet ist.
1.1	Kontrollfragen zum Prozess: Gibt es einen definierten Prozess, um ungenaue, unvollständige oder unzulässige Verarbeitungen von (Batch-)Jobs regelmäßig auszuwerten?
1.2	Innerhalb der S/4HANA Cloud bieten die Fiori-Apps „Anwendungsjobs“ und „Workflow System Jobs“ Zugriff auf die Verarbeitung von (Batch-)Jobs.
1.3	**Prozessschritte:** 1. Aufrufen der vom System generierten Liste der Job-Status oder Fehlschläge für Anwendungsjobs i. Navigation zu „Anwendungsjobs“ ii. Filtern des Felds „Status“ auf „Fehlgeschlagen, Abgebrochen, Beendet und Benutzerfehler“ iii. Filtern des Datumsbereichs iv. Bericht herunterladen v. Filter „W (Warnung) / E (Fehler)“ im Feld „Protokoll“ 2. Aufrufen der vom System generierten Liste der Job-Status oder Fehler für die Workflow-System-Jobs i. Navigation zu „Kategoriebeschreibung“ > „Workflow System Jobs – Application log“ ii. Filtern des Felds „Schweregrad“ auf „Abgebrochen, Fehler, Warnung“ iii. Filtern des Datumsbereichs iv. Bericht herunterladen
1.4	Auf der Grundlage des Risikos, das mit den Kontroll- und Auftragsüberwachungsprüfungen verbunden ist, muss validiert werden, ob im Falle eines Fehlers eine Warnmeldung generiert, das zuständige Personal benachrichtigt und Korrekturmaßnahmen zur Behebung des Fehlers ergriffen wurden.

7.8 Prüfprogramm: Protokolle und Parameter

Tabelle 28 Protokoll und Parameter

NR.	Protokoll und Parameter
	Kontrollziel: Ein angemessenes Sicherheitskonzept einer Anwendung muss eine Protokollierung aller Aktivitäten im Bereich der Berechtigungsverwaltung umfassen sowie angemessene Einstellungen der verfügbaren Systemparameter mit Wirkung auf den Authentifizierungs- und Autorisierungsprozess regeln. **Risiko:** Eine unzureichende Regelung und Anwendung von Standards für Protokolle und Parameter kann zu Beeinträchtigungen der Nachvollziehbarkeit rechnungslegungsrelevanter Vorgänge durch fehlende Zuordnungsmöglichkeit von Vorgängen zu den verursachenden Benutzern oder sogar zu unautorisierten Geschäftsvorfällen durch unautorisierte Zugriffe führen.
a)	Security Audit Log
7.1.	**Security Audit Log-Einrichtung** Hinweis: Im Gegensatz zum SAP S/4HANA OnPremise ist das Security Audit Log bereits übergreifend aktiviert. Ebenso sind keine weiteren Einstellungen der im OnPremise üblichen Filterungen erforderlich. Auch ist es für eine/einen Anwendende:n nicht möglich, die gespeicherten Logs zu löschen. Insofern entfallen hierfür Prüfungshandlungen. Gleichwohl sind die üblichen Prüfungshandlungen im Kontext der Auswertung und Überwachung der protokollierten Ereignisse durchzuführen. Hinweis: Eine genaue Beschreibung der Filter (und einer SAL-Ereignisdokumentation) kann auch in der Applikation „Statisches System-Audit anzeigen“ unter dem Reiter Ereignisdefinitionen (SAL) angezeigt werden. **Security-Audit-Log-Ereignisse:** Das Security Audit Log kann über den Pfad „Sicherheit > Security Audit Log anzeigen“ aufgerufen werden. Prüfung auf Anmeldefehler mit der Kachel „Security Audit Log anzeigen“ durch Einschränken des Zeitstempels und Selektion der relevanten Audit-Ereignisse, hier Ereignis AU2; Login gescheitert (Grund=&B, Typ=&A, Methode=&C). Eine genaue Beschreibung der Filter (und einer SAL-Ereignisdokumentation) kann auch in der Applikation „Statisches System-Audit anzeigen“ unter dem Reiter Ereignisdefinitionen (SAL) angezeigt werden.

b)	Änderungsbelege
7.2.	Die Änderungsbelege erhalten Sie, indem Sie zu External Auditing > Änderungsbelege anzeigen navigieren und entsprechende Objekttypen auswählen (zusätzlicher Parameter, z. B. Datumsbereich). Die Ergebnisse können heruntergeladen werden. Eine angemessene Vergabe von Berechtigungen ist auch für Auditor:innen anzuwenden. Prüfung auf unautorisierte Änderungsbelege bzw. Änderungsbelege durch unautorisierte Benutzer im Prüfungszeitraum.
b)	Berechtigungsparameter
7.3.	Hinweis: Im Gegensatz zum SAP S/4HANA OnPremise sind die Parametrisierungen nicht von der/dem Lösungsanwendenden konfigurierbar. Damit entfallen die hierfür üblichen Prüfungshandlungen. Siehe hierzu auch den Abschnitt „Analyse des SOC1-Typ-2-Reports“.

7.9 Prüfprogramme: Analyse des SOC1-Typ-2-Reports

Tabelle 29 Prüfprogramm: Analyse des SOC1-Typ-2-Reports

NR.	Prüfprogramm: Analyse des SOC1-Typ-2-Reports
-	In der S/4HANA Cloud wandern im Vergleich zu den OnPremise-Lösungen einige Prozesse und Kontrollen und somit die Compliance-Verantwortung vom Unternehmen zum Dienstleister (SAP SE). System- und Organisationskontrollen (SOC) für Dienstleistungsunternehmen sind interne Kontrollberichte, die von einem/einer externen Prüfenden erstellt werden. Sie sollen die von einer Dienstleistungsorganisation erbrachten Dienstleistungen untersuchen, damit die Endnutzenden das mit einer ausgelagerten Dienstleistung verbundene Risiko bewerten und angehen können. Hinweis: Der aktuelle SOC1-Typ-2-Report für S/4HANA Cloud kann im SAP Trust Center beantragt werden. https://www.sap.com/tc > Tab Compliance > Suche nach dem relevanten SOC-Report

NR.	Prüfprogramm: Analyse des SOC1-Typ-2-Reports
1.	**Kontrollziel:** Der SOC1-Typ-2-Report wird vom Unternehmen angefragt; die Vollständigkeit der Kontrollen und deren Wirksamkeit werden geprüft und potenzielle Auswirkungen auf das interne Kontrollsystem bewertet. **Risiko:** Der SOC1-Typ-2-Report ist unvollständig oder weist Feststellungen auf, die Auswirkungen auf das interne Kontrollsystem haben.
1.1	Kontrollfragen zum Prozess: Gibt es einen definierten Prozess, der sicherstellt, dass der SOC-Report durch den/die Kund:in regelmäßig analysiert wird?
1.2	Anfragen des aktuellen SOC1-Typ-2-Reports für S/4HANA Cloud im SAP Trust Center. https://www.sap.com/tc > Tab Compliance > Suche nach dem relevanten SOC-Report
1.3	Verständnis darüber gewinnen, wie die Dienstleistungen der SAP im Rahmen der Geschäftstätigkeit (Nutzung der S/4HANA Cloud) genutzt werden, einschließlich - der Art der von der SAP erbrachten Dienstleistungen und der Bedeutung dieser Dienstleistungen für die Organisation, einschließlich der Auswirkungen auf das interne Kontrollsystem der Organisation - der Art und Wesentlichkeit der von der Dienstleistungsorganisation erbrachten Leistungen oder der von ihr beeinflussten Prozesse und Kontrollen sowie der Frage, ob sich der Bericht des/der Dienstleistungs-Prüfenden angemessen auf diese Prozesse und Kontrollen bezieht - des Ausmaßes der Wechselwirkung zwischen den Tätigkeiten der Dienstleistungsorganisation und denen der Organisation - der Art der Beziehung zwischen der Organisation und der SAP, einschließlich der Vertragsbedingungen für die von der SAP durchgeführten Tätigkeiten.
1.4	Identifizierung relevanter ergänzender Kontrollen, die bei der Organisation liegen („Complementary User Entity Controls“ [CUEC]). Auf der Grundlage des gewonnenen Verständnisses, wie das Unternehmen die

NR.	Prüfprogramm: Analyse des SOC1-Typ-2-Reports
	Dienstleistungsorganisation nutzt, sind die relevanten Kontrollen, die sich auf die von der SAP erbrachten Dienstleistungen beziehen, zu identifizieren, zu testen und zu bewerten. Hinweis: Bei den CUECs handelt es sich um Kontrollen, bei denen das Management der Dienstleistungsorganisation (SAP) davon ausgeht, dass sie von den nutzenden Unternehmen implementiert werden sollten, und die notwendig sind, um die angegebenen Kontrollziele zu erreichen. Nicht alle im Bericht genannten CUECs sind immer für das Unternehmen relevant. Bei der Feststellung, ob eine CUEC relevant ist, berücksichtigt das Unternehmen Kontrollen aus dem Bericht des Wirtschaftsprüfers / der Wirtschaftsprüferin, die für das Unternehmen als relevant eingestuft werden.
1.5	Berücksichtigung des Berichtsdatums und des vom Bericht abgedeckten Zeitraums. Zudem sollte beurteilt werden, ob die im Bericht des Abschlussprüfers / der Abschlussprüferin genannten Wirksamkeitstests einen angemessenen Teil des Prüfungszeitraums des Auftrags abdecken (d. h. in Bezug auf den Stichtag der Beurteilung durch das Management und/oder für den Zeitraum).
1.6	Die von dem/der Prüfenden im Bericht festgestellten Ausnahmen („Exceptions“) werden bewertet, um festzustellen, ob sie Auswirkungen auf die Risikobewertung, die internen Kontrollen etc. haben. Die Bewertung berücksichtigt auch (falls vorhanden) mitigierende Prüfungshandlungen des/der Prüfenden, die dazu führen, dass das Kontrollziel trotz Ausnahme erreicht werden kann.
1.7	Die im Bericht genannten Subdienstleister werden vom Unternehmen bewertet, um festzustellen, ob sich die von den ausgegliederten Subdienstleistern erbrachten Leistungen auf interne Konten, Prozesse und/oder Kontrollen auswirken und ob diese Aussagen für den Jahresabschluss der Einheit von Bedeutung sind.

8 SAP HANA Datenbank

8.1 Einleitung

SAP HANA ist die Datenbankplattform von SAP S/4HANA (im Folgenden SAP S/4 HANA DB oder kurz HANA DB). Anders als bei SAP-R/3- und SAP-Business-Suite-Systemen ist der Betrieb von SAP S/4HANA auf anderen Datenbanklösungen nicht möglich. SAP HANA basiert auf einer In-Memory-Technik: Daten werden typischerweise vollständig im Arbeitsspeicher (RAM – Random-Access-Memory) gehalten und nicht wie bei herkömmlichen Systemen erst zur Bearbeitung von dem Storage-System (Festplatte) geladen.

Dies unterstützt die effektive Komprimierung und die hoch performante Auswertung großer Datenmengen. Im Arbeitsspeicher werden die Daten unverschlüsselt gehalten. Erst bei der Kommunikation mit einem Client (z. B. dem Applikationsserver des SAP-S/4-HANA-DB-Systems) oder bei der Persistenz auf der Festplatte ist eine HANA-seitige Verschlüsselung technisch möglich. Die Aktivierung der Verschlüsselung durch HANA ist technisch weiterhin für Redo-Logs und Backups möglich. Trace-Dateien und Dumps werden unverschlüsselt gespeichert, können aber durch Verschlüsselung der Speichersysteme auch abgesichert werden.

Die ausschließliche Verwendung der HANA DB betrifft alle SAP-S/4HANA-Szenarien unabhängig davon ob SAP S/4HANA (OnPremise), S/4HANA Cloud, Private Edition oder S/4HANA Cloud. Oft ist die SAP HANA Datenbank unter der vollständigen Kontrolle eines Cloud-Providers oder Service-Providers, sodass für eine Prüfung notwendige Kontrollen durch die Vorlage eines Auditberichts des Betreibers adressiert sind. Darüber hinaus bestehen aber auch weitere Kontrollmöglichkeiten:

1. Einsichtnahme in Konfiguration, Statistiken, aktive Benutzer und zugewiesene Berechtigungen aus dem DBA-Cockpit des SAP-S/4HANA-Systems.
2. Konfiguration zusätzlicher Regeln im SAP-HANA-Audit-Log. Diese können redundant oder ergänzend zu Regeln des Cloud-Providers sein und u. U. unabhängig von den Prozessen des Cloud-Providers bereitgestellt werden.
3. SAP-Services wie SAP Early Watch Alert und SAP Security Optimization Service oder vergleichbare Berichte des Cloud-Providers.

Neben den Funktionalitäten für das Datenbank-Management bietet SAP HANA aber auch Möglichkeiten für die Anwendungsentwicklung, für eine erweiterte analytische Verarbeitung der Geschäftsdaten sowie für die Integration mit entfernten Datenquellen. Es ergeben sich folgende Nutzungsszenarien für die SAP-HANA-Plattform:

- SAP HANA fungiert als standardmäßige SQL-basierte relationale Datenbank – zum Beispiel als Datenlieferant für klassische transaktionale Anwendungen wie SAP S/4HANA (OLTP) und/oder als Datenquelle für analytische Anfragen (OLAP).
- Zur Erweiterung der Funktionalität des SAP-S/4HANA-Systems können native HANA-Anwendungen implementiert werden. Von der Benutzung dieser Möglichkeit wird jedoch abgeraten, um die Daten des S/4HANA-Systems möglichst weitreichend gegen konkurrierende Zugriffe zu schützen. Empfohlen wird, Erweiterungen und native Szenarien in der SAP Cloud oder in einer entfernten Datenbank zu implementieren.

Für eine direkte Anmeldung an der SAP HANA Datenbank wird ein Benutzer in SAP HANA benötigt. Der Benutzer kann entweder ein technisches Konto, ein/eine Datenbankadministrator:in oder ein einzelner Endbenutzer sein. Für die Benutzerverwaltung werden das SAP HANA Cockpit oder das SAP HANA Studio (von SAP ab HANA2.0 nicht mehr freigegeben) oder ein externes System für Identity- und Access-Management verwendet (z. B. SAP IDM, SAP GRC).

Der Zugriff auf bestimmte Funktionen kann entweder direkt mit Privilegien oder indirekt über Rollen mit Privilegien gewährt werden. Der Standardmechanismus für die Gewährung von Privilegien in SAP HANA ist die Vergabe über Rollen. Bei der Erstellung einer Rolle werden die Privilegien zugewiesen und dann als Objekt in der Datenbank gespeichert. Rollen können entweder direkt in der HANA Datenbank als Objekt angelegt werden (Katalogrollen, nicht empfohlen) oder als Entwicklungsobjekt in SAP HANA transportiert und aktiviert werden (Repository-Rollen und HDI-Rollen).

In SAP HANA wird zwischen den folgenden fünf unterschiedlichen Typen von Privilegien unterschieden:

- **Systemprivilegien:** steuern allgemeine Systemaktivitäten. Sie werden hauptsächlich für die Systemadministration genutzt und berechtigen für Tätigkeiten des normalen Systembetriebs (Überwachung, Analyse, Backup Konfigurationsänderungen) das initiale Einrichten von Funktionalität oder Schnittstellen oder für das Anlegen von Benutzern, Rollen und anderen Datenbankobjekten. Darüber hinaus enthält diese Gruppe Privilegien aus der Anfangszeit von SAP HANA, die quasi Berechtigungen für Entwickler:innen sind, z. B. zur Erstellung von Rollen und Berechtigungen).
- **Objektprivilegien:** werden verwendet, um den Zugriff auf und die Änderung von Datenbankobjekten wie Tabellen, Ansichten und Prozeduren zu ermöglichen. Objektprivilegien können entweder auf einzelne Objekte oder auf ein komplettes Datenbankschema mit allen darin enthaltenen Objekten vergeben werden. Objektberechtigungen beziehen sich entweder auf die Definition des Objekts oder auf deren Inhalt.

- **Analytische Privilegien:** werden verwendet, um den Lesezugriff auf Daten in SAP-HANA-Informationsmodellen (d. h. analytische Ansichten, Attribut-Ansichten und Berechnungsansichten) in Abhängigkeit von bestimmten Werten oder Wertekombinationen zu ermöglichen. Analytische Privilegien werden bei der Abfrageverarbeitung ausgewertet.
- **Repository-Privilegien:** werden verwendet, um den Zugriff auf und die Arbeit in Paketen im Repository der SAP-HANA-Datenbank zu ermöglichen und auf einzelne Entwicklungspakete einzuschränken. Sie sind nur im Kontext von XS Classic relevant.
- **Applikations-Privilegien:** können von Entwickler:innen klassischer SAP-HANA-XS-Anwendungen erstellt werden, um den Benutzer- und Client-Zugriff auf ihre Anwendung zu autorisieren.

Bei den Empfängern dieser Rollen und Privilegien kann im Wesentlichen zwischen den nachfolgenden drei Personengruppen unterschieden werden:

- **Datenbankadministrator:in:** Die Verwendung von SAP HANA als Datenbank ändert nicht das traditionelle Berechtigungskonzept in der Applikationsschicht wie die Endbenutzer-Autorisierung und die Benutzerverwaltung. Diese werden weiterhin in der Anwendungsserverschicht bereitgestellt. Hierbei stellt der Anwendungsserver die Verbindung zur SAP HANA DB über ein technisches Benutzerkonto her.

  Ein direkter Zugriff auf SAP HANA ist nur für Datenbankadministrator:innen möglich und nötig, während Endbenutzer weder auf SAP HANA selbst noch auf den Server, auf dem es läuft, direkten Zugriff haben.

  Datenbankadministrator:innen haben in SAP HANA nicht automatisch Zugriff auf die Inhalte (Daten) von Schemata und Views. Ihnen müssen die entsprechenden SQL-Rechte gewährt werden. Datenbankadministrator:innen benötigen im Wesentlichen Systemprivilegien sowie Objektberechtigungen für Schemas, die Monitoringinformationen enthalten (z. B. SYS [bzw. PUBLIC], _SYS_STATISTICS) Die nachfolgenden Prüfungshandlungen beziehen sich im Schwerpunkt auf die notwendigen Berechtigungen dieser Personengruppe.

- **HANA Analytics:** Kund:innen-spezifische Berichte und Dashboards bieten direkten Lesezugriff auf diese Daten in SAP HANA mit der Option, eine breite Palette von BI-Tools, einschließlich SAP BusinessObjects Intelligence, zu verwenden. Von der Nutzung nativer analytischer Applikationen wird inzwischen abgeraten.

Die Architektur erfordert ein projektspezifisches Sicherheitsmodell. Die Berechtigungsprüfung erfolgt über (projektspezifisch modellierte) SAP-HANA-Privilegien, die den Endanwendenden in SAP HANA gewährt werden müssen. Anstelle nativer Apps können CDS-Views auf der S/4-Anwendungsebene implementiert werden. Der Zugriff erfolgt dann ebenfalls über den ABAP-Stack. Alternativ können Daten der HANA DB auch über Queries im BI/BW mit den korrespondierenden analytischen Berechtigungen genutzt werden.

Deswegen werden die Berechtigungen für die Entwicklung und Nutzung nativer HANA-Apps in den folgenden Prüfungshandlungen nur randständig in Bezug auf eine angemessene Abgrenzung insbesondere im Unterkapitel Autorisierung / Sensitive Funktionen betrachtet.

- **Anwendungsentwicklung:** SAP HANA Extended Application Services, Advanced Model (XS Advanced) ist das Standard-Framework für die native Anwendungsentwicklung auf SAP HANA.

  Anwendungen, die auf XS Advanced laufen, verwenden ihr eigenes Berechtigungskonzept in der XS-Advanced-Schicht. Der/Die zugehörige Technische Benutzer einer XS-Advanced-Anwendung wird zunächst immer ohne Berechtigungen erstellt und besitzt ausschließlich die Berechtigungen, die ihr/ihm im Rahmen der Entwicklung oder durch Vertrauensbeziehungen explizit zugewiesen wurden.

  Für Anwendungen, die auf XS Classic laufen, sind zusätzliche Anwendungsprivilegien verfügbar, die zusätzlich zu den üblichen SAP-HANA-Privilegien gelten.

  Auch diese Form der Funktion und der Berechtigungen wurde inzwischen in der Regel durch die Programmierung von CDS-Views direkt in der Anwendungsschicht abgelöst. Insofern werden auch diese Aspekte in den folgenden Prüfungshandlungen nur randständig insbesondere in Bezug auf eine angemessene Abgrenzung betrachtet.

8.2 Risiken

Die Risiken können aus den allgemeinen Kapiteln zur Authentifizierung, zur Autorisierung und zum Change-Management übernommen werden. Ergänzungen zu den Aspekten Logs und Protokolle finden sich im entsprechenden nachfolgenden Prüfprogramm.

Die Besonderheiten für Risiken der SAP-S/4HANA-DB-Schicht ergeben sich aus deren besonderer Funktion als Datenbanklösung und damit der Beschreibung, der Speicherung und dem Abrufen von Daten der darüberliegenden Anwendungs-Systeme, während die Anwendungssysteme wie insbesondere SAP S/4HANA OnPremise und Cloud primär der Erfassung von Geschäftsvorfällen dienen.

Hierdurch beschränken und konzentrieren sich die Risiken der HANA DB auf:

- eine Gefährdung der Datenintegrität durch eine direkte und unzulässige Manipulation der Daten in der Datenbankschicht mit direkter Wirkung auf die Datenintegrität der darüberliegenden verwalteten Anwendungsschichten,

- eine Gefährdung der Systemintegrität der Datenbank, ebenfalls mit einer direkten Beeinträchtigung der Verfügbarkeit der darüberliegenden verwalteten Anwendungsschichten,

- den Missbrauch von in der Datenbank gespeicherten Daten, die den Daten und damit deren Schutzbedürftigkeit in den darüberliegenden verwalteten Systemen entspricht. Dies ist sowohl über die in der Datenbank möglichen direkten Administrationsrechte als auch über die Rechte von Entwickler:innen für analytische Apps sowie über die Rechte der Endanwendenden zur Ausführung analytischer Apps mit Zugriff auf sensible Daten möglich.

8.3 Kontrollziele

Im Rahmen der SAP HANA Datenbank sind einige Aspekte besonders hervorzuheben, die in den nachfolgenden Prüfungshandlungen zusätzlich zu den generischen Prüfungshandlungen aus den Kapiteln 3 Authentifizierung, 4 Autorisierung und 5 Change-Management ergänzt werden:

Im Prüfprogramm Authentifizierung werden Prüfungshandlungen rund um die Anmeldeverfahren in der SAP HANA Datenbank beschrieben. Da die Datenbank typischerweise nicht den Endbenutzern zugänglich ist, sondern ausschließlich hochprivilegierten Administrator:innen und technischen Benutzer von IT-Infrastruktur-Anwendungen, hat die Absicherung der Zugriffe auf Datenbankebene eine wichtige Bedeutung für den Schutz der Daten. Wichtig ist dies insbesondere auch dann, wenn

die Datenbank nicht in die Standard-IT-Prozesse integriert ist, die für die S/4-HANA-Anwendungsschicht implementiert sind.

Im Rahmen des Kapitels werden umfängliche Hinweise zur Auswertung von Benutzern und Berechtigungsdaten für die Prüfungshandlungen im Kapitel Prozesse und Organisation, Erläuterungen zur Vermeidung/Kontrolle DB-spezifischer Standardbenutzer im Kapitel Benutzer und Rechte sowie von Standard- und Sonderrollen im Kapitel Rollen und Berechtigungen gegeben.

Die Prüfungshandlungen in den Kapiteln Sensitive Funktionen und Funktionstrennungen konzentrieren sich auf zwei Kontrollziele: a) die Identifikation der für die oben dargestellten Aufgabenbereiche HANA Analytics und Anwendungsentwicklung erforderlichen Privilegien, die Vermeidung der Vergabe dieser Privilegien oder zumindest deren Einschränkung sowie b) die Konkretisierung der Handhabung der Berechtigungen für die Kernaufgabe der HANA DB, nämlich der Datenbankadministration.

Die Prüfungshandlungen werden ergänzt durch eine Matrix mit einer Zuordnung der HANA-DB-Privilegien auf unterschiedliche Funktionen. Die Matrix kann als Orientierung für ein unternehmensspezifisches Rollenkonzept oder als ein erweitertes Regelwerk für sensitive Funktionen und Funktionstrennungen dienen.

Die Prüfungshandlungen zum Themenkreis Change-Management konzentrieren sich auf folgende Kontrollziele: a) die Erfassung von Produkten und Softwarekomponenten, die für den regelkonformen Betrieb des SAP-S/4-HANA-Systems besonders relevant sind. Änderungen an der Landschaft müssen einer effektiven Kontrolle unterliegen. Dies betrifft jeweils sowohl die Komponente selbst als auch die Art ihrer Verwendung. Genutzte Komponenten und Produkte müssen in regelmäßigen Abständen aktualisiert und – bei Entdeckung von Sicherheitslücken – gepatcht werden. b) Konfigurationsänderungen müssen in geeignet konfigurierten Logs aufgezeichnet werden und einer nachträglichen Prüfung zugänglich sein.

8.4 Prüfprogramm: Authentifizierung

Tabelle 30 Prüfprogramm: Authentifizierung

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
1.	**Authentifizierungsmethoden**
	Kontrollziel: Verwendete Authentifizierungsmethoden sollen dokumentiert sein und durch technische und organisatorische Maßnahmen abgesichert werden; ihre Verwendung soll klar gegeneinander abgegrenzt sein. Nicht verwendete Authentifizierungsmethoden und Authentication-Provider sind aus dem System zu entfernen. **Risiko:** Konkurrierende Authentifizierungsverfahren können Sicherheitskonzepte aushebeln, indem bei der Kontrolle nur Teilaspekte von Angriffsszenarien im Blick sind. Obsolete Authentifizierungsverfahren oder Authentication-Provider können für unberechtigten Zugriff auf das System verwendet werden, wenn eine effektive Überwachung fehlt.
1.1.	**Konfiguration Authentifizierungsmethoden:** *Sind alle erforderlichen Authentifizierungsmethoden in der Werteliste des Systems konfiguriert und alle nicht genutzten entfernt? Um die folgenden SQL-Abfragen durchzuführen, kann entweder Eclipse (Hana Studio) oder über die Transaktion DBACOCKPIT im Ordner Diagnose der SQL-Editor verwendet werden.* Eine erste Liste tatsächlich genutzter Authentifizierungsmethoden kann mit dem System-View SYS.USERS gewonnen werden, zu denen dann die folgenden Prüfungshandlungen erfolgen: a) Erzeugung einer Liste der aktiven und gültigen Benutzer aus SYS.USERS: Select * from „SYS“.„USERS“ WHERE USER_DEACTIVATED=‚FALSE‘; b) Prüfung der Spalten IS_PASSWORD_ENABLED, IS_KERBEROS_ENABLED, IS_SAML_ENABLED, IS_JWT_ENABLED, IS_LDAP_ENABLED,

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
	IS_X509_ENABLED, IS_SAP_LOGON_TICKET_ENABLED auf den Wert „TRUE“ c) Nicht genutzte Authentifizierungsmethoden sollen im System abgeschaltet sein. Per Default enthält der Parameter global.ini [authentication] authentication_methods eine Liste aller technisch im System verfügbaren Authentifizierungsmethoden: pbkdf2, password, kerberos, spnego, saml, saplogon, x509xs, jwt, sessioncookie, ldap; DBACOCKPIT - Configuration - INI Files (oder per SQL Editor > M_INIFILE_CONTENTS oder alternativ: M_CONFIGURATION_PARAMETER_VALUES). Über den View CONFIGURATION_PARAMETER_PROPERTIES können Eigenschaften von Parametern für die aktuelle HANA-DB-Version überprüft werden, z. B. ob ein Parameter einen Restart erfordert, welche Werte der Parameter annehmen kann oder in welcher Einheit die Werte erfasst sind. Prüfung der zutreffenden Pflege der genutzten Authentifizierungsparameter in der Werteliste des Systems sowie der Entfernung aller ungenutzten Methoden.
1.2.	**Benutzer mit multiplen Authentifizierungsmethoden:** *Sind Benutzer nur in begründeten und dokumentierten Ausnahmefällen mehrere Authentifizierungsmethoden zugeordnet?* Ermittelt werden können diese Nutzenden mittels der Auswertung im Punkt 1.1 b. Benutzer sollen sich nur dann mit mehreren Authentifizierungsmethoden am System anmelden können, wenn der Zweck dokumentiert und genehmigt ist. Eine solche Situation ist aber als Ausnahme zu betrachten. Hierzu sind Benutzer mit mehreren Authentifizierungsmethoden zu identifizieren. Für diese Benutzer sollte eine Dokumentation vorhanden sein, die angemessen die Notwendigkeit für diese Sachverhalte erläutert. Prüfung auf angemessene Dokumentation von Benutzern mit multiplen Authentifizierungsmethoden.

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
1.3.	**Nachvollziehbarkeit der Konfigurationsänderung von Authentifizierungsmethoden:** Sind Änderungen an der Konfiguration der Authentifizierungsmethoden gemäß einem vorgegebenen Prozess angemessen dokumentiert? Änderungen an Konfigurationen für Authentifizierungsmethoden können mit dem View M_INIFILE_CONTENT_HISTORY geprüft werden. Dieser enthält nur den jeweils aktuellen und den vorangegangenen Wert. Findet sich eine Änderung, so kann im Auditlog nach weiteren Änderungsbelegen gesucht werden über den Pfad DBACOCKPIT > Configuration > INI Files bzw. INI Files Change History (oder per SQL Editor > M_INIFILE_CONTENTS, M_INIFILE_CONTENT_HISTORY) SYS.AUDIT_LOG. Prüfung auf angemessene Dokumentation von Änderungen an der Konfiguration von Authentifizierungsmethoden.
1.4.	**Authentifizierungs-Traces:** *Werden in Trace-Files der HANA DB relevante Informationen zur Authentifizierung erfasst und sinnvoll validiert?* Die Systemeigenschaften für die Konfiguration des Auditings befinden sich im Abschnitt Auditing-Konfiguration der Systemeigenschaftendatei global.ini (Tenant-Datenbanken) oder der Datei nameserver.ini (System-Datenbank). Im Hana Cockpit unter Security auf der Kachel Auditing kann geprüft werden, ob eine oder mehrere Audit-Policies eingerichtet sind. Änderungen an Trace-Leveln (z. B. für Authentication) und nachfolgende Information (z. B. Passwörter in Klartext) System-Views, mit denen Änderungen nachvollzogen werden können: M_INIFILE_CONTENT_HISTORY oder AUDIT_LOG, M_MERGED_TRACES, M_TRACEFILE_CONTENTS In Punkt 1.5 wird auf die Policies für das Audit eingegangen. Prüfung auf angemessene Konfiguration der Policies und der Überwachung der Trace-Files. Es sollte ein Prozess implementiert sein, der die Trace-Informationen entweder an ein automatisiertes System übermittelt (SIEM) oder eine manuelle Prüfung der Informationen festlegt.

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG

1.5.	**Konfiguration Audit-Log-Authentifizierung:** *Ist das Audit Log angemessen für die Erfassung von Vorgängen mit Relevanz für die Authentifizierung eingerichtet?*
	
	Das Audit-Log der SAP S/4 HANA DB ermöglicht die Einrichtung von Audit-Policies u. a. auch für authentifizierungsrelevante Vorgänge. Eine Auswertung der Audit-Policies ist über den SQL-Befehl SELECT * FROM PUBLIC.AUDIT_POLICIES möglich. Für die Authentifizierung sind Policies zu den folgenden Sachverhalten erforderlich:
	
	a) Audit-Log-Anmeldeversuche: Es gibt eine aktive Audit-Policy zur Protokollierung von Anmeldeversuchen (Events: CONNECT, VALIDATE). Sehr aktive Benutzer wie der/die ABAP-Schema-Benutzer dürfen von der Protokollierung erfolgreicher Anmeldeversuche ausgenommen sein, nicht jedoch von der Protokollierung fehlgeschlagener Versuche.
	
	b) Audit-Log-Änderungen an Authentication-Providern und Zertifikaten: Es gibt eine aktive Audit-Policy zur Protokollierung von Änderungen an Authentication-Providern und Zertifikaten.
	
	Konfiguration des Audits unter:
	
	• SAP Note 3016478 – HANA Audit Policies for S/4HANA
	• SAP HANA Security Guide for SAP HANA Platform – Best Practices and Recommendations for Creating Audit-Policies (englisch)
	
	Prüfung auf die vollständige Anlage von Audit-Policies für Vorgänge mit Relevanz für die Authentifizierung.
	
	SQL-Statement zur Abfrage:
	
	`SELECT AUDIT_POLICY,`
	`  LPAD(COUNT, 7) COUNT,`
	`  EVENT_STATUS,`
	`  ACTIVE,`
	`  VALID,`
	`  EVENT_ACTION,`
	`  USER_NAME,`
	`  EXCEPT_USER_NAME,`
	`  OBJECT_TYPE,`
	`  OBJECT_SCHEMA,`
	`  OBJECT_NAME,`
	`  TRAIL_TYPE`
	`FROM`
	`( SELECT`
	`  CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'POLICY') != 0 THEN AP.AUDIT_POLICY_NAME ELSE MAP(BI.AUDIT_POLICY_NAME, '%', 'any', BI.AUDIT_POLICY_NAME) END AUDIT_POLICY,`
	`  CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'STATUS') != 0 THEN AP.EVENT_STATUS ELSE MAP(BI.EVENT_STATUS, '%', 'any', BI.EVENT_STATUS) END EVENT_STATUS,`
	`  CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'ACTIVE') != 0 THEN AP.IS_AUDIT_POLICY_ACTIVE ELSE MAP(BI.POLICY_ACTIVE, '%', 'any', BI.POLICY_ACTIVE) END ACTIVE,`

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG

```
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'VALID')        != 0 THEN AP.IS_VALID
ELSE MAP(BI.POLICY_VALID,     '%', 'any', BI.POLICY_VALID)     END VALID,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'ACTION')       != 0 THEN AP.EVENT_ACTION
ELSE MAP(BI.EVENT_ACTION,     '%', 'any', BI.EVENT_ACTION)     END EVENT_ACTION,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'USER_NAME')    != 0 THEN
IFNULL(AP.USER_NAME, '')       ELSE MAP(BI.USER_NAME,        '%', 'any', BI.USER_NAME)        END USER_NAME,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'EXCEPT_USER')  != 0 THEN
IFNULL(AP.EXCEPT_USER_NAME, '') ELSE MAP(BI.EXCEPT_USER_NAME,  '%', 'any', BI.EXCEPT_USER_NAME)  END
EXCEPT_USER_NAME,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'OBJECT_TYPE')  != 0 THEN
IFNULL(AP.OBJECT_TYPE, '')     ELSE MAP(BI.OBJECT_TYPE,      '%', 'any', BI.OBJECT_TYPE)      END OBJECT_TYPE,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'OBJECT_SCHEMA') != 0 THEN
IFNULL(AP.OBJECT_SCHEMA, '')    ELSE MAP(BI.OBJECT_SCHEMA,    '%', 'any', BI.OBJECT_SCHEMA)    END
OBJECT_SCHEMA,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'OBJECT_NAME')  != 0 THEN
IFNULL(AP.OBJECT_NAME, '')     ELSE MAP(BI.OBJECT_NAME,      '%', 'any', BI.OBJECT_NAME)      END OBJECT_NAME,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'TRAIL_TYPE')   != 0 THEN
IFNULL(AP.TRAIL_TYPE, '')      ELSE MAP(BI.TRAIL_TYPE,       '%', 'any', BI.TRAIL_TYPE)       END TRAIL_TYPE,
   COUNT(*) COUNT,
   BI.ORDER_BY
 FROM
 ( SELECT               /* Modification section */
    '%' AUDIT_POLICY_NAME,
    '%' EVENT_STATUS,
    '%' POLICY_ACTIVE,
    '%' POLICY_VALID,
    '%' EVENT_ACTION,
    '%' USER_NAME,
    '%' EXCEPT_USER_NAME,
    '%' OBJECT_SCHEMA,
    '%' OBJECT_NAME,
    '%' OBJECT_TYPE,
    '%' TRAIL_TYPE,
    'NONE' AGGREGATE_BY,                    /* POLICY, STATUS, ACTIVE, VALID, ACTION, USER_NAME, EXCEPT_USER,
OBJECT_TYPE, OBJECT_SCHEMA, OBJECT_NAME, TRAIL_TYPE */
    'POLICY' ORDER_BY                       /* COUNT, POLICY, OBJECT */
   FROM
    DUMMY
 ) BI,
   AUDIT_POLICIES AP
 WHERE
   UPPER(AP.AUDIT_POLICY_NAME) LIKE UPPER(BI.AUDIT_POLICY_NAME) AND
   AP.EVENT_STATUS LIKE BI.EVENT_STATUS AND
   AP.IS_AUDIT_POLICY_ACTIVE LIKE BI.POLICY_ACTIVE AND
   AP.IS_VALID LIKE BI.POLICY_VALID AND
   ( BI.EVENT_ACTION  = 'DML' AND AP.EVENT_ACTION IN ('DELETE', 'INSERT', 'SELECT', 'UPDATE', 'UPSERT') OR
     BI.EVENT_ACTION != 'DML' AND AP.EVENT_ACTION LIKE BI.EVENT_ACTION
   ) AND
   IFNULL(AP.USER_NAME, '') LIKE BI.USER_NAME AND
   IFNULL(AP.EXCEPT_USER_NAME, '') LIKE BI.EXCEPT_USER_NAME AND
   IFNULL(AP.OBJECT_SCHEMA, '') LIKE BI.OBJECT_SCHEMA AND
   IFNULL(AP.OBJECT_NAME, '') LIKE BI.OBJECT_NAME AND
   IFNULL(AP.OBJECT_TYPE, '') LIKE BI.OBJECT_TYPE
 GROUP BY
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'POLICY')       != 0 THEN
AP.AUDIT_POLICY_NAME           ELSE MAP(BI.AUDIT_POLICY_NAME, '%', 'any', BI.AUDIT_POLICY_NAME) END,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'STATUS')       != 0 THEN AP.EVENT_STATUS
ELSE MAP(BI.EVENT_STATUS,     '%', 'any', BI.EVENT_STATUS)     END,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'ACTIVE')       != 0 THEN
AP.IS_AUDIT_POLICY_ACTIVE      ELSE MAP(BI.POLICY_ACTIVE,     '%', 'any', BI.POLICY_ACTIVE)     END,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'VALID')        != 0 THEN AP.IS_VALID
ELSE MAP(BI.POLICY_VALID,     '%', 'any', BI.POLICY_VALID)     END,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'ACTION')       != 0 THEN AP.EVENT_ACTION
ELSE MAP(BI.EVENT_ACTION,     '%', 'any', BI.EVENT_ACTION)     END,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'USER_NAME')    != 0 THEN
IFNULL(AP.USER_NAME, '')       ELSE MAP(BI.USER_NAME,        '%', 'any', BI.USER_NAME)        END,
   CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'EXCEPT_USER')  != 0 THEN
IFNULL(AP.EXCEPT_USER_NAME, '') ELSE MAP(BI.EXCEPT_USER_NAME,  '%', 'any', BI.EXCEPT_USER_NAME)  END,
```

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
	CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'OBJECT_TYPE') != 0 THEN IFNULL(AP.OBJECT_TYPE, '') ELSE MAP(BI.OBJECT_TYPE, '%', 'any', BI.OBJECT_TYPE) END, CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'OBJECT_SCHEMA') != 0 THEN IFNULL(AP.OBJECT_SCHEMA, '') ELSE MAP(BI.OBJECT_SCHEMA, '%', 'any', BI.OBJECT_SCHEMA) END, CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'OBJECT_NAME') != 0 THEN IFNULL(AP.OBJECT_NAME, '') ELSE MAP(BI.OBJECT_NAME, '%', 'any', BI.OBJECT_NAME) END, CASE WHEN BI.AGGREGATE_BY = 'NONE' OR INSTR(BI.AGGREGATE_BY, 'TRAIL_TYPE') != 0 THEN IFNULL(AP.TRAIL_TYPE, '') ELSE MAP(BI.TRAIL_TYPE, '%', 'any', BI.TRAIL_TYPE) END, BI.ORDER_BY) ORDER BY MAP(ORDER_BY, 'COUNT', COUNT) DESC, MAP(ORDER_BY, 'POLICY', AUDIT_POLICY, 'OBJECT', OBJECT_SCHEMA || OBJECT_NAME) WITH HINT (IGNORE_PLAN_CACHE)
1.6.	**Zugriff aus Tenants und SystemDB:** *Wird der Zugriff von anderen Tenants oder der SystemDB entweder unterbunden oder, falls verwendet, der Zweck und die hierfür genutzten Benutzer angemessen erläutert und dokumentiert?* a) Grundsätzlich sollte der Zugriff anderer Tenants oder der SystemDB über die Einstellung mit dem Default-Parameter auf false vermieden werden. Dies kann im Eclipse (Hana Studio) unter Systems im zu prüfenden System unter dem Reiter Configuration geprüft werden (global.ini [cross_database_access] enabled = false). b) In Ausnahmefällen kann es sinnvoll sein, dass der Zugriff erlaubt ist z. B. für Tenant-übergreifendes Reporting. In diesem Fall sollten die für diese Zwecke verwendeten Benutzer über die Tabelle SYS.USERS über die Spalte HAS_REMOTE_USERS = TRUE identifiziert werden. Der Grund und die hierfür genutzten Benutzer sollten nachvollziehbar dokumentiert sein. Select USER_NAME, HAS_REMOTE_USERS from Sys.USERS Where HAS_REMOTE_USERS = ‚TRUE‘ c) Zwischen welchen Tenants eine Verbindung freigeschaltet ist, kann ebenfalls über den oben genannten Parameter in der global.ini identifiziert werden. Prüfung auf Vermeidung von Zugriffen von anderen Tenants oder der SystemDB oder im Falle einer Öffnung auf nachvollziehbare Dokumentation der Öffnung und der betroffenen Benutzer.

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
1.7.	**Sichere Netzwerk-Kommunikation:** *Erfolgt die Kommunikation zwischen Applikationsserver und Datenbankserver in einem sicheren Netzwerk?* Im Idealfall sollte eine direkte Kommunikation zwischen einem Applikationsserver und der HANA Datenbank sichergestellt werden. Im Fall einer anderen Architektur-Lösung sollten dies und die hiermit verbundenen Maßnahmen nachvollziehbar dokumentiert und umgesetzt sein. Prüfung auf eine angemessene Absicherung der Kommunikation zwischen Applikationsserver und Datenbank in einem sicheren Netzwerk.
2.	**Kennwort-basierte Authentifizierung**
	Kontrollziel: Parameter mit Einfluss auf die Passwort-basierte Authentifizierung auf Hana-DB-Systemen sind angemessen für die jeweiligen Benutzer und Typen von Benutzern eingerichtet. **Risiko:** Unzureichende Passwort-Regeln befördern das Risiko eines Brute-Force-Angriffs, von Man-in-the-Middle-Attacken oder von Identitätsdiebstahl.
2.1.	**Allgemeine Password-Policies:** *Sind die Parameter der Password-Policies gemäß den Vorgaben für angemessene Passwort-Sicherheit eingerichtet?* Die Pflege von Parametern, die die Kennwort-basierte Authentifizierung beeinflussen, erfolgt in der HANA DB über die Datei nameserver.ini. Die Datei kann über das SQL-Statement: Select * from Sys.M_PASSWORD_POLICY abgefragt und anschließend aus dem HANA-DB-System exportiert werden. In der diesem Kapitel beigefügten Tabelle finden sich Richtwerte für die Einrichtung der Parameter. Diese basieren auf der Annahme, dass die Authentifizierungs-Regeln auf HANA-Ebene zumindest gleich, wenn nicht strenger sein sollten als für Endanwendende auf der Applikationsebene. Prüfung auf Übereinstimmung der für die Kennwort-Authentifizierung eingerichteten Parameter in den Password-Policies mit den definierten Richtwerten.

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
2.2.	**Passwort-Policies für Benutzergruppen:** *Werden von den allgemeinen Passwort-Policies abweichende Passwort-Policies für Benutzergruppen verwendet? Liegen hierfür nachvollziehbare Dokumentationen vor und entsprechen die den Benutzergruppen zugeordneten Benutzern den definierten Anwendungszwecken?* a) Eine Prüfung auf die Nutzung von Benutzergruppen-spezifischen Passwort-Policies erfolgt über die System-Views SYS.USERGROUP_PARAMETERS mit dem Befehl SELECT * FROM PUBLIC USERGROUP_PARAMETERSSELECT * FROM PUBLIC USERGROUP_PARAMETERS b) Die Verwendung von Benutzergruppen und eine Liste der jeweils zugeordneten Benutzer kann im View SYS.USERS (Spalte: USERGROUP) ermittelt werden mit folgender Abfrage: Select User_NAME, USER_ID, USERGROUP_NAME from SYS.USERS Die Prüfung sollte Abweichungen zwischen den allgemeinen Policies und den Benutzergruppen-spezifischen Parametern identifizieren, insbesondere für die Parameter force_first_password_change = true, maximum_unused_inital_password_lifetime =< 14, minimal_password_length >= 8 (besser 10–15) und password_layout > A1a (es können auch andere Buchstaben oder Zahlen verwendet werden). Hierbei gilt für Technische Benutzer: höhere Anforderungen Passwortkomplexität, Länge, Sperrung bei Falschanmeldung. Passwortablauf und force_first_password_change dürfen ausgeschaltet sein. Grundsätzlich ist zertifikatsbasierte Anmeldung zu bevorzugen. Richtwerte sind: minimal_password_length (>=20), force_first_password_change (=false), maximum_password_lifetime (= 365). Für Superuser gilt: höhere Anforderungen Passwortkomplexität, Länge, Häufigkeit der Passwortänderung, kürzere maximum_unused_initial_password_lifetime. Prüfung auf angemessene Nutzung Benutzergruppen-spezifischer Passwort-Policies im Einklang mit den hier vorgeschlagenen Werten.

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
2.3.	**Passwort-Policies für Benutzer:** *Werden von den allgemeinen Passwort-Policies abweichende Passwort-Policies für einzelne Benutzer verwendet? Liegen hierfür nachvollziehbare Dokumentationen vor und entsprechen die den Benutzer definierten Parameter dem Nutzungszweck der Benutzer?* Für einzelne Passwort-Policies können Ausnahmen direkt für einzelne Benutzer konfiguriert werden, ohne die Kennwortregeln zu ändern und ohne dass dies bei Prüfung der für einen Benutzer gültigen Passwort-Policy sichtbar wird. Eine solche Benutzer-individuelle Abweichung kann über den System-View PUBLIC.EFFFECTIVE_PASSWORD_POLICY über die folgende Abfrage ermittelt werden: Select * from SYS.M_EFFECTIVE_PASSWORD_POLICY Falls keine Werte gefunden werden, wird hier die folgende Fehlermeldung ausgegeben: Error: SAP DBTech JDBC: [500]: predicates are required in a where clause: M_EFFECTIVE_PASSWORD_POLICY_ needs predicates on columns (connected by AND if more than one): an equal predicate on USER_NAME In alten Systemen findet man häufig auch benutzerspezifische Abweichungen von der Standard-Passwort-Policy; dies kann über die folgende Abfrage ermittelt werden: SELECT USER_NAME, IS_PASSWORD_LIFETIME_CHECK_ENABLED, ADMIN_GIVEN_PASSWORD, PASSWORD_CHANGE_NEEDED FROM PUBLIC.USERS. Dabei sind insbesondere die folgenden Werte IS_PASSWORD_LIFETIME_CHECK_ENABLED = FALSE und die Kombination ADMIN_GIVEN_PASSWORD = TRUE / PASSWORD_CHANGE_NEEDED = FALSE zu hinterfragen. Dies sollte nur bei Technischen Benutzern eingestellt sein. Prüfung auf angemessene Nutzung benutzerspezifischer Passwort-Policies im Einklang mit den hier vorgeschlagenen Richt-Aussagen.
3.	**Verschlüsselte Kommunikation**

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
	Kontrollziel: Die Kommunikation zwischen Client und Server einerseits und zwischen den HANA-Servern andererseits ist nach einem aktuellen Verfahren verschlüsselt. Serverzertifikate sind installiert und gültig. **Risiko:** Das Abgreifen von Anmelde-Informationen wird einem Angreifer erschwert.
3.1.	**Verschlüsselung Kommunikation Application- und HANA-Server:** *Ist die Kommunikation zwischen dem Application-Server und dem HANA-Server angemessen verschlüsselt?* *Eine verschlüsselte Kommunikation kann Seiteneffekte haben; eine Aktivierung sollte immer nur in einem überschaubaren Rahmen und nicht ad hoc durchgeführt werden. Hier sind besonders die zwei folgenden SAP-Hinweise zu beachten: SAP-Note 2475246 und SAP-Note 3168368* Für die Verschlüsselung sollte eines der beiden folgenden Verfahren verwendet werden: a) Die Verschlüsselung wird über einen HANA-Parameter erzwungen (das gilt dann für alle Client-Anwendungen, ist aber u. U. aus Kompatibilitätsgründen nicht praktikabel). Eine Prüfung kann über das DBACOCKPIT über den Pfad Configuration > INI Files > global.ini [communication] sslenforce = true oder über den SQL-Editor > SELECT * FROM PUBLIC.M_INIFILE_CONTENTS where FILE_NAME = ‚gobal.ini‘ and SECTION = ‚communication‘ and KEY = ‚sslenforce‘ erfolgen. b) Die Verschlüsselung der Verbindung ist auf ABAP-Seite durch einen Parameter konfiguriert. Zusätzlich gibt es einen Prozess, der unverschlüsselte Zugriffe auf die HANA Datenbank überprüft. Für einen kurzen Zeitraum kann die Verwendung verschlüsselter/unverschlüsselter Kommunikation durch den System-View M_CONNECTIONS überprüft werden. Relevante Spalten sind IS_ENCRYPTED, SSL_VERSION, SSL_CIPHER: DBACOCKPIT > System-Information > Connections DBACOCKPIT > SQL EDITOR → SELECT ... COUNT(*) ... FROM PUBLIC.M_CONNECTIONS WHERE CONNECTION_TYPE =‚REMOTE‘ and not AUTHENTICATION_METHOD = ‚INTERNAL‘

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
	Prüfung auf angemessene Einrichtung eines der beiden oben dargestellten Verschlüsselungsverfahren.
3.2.	**Verschlüsselung Interne Kommunikation:** *Ist die Interne Kommunikation im Falle von Scale-out- oder Single-Host-Systemen angemessen verschlüsselt?* a) Scale-out-Systeme: Ob der DB-Server auf mehrere Hosts verteilt ist (Scale-out), kann im DBACOCKPIT überprüft werden über den Pfad DBACOCKPIT > Current Status > Overview > Distributed System = Yes. Die Verschlüsselung erfolgt über den Parameter ssl über den Pfad DBACOCKPIT > Configuration > INI Files > global.ini [communication] ssl = systempki (empfohlener Wert, verboten: off) b) Single-Host-Systeme: Ob der DB-Server auf nur einem Host läuft, kann im DBACOCKPIT überprüft werden über den Pfad DBACOCKPIT > Current Status > Overview > Distributed System = No; DBACOCKPIT > Configuration > INI Files > global.ini [communication] listeninterface = .local c) Disaster-Recovery-Scenario (System-Replication): Ob System-Replication verwendet wird, lässt sich im DBACOCKPIT prüfen über den Pfad DBACOCKPIT > Current Status > Overview > System Replication = Yes; DBACOCKPIT > System Information > Data-Browser for System-Tables > Schema SYS > M_SYSTEM_REPLICATION; die Verschlüsselung wird über den Parameter enable_ssl über den Pfad DBACOCKPIT > Configuration > INI Files > global.ini [system_replication_communication] enable_ssl = on konfiguriert. Wenn System-Replication auf Host-Ebene konfiguriert ist, sind entsprechende Prüfungen dort notwendig. Prüfung auf angemessene Verschlüsselung der internen Kommunikation im Rahmen der jeweils zutreffenden System-Szenarien.

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
3.3.	Allgemeine Verschlüsselungs-Parameter: Sind die allgemeinen Kommunikationsparameter angemessen konfiguriert? Die Einstellungen der wichtigsten Parameter sollen überprüft werden über den Pfad DBACOCKPIT > Configuration > INI Files > global.ini [communication], insbesondere: a) TLS-Version mindestens 1.2: Parameter sslminprotocolversion = TLS12 b) Starke Cipher-Suites (gegebenenfalls individuell auszuwerten): Parameter: sslciphersuites Der Aufbau ist folgender: <Protocol_Bit-mask>:<Cipher_config>::<Elliptic_Curves_config> **Beispiel Konfiguration: PFS:HIGH::EC_HIGH:+EC_OPT** Erklärung Protokoll: „DEFAULT“: Standard-Chiffre-Suiten (HIGH:PFS:!aNULL:!eNULL) „ALL“: Alle unterstützten Cipher-Suites „PFS“: Perfect Forward-Secrecy: Schlüsselvereinbarung mit ephemeren Schlüsseln „HIGH“: Hochsichere Cipher-Suites (außer PFS) „MEDIUM“: Mittlere Sicherheits-Chiffre-Suites „LOW“: (nicht mehr verwendet) Erklärung Eliptische Kurven: „EC_DEFAULT“ (=EC_HIGH:EC_MEDIUM), „EC_ALL“: Alle unterstützten elliptischen Kurven „EC_HIGH“: Hochsichere elliptische Kurven „EC_MEDIUM“: Elliptische Kurven mit mittlerer Sicherheit „EC_LOW“: Geringe Sicherheit elliptischer Kurven „EC_NIST“: NIST-standardisierte elliptische Kurven, empfohlen in Suite B

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
	„EC_IETF“. Weitere Erläuterungen finden sich z. B. in dem SAP-Hinweis 2415828 (https://launchpad.support.sap.com/#/notes/2415828) und in der Sicherheitsklassifizierung von Cipher-Suite (https://ciphersuite.info/cs/). Prüfung auf angemessene Konfiguration der allgemeinen Kommunikationsparameter.
4.	**Zertifikate**
	Kontrollziel: Die eingesetzten Serverzertifikate sind sicher. **Risiko:** Aufgrund der webbasierten Anmeldung (Fiori) kann mittels eines gefälschten Zertifikats ein Benutzer beim Anmeldeprozess ausgespäht werden.
4.1.	Kontrollziel: Im System hinterlegte Zertifikate sind gültig und entsprechen den Richtlinien der Organisation, z. B. hinsichtlich ausstellender Zertifizierungsstelle, verwendeter Algorithmen und Schlüssellängen. Prüfung: Prüfung erfolgt anhand des System-View CERTIFICATES (VALID_FROM, VALID_TO). In dem View können nach Bedarf weitere Attribute überprüft werden.
5.	**Externe Authentifizierung**
	Kontrollziel: Nur betrieblich notwendige Authentifizierungs-Anbieter sollen konfiguriert sein. Eine technische Absicherung mit geeigneten Maßnahmen ist erforderlich. **Risiko:** Bei Verwendung externer Authentifizierungs-Anbieter können Sicherheitslücken in der Konfiguration dazu führen, dass eine zweifelsfreie Authentifizierung nicht gegeben ist.

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
5.1.	**Nutzung externer Service-Provider:** *Werden neben den internen Authentifizierungsmethoden noch andere Methoden genutzt und sind diese angemessen dokumentiert und abgesichert?* Ob andere Authentifizierungsmethoden konfiguriert sind, kann über die folgenden System-Views festgestellt werden: LDAP_PROVIDERS (Spalten: LDAP_PROVIDER_NAME, CREATE_TIME, IS_DEFAULT, IS_SSL_USED, IS_PROVIDER_ENABLED), SAML_PROVIDERS, JWT_PROVIDERS, X509_PROVIDERS. Zu den konfigurierten Verfahren sollten nachvollziehbare Dokumentationen zum Einsatzzweck und den korrespondierenden Absicherungen vorliegen. Prüfung auf die konfigurierten Authentifizierungsverfahren und die hierfür verfügbaren Dokumentationen.
5.2.	**LDAP-Authentifizierung:** Wird z. B. LDAP verwendet, so muss auf LDAP-Seite überprüft werden, ob die Kommunikation mit HANA verschlüsselt ist. Wird LDAP für die Berechtigungsvergabe verwendet, so ist zu prüfen, wie der Refresh der Informationen konfiguriert ist: Wird LDAP auch für die Vergabe von Berechtigungen verwendet? Sys.users-IS_LDAP_ENABLED, AUTHORIZATION_MODE=LDAP ROLE_LDAP_GROUPS -> ROLE_SCHEMA_NAME, ROLE_NAME, LDAP_GROUP_NAME Refreshzeit für im System aktive Benutzer: indexserver.ini [authorization] ldap_authorization_role_reuse_duration Sys.LDAP_USERS (Spalten: USER_NAME, LAST_AUTHORIZATION_REFRESH_TIME) vs SYS.USERS (Spalte: LAST_SUCCESSFUL_CONNECT)

Nr.	PRÜFPROGRAMM: AUTHENTIFIZIERUNG
5.3.	**Schutz Passwort-Informationen im HDB User Store:** *Wird der Zugriff auf gespeicherte Kennwörter im HDB User Store der HANA DB angemessen geschützt?* Der HDB User Store befindet sich (nur) in dem dafür vorgesehenen Pfad. Der Zugriff auf das Verzeichnis auf Betriebssystemebene ist angemessen beschränkt und überwacht. Prüfung auf die Speicherung der Passwort-Daten des HDB User Store nur im vorgesehenen Pfad und auf angemessenen Schutz des Zugriffs auf diesen Pfad. Die betroffenen Dateien sind „SSFS_HDB.DAT“ und „SSFS_HDB.KEY“, und auf diese Dateien darf nur der Eigentümer des Verzeichnisses zugreifen, unabhängig von der erweiterten Dateiberechtigung. Dies kann mittels eines Befehls auf der Linux-Shell geprüft werden: find /usr/sap/hana/home \(-iname SSFS_*.KEY -o -iname SSFS_*.DAT \) -type f -ls && find /usr/sap/hana \(-iname SSFS_*.KEY -o -iname SSFS_*.DAT \) -type f | xardirgs name | xargs ls -ld Die Berechtigung sollte auf 700 (drwx------) gesetzt sein. Risiko: Ein Betriebssystem-Benutzer kann auf die gespeicherten Daten im User Store zugreifen und erhält damit unautorisierte Zugänge auf die Datenbank.

Tabelle 31 Parameter

Parameter-Name	Beschreibung	DSAG Empfehlung
detailed_error_on_connect	Bei der Einstellung »FALSE« wird nur die Meldung »authentication failed« bei Anmeldefehlern ausgegeben. Ansonsten werden Details angezeigt: Invalid user or password User is locked Connect try is outside validity period User is deactivated	FALSE
force_first_password_change	Legt fest, ob Benutzer ihr Initialkennwort bei der ersten Anmeldung ändern müssen.	TRUE
last_used_passwords	Anzahl der letzten Kennwörter, die nicht erneut genutzt werden dürfen. Der Wert »0« bedeutet, dass alle letzten Kennwörter wieder genutzt werden können.	6
maximum_invalid_connect_attempts	Anzahl möglicher Falschanmeldungen bis zur Sperrung von Benutzern.	6
maximum_password_lifetime	Anzahl der Tage, bis ein neues Kennwort erzwungen wird.	90
maximum_unused_initial_password_lifetime	Anzahl der Tage, bis ein Initialkennwort abläuft. Danach ist keine Anmeldung mehr möglich und es muss ein neues Initialkennwort vergeben werden	3
maximum_unused_productive_password_lifetime	Anzahl der Tage, bis ein produktives Kennwort abläuft. Danach ist keine Anmeldung mehr möglich und es muss ein neues Initialkennwort vergeben werden	90
minimal_password_length	Minimale Kennwortlänge.	10
minimum_password_lifetime	Anzahl der Tage, bevor Benutzer nach einer Kennwortänderung erneut ändern kann.	2

8.5 Prüfprogramm: Autorisierung

Tabelle 32 Prüfprogramm: Autorisierung

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
1.	Dokumentation und Standards
	Kontrollziel: Die für Benutzer und Berechtigungen vorliegenden Dokumentationen und Standards ermöglichen es den am Prozess Beteiligten, die korrespondierenden Strukturen, die Prozesse, die Organisation und die hierbei zu beachtenden Vorgaben in angemessener Zeit nachzuvollziehen. **Risiko:** Durch fehlende, unvollständige oder unverständliche Dokumentation können die Beteiligten die Benutzer und Berechtigungen und ihre eigenen Aufgaben im Prozess nicht verstehen. Daraus ergeben sich Risiken für eine unsachgemäße Pflege und Vergabe der Rollen.
1.1.	**Platzhalter Dokumentation und Standards:** *Sind alle im Prüfprogramm in Kapitel 4.5 Dokumentation und Standards enthaltenen, im HANA-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Dokumentation und Standards vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das HANA-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag.
2.	Prozesse und Organisation
	Kontrollziel: Die für Benutzer und Berechtigungen etablierten Prozesse und organisatorischen Rollen gewährleisten, dass der Zustand der Vergabekette zwischen Benutzern, Rollen und technischen Berechtigungen auf einem angemessenen Niveau unter Beachtung der regulatorischen Anforderungen verbleibt. **Risiko:** Aus fehlenden Vorgaben oder unzureichender Anwendung der Vorgaben für Prozesse und organisatorische Rollen folgt eine Verschlechterung der Benutzer und Berechtigungsstrukturen mit der Folge der Verletzungen des Minimalprinzips und der sich ergebenden Gefährdungen der Integrität, Verfügbarkeit und Vertraulichkeit von Daten.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
2.1.	**Platzhalter Prozesse und Organisation:** *Sind alle im Prüfprogramm in Kapitel 4.6 Prozesse und Organisation enthaltenen, im HANA-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Prozesse und Organisation vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das HANA-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag.
2.2.	**Nachvollziehbarkeit Benutzer und Rollenzuordnungsänderungen:** *Sind alle Änderungen an Benutzern und Rollenzuordnungen zu Benutzern unter Anwendung der hierfür anwendbaren Vorgaben dokumentiert und genehmigt?* Änderungen für Benutzer und Rollenzuordnungen sind ermittelbar im HANA-Audit-Log. Hierbei ist auf die Audit-Policy User and Role Management mit den Actions: • ALTER ROLE, ALTER USER, ALTER USER GROUP, • CREATE ROLE, CREATE USER, CREATE USER GROUP, • DROP ROLE, DROP USER, DROP USER GROUP für Benutzeränderungen und auf die Audit-Policy Granting and Revoking of Authorization mit den Actions GRANT ANY, REVOKE ANY für Rollenzuordnungen und -entziehungen einzugrenzen. Bei Verwendung von XS Classic oder XS Advanced ist zusätzlich die Auditierung der EXECUTE-Berechtigungen für die HANA-Prozeduren nötig, die zur Berechtigungsvergabe verwendet werden. Im SAP-Standard sind dies für XS Classic: • _SYS_REPO.GRANT_ACTIVATED_ANALYTICAL_PRIVILEGE, • _SYS_REPO.GRANT_ACTIVATED_ROLE, • _SYS_REPO.GRANT_APPLICATION_PRIVILEGE, • _SYS_REPO.GRANT_PRIVILEGE_ON_ACTIVATED_CONTENT, • _SYS_REPO.GRANT_SCHEMA_PRIVILEGE_ON_ACTIVATED_CONTENT, • _SYS_REPO.REVOKE_ACTIVATED_ANALYTICAL_PRIVILEGE, • _SYS_REPO.REVOKE_ACTIVATED_ROLE, • _SYS_REPO.REVOKE_APPLICATION_PRIVILEGE, • _SYS_REPO.REVOKE_PRIVILEGE_ON_ACTIVATED_CONTENT,

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	• _SYS_REPO.REVOKE_SCHEMA_PRIVILEGE_ON_ACTIVATED_CONTENT Wenn Kund:innen-eigene Prozeduren verwendet werden oder wenn die Prozeduren von anderen Prozeduren aufgerufen werden, so ist deren Ausführung ebenfalls zu auditieren. Für XS Advanced sind die entsprechenden Prozeduren der relevanten HDI-Container zu auditieren (HDI = HANA Deployment Infrastructure). Es müssen die Parameter zur Aktivierung des Auditings gesetzt sein und die entsprechenden individuellen Audit-Policies eingerichtet sein (siehe Kapitel Logs und Protokolle). Prüfung der Dokumentation der Genehmigung der Benutzeranlage und der Rollenzuordnungen durch Manager und Rollen-Zuordnungsverantwortliche für ausgewählte Stichproben aus der Änderungsprotokollierung für Benutzer und Rollenzuordnungen.
2.3.	**Nachvollziehbarkeit Rollenänderungen:** *Sind alle Änderungen an Rollen unter Anwendung der hierfür anwendbaren Vorgaben dokumentiert und genehmigt?* Rollenänderungen sind im Audit-Log des Entwicklungssystems ermittelbar. In der HANA Datenbank des Produktivsystems ist u. U. nur der Import des Transports nachvollziehbar, jedoch keine Details. Über das Audit-Log in produktiven Systemen sollten insofern keinerlei Änderungen protokolliert sein. Bei der Analyse sind alle Audit-Policies zu berücksichtigen, die Änderungsbelege von Rollen oder Privilegien betreffen – z. B. auch die Audit-Policy für Structured-Privilege-Management mit den Actions ALTER STRUCTURED PRIVILEGE, CREATE STRUCTURED PRIVILEGE, DROP STRUCTURED PRIVILEGE und die Audit-Policy für Repository-Privilege-Management mit den Actions ACTIVATE REPOSITORY CONTENT, EXPORT REPOSITORY CONTENT, IMPORT REPOSITORY CONTENT. Hierzu müssen die Parameter zur Aktivierung des Auditings gesetzt sein und die entsprechenden individuellen Audit-Policies eingerichtet sein (siehe Kapitel Logs und Protokolle). Prüfung der Dokumentation der Genehmigung der Rollenänderungen durch Rolleneigner:innen/-koordinator:innen für ausgewählte Stichproben aus der Änderungsprotokollierung für Rollenänderungen im Entwicklungssystem.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
3.	Benutzer und Rechte
	Kontrollziel: Die Vorgaben für Benutzer und die Zuordnung von Rollen und Berechtigungen und deren Umsetzung sorgen für eine vollständige Nachvollziehbarkeit der Rollen und ggf. der Berechtigungen und deren Zuordnung zu Benutzern und Identitäten. **Risiko:** Bei fehlender Nachvollziehbarkeit auf einer oder mehreren Ebenen eines Benutzer- und Berechtigungskonzepts ergeben sich automatisch Mängel im Minimal- und Funktionstrennungsprinzip und damit eine Gefährdung der Integrität, Verfügbarkeit und Vertraulichkeit von Daten. Hinweis: Das Auslesen von Informationen zu Benutzern erfolgt in HANA über die folgenden Pfade im DBACOCKPIT > System Information > Databrowser for System Tables > Schema SYS > USERS oder über DBACOCKPIT > SQL Editor > SELECT * FROM PUBLIC.USERS und zu Rollen und Privilegien über DBACOCKPIT > System Information > Databrowser for System Tables > Schema SYS > GRANTED ROLES oder GRANT PRIVILEGES oder über DBACOCKPIT > Diagnostics > SQL Editor > SELECT * FROM PUBLIC.GRANTED ROLES oder PUBLIC.GRANT PRIVILEGES
3.1.	**Platzhalter Benutzer und Rechte:** *Sind alle im Prüfprogramm in Kapitel 4.7 Benutzer und Rechte enthaltenen und im HANA-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Benutzer und Rechte vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das HANA-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag.
3.2	**Benutzer und Minimalprinzip:** *Sind nur notwendige Benutzer in der Datenbank aktiv? Entsteht durch die Benutzer eine Gefährdung für die Integrität des SAP-Systems?* Die Prüfung der im System aktiven Benutzer erfolgt mit dem System-View SYS.USERS. Zu betrachten sind alle Benutzer, die aktiv sind (IS_DEACTIVATED = FALSE) und die in dem betrachteten Zeitraum gültig sind (VALID_FROM, VALID_TO). Änderungen der Gültigkeit können über das Audit-Log ermittelt werden. Im View SYS.USERS sind zusätzlich das Datum der letzten Deaktivierung und die letzten Einträge für den Gültigkeitszeitraum auswertbar.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Für Technische Benutzer von Anwendungen ist gegebenenfalls die Gesamtheit der Anwendungsbenutzer zu betrachten. Bei kritischen Berechtigungen auf Datenbankebene ist auch das Berechtigungskonzept der Anwendung relevant. Anwendungsberechtigungen können innerhalb (z. B. XS-Classic-Anwendungen) oder außerhalb (z. B. XS-Advanced-Anwendungen, Monitoring oder Backup-Tools) der Datenbank abgebildet sein. Prüfung auf Dokumentation der Benutzer und ihres Verwendungszwecks sowie der Erforderlichkeit der Berechtigungen entsprechend einem Berechtigungskonzept auf das für die erforderlichen Tätigkeiten minimal notwendige Maß.
3.3	**Inaktive Benutzer:** *Werden Benutzer ohne erkennbare Systemaktivität regelmäßig geprüft und nach Prüfung über die Pflege des Enddatums deaktiviert?* Eine Prüfung nicht deaktivierter Benutzer ohne Anmeldungen in einer betrachteten Periode ist über die Selektion aller Benutzer über den System-View: USERS, Spalten User Deactivated = FALSE über die Spalte „Last successful Connect“ möglich. Für diese Benutzer sollte eine angemessene Erklärung der Notwendigkeit der aktiven Benutzerkonten trotz fehlender Anmeldung vorliegen. Insgesamt sollte ein Nachweis einer regelmäßigen, mindestens jährlichen Validierung aktiver Konten ohne Anmeldungen vorliegen. Prüfung auf regelmäßige Validierung von aktiven Benutzern ohne Anmeldungen.
3.4	**Technische Benutzer:** *Welche Anwendungen haben durch Technische Benutzer Zugriff auf die HANA Datenbank? Sind die Funktionalität und die zugewiesenen Rechte potenziell kritisch für die Integrität des SAP-Systems?* Im Gegensatz zur OnPremise-Schicht sind Technische Benutzer in der HANA-DB-Schicht nicht über ein eindeutiges Benutzer-Attribut erkennbar. Dies ist nur über eine sinnvolle Namenskonvention, über Benutzergruppen oder eine Auflistung im Rahmen einer Dokumentation identifizierbar. Darüber hinaus zählen hierzu auch die von SAP ausgelieferten Technischen Standardbenutzer. Letztere sind über den Creator SYS, _SYS_REPO, _SYS_DI_SU identifizierbar.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Prüfung der Benutzer auf Kund:innen-eigene Technische Benutzer oder technische SAP-Standardbenutzer.
3.5	**Vermeidung von Shared Usern:** *Werden Shared User verwendet und sind sie für diese Verfahren etabliert, die eine Nachvollziehbarkeit von Datenänderungen zu den zugrunde liegenden personalisierten Benutzern zulassen?* Datenbankbenutzer, die von unterschiedlichen Personen benutzt werden dürfen, können über Einträge im Audit-Log zu einem USER_NAME mit unterschiedlichem APPLICATION_USER_NAME bzw. XS_APPLICATION_USER_NAME (eventuell erweiterbar: CLIENT_HOST, CLIENT_IP) identifiziert werden. Diese Prüfung bietet sich insbesondere für Standardbenutzer (z. B. Benutzer SYSTEM) und weitere Benutzer an, die als Shared User erkennbar sind. Prüfung auf Vermeidung von Shared Users oder auf angemessene Verfahren und deren Anwendung zur Wahrung der Nachvollziehbarkeit der Nutzung durch unterschiedliche Anwendende.
3.6	**Vermeidung von Standardbenutzern:** *Wird die Nutzung von HANA-Standardbenutzern mit ihren teilweise sehr weitreichenden Privilegien insbesondere in der Produktionsumgebung durch geeignete Maßnahmen auf das für die Benutzer vorgesehene Maß eingeschränkt?* Für alle Benutzer, die bereits als Standardbenutzer identifiziert sind, können die folgenden relevanten Vorgänge im Zusammenhang mit einer temporären Nutzung über die folgenden Felder der SYS.USERS identifiziert werden: LAST_PASSWORD_CHANGE_TIME, ADMIN_GIVEN_PASSWORD = FALSE/TRUE; False = User changed password, DEACTIVATION_TIME, VALID_FROM, VALID_UNTIL, LAST_SUCCESSFUL_CONNECT). Eine Identifizierung der letzten Nutzung der Benutzer über den Zeitpunkt der letzten Deaktivierung ist über die Felder USER_DEACTIVATED, DEACTIVATION_TIME sowie für den letzten Verbindungsaufbau über das Feld LAST_SUCCESSFUL_CONNECT möglich. Ein umfassenderer Überblick lässt sich mit dem Audit-Log erreichen, indem z. B. nach erfolgreichem CONNECT gesucht wird. Mit Stichproben lässt sich so der Umfang der Benutzer überprüfen.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Prüfung der in den folgenden Prüfungshandlungen beschriebenen Standardbenutzer a) auf organisatorische Maßnahmen zum Schutz des Passworts und b) auf Nutzung im Prüfungszeitraum.
3.7	**Handhabung Standardbenutzer SYSTEM:** *Ist sichergestellt, dass der Standardbenutzer System nur für den vorgesehenen Einsatzzweck als Installations- und Update-Benutzer verwendet wird und im laufenden Betrieb nur in Ausnahmefällen aktiviert wird?* Der Benutzer verfügt über alle Systemprivilegien, darf aber nicht die Daten anderer Benutzer sehen. Diesem Benutzer können weitere Privilegien gewährt und entzogen werden; seine ursprünglichen Privilegien können jedoch nicht entzogen werden. Prüfung des Benutzers auf das Datum der letzten Anmeldung, um sicherzustellen, dass keine Aktivitäten innerhalb des Prüfungszeitraums stattgefunden haben. Im Falle von Aktivitäten: Recherche der zugehörigen Nutzungsbelege. Prüfung der Belege auf Protokollierung, Prüfung und Genehmigung aller korrespondierenden Aktivitäten durch einen unabhängigen Dritten. Prüfung, ob die Nutzungsdauer angemessen beschränkt wurde. Prüfung organisatorischer Maßnahmen zum Schutz des Passworts.
3.8	**Handhabung Technischer Benutzer des SAP-Systems:** *Ist sichergestellt, dass die Standardbenutzer des SAP-Systems SAP<SID> bzw. SAPABAP1, SAPHANADB und SAP<SID>SHD nur für den vorgesehenen Einsatzzweck als Technische Benutzer des laufenden SAP-Systems (bzw. für Aktivitäten im Upgrade) verwendet werden?* Eine Protokollierung der normalen Aktivitäten (z. B. SELECT, INSERT, UPDATE, DELETE, CREATE, ALTER) im Audit-Log ist für diese Benutzer aus Performance-Gründen nicht möglich. In die Auditierung von Administrationstätigkeiten sollen die Benutzer jedoch eingeschlossen sein, sofern es sich nicht um Massenänderungen im Upgrade handelt. Der Name SAPABAP1 oder SAPHANADB wird in SAP-S/4HANA-Systemen oft verwendet. In anderen Systemen heißt der entsprechende Benutzer meist SAP<SID>. Der ABAP-Benutzer sollte nur die nötigen Rechte auf der HANA DB haben; insbesondere darf der Benutzer nicht über die Privilegien USER ADMIN und ROLE ADMIN verfügen.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Prüfung organisatorischer Maßnahmen, die den Zugriff auf diese Benutzer verhindern. Prüfung auf Einschränkung der Benutzer nur auf notwendige Rechte, insbesondere Ausschluss von Administrations-Rechten. Prüfung im Audit-Log, ob mit den Benutzern verdächtige Aktivitäten durchgeführt wurden.
3.9	**Handhabung Standardbenutzer XSA_ADMIN:** *Ist sichergestellt, dass der Standardbenutzer XSA_ADMIN nach dem initialen Setup der XSA-Funktionalität deaktiviert und nicht für regelmäßige Administrationstätigkeit verwendet wird?* XSA wird nicht automatisch mit einer HANA DB installiert und ist auch nicht zwingend für den Betrieb von S/4HANA. Damit ist der XSA_ADMIN-Benutzer insofern auch nur sinnvoll, wenn die XSA bewusst genutzt werden soll. Der XSA_ADMIN-Benutzer hat umfassende Berechtigung für XSA Advanced – vergleichbar dem Benutzer SYSTEM in der HANA Datenbankadministration. Zum Beispiel kann der Benutzer XSA_ADMIN den Controller ohne Einschränkungen verwenden, und er ist der einzige Benutzer, der die Ersteinrichtung der XSA-Advanced-Funktionalität vornehmen kann. Dazu gehört die Ernennung mindestens eines Org-Managers, der in der Lage ist, Spaces einzurichten und globale Ressourcen wie Buildpacks und Externe Broker zu verwalten. Prüfung des Benutzers auf das Datum der letzten Anmeldung, um sicherzustellen, dass keine Aktivitäten innerhalb des Prüfungszeitraums stattgefunden haben. Im Falle von Aktivitäten: Recherche der zugehörigen Nutzungsbelege. Prüfung der Belege auf Protokollierung, Prüfung und Genehmigung aller korrespondierenden Aktivitäten durch einen unabhängigen Dritten. Prüfung auf Änderung des Initialpassworts.
3.10	**Handhabung Standardbenutzer DBACOCKPIT:** *Wird der Standardbenutzer DBACOCKPIT verwendet? Ist sein Einsatzgebiet (im Vergleich zu anderen Administrator:in-Benutzern) abgegrenzt und sind die zugewiesenen Berechtigungen entsprechend angepasst?* Der Benutzer DBACOCKPIT wird bei der Installation eines SAP-Systems automatisch angelegt und hat die für das DBA-Cockpit des SAP-Systems (ABAP-Stack) erforderlichen Berechtigungen. Standardmäßig wird die Datenbankverbindung für das DBA-COCKPIT jedoch in den aktuellen HANA-

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Versionen mit dem Benutzer SAP<SID> konfiguriert, sodass der Benutzer DBACOCKPIT oft obsolet ist (vgl. SAP-Hinweis 1640741). Obwohl der Benutzer keine hochkritischen Berechtigungen besitzt, sollte er/sie bei Nichtverwendung gesperrt sein. Wird der Benutzer verwendet, so sollten alle diejenigen Berechtigungen entzogen sein, die sich auf Tätigkeiten beziehen, deren Ausführung aus der SAP-Transaktion DBACOCKPIT heraus nicht vorgesehen ist. Typischerweise betrifft dies alle Änderungsberechtigungen, da die Systemadministration meist mit dem HANA Cockpit (vereinzelt auch: HANA Studio) ausgeführt wird. Statt auf Datenbankebene kann das Entziehen der Berechtigungen auch im SAP-System mit den dort vorhandenen Berechtigungsobjekten erfolgen (siehe Kapitel S/4HANA OnPremise – 4.10). Prüfung, ob der Benutzer aktiv ist. Prüfung des Benutzers auf das Datum der letzten Anmeldung, um sicherzustellen, dass keine ungeplanten Aktivitäten innerhalb des Prüfungszeitraums stattgefunden haben. Im Falle von Aktivitäten: Recherche der zugehörigen Nutzungsbelege.
3.11.	**Handhabung Standardbenutzer SAPDBCTRL:** *Ist sichergestellt, dass der Standardbenutzer SAPDBCTRL nur für den vorgesehenen Einsatzzweck verwendet wird?* Der Benutzer SAPDBCTRL wird von dem/der Betriebssystemnutzenden des SAP Host Agent zur Überwachung der SAP HANA Datenbank genutzt. Prüfung, ob dem Benutzer zusätzliche Rechte zugewiesen sind, die über den Umfang der Rollen MONITORING und PUBLIC hinausgehen. Wenn der Benutzer zu kritischen Änderungen autorisiert ist, Prüfung der Maßnahmen zur Verhinderung unautorisierter Verwendung. Zu prüfen sind dann auch die Änderungsprozesse, die den SAP Host Agent mit erweiterter Funktionalität versorgen.
3.12	**Handhabung Technischer Standardbenutzer:** *Ist sichergestellt, dass technische Standardbenutzer nur die für ihren Einsatzzweck erforderlichen Berechtigungen haben?* Während die Technischen Benutzer externer Tools und Applikationen wie normale Benutzer auch mit passenden Berechtigungen versehen werden müssen, sind die von SAP HANA generierten Technischen Benutzer mit fest vorgegebenen Berechtigungen versehen und erhalten durch zusätzliche

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Berechtigungen keine zusätzliche Funktionalität. Beispiele sind: SYS, _SYS_~, XSSQLCC_AUTO_USER_~. Eine Ausnahme bilden Benutzer im XS-Advanced-Kontext. So wird der/die Schema-Benutzer, der/die einen HDI-Container besitzt (~#OO), ohne Berechtigungen angelegt und bekommt diese erst im Rahmen des Entwicklungsprozesses (HDI = HANA Deployment Infrastruktur). Prüfung der SAP-Standardbenutzer zugewiesenen Berechtigungen auf Erforderlichkeit, insbesondere der zugewiesenen Berechtigungen des HDI-Container-Owners (~#OO) und der Verwendung dieser Berechtigungen.
	Handhabung Standardbenutzer <SID>ADM (HANA Datenbank): *Ist sichergestellt, dass der Standardbenutzer <SID>ADM nur für diesen vorgesehenen Einsatzzweck als Technischer Benutzer der HANA Datenbank auf Betriebssystemebene verwendet wird und dass geeignete Maßnahmen gegen missbräuchliche Verwendung durch andere Betriebssystembenutzer implementiert sind?* Der Benutzer <SID>ADM wird bei der initialen Erstellung einer neuen Instanz automatisch bereitgestellt. <SID> ist die ID des SAP-HANA-Systems. Es handelt sich um einen Betriebssystembenutzer, der/die Eigentümer:in aller zum SAP-HANA-System gehörenden Dateien und Betriebssystemprozesse ist. Der Benutzer wird u. a. dafür genutzt, Datenbankprozesse zu starten und zu stoppen oder eine Wiederherstellung der Datenbank durchzuführen. Wenn die Persistenz der Datenbank verschlüsselt ist, hat der Benutzer <SID>ADM zwar Zugriff auf die HANA Datenbank, kann die Daten aber ohne Schlüssel nicht lesen. In diesem Fall sind Zugriffe auf die Dateien, die die Schlüssel enthalten, relevant. Alle Prüfungshandlungen hierzu müssen auf Betriebssystemebene erfolgen, z. B. durch Prüfung des Security-Audit-Log des Betriebssystems. Prüfung, welche Benutzer auf Betriebssystemebene auf den Benutzer <SID>ADM Zugriff erhalten können. Prüfung, welche Benutzer Zugriff auf das Verzeichnis mit den Schlüsseln haben. Recherche der zugehörigen Nutzungsbelege im Audit-Log des Betriebssystems auf Unregelmäßigkeiten und verdächtige Aktivitäten. Prüfung der Belege auf Protokollierung, Prüfung und Genehmigung aller korrespondierenden Aktivitäten durch eine:n unabhängige:n Dritte:n.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
4.	Rollen und Berechtigungen
	Kontrollziel: Die Vorgaben für Rollen und technische Berechtigungen und deren Umsetzung sorgen für eine vollständige Nachvollziehbarkeit der technischen Berechtigungen auf der untersten Ebene bis zu den Rollen als Zwischenebene. **Risiko:** Bei fehlender Nachvollziehbarkeit auf einer oder mehreren Ebenen eines Benutzer- und Berechtigungskonzepts ergeben sich automatisch Mängel im Minimal- und Funktionstrennungsprinzip und damit eine Gefährdung der Integrität, Verfügbarkeit und Vertraulichkeit von Daten. Hinweis: Anzeige der zugeordneten Standardrollen über den Pfad im DBACOCKPIT > System Information > Databrowser for System Tables > Schema SYS > EFFECTIVE_ROLES oder über DBACOCKPIT > SQL Editor > SELECT * FROM PUBLIC.EFFECTIVE_ROLES
4.1.	**Platzhalter Rollen und Berechtigungen:** *Sind alle im Prüfprogramm in Kapitel 4.8 Rollen und Berechtigungen enthaltenen, im HANA-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Rollen und Berechtigungen vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das HANA-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag.
4.2.	**Vermeidung von Standardrollen:** *Wird die Nutzung von HANA-Standardrollen mit ihren in der Regel weitreichenden Privilegien insbesondere in der Produktionsumgebung weitgehend vermieden und durch angemessene Kund:innen-eigene Rollen ersetzt?* SAP-Standardrollen für HANA weisen neben einer relativ umfangreichen Ausstattung mit Privilegien häufig auch eine Hierarchie von Rollen auf, die die Nachvollziehbarkeit zwischen Rolle und enthaltenen Privilegien über mehrere

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Ebenen behindern. Beispiele für SAP-Standardrollen sind Designzeitrollen des Erstellers _SYS_REPO (meist beginnend mit *sap.hana.* oder *sap.bc.*) sowie die Katalogrollen CONTENT_ADMIN, MODELING (Ersteller: SYSTEM), SAP_INTERNAL_HANA_SUPPORT (ERSTELLER: SYS) und weitere Katalogrollen interner SAP-HANA-Benutzer (Name des Erstellers beginnend mit _SYS_). Manche Standardrollen, wie z. B. PUBLIC, MONITORING, RESTRICTED_USER_JDBC_ACCESS und RESTRICTED_USER_ODBC_ACCESS sind unkritisch. Prüfung der in den folgenden Prüfungshandlungen beschriebenen Standardrollen a) auf unterbliebene Vergabe an Benutzer und b) auf Nutzung im Prüfungszeitraum.
4.3.	**Handhabung Standardrolle SAP_INTERNAL_HANA_SUPPORT:** *Wird die Nutzung der Standardrolle SAP_INTERNAL_HANA_SUPPORT über geeignete Maßnahmen beschränkt?* Die Standardrolle SAP_INTERNAL_HANA_SUPPORT verfügt über Privilegien für alle Metadaten der Datenbank, den aktuellen Systemstatus, die Trace-Konfiguration, die Daten des Statistikservers und alle Systeminformationen des SYS-Schemas. Die Leserechte sind nur über diese Rolle und den Standardbenutzer SYSTEM zugänglich. Die in dieser Rolle hinterlegte Kombination von Berechtigungen ist in der Regel nur für SAP-Mitarbeitende des HANA Development Support notwendig und keinesfalls als Standard-Supportrolle zu betrachten. Die Rolle kann per SAP-Default nur an einen Benutzer vergeben werden. Die Anzahl der maximalen Rollenvergabe kann über den Parameter internal_support_user limit der Datei nameserver.ini für Systemdatenbanken und indexserver.ini für Tenant-Datenbanken erhöht werden. Eine Vergabe sollte auf wenige Kund:innen-eigene SAP-Support-Benutzer des HANA Development Support und einen internen privilegierten Notfallbenutzer erteilt werden. Für normale Support -Zwecke reichen reine Anzeigeberechtigungen. Prüfung der Vergabe der Rolle nur an Mitarbeitende des SAP HANA Development Support und an interne privilegierte Notfallbenutzer. Prüfung auf begrenzte Freischaltung und Einhaltung der Protokollierung und Dokumentation.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
4.4.	**Handhabung Standardrollen CONTENT ADMIN und MODELING:** *Wird die Nutzung der Standardrollen CONTENT ADMIN und MODELING über geeignete Maßnahmen verhindert?* Die Standardrollen CONTENT_ADMIN und MODELING verfügen standardmäßig über verschiedene Entwickler:innen-Berechtigungen sowie über das umfangreiche Analyseprivileg _SYS_BI_CP_ALL, über das sonst nur der/die kritische Standardbenutzer SYSTEM verfügt. Zusammen mit Objektberechtigungen auf Tabellen ermöglicht _SYS_BI_CP_ALL umfassende analytische Berechtigungen, die eine Funktionstrennung unterlaufen können. Diese Standardrollen dürfen an keinen Benutzer auf der Produktionsdatenbank vergeben werden. Prüfung, ob die Standardrollen CONTENT ADMIN und MODELING an keinen Benutzer im produktiven System vergeben sind.
4.5.	**Vermeidung von Katalogrollen (Runtime-Rollen):** *Wird die Vergabe von Katalogrollen insbesondere in den Produktivsystemen vermieden?* Katalogrollen sind Rollen, die zur Laufzeit von Benutzern angelegt werden. Die Rollen können nicht transportiert oder versioniert werden und sind in ihrer Vergabe an den erstellenden Benutzer gebunden. Mit dem Löschen der Benutzer, die eine solche Rolle erstellt oder vergeben haben, werden auch die erstellten Rollen und Verknüpfungen gelöscht. Ergänzend muss ein Benutzer, die/der Katalogrollen pflegt, auch dieselben Rechte haben, die sie/er in den Rollen pflegen will. Dies ist unter dem Gesichtspunkt der Trennung von administrativen und fachbereichsbezogenen Tätigkeiten, aber auch generell jeglicher Funktionstrennungsaspekte unzulässig. Darüber hinaus sollte eine Pflege prinzipiell nicht in der Produktion erfolgen, da hierdurch das Transport- und Änderungsverfahren unterlaufen wird. Prüfung, ob Kund:innen-eigene Katalogrollen aktiv und insbesondere in Produktivsystemen vergeben sind. Dies sollte nicht der Fall sein.
4.6.	**Vorgaben für Designzeitrollen (Repository-Rollen):** *Werden für Repository-Rollen sinnvolle Gestaltungsvorgaben eingehalten, um ein hohes Maß an Nachvollziehbarkeit der Rollen zu ermöglichen?* Bei der Gestaltung von HANA-Rollen können nicht nur Privilegien an Rollen vergeben werden, sondern auch Rollen an Rollen. Durch eine unstrukturierte

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Nutzung dieser inneren Verschachtelungen kann die Transparenz der Rollen beeinträchtigt werden. Grundsätzlich sollten Rollen nur dann an Rollen vergeben werden, wenn eine Kombination von Task-basierten Rollen in Job-basierten Rollen in Anlehnung an die Einzel- und Sammelrollen in S/4HANA OnPremise angestrebt wird. Für Rollen, die besonders kritische Berechtigungen enthalten, sollte eine Verschachtelung auf HANA-Datenbank-Ebene grundsätzlich vermieden werden. Prüfung, dass Kund:innen-eigene Rollen in der Regel nicht an Rollen vergeben sind und dass in Ausnahmefällen die Rollenvergabe an Rollen der Abbildung von Arbeitsplätzen dient.
5.	Sensitive Funktionen
	Kontrollziel: Für die SAP HANA Datenbank liegt ein Regelwerk mit sensitiven Funktionen vor. Sensitive Funktionen werden ausschließlich über Rollen vergeben, deren Deklaration die beinhalteten sensitiven Funktionen eindeutig erkennbar machen. Für Rollen mit sensitiven Funktionen ist ausgewiesen, für welche Instanzen und an welche Benutzergruppen eine Vergabe zulässig ist. Benutzer erhalten Berechtigungen für sensitive Funktionen unter strenger Beachtung des Minimalprinzips. **Risiko:** Die Nutzung von Rollen mit nicht nachvollziehbaren sensitiven Berechtigungen und die Vergabe sensitiver Berechtigungen an Benutzer unter Verstoß gegen Minimalprinzip und Funktionstrennungsregeln gefährdet die Integrität, Verfügbarkeit und Vertraulichkeit von Information. Hinweis: Der Blog Caution: System Privilege! Managing Critical System Privileges in SAP HANA enthält eine Klassifizierung der Systemprivilegien hinsichtlich ihrer Kritikalität und hinsichtlich Implikationen für die Vergabe. Der Blog beschreibt die Sicht des SAP-HANA-Produkt-Managements und sollte bei der Erstellung eines Berechtigungskonzepts ebenso berücksichtigt werden wie die jeweils aktuelle SAP-Doku im SAP Help Portal.
5.1.	**Sensitive Funktionen:** Hinweis 1: Bei den im Folgenden aufgeführten spezifischen sensitiven Funktionen handelt es sich um ausgewählte Beispiele. Ein vollständiges und unternehmensindividuelles Regelwerk geht im Umfang weit darüber hinaus.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
5.2.	**Sensitive Funktionen:** Hinweis 2: Eine Ermittlung der den Benutzer zugeordneten Privilegien ist über das DBACOCKPIT > System Information > Databrowser for System Tables > Schema SYS > EFFECTIVE_ROLES oder über DBACOCKPIT > SQL Editor > SELECT * FROM PUBLIC.EFFECTIVE_PRIVILEGES möglich. Weitere System-Views, die für die Prüfung verwendet werden können, sind außerdem: SYS.GRANTED_ROLES, SYS.GRANED_PRIVILEGES, SYS.EFFECTIVE_APPLICATION_PRIVILEGES, SYS.EFFECTIVE_ROLE_GRANTEES und SYS.EFFECTIVE_PRIVILEGE_GRANTEES. Zur effizienten Analyse können auch konfigurierbare SQL-Skripte aus SAP-Hinweis 1969700 – SQL Statement Collection for SAP HANA verwendet werden, z. B. HANA_Security_GrantedRolesAndPrivileges_2.00.000+.txt. Mit dem Skript lassen sich kritische Berechtigungen auch bei Zuordnung über stark verschachtelte Rollenhierarchien flexibel analysieren.
5.3.	**Platzhalter Sensitive Funktionen:** *Sind alle im Prüfprogramm in Kapitel 4.9 Sensitive Funktionen und Funktionstrennungen enthaltenen, im HANA-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Sensitive Funktionen vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das HANA-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag.
5.4.	**Benutzeradministration:** *Werden die Privilegien der Benutzeradministration angemessen vergeben?* Das Privileg USER ADMIN für die Benutzeradministration bezieht sich auf Funktionen der Erstellung und Änderung von Benutzern mit den Befehlen CREATE USER, ALTER USER und DROP USER. Die Berechtigung USER ADMIN enthält auch die Berechtigung für das Zurücksetzen von Passwörtern,

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	die nicht separat vergeben werden kann. Die Erstellung von Benutzergruppen erlaubt es, die Pflege von Benutzern dem zentralen USER ADMIN zu entziehen und stattdessen die Pflege an unterschiedliche Teams zu delegieren (siehe Unterkapitel Funktionstrennung). Prüfung der Zuordnung der Benutzer-Administrations-Privilegien USER ADMIN in allen Instanzen nur an Anwendende mit Aufgaben der Benutzeradministration in strenger Anwendung des Minimalprinzips. Bei Verwendung von Benutzergruppen sind zusätzlich die Privilegien USERGROUP ADMIN und USERGROUP OPERATOR zu überprüfen. Für Benutzergruppen, die nur dezentral gepflegt werden, Prüfen des Attributs IS_USER_ADMIN_ENABLED=FALSE im View SYS.USERGROUPS.
5.5.	**Rollenadministration, Privileg ROLE ADMIN:** *Wird das Privileg ROLE ADMIN angemessen verhindert bzw. eingeschränkt?* Das Privileg ROLE ADMIN berechtigt zur Erstellung und Löschung von Katalogrollen mit den Befehlen CREATE ROLE und DROP ROLE sowie zum Gewähren und Entziehen von Rollen mit den Befehlen GRANT und REVOKE. Bei Verwendung von HDI-Rollen (die im Rahmen einer Rollenentwicklung unter XS Advanced erstellt wurden) berechtigt ROLE ADMIN zum Gewähren und Entziehen beliebiger HDI-Rollen in der HANA Datenbank. Rollen, die durch den Benutzer _SYS_REPO (im Rahmen einer Rollenentwicklung unter XS Classic) erstellt werden, können mit dem Privileg ROLE ADMIN nicht vergeben werden. Bei der Erstellung von Katalogrollen können nur solche Berechtigungen zugewiesen werden, für die der Benutzer selbst berechtigt ist. Sofern die Rollenpflege über Katalogrollen umgesetzt ist, muss die Benutzung des Superusers, der die Rollen erstellt, angemessen eingeschränkt und überwacht sein. Prüfung, dass das Privileg ROLE ADMIN in allen Instanzen in strenger Anwendung des Minimalprinzips nur an Benutzer mit Aufgaben der Berechtigungsvergabe von HDI-Rollen vergeben wird. Prüfung, dass Benutzer mit dem Privileg ROLE ADMIN nur minimale weitere Berechtigungen zugewiesen sind.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
5.6.	**Rollenadministration von Designtime-Rollen (XS Classic, XS Advanced):** *Werden die Privilegien der Rollenadministration angemessen vergeben?* Designtime-Rollen werden in einem Entwicklungssystem erstellt und von dort in das Produktivsystem transportiert. Die Vergabe sollte durch HANA-Prozeduren erfolgen (z. B. _SYS_REPO.GRANT_ACTIVATED_ROLE, _SYS_REPO.REVOKE_ACTIVATED_ROLE). Namen und Funktionsumfang der verwendeten Prozeduren können abhängig von der Implementierung variieren. In XS ADVANCED hat jeder HDI-Container seine eigenen Prozeduren für GRANT und REVOKE. Prozeduren können über den View SYS.PROCEDURES identifiziert werden. Prüfung, dass für die Aufgaben bezüglich Entwicklung, Transport und Vergabe von Rollen Standardprozesse und eine angemessene Funktionstrennung implementiert sind und dass alle Aktivitäten durch Belege im HANA-Audit-Log erfasst sind. Außerdem sollen keine Änderungen an Rollen direkt im Produktivsystem vorgenommen werden.
5.7.	**Vermeidung der unkontrollierten Weitergabe von Berechtigungen:** *Erfolgt die Vergabe von Berechtigungen ausschließlich über die vorgesehenen Standardprozesse?* Rollen und Berechtigungen können Benutzer zusammen mit dem Attribut IS_GRANTABLE=TRUE vergeben werden. Dieses Attribut ermöglicht die Weitergabe einer erhaltenen Berechtigung an weitere Benutzer. Die weitergegebene Berechtigung wird automatisch entzogen, wenn der weitergebende Benutzer gelöscht wird. Prüfung, ob die Berechtigung zur Weitergabe von Rollen und Privilegien auf autorisierte Benutzer-Administrator:innen und am Vergabeprozess beteiligte Technische Benutzer beschränkt ist.
5.8.	**Objekt-Privilegien-Sammler:** *Wird die Vergabe des Objekt-Privilegien-Sammlers ALL PRIVILEGES vermieden?* Das Objekt-Privileg ALL PRIVILEGES ist ein Objektsammler, der neben einer Vielzahl weiterer Berechtigungen das Objekt des/der Berechtigungserteilenden (Grantor) beinhaltet. Die Berechtigungen werden dynamisch ausgewertet. Das Projektprivileg sollte nicht, oder wenn nicht

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	vermeidbar, nur äußerst restriktiv vergeben werden. Keinesfalls darf das Privileg auf Objekte mit Daten des SAP-Systems vergeben werden Prüfung der Vermeidung der Zuordnung des Objekt-Privilegs ALL PRIVILEGES an Dialogbenutzer. Eine Vergabe ist nur an Technische Benutzer mit berechtigtem Anlass zulässig.
5.9.	**Auditing:** *Wird der Zugriff auf Privilegien für Auditing angemessen vergeben?* Die Privilegien für Auditing beziehen sich auf Funktionen der Pflege der Audit-Policies sowie auf Änderungen an der Revisionskonfiguration (AUDIT ADMIN – Create, Drop and Alter Audit Policies), auf die Löschung von Audit-Logs (AUDIT OPERATOR – Alter System Clear Audit Log) sowie auf den ausschließlich lesenden Zugriff auf das Audit-Log (AUDIT READ). Prüfung, dass die Auditing-Privilegien nur an Anwendende in strenger Anwendung des Minimalprinzips vergeben werden.
5.10.	**Transportadministration (XS Classic):** *Werden die Privilegien für Transporte angemessen vergeben?* Im Kontext XS Classic ermöglichen es die Privilegien REPO.ACTIVATE_IMPORTED_OBJECTS und REPO.MAINTAIN_IMPORTED_PACKAGES, Import-Fehler durch die manuelle Aktivierung oder die Bearbeitung von Metadaten an den transportierten Paketen oder Objekten zu beheben. Bei Nutzung externer Transportwerkzeuge sind die Berechtigungen typischerweise an den Technischen Benutzer des Werkzeugs vergeben. Prüfung der Zuordnung der Privilegien in allen Instanzen nur an Anwendende mit Aufgaben der Transportadministration in strenger Anwendung des Minimalprinzips.
5.11.	**Entwicklung – XS Classic:** *Werden die Privilegien für Entwicklungsarbeiten in XS Classic angemessen vergeben?* Im Kontext XS Classic berechtigen die Paketprivilegien REPO.ACTIVATE_NATIVE_OBJECTS, REPO.EDIT_NATIVE_OBJECTS und REPO.MAINTAIN_NATIVE_PACKAGES zur Änderung von Daten und zur Änderung von Designzeitobjekten in Paketen, die aus dem System

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	stammen, in dem der Benutzer arbeitet. Analog ermöglicht die Berechtigung REPO.EDIT_IMPORTED_OBJECTS die Bearbeitung importierter Objekte. Prüfung, dass die Privilegien zur Entwicklung von Programmen in XS Classic in produktiven Umgebungen nicht an Benutzer vergeben sind.
5.12.	**Entwicklung – XS Advanced:** *Werden die Privilegien für Entwicklungsarbeiten in XS Advanced angemessen vergeben?* Bei Verwendung von XS Advanced erfolgen Entwicklung und Deployment in HDI-Containern. Dadurch können unterschiedliche Entwicklungsprojekte voneinander isoliert werden (z. B. Entwicklung von Anwendung und Rollen). Die von der HANA-Deployment-Infrastruktur (HDI) angelegten Standardbenutzer und Rollen verfügen zunächst nur über die Berechtigungen, die für die Nutzung der Infrastruktur nötig sind. Jegliche Privilegien in der SAP HANA Datenbank müssen nach dem initialen Setup zugewiesen werden. Anwendungsberechtigungen werden außerhalb der HANA Datenbank entwickelt und vergeben. Prüfung, dass bei Nutzung von XS Advanced und der HANA-Deployment-Infrastruktur ein Berechtigungskonzept implementiert und dokumentiert wurde. Berechtigungen für Entwickler:innen dürfen nicht im produktiven Kontext vergeben werden und die Durchführung sensitiver Funktionen in der HANA Datenbank ermöglichen.
5.13.	**Änderungsberechtigung auf Daten im Schema des SAP-Systems:** *Wird die Vergabe von Änderungsberechtigungen auf die Daten des SAP-Systems durch angemessene Maßnahmen verhindert?* Datenbankbenutzer (abgesehen vom Technischen Benutzer des SAP-Systems) dürfen keine Berechtigung für die Änderung von Daten des SAP-Systems besitzen. Änderungsberechtigungen gefährden die Integrität des Systems und sind verboten. Objektprivilegien: INSERT, UPDATE, DELETE, DEBUG MODIFY (nur von SAP-Mitarbeitenden verwendbar), ALL PRIVILEGES, CREATE ANY. Die Berechtigungen DEBUG und ATTACH DEBUGGER erlauben eine detaillierte (lesende) Analyse des Programmablaufs, jedoch keine Änderungen an Programmfluss und Daten in der Art, wie sie aus dem ABAP-Umfeld bekannt sind. Prüfung, dass Änderungsberechtigungen nicht für das Datenbankschema des SAP-Systems oder einzelne Objekte darin vergeben wurden.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
5.14.	**Leseberechtigungen auf das Schema des SAP-Systems:** *Wird die Vergabe von Leseberechtigungen auf die Daten des SAP-Systems durch angemessene Maßnahmen beschränkt?* Die Vergabe von anwendungsspezifischen Leseberechtigungen auf das Schema des SAP-Systems (Objekt Privileg SELECT) erfordert die Wiederholung aller relevanten Prüfungen aus dem ABAP-Teil und eventuell eine Analyse, inwieweit durch die Vergabe auf Datenbankebene Risiken für das Gesamtsystem entstehen. Zu beachten ist, dass die Vergabe von Berechtigungen sowohl für das komplette Datenbankschema als auch für einzelne Objekte (Tabellen, Views) erfolgen kann. Prüfung auf angemessene Vergabe des Objekt-Privilegs mit lesendem Zugriff auf sensible Daten des SAP-Systems insbesondere aus IP- und Datenschutzgründen.
5.15.	**Änderungsberechtigung auf Objekte des SAP-Systems:** *Wird die Vergabe von Berechtigungen, die Änderungen an Datenbankobjekten des Schemas des SAP-Systems erlauben, durch angemessene Maßnahmen verhindert?* Datenbankbenutzer (abgesehen vom Technischen Benutzer des SAP-Systems) sollen keine Berechtigung für Änderungen von Datenbankobjekten innerhalb des Schemas des SAP-Systems besitzen, da diese die Integrität und Verfügbarkeit des Systems gefährden. Dies bezieht sich auf alle Objektberechtigungen, die sich nicht auf das Lesen oder Ändern von Datensätzen beziehen (z. B.: ALTER, CREATE ANY, DROP). Eine komplette Liste findet sich im SAP Help Portal: HANA Object Privileges (Reference). Prüfung, dass keine Änderungsberechtigung auf Objekte des SAP-Systems vergeben sind.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
5.16.	**IMPORT-Berechtigung IMPORT auf Objekte oder Schema des SAP-Systems:** *Wird die Vergabe von Importberechtigungen auf Objekte des SAP-Systems durch angemessene Maßnahmen verhindert?* Die Kombination des Systemprivilegs IMPORT und der Objektberechtigung CREATE ANY erlaubt es, die Struktur oder den Inhalt von Datenbankobjekten durch Import zu verändern. Prüfung, dass die Vergabe der Kombination der Privilegien durch geeignete Maßnahmen verhindert wird.
5.17.	**EXECUTE-Berechtigungen in der HANA Datenbank:** *Wird die Vergabe der Execute-Berechtigung für die Ausführung von Prozeduren strikt begrenzt?* In Prozeduren kann beliebige Funktionalität versteckt sein. Prozeduren können im Definer-Mode implementiert sein: Dann erfolgt die Ausführung des Codings innerhalb der Prozedur unter einem fremden Benutzer, der sogar inaktiv sein kann. Die Berechtigung für Prozeduren kann deshalb gravierende Auswirkungen auf die Sicherheit des Systems haben. Prüfung, dass der Verwendungszweck von Prozeduren dokumentiert ist und dass die Berechtigungsvergabe unter strikter Anwendung des Minimalprinzips erfolgt.
5.18.	**Berechtigung DATA ADMIN:** *Ist das Systemprivileg DATA ADMIN ausschließlich an den Standardbenutzer SYSTEM und _SYS_REPO vergeben?* Das Systemprivileg DATA ADMIN erlaubt es dem Benutzer, beliebige Data-Definition-Language(DDL)-Befehle in der SAP HANA Datenbank auszuführen, unabhängig von weiteren Objektberechtigungen. Dadurch können sowohl die Datenbankobjekte selbst als auch ihre Inhalte verändert werden. Die Berechtigung ist in keinem Kontext erforderlich und wurde in SAP HANA Cloud bereits im SAP-Standard entfernt. Für die SAP-Standardbenutzer SYSTEM und _SYS_REPO kann die Berechtigung nicht entzogen werden. Prüfung, dass das Systemprivileg DATA ADMIN weder an Benutzer noch an Rollen vergeben ist.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
5.19.	**Berechtigung DEVELOPMENT:** *Ist das Systemprivileg DEVELOPMENT ausschließlich an die Standardbenutzer SYSTEM und _SYS_REPO vergeben?* Das Systemprivileg Development berechtigt den Benutzer zur Ausführung des internen ALTER-SYSTEM-Befehls. Es gibt keine Tätigkeit von Entwickler:innen und keine Aufgabe in dem Betrieb eines SAP-HANA-Systems, für die diese Berechtigung erforderlich wäre. Auch seitens SAP wird das Privileg nicht mehr verwendet. Für die SAP-Standardbenutzer SYSTEM und _SYS_REPO kann die Berechtigung nicht entzogen werden. Prüfung, dass das Systemprivileg DEVELOPMENT weder an Benutzer noch an Rollen vergeben ist.
5.20.	**Schreibzugriff: CREATE R SCRIPT:** *Wird die Vergabe der Berechtigung CREATE R SCRIPT durch angemessene Maßnahmen entweder ausgeschlossen oder aber auf das minimal notwendige Maß eingeschränkt und mit einer geeigneten Systemarchitektur flankiert?* Das Privileg CREATE R SCRIPT bezieht sich auf Funktionen der Application Function Library. Das Privileg erlaubt auch den Zugriff auf das File-System und darf deshalb nur zugewiesen werden, wenn der R Server auf einem separaten Server konfiguriert ist und geeignete Sicherheitsmaßnahmen bestehen, die das produktive SAP-System gegen Zugriffe schützen. Prüfung, dass das Systemprivileg CREATE R SCRIPT weder an Benutzer noch an Rollen vergeben ist.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
5.21.	**Schreibzugriff durch Benutzer mit eigenem Datenbankschema:** *Ist die Anzahl von Benutzern, die ein eigenes Datenbankschema besitzen oder dieses anlegen dürfen, auf das für den Betrieb minimal Notwendige beschränkt?* Benutzer, die als Standardbenutzer in der HANA Datenbank angelegt wurden, besitzen ein eigenes Datenbankschema (namensgleich mit dem Anmeldenamen), in dem sie nach Belieben Datenbankobjekte wie Tabellen, Views, Rollen oder Prozeduren anlegen und ändern können. In produktiven Systemen besteht das Risiko, dass Objekte angelegt und verwendet werden, die sich negativ auf die Integrität oder die Verfügbarkeit von Daten auswirken. Die Berechtigung sollte deshalb nicht an Administrator:innen oder andere Benutzer vergeben werden. Prüfung der vorhandenen Datenbankschemas mit View SYS.SCHEMAS. Prüfung auf angelegte Objekte und deren Verwendung. Prüfung auf Benutzer mit dem Systemprivileg CREATE SCHEMA. Dieses sollte nicht vergeben sein.
5.22.	**Backup and Restore:** *Werden die Privilegien für Backup and Restore angemessen vergeben?* Privilegien für Backup and Restore beziehen sich auf Funktionen der Definition und Einleitung von Sicherungs- und Wiederherstellungsvorgängen einschl. der korrespondierenden Systemkonfiguration. Prüfung der Zuordnung der Backup-Privilegien BACKUP ADMIN zur umfangreichen Konfiguration und Administration und BACKUP OPERATOR zur reinen Initiierung von Backups in Kombination mit den Privilegien DELETE und SELECT für die Tabelle _SYS_XS.JOB_SCHEDULES nur an Anwendende oder Technische Benutzer mit Aufgaben der Backup-Administration in strenger Anwendung des Minimalprinzips.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
5.23.	**Zertifikatsadministration:** *Werden die Privilegien für Zertifikate angemessen vergeben?* Privilegien für Zertifikate beziehen sich auf Funktionen der Verwaltung von Zertifikaten im datenbankinternen Zertifikatsspeicher, die für die zertifikatsbasierte Authentifizierung der Benutzer und die sichere Client-Server-Kommunikation mit dem Secure-Sockets-Layer(SSL)-Protokoll verwendet werden, sowie für die Aktualisierung von vertrauenswürdigen Zertifikaten im Trust Store. Prüfung der angemessenen Zuordnung der Zertifikats-Privilegien CERTIFICATE ADMIN, SSL ADMIN und TRUST ADMIN in allen Instanzen nur an Anwendende mit Aufgaben der Sicherheitsadministration in strenger Anwendung des Minimalprinzips.
6.	Funktionstrennung
	Kontrollziel: für SAP HANA liegt ein Regelwerk mit Funktionstrennungen sowie mit korrespondierenden mitigierenden Kontrollen vor. Das Regelwerk bezieht sich auf einzelne sensitive Funktionen, die in Kombination ein höheres Risiko aufweisen, als sich aus den jeweils einzelnen Risiken ergibt. Rollen und Berechtigungen werden unter Vermeidung von Funktionstrennungen erstellt. Funktionstrennungsverletzungen aus der Vergabe von Rollen und Berechtigungen an Benutzer werden vermieden oder durch Zuordnung mitigierender Kontrollen kompensiert. **Risiko:** Durch das Auftreten von Funktionstrennungsverletzungen in Benutzern ergeben sich Risiken für die Integrität und Verfügbarkeit von Daten.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
6.1.	**Platzhalter Funktionstrennungen:** *Sind alle im Prüfprogramm in Kapitel 4.9 Sensitive Funktionen und Funktionstrennungen enthaltenen, im HANA-Kontext anwendbaren Prüfungshandlungen angemessen behandelt?* Übertragung und Ausführung aller im Prüfprogramm Funktionstrennungen vorgegebenen und anwendbaren Prüfungshandlungen an dieser Stelle in das HANA-Prüfprogramm als Ersatz für diesen Platzhalter-Eintrag.
6.2.	**Funktionstrennung Benutzer- vs. Rollenadministration:** *Wird die Administration von Rollen und Benutzern in Personalunion durch geeignete Verfahren vermieden?* Gemäß allgemeiner Vorgabe für Funktionstrennungen im IT-Bereich sollten die Aufgaben der Benutzer- und Rollenadministration getrennt bearbeitet werden. Dies erfolgt in HANA über die Privilegien USER ADMIN und die Berechtigung EXECUTE für Prozeduren zur Berechtigungsvergabe. Diese enthalten typischerweise „GRANT“ oder „REVOKE“ im Namen. Die Namen der Prozeduren können variieren. Benutzer, die diese Berechtigungen haben, sollen keine Berechtigung für die Erstellung oder Änderung von Rollen haben. Die Funktionstrennung muss systemübergreifend umgesetzt sein, d. h., sie muss sich auch auf Entwicklungssysteme und Transportberechtigungen erstrecken. Das Privileg ROLE ADMIN darf nicht verwendet werden, da es die Berechtigung für das Anlegen neuer Katalogrollen umfasst. Ausnahme: Das ROLE-ADMIN-Privileg darf an den Technischen Benutzer eines Systems zur Berechtigungsvergabe zugewiesen werden, wenn das Rollenmanagement mit HDI-Rollen erfolgt (Kontext: Rollenentwicklung und Deployment mit XSA Advanced) und wenn die Benutzung angemessen überwacht ist. Prüfung, dass die Vergabe der Privilegien für Benutzerpflege, Rollenvergabe und Rollenpflege angemessen auf getrennte Personengruppen verteilt ist.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
6.3.	**Funktionstrennung Benutzergruppen:** *Ist die Pflege sensibler Benutzer speziellen Administrator:innen vorbehalten?* Benutzergruppen ermöglichen es, zusammengehörige Benutzer durch Gruppen-Administrator:innen gemeinsam zu verwalten. Wenn eine Benutzergruppe mit DISABLE USER ADMIN eingerichtet ist, können nur Benutzer-Administrator:innen mit der Berechtigung USERGROUP OPERATOR die Benutzergruppe verwalten. Dies ist zum Schutz hochprivilegierter oder Technischer Benutzer vor versehentlichem Löschen oder Manipulieren sinnvoll. Die Zuordnung von Benutzern zu Benutzergruppen kann im View SYS.USERS überprüft werden; die Benutzergruppen selbst und ihre Attribute sind im View SYS.USERGROUPS definiert. Prüfung, ob hochprivilegierte oder Technische Benutzer eigenständigen Benutzergruppen zugeordnet und mit der Einstellung DISABLE USER ADMIN eingerichtet sind. Prüfung, ob und wem das Privileg USERGROUP OPERATOR zugewiesen ist. Dies unter der Prämisse, dass es eine dezentrale Benutzeradministration gibt und insofern eine Abgrenzung sensibler Benutzer sinnvoll ist.
6.4.	**Funktionstrennung HANA-Audit-Log-Administration:** *Wird durch geeignete Funktionstrennung vermieden, dass ein einzelner Benutzer die Belege des Audit-Log zerstören oder manipulieren kann?* Eine Funktionstrennung kann über die Systemprivilegien AUDIT ADMIN, AUDIT OPERATOR und AUDIT READ erzielt werden. AUDIT ADMIN berechtigt zur Pflege der Audit-Policies und zur Anzeige des Audit-Log; AUDIT OPERATOR erlaubt die Löschung von Audit-Log-Einträgen, die in die HANA Datenbank geschrieben werden, sowie die Anzeige des Audit-Log. AUDIT READ erlaubt ausschließlich das Anzeigen des Audit-Log. Für Konfigurationen, in denen das Audit-Log in das SYSLOG des Betriebssystems geschrieben wird, sind diese Privilegien nicht relevant. Da Administrator:innen typischerweise die Berechtigung INIFILE ADMIN zur Parameterpflege besitzen, kann mit den genannten Berechtigungen nur eine unbefugte Manipulation an Inhalten vermieden werden, nicht jedoch das vollständige Abschalten des Audit-Log.

Nr.	PRÜFPROGRAMM: AUTORISIERUNG
	Prüfung, dass der Zugriff auf die Inhalte der Audit-Log-Dateien angemessen geschützt ist, insbesondere dass die Privilegien AUDIT ADMIN und AUDIT OPERATOR nur an Benutzer vergeben sind, die selbst keine Berechtigung für sicherheitskritische Änderungen im System haben und die zum Lesen personenbezogener Daten befugt sind.
6.5.	**Funktionstrennung Endanwendenden-Berechtigungen vs. Administrations-Berechtigungen:** Ist die Vergabe von Endanwendenden-Berechtigungen und Administrations-Berechtigungen für die HANA Datenbank strikt getrennt? Endanwendende sollten grundsätzlich keinen Zugriff auf die HANA Datenbank eines SAP-Systems haben, weder direkt noch über Business-Anwendungen. Alle Endanwendenden-Zugriffe auf die HANA Datenbank sollten über das SAP-System erfolgen und dort auditiert werden. Darüber hinaus gehende Anforderungen sollten so abgebildet sein, dass die Daten extrahiert werden, z. B. in einen anderen Datenbank-Tenant auf dem gleichen HANA-System. Sollte die Vergabe von Anwendenden-Berechtigungen dennoch unumgänglich sein, so ist eine strikte Trennung von Administrations-Berechtigungen einzuhalten. Prüfen, dass die Vergabe von Berechtigungen an Endanwendende angemessen eingeschränkt oder verhindert ist und dass Endanwendenden-Berechtigungen keinesfalls in Kombination mit Administrationsberechtigungen vergeben werden.
6.6.	**Funktionstrennung – Administrationstätigkeiten:** *Sind die Berechtigungen für die Datenbankadministration angemessen eingeschränkt und gemäß den Zuständigkeiten der Benutzer vergeben?* Die für die Datenbankadministration erforderlichen Rollen und deren Privilegien sollten gemäß der Aufgabenverteilung für diese Tätigkeiten gestaltet sein. Dazu liegt in Ergänzung dieses Prüfleitfadens eine Matrix mit einer Zuordnung der HANA-DB-Privilegien (Zeilen) zu generischen HANA-DB-Funktionen (Zeilen) als Orientierung vor. Prüfung der für die Administration verwendeten Rollen auf Übereinstimmung mit den Aufgabenbeschreibungen/-trennungen der HANA-DB-Administration und auf Übereinstimmung der Rollendeklaration mit den in den Rollen enthaltenen Privilegien.

8.6 Prüfprogramm: Change-Management

Tabelle 33 Prüfprogramm: Change-Management

Nr.	PRÜFPROGRAMM: CHANGE-MANAGEMENT
1.	Versionierung
	Kontrollziel: Die SAP HANA Datenbank sowie weitere für den Betrieb erforderliche technische Komponenten sind auf aktuellen, von SAP mit Sicherheitskorrekturen und -Features versorgten Release- und Support-Package-Ständen. Updates auf aktuelle Versionen erfolgen sowohl proaktiv in regelmäßigen Wartungsintervallen, die unabhängig von spezifischen Bedrohungsanalysen sind, als auch reaktiv zur Schließung spezifischer Schwachstellen und Bedrohungsszenarien. Dazu existieren zwischen IT und Business verbindliche Vereinbarungen, die sich in den tatsächlich vorgefundenen Versionen widerspiegeln. **Risiko:** Sicherheitslücken in der verwendeten Software können die unautorisierte oder unbeabsichtigte Veränderung, Zerstörung oder Verwendung von Daten ermöglichen. Auch Schwachstellen, die für sich genommen wenig kritisch erscheinen, können in Kombination wichtige Puzzlestücke für einen erfolgreichen Angriff sein, indem z. B. nutzbare Informationen zugänglich gemacht werden. Hinweis: Das Beheben von Sicherheitslücken wird von SAP nicht zwingend in Sicherheitshinweisen und Release-Informationen veröffentlicht. Die Mehrzahl implementierter Korrekturen wird ohne konkretisierende Information in neuen Softwareversionen ausgeliefert.
1.1.	Version HANA Datenbank: *Sind die HANA-DB-Version und das Datum der letzten Aktualisierung der HANA Datenbank auf einem angemessenen Stand?* Version und Aktualisierungsstand der HANA DB sollten regelmäßig dem von der SAP verfügbaren Status entsprechen. Beides kann über die folgenden Maßnahmen identifiziert werden: a) Abgleich der vorgefundenen HANA-DB-Version gegen Informationen in Hinweisen auf dem SAP-Service-Marktplatz: Hinweis 2378962 – SAP HANA 2.0 Revision and Maintenance Strategy beschreibt die aktuelle Wartungstrategie. Als Minimum muss eine HANA DB der Version 2.00.05 genutzt werden. Informationen zu aktuellen SAP-Sicherheitshinweisen finden sich im SAP-Service-Marktplatz. Für die HANA Datenbank relevante Hinweise können in der SAP Application Component Hierarchy über die

Nr.	PRÜFPROGRAMM: CHANGE-MANAGEMENT
	Softwarekomponenten der SAP HANA Datenbank (hauptsächlich: HAN*) und über dass Hinweisattribut (Relevant für) gefunden werden. b) Das Implementierungsdatum soll innerhalb der letzten 12 Monate liegen, mindestens aber innerhalb des von der Organisation vereinbarten Aktualisierungszeitraums. Informationen über die komplette Versionshistorie der HANA Datenbank kann im DBACOCKPIT des S/4HANA-Systems über den Pfad DBACOCKPIT > System Information > Databrowser for System Tables > Schema SYS > M_DATABASE_HISTORY > Display Table/View Content und über DBACOCKPIT > Diagnostics > SQL Editor > SELECT * FROM PUBLIC.M_DATABASE_HISTORY ORDER BY INSTALL_TIME DESC angezeigt werden. Prüfung auf angemessene Aktualität der Version und Aktualisierung der HANA Datenbank.
1.3.	Version erweiterte Peripherie: *Sind auch die Versionen der erweiterten Peripherie der HANA DB auf einem aktuellen Stand?* In Abhängigkeit von den vollständigen, relevanten IT-Komponenten der HANA DB sollten noch weitere Komponenten mit in die Versionsprüfung einbezogen werden. Hierzu sollten ein Architekturbild und eine Liste relevanter Softwarekomponenten und Konfigurationspartner verfügbar sein. Naheliegend ist z. B. die Betrachtung von entfernten Installationen (z. B. SAP HANA Cockpit, HANA Studio, HANA Client – eventuell auch XS Advanced) oder auch die Version des SAP-Host-Agenten. Das Prüfverfahren muss individuell mit dem/der Kund:in abgestimmt werden. In einigen Fällen ist eine Prüfung mithilfe des System-View LCM_SOFTWARE_COMPONENTS möglich, z. B. für lokal installierte HANA Clients (HDB_CLIENT), HANA Application Function Library (HANA_AFL) oder dem HANA Local Secure Store (LOCAL_SECURE_STORE). Der Pfad hierfür ist DBACOCKPIT > System-Information > Databrowser for System Tables > Schema SYS > LCM_SOFTWARE_COMPONENTS > Display Table/View Content und DBACOCKPIT > Diagnostics > SQL Editor > SELECT * FROM PUBLIC.LCM_SOFTWARE_COMPONENTS. Prüfung auf angemessene Aktualität auch der Versionierung der erweiterten HANA-DB-Peripherie.

Nr.	PRÜFPROGRAMM: CHANGE-MANAGEMENT
2.	Konfigurationsänderungen
	Kontrollziel: Konfigurationsänderungen in der SAP HANA Datenbank sollen nach einem standardisierten Verfahren implementiert, protokolliert und überwacht werden. **Risiko:** Konfigurationsänderungen in der SAP HANA Datenbank können die Sicherheit des Systems kompromittieren
2.1.	Überwachung sicherheitsrelevanter Konfigurationsänderungen HANA DB: *Werden sicherheitsrelevante Konfigurationen der HANA DB protokolliert und werden die Protokolle regelmäßig überwacht?* Sicherheitsrelevante Konfigurationsänderungen der HANA DB werden über das Security Audit Log aufgezeichnet. Zur Aktivierung und Einrichtung der entsprechenden Audit-Policies siehe unter Logs und Protokolle. Dabei wirkt sich die Protokollierung von Änderungen, die nur vereinzelt und selten erfolgen, im Regelfall nicht auf die Antwortzeiten oder die Last des Systems aus. Prüfung auf Einrichtung des Audit-Logs für Änderungen an sicherheitsrelevanten HANA-DB-Konfigurationen und auf Überwachung der Log-Einträge.
2.2.	**Überwachung sicherheitsrelevanter Konfigurationsänderungen Betriebssystem:** *Werden sicherheitsrelevante Konfigurationen der HANA DB auf Betriebssystemebene protokolliert und werden die Protokolle regelmäßig überwacht?* Da einige Konfigurationen der HANA DB auch auf Betriebssystemebene änderbar sind (und dann vom Audit Log der Datenbank nicht erfasst werden), sind analoge Maßnahmen auf Betriebssystemebene zu implementieren. Prüfung auf angemessene Protokollierung für Änderungen an sicherheitsrelevanten HANA-DB-Konfigurationen auf Betriebssystemebene und auf Überwachung der Log-Einträge (bei Linux und Unix-Derivaten im Systlog oder Remote-Syslog, siehe Betriebssystemkapitel).

Nr.	PRÜFPROGRAMM: CHANGE-MANAGEMENT
3.	Kund:innen-eigene Entwicklung
	Kontrollziel: Es soll keine Kund:innen-eigenen Entwicklungen und 3rd-Party-Applikationen im HANA-Tenant des S/4HANA-Systems geben. **Risiko:** Durch Installation weiterer Applikationen können Daten verändert und die Integrität des Systems geschädigt werden.
2.2.	*Ist das SAP-S/4-HANA-System angemessen gegen den Zugriff Kund:innen-eigener und externer Anwendungen auf die Daten geschützt?* Um Verfügbarkeit, Integrität und Vertraulichkeit der Daten des SAP-S/4-HANA-Systems zu schützen, sollen Kund:innen-eigene Anwendungen und Anwendungen von Drittanbietern nicht innerhalb des produktiven HANA-Tenants betrieben werden. Empfohlen ist, Daten in einen separaten Tenant zu replizieren und dort zu verarbeiten (vgl. SAP-Hinweis 2511210). Die System-Views EFFECTIVE_PRIVILEGE_GRANTEES und GRANTED_PRIVILEGES können verwendet werden, um zu prüfen, welche Benutzer Berechtigung haben, Objekte des SAP-Schemas zu lesen oder zu ändern. Prüfung, ob neben dem Benutzer, dem das Datenbankschema des S/4-HANA-Systems gehört, weitere Benutzer Lese- oder Schreib-berechtigungen haben und ob Zweck und Umfang der Berechtigungen angemessen dokumentiert und genehmigt sind.

8.7 Prüfprogramm: Logs und Protokolle

Tabelle 34 Prüfprogramm: Logs und Protokolle

Nr.	PRÜFPROGRAMM: LOGS UND PROTOKOLLE
1.	**HANA Audit Log**
	Kontrollziel: Das HANA Audit Log ist aktiv und angemessen konfiguriert. Organisatorisch sind effektive Verfahren zu seiner fortlaufenden Überwachung implementiert. **Risiko:** Fehlt eine umfassende und systematische Protokollierung potenziell sicherheitsrelevanter Ereignisse, so sind temporäre Änderungen, die die Integrität der SAP HANA Datenbank berühren, nicht nachvollziehbar, und eine sinnvolle Analyse ist in vielen Fällen nicht möglich.
1.1.	**Aktivierung Datenbankprotokollierung:** *Ist die Protokollierung von Änderungen an Datenbankobjekten über die richtige Einstellung des Globalen Auditing-Log-Parameters aktiviert?* Eine Prüfung der Aktivierung des Protokollierungsparameters sollte für den Tenant der HANA DB in der Datei global.ini und für die System DB in der Datei nameserver.ini vorgenommen werden über eine der beiden folgenden Pfade: a) DBACOCKPIT: SQL > SELECT KEY, VALUE FROM M_INIFILE_CONTENTS WHERE KEY = ‚global_auditing_state‘ AND VALUE = ‚true‘; oder b) DBACOCKPIT: > Right Click on the database and select „Security“ > go to Tab „Auditing“ > Check if „Auditing Status“ is enabled Prüfung auf Aktivierung der Protokollierung für die Tenant und System DB.

Nr.	PRÜFPROGRAMM: LOGS UND PROTOKOLLE
1.2.	**Einrichtung Audit-Policies:** *Sind bei aktivierter Protokollierung angemessene Audit-Policies eingerichtet und angepasst?* Es sind verpflichtend Audit-Policies zur Verwendung als Security-Changelog, System-Changelog, Recovery, Intrusion-Detection und den unerwarteten Zugriff auf die Daten des S/4HANA-Schemas anzusehen. Anpassungen bezüglich zu überwachender Benutzer sind zwingend nötig. Eine Hilfestellung empfohlener Audit-Einstellungen liefert SAP-Hinweis 3016478 – HANA Audit Policies for S/4HANA. Je nach Landschaft kann eine Teilmenge ausreichen. Prüfung auf Einrichtung der verpflichtenden Audit-Policies und Anpassung, sodass die tatsächlich existierenden Benutzer dem Zweck der Policies entsprechend erfasst sind.
1.3.	**Geschützte Log-Datei:** *Wird das Audit Log an einen sicheren Ort geschrieben und angemessen vor Manipulation geschützt?* Eine Speicherung der Log-Datei sollte über die Einrichtung des Audit-Trails entweder auf die Datenbank oder das Systemlog geschrieben werden. Eine Prüfung des Default Audit-Trail erfolgt über den Pfad SELECT file_name > section > key > value FROM SYS.M_INIFILE_CONTENTS WHERE file_name = ‚global.ini‘ AND KEY = ‚default_audit_trail_type‘. Die Konfiguration eines Default Audit-Trail kann auch für jede einzelne Policy überschrieben werden. Dies kann über den Pfad SELECT audit_policy_name > trail_type from SYS.AUDIT_POLICIES geprüft werden. Diese individuelle Anpassung sollte unterbleiben. Prüfung auf Einrichtung des Audit-Trail ausschließlich auf die Datenbank oder das Systemlog.
1.4.	**Überwachung sicherheitsrelevanter Ereignisse:** *Sind angemessene Verfahren zur Überwachung sicherheitsrelevanter Ereignisse definiert und etabliert?* Die aufgezeichneten Audit Logs sollten regelmäßig durch qualifiziertes und von der Administration unabhängiges Personal auf sicherheitsrelevante Ereignisse geprüft und angemessene Maßnahmen bei Auffälligkeiten abgeleitet werden. Prüfung auf etablierte Verfahren zur Überwachung sicherheitsrelevanter Ereignisse des Audit Logs.

Nr.	PRÜFPROGRAMM: LOGS UND PROTOKOLLE
1.5.	**Geschützte Diagnosedateien:** *Werden Diagnosedateien mit potenziell sicherheitsrelevanten Daten vor unbefugtem Zugriff und Missbrauch geschützt?* Diagnosedateien wie Dumps, Logs und Traces können sensitive Daten enthalten, die bei Abbrüchen oder im Rahmen technischer Analysen geschrieben werden. Die Speicherung erfolgt zunächst in einem zentralen Verzeichnis, das wenig geschützt ist. Dateien müssen deshalb auch ohne Anlass in einem angemessenen Zeitraum entfernt werden. Dazu können im DBACOCKPIT die Zeitstempel von Diagnosedateien überprüft werden. Eine Prüfung auf Löschung/Archivierung von alten Diagnosedaten kann über die Identifizierung veralteter Daten über den Pfad DBACOCKPIT > Diagnostics > Diagnosis Files Select Top 100 * from PUBLIC.M_MERGED_TRACES order by TIMESTAMP asc erfolgen. Prüfung auf angemessene Löschung/Archivierung veralteter Diagnosedaten.
1.6.	**Sensible SQL-Traces:** *SQL-Traces sollten grundsätzlich konfiguriert werden, ohne die Inhalte der bearbeiteten Tabellen und Views zu schreiben.* Der SQL-Trace erlaubt es, mit der Einstellung all_with_results auch die tatsächlichen Inhalte der bearbeiteten Tabellen und Views zu schreiben. Diese Information darf nur anlassbezogen genutzt werden. a) Eine Prüfung der Konfiguration zu SQL-Traces auf eine aktuelle Einstellung mit all_with_results kann über den Pfad DBACOCKPIT > Configuration > Trace Files > SQL Trace DBACOCKPIT > Configuration > INI Files > indexserver.ini > sqltrace > level und auf zurückliegende Pflegen über das Audit Log oder der Änderungshistorie über den Pfad DBACOCKPIT > Configuration > INI Files Change History > indexserver.ini [sqltrace] level erfolgen. b) Lagen Traces mit all_with_results vor, sollten diese innerhalb angemessener Zeit aus dem zentralen Verzeichnis entfernt werden. Eine Prüfung tatsächlich geschriebener Inhalte in den Trace-Files kann über Select * from SYS.M_MERGED_TRACES where TRACE_LEVEL= ‚all_with_results‘ geprüft werden. Prüfung auf Vermeidung von SQL-Traces mit Einstellung all_with_results und auf zeitnahe Löschung solcher Traces.
1.7.	**Sensible SQL-Traces (DEBUG):** *Werden SQL-Traces grundsätzlich ohne Einstellung DEBUG für den Zweck der Authentifizierung konfiguriert und*

Nr.	PRÜFPROGRAMM: LOGS UND PROTOKOLLE
	damit ohne sicherheitsrelevante Informationen mit detailliertem Trace-Level? Der SQL-Trace erlaubt es, mit der Einstellung DEBUG auch sicherheitsrelevante Informationen mit detailliertem Trace-Level zu schreiben. Diese Information darf, wenn überhaupt, nur anlassbezogen genutzt werden. Prüfung erfolgt wie bei der Prüfungshandlung Sensible SQL-Traces (all_with_result). Prüfung auf Vermeidung von SQL-Traces mit Einstellung DEBUG.

9 Betriebssysteme – Linux/Unix/Windows

9.1 Einleitung

Das Betriebssystem bildet die operative Plattform für ein SAP-System. Auf dem Betriebssystem werden die Anwendungen von SAP installiert, konfiguriert und betrieben. In diesem Zusammenhang bietet das Betriebssystem diverse Zugriffsmöglichkeiten auf Programme und Daten eines SAP-Systems, die über die verfügbaren Sicherheitsmaßnahmen anforderungsgerecht zu kontrollieren sind. Die Sicherheitskontrollen von SAP-Anwendungen haben nur begrenzt Möglichkeiten, Zugriffe auf das darunterliegende Betriebssystem zu unterbinden. Dabei können Programme und Daten geändert werden – unabhängig von dem Zugriffsschutz, der über die SAP-Anwendungen eingerichtet ist.

Das Betriebssystem ermöglicht den Zugriff auf das SAP-System sowohl auf Netzwerk- als auch auf Dateisystemebene. Angriffe aus dem Netzwerk zielen auf Sicherheitsschwachstellen in der Konfiguration der verfügbaren Dienste und auf technische Verwundbarkeiten des Betriebssystems.

Spezielle Sicherheitsanforderungen ergeben sich aus

- der SAP-spezifischen Nutzung von Betriebssystemfunktionen,
- der proprietären Ausprägung der Sicherheitseinstellungen des jeweiligen Betriebssystems und
- den proprietären technischen Schnittstellen zu anderen Anwendungen, z. B. Datenbanken oder Diensten, die über das Netzwerk aufrufbar sind.

Im Rahmen der Betriebssystemsicherheit sind folgende Hinweise zu berücksichtigen:

- SAP S/4HANA Security Guide (> Implement > Security Guide)
- SAP ABAP Platform Security Guide
  - Linux
  - Windows
- Security Guides der jeweiligen Betriebssystemhersteller (sofern verfügbar)

Aufgrund der Unterschiede der Betriebssysteme bzw. Betriebssystemversionen wurde darauf verzichtet, konkrete Prüfungshandlungen zu beschreiben. Detaillierte Informationen, wie die Konfigurationen geprüft werden können, sind in den Betriebssystemdokumentationen der jeweiligen Hersteller nachzuschauen.

9.2 Risiken

Risiken können sich daraus ergeben, dass die Sicherheitsempfehlungen von SAP oder andere sicherheitsrelevante Einstellungen des Betriebssystems gemäß den Hinweisen des Herstellers des Betriebssystems nicht umgesetzt sind:

- Die Kennwörter der SAP-Systembenutzer, der Standard-Betriebssystembenutzer oder zusätzlich eingerichteter Administrator:innen sind noch auf dem Standard der Auslieferung oder lassen sich leicht erraten und ermöglichen das unautorisierte Anmelden an das Betriebssystem. Diese potenzielle Schwachstelle birgt das Risiko, dass (rechnungslegungsrelevante) Programme und Daten geändert werden können – unabhängig von dem Zugriffsschutz, der über die SAP-Anwendungen eingerichtet ist.
- Der Zugriff auf der Ebene des Betriebssystems durch Benutzer oder über für sie eigens eingerichtete Benutzerfunktionen, z. B. File-Transfer, ist schlecht konfiguriert und unzureichend abgesichert. Folgend könnte eine Fehlkonfiguration / fehlender Zugriffsschutz auf Betriebssystemebene diverse Zugriffs- und somit Änderungsmöglichkeiten auf (rechnungslegungsrelevante) Programme und Daten eines SAP-Systems ermöglichen.
- Aufgrund von unzureichend gesetzten Zugriffsprivilegien können beliebige Anwendende auf ein Verzeichnis mit streng vertraulichen Informationen oder ausführbaren SAP-Programmen zugreifen, das über das Netzwerk nur für eine bestimmte Benutzergruppe bereitgestellt sein soll.
- Bei mangelndem physischen Zugriffsschutz können unbefugte Personen Festplatten oder andere Medien stehlen oder die Hardware des Servers manipulieren bzw. sabotieren.
- Anmeldungen an das Betriebssystem werden nicht protokolliert und überwacht. Dies birgt ein Risiko, dass Änderungen am System nicht nachvollzogen werden können, wodurch unentdeckte Manipulationen möglich sind.
- Das Betriebssystem hat eine bekannte Sicherheitsschwachstelle, die ein Angreifer über das Netzwerk erkennen und ausnutzen kann. Dieses kann zur Offenlegung sensibler Daten oder zur Kompromittierung des Systems führen.
- Eine (nicht autorisierte) Dritt-Anwendung ist eingerichtet, die einen ungeschützten Zugriff auf Dateien und Anwendungen erlaubt.
- Die Manipulation eines SAP-Programms oder systemrelevanter Dateien wird nicht erkannt.

9.3 Kontrollziele

- Die Sicherheitsempfehlungen von SAP zur sicheren Konfiguration des Betriebssystems sind umgesetzt.
- Zusätzliche Sicherheitsempfehlungen des Herstellers des Betriebssystems sind umgesetzt.
- Das Betriebssystem verfügt über alle aktuellen Sicherheitsaktualisierungen.
- Die physische Sicherheit des Systems ist gewährleistet.
- Der Zugriff über das Netzwerk auf das Betriebssystem ist restriktiv gesetzt und sicher konfiguriert.
- Netzwerkfreigaben sind mit restriktiven Zugriffsrechten nur für die zugelassene Benutzergruppe gesetzt. Sie werden auf fehlerhafte Zugriffsvergaben (Windows: Everyone, Linux: Everyone und/oder world-readable oder world-writeable) überwacht.
- Die Funktionen zur Anmeldekontrolle, die das Betriebssystem bereitstellt, werden genutzt. Insbesondere werden Fehlversuche bei der Anmeldung protokolliert und überwacht.
- Nicht autorisierte Anwendungen und Systemdienste wurden entweder deaktiviert oder vom System entfernt.
- Die SAP-Programme und -Dateien unterliegen einem Integritätscheck.

9.4 Prüfprogramm: Systemintegrität von Unix/Linux

9.4.1 Physischer Schutz

Tabelle 35 Prüfprogramm: Physischer Schutz

NR.	Prüfprogramm: Physischer Schutz
1	**Kontrollziel: Angemessener physischer Schutz des Systems** - Nur wenige autorisierte Personen sollten physischen Zugriff zu dem Betriebssystem besitzen. - Das unkontrollierte Neustarten eines Betriebssystems sowie das Booten von anderen Medien (CD, USB-Medium etc.) sollte verhindert werden. **Risiko:** Unbefugte Personen können Festplatten oder andere Medien stehlen oder die Hardware des Servers manipulieren bzw. sabotieren.
1.1 TOP	Welche Zertifizierungen hat das Rechenzentrum, in dem die Systeme physikalisch stehen (bspw. ISO 27001)?

NR.	Prüfprogramm: Physischer Schutz
1.2 TOP	Welche Personen haben physischen Zugang zu dem System? Sind diese Personen für den Zugang zu den Rechnerräumen oder Rechenzentren autorisiert? Hinweis zu 1.2 und 1.3: Bei Auslagerung sollte die Prüfungshandlung, dass nur wenige autorisierte Personen physischen Zugriff zu dem Betriebssystem besitzen, in der Zertifizierung eingeschlossen sein.
1.3 TOP	In welchen Zyklen werden die Zutrittsberechtigungen der Personen mit physischem Zugang auf Aktualität und Rechtmäßigkeit geprüft (z. B. regelmäßig, beim Abteilungswechsel, beim Austritt)? Existiert hierfür ein dokumentierter Prozess?

9.4.2 Aktualität des Betriebssystems

Tabelle 36 Aktualität des Betriebssystems

NR.	Prüfprogramm: Aktualität des Betriebssystems
2	**Kontrollziel: Aktualität des Betriebssystems** - Betriebssystemhersteller veröffentlichen regelmäßig Sicherheitsaktualisierungen für bekannt gewordene Sicherheitsschwachstellen. Diese Sicherheitsaktualisierungen sind zu installieren, um eine Kompromittierung des Systems zu vermeiden. **Risiko:** Nicht autorisierte Benutzer können durch die Ausnutzung von bekannten Sicherheitsschwachstellen Zugriff auf das Betriebssystem erlangen. Hinweis: Bei Auslagerung sollten die Prüfungshandlungen in der Zertifizierung eingeschlossen sein.
2.1 TOP	**Wird die Betriebssystemversion vom UNIX/Linux-Distributor noch mit Sicherheitsaktualisierungen versorgt oder werden keine Aktualisierungen mehr geliefert?** Betriebssystemversionen werden von den Herstellern nur mit Sicherheitsaktualisierungen versorgt, solange sich die entsprechende Version noch in Wartung befindet. Es dürfen nur Betriebssystemversionen verwendet werden, die vom Hersteller noch gewartet werden, um sicherzustellen, dass Aktualisierungen für bekannt gewordene Sicherheitsschwachstellen verfügbar sind.

NR.	Prüfprogramm: Aktualität des Betriebssystems
2.2 TOP	**Wird das Betriebssystem mit den vom UNIX/Linux-Distributor freigegebenen Sicherheits-Patches auf dem neusten Stand gehalten?** **Kann ein Patch nicht angewandt werden: Wie wird dies dokumentiert und nachvollzogen?**

9.4.3 Zugriffsprivilegien und -kontrollen

Tabelle 37 Zugriffsprivilegien und -kontrollen

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
3	**Kontrollziel: Angemessene Zugriffsprivilegien und -kontrollen auf UNIX/Linux-Ebene** - Der Zugriff personenbezogener Benutzer auf das Betriebssystem ist auf wenige Systemadministrator:innen beschränkt. - Benutzer aus Fachabteilungen haben keinen Zugriff auf das Betriebssystem. - Es existieren (bis auf die notwendigen Standardbenutzer „`root`“, `<sid>adm` und `<db><sid>`) keine generischen Benutzer bzw. personenübergreifenden Benutzer auf dem Betriebssystem. - Automatisierte Anmeldekontrollen und Passwortbildungsregeln auf der Ebene des Betriebssystems sind für die personenbezogenen Benutzer aktiviert. - Die Anmeldungen werden protokolliert und überwacht. - Die Zugriffsrechte sind nach dem Prinzip der minimalen Berechtigung vergeben. - Die für UNIX/Linux-Systeme spezifischen und verschiedenen technischen Möglichkeiten, Eigentümerrechte auf Verzeichnisse und Dateien zu vergeben, sind kontrolliert eingesetzt. **Risiko:** - Personenbezogene Benutzer haben leicht erratbare Kennwörter gewählt, die keinem Änderungszwang unterliegen. - Versuche, die Kennwörter von Benutzern auszuprobieren, werden nicht protokolliert und überwacht. - Nicht autorisierte Benutzer können Zugriff auf das Betriebssystem erlangen. - Personenbezogenen Benutzer sind Standardumgebungen, z. B. Login-Shell, eingerichtet, die zu weit reichende automatische Rechtevergaben

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
	beinhalten. Unbefugte Aktionen auf der Betriebssystemebene sind möglich. Die Integrität der System- und Datendateien des SAP-Systems ist gefährdet.
3.1 TOP	**Wird ein sicheres Authentifizierungsverfahren (z. B. schlüsselbasiert) eingesetzt?** **Werden Zugangsdaten durch ein zentrales Anmeldesystem (z. B. LDAP, Active Directory) verwaltet?** In Unix/Linux besteht die Möglichkeit, sichere Anmeldeverfahren wie z. B. LDAP oder Authentifizierung innerhalb von Active Directory, basierend auf Kerberos, zu verwenden. Hierdurch können Administrator:innen zentral und systemübergreifend verwaltet werden. Zudem werden schützenswerte Zugangsdaten zentral abgelegt und systemübergreifend bereitgestellt. Eine lokale Speicherung auf dem Host ist nicht erforderlich.
3.2	**Wird ein Privileged-Access-Management(PAM)-System zur Verwaltung der Zugangsdaten genutzt?** Zusätzlich zu sicheren und zentralisierten Anmeldesystemen können Privileged-Access-Management-Lösungen eingesetzt werden, um die Zugriffsprivilegien granularer steuern zu können.
3.3 TOP	**Existiert für die administrativen Benutzer eine Multi-Faktor-Authentifizierung?** Für administrative Benutzer sollte eine Multi-Faktor-Authentifizierung eingerichtet werden, um unautorisierten Zugriff nach einem Passwort-Diebstahl zu vermeiden. Anstelle der Aktivierung von Multi-Faktor-Authentifizierung auf jedem Host wird häufig ein Konzept gewählt, in dem der Betriebssystemzugang auf die Landschaft nur über zentrale Zugangsserver möglich ist, und nur auf diesem zentralen Zugangsserver wird Multi-Faktor-Authentifizierung aktiviert. Hierbei ist jedoch sicherzustellen, dass die zentralen Zugangsserver nicht umgangen werden können.

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
3.4 TOP	**Welche Benutzer sind auf dem System eingerichtet?** **Werden primär personalisierte Benutzer verwendet?** **Sind die Berechtigungen den Aufgaben entsprechend für personalisierte Benutzer angepasst?** **Wurden die Standardbenutzer, soweit möglich, gesperrt?** **Wird die Verwendung von Standardbenutzern überwacht und/oder dokumentiert?** Die Standardbenutzer „`root`“, `<sid>adm` und `<db><sid>` sollten neben wenigen Spezialsystembenutzern die einzigen Benutzer auf den Anwendungsservern und der Hauptinstanz sein. Nach der Installation kann und sollte der Benutzer `<db><sid>` auf den Anwendungsservern gesperrt werden. Existieren neben den Standardsystembenutzern auch personenbezogene Benutzer? Welche Aufgaben und Betriebssystem-Berechtigungen haben diese? Haben nur nötige Benutzer Root- bzw. Root-ähnliche Berechtigungen? Hinweis: Die Standardbenutzer sind in der Systemdokumentation des Herstellers und von SAP aufgeführt.
3.5 TOP	**Sind für alle Benutzer komplexe Passwörter vergeben?** Entsprechen die gewählten Passwörter der unternehmensspezifischen Password-Policy? **Sind Regeln für die Bildung und Änderung des Passworts aktiviert?** **Sind die folgenden Eigenschaften für die Passwörter definiert?** - Mindestlänge - Mindestanzahl Kleinbuchstaben - Mindestanzahl Großbuchstaben - Mindestanzahl Zahlen - Mindestanzahl Zeichen - Maximale Anmeldeversuche - Maximale Gültigkeitsdauer Die Bildung des Kennworts sollte definierten Komplexitätsregeln unterliegen, d. h., das Kennwort sollte unter anderem eine gewisse Länge und unterschiedliche Zeichen (alphanumerisches Zeichen und Sonderzeichen) aufweisen müssen. Sichere Passwörter können nach unterschiedlichen Kriterien gebildet werden, bspw. sehr lange Passwörter ohne Rotation vs. 8-stellige Passwörter mit regelmäßigem Wechsel (siehe BSI IT-Grundschutz ORP.4.A23).

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
	Hinweis: Zum Beispiel mittels PAM (Pluggable Authentication-Module) oder der Datei `/etc/login.defs` können Richtlinien bezüglich der Passwortkomplexität umgesetzt werden. Die Systemdokumentation des Herstellers informiert jedoch darüber, welche Anmelde- und Kennwortkontrollen das betreffende UNIX/Linux-System unterstützt.
3.6 TOP	**Werden Anmeldungen von Benutzern, insbesondere fehlerhafte Anmeldeversuche, protokolliert und überwacht?** **Wird ein Benutzer nach Erreichen der maximalen Anmeldeversuche (temporär) gesperrt?** Bei Linux werden verhaltensrelevante Ereignisse wie bspw. fehlerhafte Anmeldeversuche oder Erreichen der maximalen Anmeldeversuche durch den Syslog in sogenannten Log-Files gespeichert, die meist unter `/var/log` zu finden sind. Hier sollte vor allem die Datei auth.log regelmäßig ausgewertet werden. Hinweis: Die Systemdokumentation des Herstellers informiert darüber, ob und wie das betreffende UNIX/Linux-System die Protokollierung der Anmeldungen unterstützt.
3.7 TOP	**Bietet das UNIX/Linux-Betriebssystem eine Shadow-Datei, in der die gehashten Passwörter gespeichert sind und auf die nur der Superuser „`root`“ Zugriff hat?** **Ist innerhalb der `/etc/passwd` bei allen Benutzern im Passwort-Feld ein „X“ eingetragen?** Für die Speicherung der gehashten Passwörter sollte immer die separate Shadow-Datei (`/etc/shadow`) verwendet werden, da die Datei `/etc/passwd` für alle Benutzer lesbar sein muss. Ein „X“ innerhalb des Passwort-Felds der Datei `/etc/passwd` zeigt an, dass das gehashte Passwort in der `/etc/shadow` Datei hinterlegt ist.
3.8 TOP	**Welche Benutzer und Gruppen sind in den administrativen Gruppen des SAP-Systems und der UNIX/Linux-Administrator:innen-Gruppe hinzugefügt?** Die administrativen Gruppen des SAP-Systems sind sapsys und bei HANA zusätzlich <sid>shm. Hinweis: Sofern Gruppen in den administrativen Gruppen hinzugefügt sind, sind auch die Mitglieder der entsprechenden Gruppen wieder zu prüfen.
3.9	**Welche Gruppen sind auf dem System eingerichtet?**

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
	Wurden neben den Standardgruppen des Betriebssystems auch unternehmensspezifische Gruppen angelegt? **Welche Benutzer sind den unternehmensspezifischen Gruppen zugeordnet?** **Welche Rechte wurden den jeweiligen Gruppen zugeordnet?** Hinweis: Die Standardgruppen sind in der Systemdokumentation des Herstellers aufgeführt.
3.10	**Sind die Zugriffsprivilegien auf die SAP-Datei- und Systemverzeichnisse so gesetzt, wie es von SAP vorgesehen ist und bei der Installation standardmäßig durchgeführt wird?** Hinweis: Die Zugriffsberechtigungen werden bei der Installation automatisch gesetzt. Ggf. können diese Zugriffsprivilegien an die Sicherheitsrichtlinien und -standards des Unternehmens angepasst worden sein:
3.11	**Welche UMASK-Definitionen sind in den relevanten Dateien, z. B. in `.login`, `.cshrc`, `.profile`, `/etc/profile`, vergeben?**

SAP Verzeichnis oder Dateien	Zugriffsrecht (Oktal)	Besitzer	Gruppe
/<sapmnt>/<SAPSID>/exe	755	<sapsid>adm	sapsys
/<sapmnt>/<SAPSID>/global	700	<sapsid>adm	sapsys
/<sapmnt>/<SAPSID>/profile	755	<sapsid>adm	sapsys
/usr/sap/<SAPSID>	751	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/<Instance ID>	755	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/<Instance ID>/sec	700	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/SYS	755	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/SYS/*	755	<sapsid>adm	sapsys
/usr/sap/trans	775	<sapsid>adm	sapsys
/usr/sap/trans/*	770	<sapsid>adm	sapsys
/usr/sap/trans/.sapconf	775	<sapsid>adm	sapsys
<home Verzeichnis von <sapsid>adm>	700	<sapsid>adm	sapsys
<home Verzeichnis von <sapsid>adm>/*	700	<sapsid>adm	sapsys

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
	UMASK kann dazu verwendet werden, die Berechtigungen für neu erstellte Dateien automatisch zu beschränken. Zum Beispiel gibt ein UMASK-Wert von 0027 an, dass Dateien mit den Rechten 640 (der Besitzer darf die Dateien lesen sowie verändern und die Gruppe darf die Dateien lesen) und Ordner mit den Zugriffsrechten 750 (der Besitzer darf Dateien innerhalb der Ordner erstellen sowie löschen und die Gruppe kann die Verzeichnisinhalte einsehen) erstellt werden. Die festgelegten Vorgaben müssen insbesondere für alle Login-Umgebungen personenbezogener Benutzer gelten.
3.12	**Werden SUID/SGID-Dateien überwacht, insbesondere bei der Installation neuer zusätzlicher Software auf dem Betriebssystem?** Hinweis: Dateien, bei denen das SUID- oder SGID-Bit gesetzt ist, werden mit den Rechten der Benutzer bzw. der Gruppe ausgeführt, dem/der diese Datei gehört. Normalerweise werden diese Bits bei Dateien verwendet, die als Superuser „Root“ ausgeführt werden müssen, um auf Systemressourcen zuzugreifen, die erweiterte Berechtigungen benötigen. **Risiko**: Diese Dateien sind beliebte Ziele von Angreifern, um erweiterte Privilegien, z. B. des Superusers, zu erhalten.

9.4.4 Konfiguration von Netzwerkzugriffen

Tabelle 38 Konfiguration von Netzwerkzugriffen

NR.	Prüfprogramm: Konfiguration Netzwerkzugriffe
4	**Kontrollziel: Sichere Konfiguration von Netzwerkzugriffen** Schwachstellen in der Konfiguration eines Diensts bzw. innerhalb des Diensts selbst können die Sicherheit des Systems erheblich beeinträchtigen. Daher sollten für normale Benutzer nur zwingend notwendige Dienste auf dem System erreichbar sein. **Risiko:** Schwachstellen in Netzwerkdiensten können zur Kompromittierung des Systems führen.
4.1 TOP	**Wird eine Firewall oder eine Paketfilterung eingesetzt, die nur autorisierten Netzwerkverkehr zulässt?** Hinweis: Eine Liste von Ports, die durch SAP-Software genutzt werden, wird von SAP bereitgestellt. Eine zentrale, netzwerkbasierte Paketfilterung erhöht

NR.	Prüfprogramm: Konfiguration Netzwerkzugriffe
	die Sicherheit der gesamten SAP-Landschaft und erleichtert die Verwaltung und Wartung der Regelwerke.
4.2 TOP	**Wird Network Information System (NIS) verwendet? Wenn ja, ist das NIS restriktiv und kontrolliert eingesetzt?** **Risiko**: NIS erlaubt es jedem UNIX-System, in einem lokalen Netzwerk mit dem Befehl „`ypcat passwd`“ die mittels NIS zentral gehaltene Passwortdatei zu lesen und zu verwenden. Alternative: Dieser Service wird nur innerhalb eines abgesicherten lokalen Netzwerks eingesetzt.
4.3 TOP	**Welche Protokolle/Werkzeuge (z. B. SSH) werden zum Remote-Zugriff auf die Systeme regelmäßig verwendet?** **Übertragen diese die Daten verschlüsselt und sind diese sicher konfiguriert?** **Sind weitere Protokolle/Werkzeuge auf den Systemen aktiv, die Remote-Zugriff erlauben? Sind diese sicher konfiguriert?** Remote-Werkzeuge, die Daten unverschlüsselt übertragen, dürfen nicht mehr verwendet werden (z. B. `ftp`, `telnet` oder BSD-Dienste `rlogin` und `remsh/rsh`). Daher wird der Einsatz verschlüsselter Alternativen wie `ssh`, `scp` oder `sftp` empfohlen. Neben den regelmäßig verwendeten Werkzeugen zum Remote-Zugriff können zusätzliche Dienste auf den Systemen installiert und gestartet sein, die nicht bekannt sind und die oft eine unsichere Standardkonfiguration haben (z. B. nicht geänderte Standardkennwörter). Hinweis: Die sicherere Konfiguration des jeweiligen Diensts kann entsprechenden Sicherheitshandbüchern entnommen werden.
4.4 TOP	**Ist ein grafischer Desktop (z. B. X-Windows) aktiviert? Wird dieser zur Administration verwendet?** **Ist er gemäß den Sicherheitsempfehlungen des UNIX/Linux-Herstellers konfiguriert? Erfolgt der Zugriff auf den Linux-Desktop über ein verschlüsseltes Protokoll?**

NR.	Prüfprogramm: Konfiguration Netzwerkzugriffe
	Remote-Werkzeuge, die Daten unverschlüsselt übertragen, dürfen nicht mehr verwendet werden. Wenn ein grafischer Linux-Desktop notwendig ist, muss sichergestellt werden, dass die Daten verschlüsselt übertragen werden. Dies kann bspw. über ein X11-Forwarding mit dem SSH-Protokoll erreicht werden.
4.5 TOP	**Welche Version des Network File System (NFS) wird eingesetzt?** **Ist das Network File System (NFS) restriktiv und kontrolliert eingesetzt?** NFSv3-Exporte (oder älter) mit vertraulichen Daten (z. B. /sapmnt) dürfen nur für vertrauenswürdige definierte Hosts/Servernetzwerke bereitgestellt werden. Eine Einschränkung auf Benutzer ist nicht ausreichend. Über NFSv3 (oder älter) dürfen keine Home-Verzeichnisse – von welchen Benutzern auch immer – mit Schreibberechtigung exportiert werden. **Risiko**: Die über NFS exportierten Verzeichnisse können vertrauliche Daten enthalten, die für alle Benutzer im Netz lesbar sind. Wird ein für alle beschreibbares Home-Verzeichnis eines UNIX/Linux-Benutzers exportiert, ist darüber ein Angriff auf das UNIX/Linux-System möglich, der dem Angreifer die Übernahme der Privilegien des Superusers „`root`“ ermöglicht.

9.4.5 Konfiguration von Diensten

Tabelle 39 Konfiguration von Diensten

NR.	Prüfprogramm: Sichere Konfiguration von Diensten
5	**Kontrollziel: Sichere Konfiguration von Diensten** Schwachstellen in der Konfiguration eines Diensts bzw. innerhalb des Diensts selbst können die Sicherheit des Systems erheblich beeinträchtigen. Auf einem System sollten nur Anwendungen installiert sein, die das System zur Durchführung seiner Aufgabe benötigt. Daher sollte das System auf die Bereitstellung eines Diensts oder einer Gruppe gleichartiger Dienste beschränkt sein. Unterschiedliche Dienste sollten auf separaten Systemen eingerichtet sein. Die Sicherheitsbewertung und die Gruppierung der Dienste wurden mit dem Sicherheitsbeauftragten abgestimmt. **Risiko:** Schwachstellen in Programmen bzw. Diensten können zur Offenlegung sensibler Daten bzw. zur Kompromittierung des Systems führen.
5.1 TOP	**Sind die Sicherheitshinweise des UNIX/Linux-Distributors zum Härten des Systems, z. B. Hinweise zum Deaktivieren nicht benötigter Dienste, bekannt und, soweit sinnvoll, umgesetzt?** Die meisten UNIX/Linux-Distributoren stellen eine Dokumentation mit weitergehenden Sicherheitskonfigurationen zur Verfügung, die in Abhängigkeit vom Sicherheitslevel und der Kund:innen-Umgebung implementiert werden können. Diese Dokumentation sollte für die eingesetzte UNIX/Linux-Version bekannt sein und von dem/der Kund:in, soweit sinnvoll, umgesetzt worden sein.
5.2	**Werden zusätzlich Benchmarks oder technische Richtlinien (z. B. CIS, NIST, BSI) angewandt?** **In welchen Zyklen werden die angewandten Benchmarks oder technischen Richtlinien auf ihre Aktualität hin überprüft und die Systemkonfigurationen entsprechend angepasst?** Neben der Herstellerdokumentation gibt es noch Härtungsempfehlungen, Benchmarks oder technische Richtlinien von weiteren Organisationen. Diese gehen üblicherweise über die Herstellerempfehlungen hinaus. Hier sollte geprüft werden, ob diese zusätzlichen Empfehlungen bekannt sind, auf Anwendbarkeit geprüft wurden und, soweit sinnvoll, umgesetzt wurden.

9.4.6 Protokollierung und Sicherheitsüberwachung

Tabelle 40 Protokollierung und Sicherheitsüberwachung

NR.	Prüfprogramm: Protokollierung und Sicherheitsüberwachung
6	**Kontrollziel: Protokollierung und Sicherheitsüberwachung** Welche Maßnahmen sind eingerichtet, um die Integrität sowie den Schutz der Vertraulichkeit des Systems sicherzustellen und zu überwachen? **Risiko:** Bei unzureichenden Maßnahmen ist es nicht möglich, Angriffe auf das System festzustellen und zeitnah darauf zu reagieren.
6.1 TOP	**Wird das System (z. B. durch einen Syslog-Dienst) durchgängig überwacht?** **Ist der Zugriff auf die Log-Dateien restriktiv vergeben und werden die Log-Dateien revisionssicher auf einem zentralen Log-Host gespeichert?** Damit die durchgängige Systemfunktionalität sichergestellt werden kann, muss das System überwacht und bestimmte Ereignisse protokolliert werden. Da die Protokolldateien wichtige Systeminformationen und persönliche Daten enthalten können, muss der Zugriff auf diese Protokolldateien eingeschränkt werden. Nur berechtigte Benutzer sollten daher Zugriff auf die Dateien erhalten. Protokolldateien sind an einen zentralen Log-Host weiterzuleiten.
6.2 TOP	**Werden regelmäßige Auswertungen auf verdächtige Aktivitäten durchgeführt?** **Ist das System an ein zentrales Logging- und Monitoring-System, SIEM, Security Operations Center (SOC) angebunden?** Eine Zentralisierung der Protokolldateien auf einen dedizierten Log-Server sollte implementiert werden, um lokale Manipulationen an den Protokolldateien zu erschweren und eine zentrale Analyse zu ermöglichen. In der Praxis können sogenannte SIEM-Systeme (Security-Incident- und Event-Management-Systeme) klassische Log-Hosts ersetzen. Intelligente Abfragen unterstützen dabei die Analyse verdächtiger Vorgänge.

9.4.7 Datensicherung, Wiederherstellung und Löschung

NR.	Prüfprogramm: Datensicherung, Wiederherstellung und Löschung
7	**Kontrollziel: Datensicherung, Wiederherstellung und Löschung** - Welche Maßnahmen sind eingerichtet, um einen Datenverlust des Systems zu vermeiden? - Werden Daten sicher gelöscht? **Risiko:** - Bei unzureichenden Maßnahmen kann es zum Datenverlust kommen. Sofern Daten nicht sicher gelöscht werden, kann dies dazu führen, dass diese ungewollt durch Dritte wieder lesbar gemacht werden können.
7.1 TOP	**Wird ein Backup des Systems auf einem dedizierten Medium (separatem Backup-Server) durchgeführt?** **In welchen Zyklen werden die Backups erstellt?** Ein Backup kann einerseits dabei helfen, gelöschte oder beschädigte Daten wiederherzustellen. Andererseits kann es auch dem Abgleich mit vorhandenen Daten dienen, um so kompromittierte Daten ausfindig zu machen. Es muss jedoch darauf geachtet werden, dass das Backup-Medium in einer sicheren Umgebung aufbewahrt wird, sodass es gegen Manipulation geschützt ist.
7.2 TOP	**Werden die Backups regelmäßig auf ihre Funktionalität hin überprüft? Gibt es regelmäßige Wiederherstellungen oder Wiederherstellungstests?** Sofern Wiederherstellungen von Backups nicht regelmäßig durchgeführt oder getestet werden, kann dies dazu führen, dass im Ernstfall eine Wiederherstellung des Systems nicht möglich ist. Daher ist sicherzustellen, dass Wiederherstellungen regelmäßig durchgeführt werden oder es regelmäßige Wiederherstellungstests gibt.
7.3 TOP	**Gibt es eine Richtlinie, wie Daten auf stillgelegten Systemen oder von nicht mehr verwendeten Datenmedien gelöscht werden?** **Wie wird (technisch) sichergestellt, dass die Richtlinie umgesetzt wird?** Werden Systeme stillgelegt bzw. Datenmedien nicht mehr verwendet, müssen die darauf enthaltenen sensiblen Daten so gelöscht werden, dass sie nicht wiederhergestellt werden können. Um dieses zu erreichen, können sogenannte Wipe-Tools eingesetzt werden.

9.5 Prüfprogramm: Systemintegrität von Windows

9.5.1 Physischer Schutz

Tabelle 41 Physischer Schutz

NR.	Prüfprogramm: Physischer Schutz
1	**Kontrollziel: Angemessener physischer Schutz des Systems** - Nur wenige autorisierte Personen sollten physischen Zugriff zu dem Betriebssystem besitzen. - Das unkontrollierte Neustarten eines Betriebssystems sowie das Booten von anderen Medien (CD, USB-Medium etc.) sollte verhindert werden **Risiko:** Unbefugte Personen können Festplatten oder andere Medien stehlen oder die Hardware des Servers manipulieren bzw. sabotieren.
1.1 TOP	Welche Zertifizierungen hat das Rechenzentrum, in dem die Systeme physikalisch stehen (bspw. ISO 27001)?
1.2 TOP	Welche Personen haben physischen Zugang zu dem System? Sind diese Personen für den Zugang zu den Rechnerräumen oder Rechenzentren autorisiert? Hinweis zu 1.2 und 1.3: Bei Auslagerung sollte die Prüfungshandlung, dass nur wenige autorisierte Personen physischen Zugriff zu dem Betriebssystem besitzen, in der Zertifizierung eingeschlossen sein.
1.3 TOP	In welchen Zyklen werden die Zutrittsberechtigungen der Personen mit physischem Zugang auf Aktualität und Rechtmäßigkeit geprüft (z. B. regelmäßig, beim Abteilungswechsel, beim Austritt)? Existiert hierfür ein dokumentierter Prozess?

9.5.2 Aktualität des Betriebssystems

NR.	Prüfprogramm: Aktualität des Betriebssystems
2	**Kontrollziel: Aktualität des Betriebssystems** Betriebssystemhersteller veröffentlichen regelmäßig Sicherheitsaktualisierungen für bekannt gewordene Sicherheitsschwachstellen. Diese Sicherheitsaktualisierungen sind zu installieren, um eine Kompromittierung des Systems zu vermeiden. **Risiko:** Nicht autorisierte Benutzer können durch die Ausnutzung von bekannten Sicherheitsschwachstellen Zugriff auf das Betriebssystem erlangen. Hinweis: Bei Auslagerung sollten die Prüfungshandlungen in der Zertifizierung eingeschlossen sein.
2.1 TOP	**Wird die Betriebssystemversion von Microsoft noch mit Sicherheitsaktualisierungen versorgt oder werden keine Aktualisierungen mehr geliefert?** Betriebssystemversionen werden von Microsoft nur mit Sicherheitsaktualisierungen versorgt, solange sich die entsprechende Version noch in Wartung befindet. Es dürfen nur Betriebssystemversionen verwendet werden, die von Microsoft noch gewartet werden, um sicherzustellen, dass Aktualisierungen für bekannt gewordene Sicherheitsschwachstellen verfügbar sind.
2.2 TOP	**Wird das Betriebssystem mit den von Microsoft freigegebenen Sicherheits-Patches auf dem neusten Stand gehalten?** **Kann ein Patch nicht angewandt werden: Wie wird dies dokumentiert und nachvollzogen?**

9.5.3 Zugriffsprivilegien und -kontrollen

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
3	**Kontrollziel: Angemessene Zugriffsprivilegien und -kontrollen auf Windows-Ebene** - Der Zugriff personenbezogener Benutzer auf das Betriebssystem ist auf wenige Systemadministrator:innen beschränkt. - Benutzer aus Fachabteilungen haben keinen Zugriff auf das Betriebssystem. - Es existieren (bis auf die notwendigen Standardbenutzer „Administrator“, „System“, <SID>ADM, SAPService<SID> und des Datenbankbenutzers) keine generischen Benutzer bzw. personenübergreifenden Benutzer auf dem Betriebssystem. - Automatisierte Anmeldekontrollen und Passwortbildungsregeln auf der Ebene des Betriebssystems sind für die personenbezogenen Benutzer aktiviert. - Die Anmeldungen werden protokolliert und überwacht. - Die Zugriffsrechte sind nach dem Prinzip der minimalen Berechtigung vergeben. - Die für Windows-Systeme spezifischen und verschiedenen technischen Möglichkeiten, Eigentümerrechte auf Verzeichnisse und Dateien zu vergeben, sind kontrolliert eingesetzt. **Risiko:** - Personenbezogene Benutzer haben leicht erratbare Kennwörter gewählt, die keinem Änderungszwang unterliegen. - Versuche, die Kennwörter von Benutzern auszuprobieren, werden nicht protokolliert und überwacht. - Nicht autorisierte Benutzer können Zugriff auf das Betriebssystem erlangen. - Personenbezogenen Benutzer sind zu weit reichende Rechte vergeben. Unbefugte Aktionen auf Betriebssystemebene sind möglich. Die Integrität der System- und Datendateien des SAP-Systems ist gefährdet.

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
3.1	**Werden Zugangsdaten durch ein zentrales Anmeldesystem (z. B. Active Directory, LDAP) verwaltet?** In Microsoft-Umgebungen besteht die Möglichkeit, sichere und zentrale Anmeldeverfahren basierend auf Active-Directory-Services umzusetzen. Hierdurch können Administrator:innen zentral und systemübergreifend verwaltet werden. Zudem werden schützenswerte Zugangsdaten zentral abgelegt und systemübergreifend bereitgestellt. Eine lokale Speicherung auf dem Host ist nicht erforderlich.
3.2	**Wird ein Privileged-Access-Management(PAM)-System zur Verwaltung der Zugangsdaten genutzt?** Zusätzlich zu sicheren und zentralisierten Anmeldesystemen können Privileged-Access-Management-Lösungen eingesetzt werden, um die Zugriffsprivilegien granularer steuern zu können.

3.3	**Werden – insbesondere bei großen Systemlandschaften – die SAP-Systeme durch eine separate Domäne von den Unternehmensdaten getrennt?**
	SAP empfiehlt eine getrennte Windows Domäne für die SAP-Systeme einzurichten.
	- In der Unternehmens-Domäne sind die Domänenbenutzer (einschließlich der SAP-Systembenutzer) und der/die Unternehmens-Domänenadministrator:in eingerichtet.
	- In der davon getrennten SAP-Domäne sind die SAP-System-Server, Dienste und Administrator:innen eingerichtet. Dazu zählen:
	  ○ SAP-System-Anwendungsserver und -Datenbankserver
	  ○ SAP-System- oder Datenbank-Dienste
	  ○ SAP-Systemadministrator:innen
	  ○ Windows-Administrator:innen
	  ○ Administrator:innen der SAP-Domäne

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
3.4	**Welche Vertrauensbeziehungen sind zwischen anderen Windows-Domänen und der Windows-Domäne für die SAP-Systeme definiert?** Hinweis: In den Standard-Installationsvorgehensweisen empfiehlt SAP, getrennte Domänen einzurichten. Zu beachten ist jedoch, dass bestimmte SAP-spezifische Funktionen und Windows-spezifische Services eine Vertrauensbeziehung zwischen Domänen erfordern. - Es gibt bestimmte Services, die nur eine einseitige Vertrauensbeziehung erfordern, z. B. das Drucken im Netzwerk mit dem Print Manager oder die Dateienübertragung mit Betriebssystembefehlen wie z. B. xcopy oder move. - Einige Services erfordern eine beiderseitige Vertrauensbeziehung, z. B. Single-Sign-On über das Microsoft LAN Manager Security Service Provider Interface (NTLMSSPI). Hinweis: Wenn das SAP-System standardmäßig installiert wird, implementiert das Installationswerkzeug, SWPM genannt, automatisch alle notwendigen Maßnahmen, die relevant sind, um das SAP-System gegen nicht autorisierten Zugriff zu schützen.
3.5 TOP	**Existiert für die administrativen Benutzer eine Multi-Faktor-Authentifizierung?** Für administrative Benutzer sollte eine Multi-Faktor-Authentifizierung eingerichtet werden, um unautorisierten Zugriff nach einem Passwort-Diebstahl zu vermeiden. Anstelle der Aktivierung von Multi-Faktor-Authentifizierung auf jedem Host wird häufig ein Konzept gewählt, in dem der Betriebssystemzugang auf die Landschaft nur über zentrale Zugangsserver möglich ist und nur auf diesen zentralen Zugangsservern wird Multi-Faktor-Authentifizierung aktiviert. Hierbei ist jedoch sicherzustellen, dass die zentralen Zugangsserver nicht umgangen werden können.
3.6 TOP	**Welche Benutzer sind auf dem System eingerichtet?** **Werden primär personalisierte Benutzer verwendet?** **Sind die Berechtigungen den Aufgaben entsprechend für personalisierte Benutzer angepasst?** Sind neben den Standardsystembenutzern auch personenbezogene Benutzer vergeben? Welche Aufgaben haben diese eingerichteten personenbezogenen Benutzer? Haben nur nötige Benutzer Root- bzw. Root-ähnliche Berechtigungen? Hinweis: Die Standardbenutzer sind in der Systemdokumentation des Herstellers und von SAP aufgeführt.

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
3.7 TOP	**Ist der Standardbenutzer „Administrator“ gesichert?** Der/Die in Windows eingebaute Administrator:in hat unbeschränkten Zugriff auf alle Windows-Ressourcen. Er/Sie kann z. B. - Dateien, Festplatten und Shares anlegen, verwalten und deren Besitzer werden. - lokale Benutzer anlegen und ihre Rechte verwalten - Peripheriegeräte, Kernel- und Benutzer-Services anlegen und verwalten SAP empfiehlt, diesen Benutzer zu deaktivieren, um ihn vor unberechtigtem Zugriff zu schützen. Der Anmeldename sollte geändert werden und das Kennwort in einem Kennwort-Safe geheim gehalten werden, der nur für wenige natürliche Personen zugänglich ist. Für Verwaltungsaufgaben sollten andere Benutzer angelegt und deren Rechte auf die Aufgaben, für die sie verwendet werden, z. B. Benutzer-Administrator:in, Sicherungs- und Server-Operator:innen, beschränkt sein.
3.8 TOP	**Ist der Benutzer <SID>ADM gesichert?** <SID>ADM ist der Windows-Benutzer für die SAP-Systemverwaltung. Der Benutzer wird während des SAP-Systeminstallationsverfahrens, normalerweise als Domänenbenutzer für das SAP-System, angelegt. Der Benutzer kann sich daher an allen Windows-Rechnern in der Domäne anmelden. <SID>ADM benötigt vollen Zugriff auf alle Instanz-spezifischen Ressourcen des SAP-Systems wie Dateien, Shares, Peripheriegeräte (z. B. Bandlaufwerke oder Drucker) und Netzwerkressourcen (z. B. den SAProuter-Service). Des Weiteren ist <SID>ADM Mitglied der lokalen Administrations-Gruppe und besitzt weitreichende Privilegien, um das SAP-System zu administrieren oder zu erweitern. SAP empfiehlt, die folgenden Maßnahmen zu ergreifen, um diesen Benutzer vor unberechtigtem Zugriff zu schützen: - ihr/sein Kennwort regelmäßig zu ändern. - den Benutzer zu sperren (nicht löschen). Hinweis: Obwohl <SID>ADM auf SAP-System-Dateien zugreifen kann, wird das SAP-System von einem anderen Benutzer (SAPService<SID>) gestartet.
3.9	**Ist der Benutzer SAPService<SID> gesichert?** Hinweis: SAPService<SID> wird bei der Installation des SAP-Systems angelegt. Der Benutzer wird normalerweise als ein Domänenbenutzer

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
	angelegt, die/der das SAP-System ausführt und Datenbankressourcen verwaltet. Der Benutzer kann sich lokal auf allen Windows-Rechnern in der Domäne anmelden. Da das SAP-System selbst dann laufen muss, wenn kein Benutzer an dem lokalen Windows-Rechner angemeldet ist, läuft das SAP-System als Windows-Dienst. Aus diesem Grund erhält der Benutzer SAPService<SID> während der Installation das Recht „Logon as a service“ auf dem lokalen Rechner. Hinweis: Das Kennwort dieser Windows-Service-Benutzer zu ändern, bedingt einen Neustart des SAP-Systems. SAP empfiehlt, folgende Vorkehrungen treffen, um SAPService<SID> zu schützen: - das Benutzerrecht „Log on locally“ und „Log on through Terminal Services“ zu verbieten. Dies wird automatisch durch das SAP-Installationswerkzeug SWPM vorgenommen.
3.10 TOP	**Ist der Benutzer SAPService<SID> Teil der lokalen Administrator:innen-Gruppe?** Der SAPService<SID> darf kein Mitglied der lokalen Administrator:innen-Gruppe sein, da damit das SAP-System selbst Teil der Administrator:innen-Gruppe werden würde.
3.11	**Ist der Benutzer „Gast“ gesperrt?**
3.12 TOP	**Sind für alle Benutzer komplexe Passwörter vergeben?** Entsprechen die gewählten Passwörter der unternehmensspezifischen Password-Policy? **Sind Regeln für die Bildung und Änderung des Passworts aktiviert?** **Sind die folgenden Eigenschaften für die Passwörter definiert?**

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen
	- Mindestlänge - Mindestanzahl Kleinbuchstaben - Mindestanzahl Großbuchstaben - Mindestanzahl Zahlen - Mindestanzahl Zeichen - Maximale Anmeldeversuche - Maximale Gültigkeitsdauer Die Bildung des Kennworts sollte definierten Komplexitätsregeln unterliegen, d. h., das Kennwort sollte unter anderem eine gewisse Länge und unterschiedliche Zeichen (alphanumerisches Zeichen und Sonderzeichen) aufweisen müssen. Sichere Passwörter können nach unterschiedlichen Kriterien gebildet werden, bspw. sehr lange Passwörter ohne Rotation vs. 8-stellige Passwörter mit regelmäßigem Wechsel (siehe BSI IT-Grundschutz ORP.4.A23). Hinweis: Die Komplexitätsvoraussetzungen für ein Kennwort können unter Windows über eine sogenannte Kontorichtlinie festgelegt werden. Die Systemdokumentation des Herstellers informiert jedoch darüber, welche Anmelde- und Kennwortkontrollen das betreffende Windows-System unterstützt.
3.13 TOP	**Werden Anmeldungen von Benutzern, insbesondere fehlerhafte Anmeldeversuche, protokolliert und überwacht?** **Wird ein Benutzer nach Erreichen der maximalen Anmeldeversuche (temporär) gesperrt?** Als Minimum ist sicherzustellen, dass fehlerhafte Ereignisse für alle Überwachungsrichtlinien aktiviert werden (secpol.msc > „Sicherheit Einstellungen\Lokale Richtlinien\Überwachungsrichtlinie“).
3.14 TOP	**Wer darf das SAP-System starten oder stoppen?** Neben den SAP spezifischen Windows-Gruppen, dürfen auch alle Mitglieder der lokalen Administrator:innen-Gruppe SAP-Systeme starten und stoppen. Diese Gruppe kann ggf. Benutzer oder Gruppen beinhalten, die nicht berechtigt sein sollen, das SAP-System zu starten oder zu stoppen.
3.15 TOP	**Welche Benutzer und Gruppen sind in den administrativen Gruppen des SAP-Systems und der Windows-Administrator:innen-Gruppe hinzugefügt?** Die administrativen Gruppen des SAP-Systems beginnen mit dem Prefix SAP_, aber unterscheiden sich dadurch, ob eine SAP-Installation auf einem

<table>
<tr><th>NR.</th><th>Prüfprogramm: Zugriffsprivilegien und -kontrollen</th></tr>
<tr><td></td><td>Windows-Server erfolgt, der Mitglied einer Windows-Domäne ist oder nicht (z. B. SAP_<SID>_GlobalAdmin, SAP_<SID>_LocalAdmin).
Hinweis: Sofern Gruppen in den administrativen Gruppen hinzugefügt sind, sind auch die Mitglieder der entsprechenden Gruppen wieder zu prüfen.</td></tr>
<tr><td>3.16</td><td>Welche Gruppen sind auf dem System eingerichtet?
Wurden neben den Standardgruppen des Betriebssystems auch unternehmensspezifische Gruppen angelegt?
Welche Benutzer sind den unternehmensspezifischen Gruppen zugeordnet?
Welche Rechte wurden den jeweiligen Gruppen zugeordnet?
Hinweis: Die Standardgruppen sind in der Systemdokumentation des Herstellers aufgeführt.</td></tr>
<tr><td>3.17</td><td>Sind die Zugriffsprivilegien auf die SAP-Datei- und Systemverzeichnisse so gesetzt, wie es von SAP vorgesehen ist und bei der Installation standardmäßig durchgeführt wird?
Hinweis: Die Zugriffsberechtigungen werden bei der Installation automatisch gesetzt. Gegebenenfalls können diese Zugriffsprivilegien an die Sicherheitsrichtlinien und -standards des Unternehmens angepasst worden sein.
Dies kann mit dem Skript aus SAP-Note 3125128 überprüft werden.
Empfehlung bei lokaler Installation:
<table>
<tr><th>SAP-Verzeichnis oder Dateien</th><th>Lokale Benutzergruppen</th><th>Berechtigungen</th></tr>
<tr><td>\<usr>\<sap></td><td>SAP_<SID>_LocalAdmin</td><td>Vollzugriff</td></tr>
<tr><td>\<usr>\<sap>\<trans></td><td>SAP_<SID>_LocalAdmin</td><td>Vollzugriff</td></tr>
<tr><td>\<usr>\<sap>\<SID>\<sys>\<global>\<security></td><td>SAP_<SID>_LocalAdmin</td><td>Vollzugriff
The folder security should only be accessible by SAP users and not by the administrators group. Remove the group if it exists, but don't add a Deny rule for the administrators group to the security folder.</td></tr>
</table>
Empfehlung bei der Installation über die Domäne:</td></tr>
</table>

NR.	Prüfprogramm: Zugriffsprivilegien und -kontrollen

SAP-Verzeichnis oder Dateien	Lokale Benutzergruppen	Berechtigungen
\<usr>\<sap>	*SAP_<SID>_GlobalAdmin*	Vollzugriff
\<usr>\<sap>\<trans>	*SAP_<SID>_GlobalAdmin*	Vollzugriff
\<usr>\<sap>\<SID>\<sys>\<global>\<security>	*SAP_<SID>_GlobalAdmin*	Vollzugriff The folder security should only be accessible by SAP users and not by the administrators group. Remove the group if it exists, but don't add a Deny rule for the administrators group to the security folder.

9.5.4 Konfiguration von Netzwerkzugriffen

Tabelle 42 Konfiguration von Netzwerkzugriffen

NR.	Prüfprogramm: Konfiguration Netzwerkzugriffe
4	**Kontrollziel: Sichere Konfiguration von Netzwerkzugriffen** Schwachstellen in der Konfiguration eines Diensts bzw. innerhalb des Diensts selbst können die Sicherheit des Systems erheblich beeinträchtigen. Auf einem System sollten nur Pakete installiert sein, die das System zur Durchführung seiner Aufgabe benötigt. Ein Programm oder ein Dienst, welcher nicht installiert ist, kann durch einen Angreifer nicht verwendet werden. Daher sollte das System auf die Bereitstellung eines Diensts beschränkt sein. Unterschiedliche Dienste sollten auf separaten Systemen eingerichtet sein. **Risiko:** Schwachstellen in Programmen bzw. Diensten können zur Offenlegung von sensiblen Daten bzw. zur Kompromittierung des Systems führen.
4.1 TOP	**Wird eine Firewall oder eine Paketfilterung eingesetzt, die nur autorisierten Netzwerkverkehr zulässt?**

NR.	Prüfprogramm: Konfiguration Netzwerkzugriffe
	Hinweis: Eine Liste von Ports, die durch SAP-Software genutzt werden, wird von SAP bereitgestellt (https://help.sap.com/viewer/ports). Eine zentrale, netzwerkbasierte Paketfilterung erhöht die Sicherheit der gesamten SAP-Landschaft und erleichtert die Verwaltung und Wartung der Regelwerke. Hinweis: SAP empfiehlt, eine Firewall oder Paketfilterung für das Netzwerk der SAP-Systeme einzurichten und keine Firewalls zwischen den Servern der SAP-Systeme und der Datenbank zu konfigurieren. Siehe auch SAP Help Link.
4.2 TOP	**Welche Protokolle/Werkzeuge (z. B. RDP, SSH) werden zum Remote-Zugriff auf die Systeme regelmäßig verwendet?** **Übertragen diese die Daten verschlüsselt und sind diese sicher konfiguriert?** **Sind weitere Protokolle/Werkzeuge auf den Systemen aktiv, die Remote-Zugriff erlauben? Sind diese sicher konfiguriert?** Remote-Werkzeuge, die Daten unverschlüsselt übertragen, dürfen nicht mehr verwendet werden. Daher wird der Einsatz von verschlüsselten Alternativen wie `rdp` oder `ssh` empfohlen. Neben den regelmäßig verwendeten Werkzeugen zum Remote-Zugriff, können zusätzliche Dienste auf den Systemen installiert und gestartet sein, die nicht bekannt sind und oft eine unsichere Standardkonfiguration haben (z. B. nicht geänderte Standardkennwörter). Hinweis: Die sicherere Konfiguration des jeweiligen Diensts kann entsprechenden Sicherheitshandbüchern entnommen werden.
4.3 TOP	**Sind Windows-Freigaben restriktiv und kontrolliert eingesetzt?** Windows-Freigaben sollten keine Full-Control-Rechte für jedermann aufweisen. Besonders die Rechte auf das Transport-Verzeichnis sollten beschränkt sein.

9.5.5 Konfiguration von Diensten

Tabelle 43 Konfiguration von Diensten

NR.	Prüfprogramm: Sichere Konfiguration von Diensten
5	**Kontrollziel: Sichere Konfiguration von Diensten** Schwachstellen in der Konfiguration eines Diensts bzw. innerhalb des Diensts selbst können die Sicherheit des Systems erheblich beeinträchtigen. Auf einem System sollten nur Anwendungen installiert sein, die das System zur Durchführung seiner Aufgabe benötigt. Daher sollte das System auf die Bereitstellung eines Diensts oder einer Gruppe gleichartiger Dienste beschränkt sein. Unterschiedliche Dienste sollten auf separaten Systemen eingerichtet sein. Die Sicherheitsbewertung und die Gruppierung der Dienste wurden mit dem Sicherheitsbeauftragten abgestimmt. **Risiko:** Schwachstellen in Programmen bzw. Diensten können zur Offenlegung von sensiblen Daten bzw. zur Kompromittierung des Systems führen.
5.1 TOP	**Sind die Sicherheitshinweise von Microsoft zum Härten des Systems bekannt und umgesetzt?** Microsoft stellt eine Dokumentation mit weitergehenden Sicherheits-konfigurationen zur Verfügung, die in Abhängigkeit vom Sicherheitslevel und der Kund:innen-Umgebung implementiert werden kann. Diese Dokumentation sollte für die eingesetzte Windows-Version bekannt sein und von dem/der Kund:in, soweit sinnvoll, umgesetzt worden sein. Hinweis: Als Referenz können hier die von Microsoft bereitgestellten Dokumente zum Thema „Windows-Security-Baselines“ dienen (Link).
5.2	**Werden zusätzlich Benchmarks oder technische Richtlinien (z. B. CIS, NIST, BSI) angewandt?** **In welchen Zyklen werden die angewandten Benchmarks oder technischen Richtlinien auf ihre Aktualität hin überprüft und die Systemkonfigurationen entsprechend angepasst?** Neben der Herstellerdokumentation gibt es noch Härtungsempfehlungen, Benchmarks oder technische Richtlinien von weiteren Organisationen. Diese gehen üblicherweise über die Herstellerempfehlungen hinaus. Hier sollte geprüft werden, ob diese zusätzlichen Empfehlungen bekannt sind, auf Anwendbarkeit geprüft wurden und, soweit sinnvoll, umgesetzt wurden.
5.3 TOP	**Ist ein Antivirus-Scanner für das Windows Betriebssystem aktiviert?** Wenn ja, sind die notwendigen Ausnahmen für den Realtime-Scan definiert (siehe auch SAP-Note 106267)?

9.6 Protokollierung und Sicherheitsüberwachung

Tabelle 44 Protokollierung und Sicherheitsüberwachung

NR.	Prüfprogramm: Protokollierung und Sicherheitsüberwachung
6	**Kontrollziel: Protokollierung und Sicherheitsüberwachung** Welche Maßnahmen sind eingerichtet, um die Integrität sowie den Schutz der Vertraulichkeit des Systems sicherzustellen und zu überwachen? **Risiko:** Bei unzureichenden Maßnahmen ist es nicht möglich, Angriffe auf das System festzustellen und zeitnah darauf zu reagieren.
6.1 TOP	**Wird das System (z. B. durch einen Event-Log-Dienst) durchgängig überwacht?** **Ist der Zugriff auf die Log-Dateien restriktiv vergeben und werden die Log-Dateien revisionssicher auf einem zentralen Log-Host gespeichert?** Damit die durchgängige Systemfunktionalität sichergestellt werden kann, muss das System überwacht und bestimmte Ereignisse protokolliert werden. Da die Protokolldateien wichtige Systeminformationen und persönliche Daten enthalten können, muss der Zugriff auf diese Protokolldateien eingeschränkt werden. Nur berechtigte Benutzer sollten daher Zugriff auf die Dateien erhalten. Protokolldateien sind an einen zentralen Log-Host weiterzuleiten.
6.2 TOP	**Werden regelmäßige Auswertungen auf verdächtige Aktivitäten hin durchgeführt?** **Ist das System an ein zentrales Logging- und Monitoring-System, SIEM, Security Operations Center (SOC) angebunden?** Eine Zentralisierung der Protokolldateien auf einen dedizierten Log-Server sollte implementiert werden, um lokale Manipulationen an den Protokolldateien zu erschweren und eine zentrale Analyse zu ermöglichen. In der Praxis können sogenannte SIEM-Systeme (Security-Incident- und Event-Management-Systeme) klassische Log-Hosts ersetzen. Intelligente Abfragen unterstützen dabei die Analyse verdächtiger Vorgänge.

9.7 Datensicherung, Wiederherstellung und Löschung

NR.	Prüfprogramm: Datensicherung, Wiederherstellung und Löschung
7	**Kontrollziel: Datensicherung, Wiederherstellung und Löschung** - Welche Maßnahmen sind eingerichtet, um einen Datenverlust des Systems zu vermeiden? - Werden Daten sicher gelöscht? **Risiko:** - Bei unzureichenden Maßnahmen kann es zu einem Datenverlust kommen. Sofern Daten nicht sicher gelöscht werden, kann dies dazu führen, dass sie ungewollt durch Dritte wieder lesbar gemacht werden.
7.1 TOP	**Wird ein Backup des Systems auf einem dedizierten Medium (separatem Backup-Server) durchgeführt?** **In welchen Zyklen werden die Backups erstellt?** Ein Backup kann einerseits dabei helfen, gelöschte oder beschädigte Daten wiederherzustellen. Andererseits kann es auch dem Abgleich mit vorhandenen Daten dienen, um so kompromittierte Daten ausfindig zu machen. Es muss jedoch darauf geachtet werden, dass das Backup-Medium in einer sicheren Umgebung aufbewahrt wird, sodass es gegen Manipulation geschützt ist.
7.2 TOP	**Werden die Backups regelmäßig auf ihre Funktionalität hin überprüft? Gibt es regelmäßige Wiederherstellungen oder Wiederherstellungstests?** Sofern Wiederherstellungen von Backups nicht regelmäßig durchgeführt oder getestet werden, kann dies dazu führen, dass im Ernstfall eine Wiederherstellung des Systems nicht möglich ist. Daher ist sicherzustellen, dass Wiederherstellungen regelmäßig durchgeführt werden oder es regelmäßige Wiederherstellungstests gibt.
7.3 TOP	**Gibt es eine Richtlinie, wie Daten auf stillgelegten Systemen oder von nicht mehr verwendeten Datenmedien gelöscht werden?** **Wie wird (technisch) sichergestellt, dass die Richtlinie umgesetzt wird?** Werden Systeme stillgelegt bzw. Datenmedien nicht mehr verwendet, müssen die darauf enthaltenen sensiblen Daten so gelöscht werden, dass sie nicht wiederhergestellt werden können. Um dieses zu erreichen, können sogenannte Wipe-Tools eingesetzt werden.

10 Risiken aus dem Einsatz von SAP GRC

Die Risiken durch Zugriffe auf Daten und Systeme gewinnen in den meisten Organisationen immer mehr an Bedeutung. Deshalb haben die meisten Unternehmen bereits Maßnahmen getroffen, um diesen Risiken entgegenzuwirken. Oftmals ist es unumgänglich, auf bewährte Compliance-Tools zurückzugreifen, um Kontrollen zu automatisieren. Diese unterstützen Organisationen, um Transparenz zu schaffen und bei einem angemessenen Umgang mit Zugriffsrechten. Die Umsetzung und Überwachung von Revisionsaufgaben wird idealerweise von zentralen Stabsstellen durchgeführt. Ähnliches gilt auch für den Einsatz von Compliance-Tools.

SAP GRC Access Control ist eines der Tools, die Unternehmen ganzheitlich in der Sicherstellung von IT-Compliance im Access-Management unterstützen. Da es wesentliche Abweichungen in den unterschiedlichen Releases des GRC-Tools gibt, beziehen wir uns hier auf die aktuellen SAP-GRC-Access-Control-12.X-Funktionen. Die Annahme zur Beschreibung von Prüfungshandlungen für SAP GRC ist die Nutzung als Einzellösung, d. h. beispielsweise ohne die Integration von Identity-Management-Systemen.

10.1 Access-Management-Prozesse

Um ein einheitliches Verständnis über IT-Prozesse zu erhalten, die durch den Einsatz von SAP GRC Access Control 12.X unterstützt werden, soll dies mithilfe folgender Darstellung beschrieben werden.

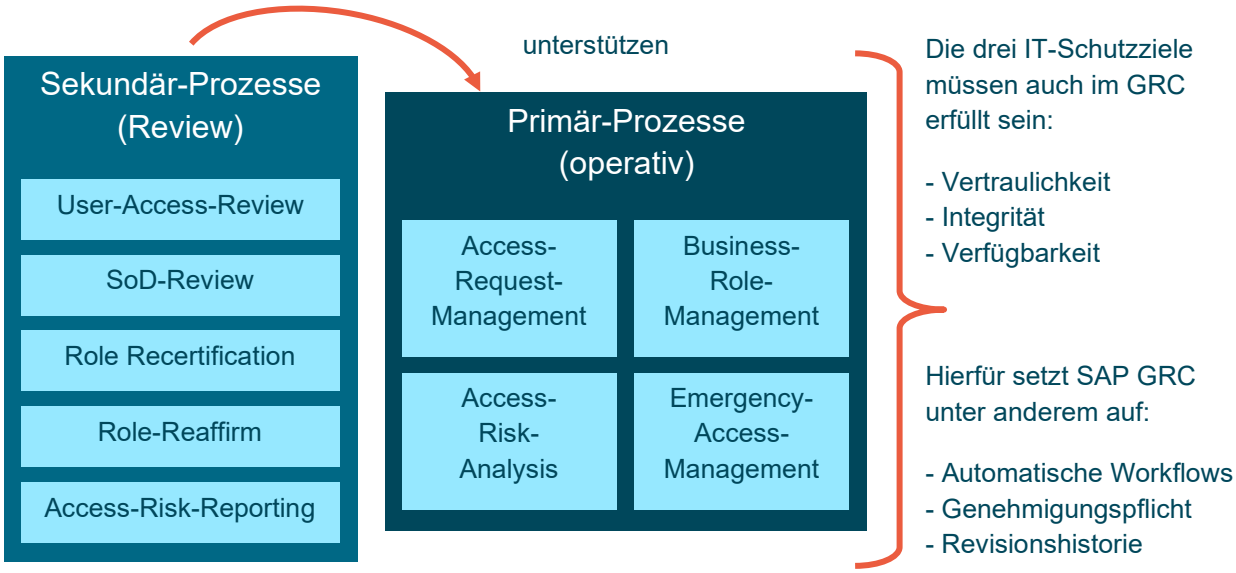

Abbildung 4 Access-Management-Prozesse

Im Kontext des IT-Audits hat die Einführung von SAP GRC oder ähnlichen Tools Auswirkung auf die Benutzerverwaltung, die Rollenverwaltung und die Notfallbenutzer-Prozesse (Primärprozesse). Diese können vollständig über das GRC-Tool unterstützt werden. Darüber hinaus können sie durch Review-Prozesse (Sekundärprozesse) unterstützt werden und gewährleisten somit eine kontinuierliche Kontrolle im Access-Management. Diese Sekundärprozesse ersetzen weniger, sondern ergänzen die Compliance-Prozesse und sollten bei der Gesamtbeurteilung des IKS berücksichtigt werden. Durch den vollständigen Einsatz und die adäquate Ausprägung der Funktionen können die Prozesse durch die Workflow-Unterstützung, die Funktionstrennungen, die Genehmigungspflichten und die Revisionshistorien wesentlich zur IKS-Optimierung beisteuern.

Relevante Komponenten und Funktionen des SAP GRC Access Control 12.X:

- Access-Request-Management (ARM)
- Access-Risk-Analysis (ARA)
- Business-Role-Management (BRM)
- Emergency-Access-Management (EAM)
- User-Access-Review (UAR)
- SoD-Review
- Role-Certification
- Role-Reaffirm
- Access-Risk-Reporting

10.2 Anpassung von Prüfungshandlungen beim Einsatz von SAP GRC Access Control 12

Der Einsatz von GRC-Tools bringt nicht nur Vorteile für die betroffenen Unternehmen, sondern erfordert auch ein Umdenken für die Prüfungseinheiten wie externe oder interne Auditor:innen. Folgende Aspekte sollen mögliche Eingriffsfelder beim Einsatz der Tools aufzeigen und eine erste Abwägung für Auditor:innen erlauben, in welchem Kontext eine Anpassung der Prüfungshandlungen erfolgen muss.

1. Konsolidierung und Zentralisierung von Kontrollaktivitäten
2. Automatisierung von kritischen Genehmigungs-Workflows
3. Automatische Ermittlung von adäquaten Genehmigenden
4. Präventive Vermeidung von kritischen Zugriffen (Risikoanalyse)
5. Zentrale Verwaltung von kritischen IT-Prozessen und Stammdaten
6. Sicherstellung einer lückenlosen Dokumentation (Logs/Pflichtfelder)

Tabelle 45 Anforderungen für Prüfungshandlungen

Einflussfelder	SAP-GRC-Funktionen	Anforderungen für die Prüfungshandlungen
Konsolidierung und Zentralisierung von Kontroll-aktivitäten	Durch die Einführung von SAP-GRC-Funktionen werden dezentrale Prozesse wie die Provisionierung von Benutzern zentralisiert. Hierdurch werden Kontrollaktivitäten effizienter.	Die dezentrale Überprüfung von Access-Management-Prozessen muss wesentlich infrage gestellt werden, sofern die relevanten Prozesse zentral gesteuert werden. Neben Akzeptanzproblemen durch die geprüfte Organisation erzeugt dies auch eine Ineffizienz in der Prüfungsdurchführung. Entscheidend sind die Identifizierung von Prozessen und Systemen im Scope, die durch das zentrale Tool gesteuert werden, und der Ausschluss der Umgehung dieser zentralen Prozesse.
Automatisierung von kritischen Genehmigungs-Workflows	SAP GRC ermöglicht es, für das Access-Management Genehmigungs-Workflows zu hinterlegen, sodass o. g. Effizienz in der Kontrolldurchführung realisiert werden kann. Workflows können dabei in Abhängigkeit von diversen Faktoren wie der System-ID oder des Geschäftsprozesses variiert werden. Die Realisierung erfolgt mithilfe der integrierten Komponenten MSMP und BRF+.	Der/Die Auditor:in sollte ähnlich wie bei manuell durchgeführten Prozessen das Design der Umsetzung auf Angemessenheit hin überprüfen. Sofern dieser automatisierte Prozess für die Prozesse im Scope nicht umgangen werden kann, ist das Testen eines einzelnen Vorgangs des automatisierten Workflows ausreichend.

Einflussfelder	SAP-GRC-Funktionen	Anforderungen für die Prüfungshandlungen
Automatische Ermittlung von adäquaten Genehmigenden	In Kombination mit den Workflow-Komponenten MSMP und BRF+ können Access-Management-Prozesse so weit automatisiert werden, dass selbst die Genehmigenden systemseitig ermittelt werden können. Dies erfolgt bspw. über die Einbindung von Entscheidungstabellen.	Der Einsatz von Entscheidungstabellen zur systemseitigen Ermittlung von adäquaten Genehmigenden ermöglicht es auch dem/der Prüfenden, durch wenige Checks die Angemessenheit der hinterlegten Logik zu verstehen und zu validieren. Hierbei gibt es technische Voraussetzungen, die überprüft werden sollten. Dabei handelt es sich u. a. um die gepflegten Access-Control-Owner im System (potenzielle Genehmigende) als auch um Eskalationspfade (Escape-Conditions).
Präventive Vermeidung von kritischen Zugriffen (Risikoanalyse)	Die Basis für das Management von Funktionstrennungen (SoD) und sämtlicher Compliance-Funktionen ist das hinterlegte SoD-Regelwerk. Sofern ein technisches Regelwerk systemisch hinterlegt ist, kann diese Risikoanalyse ad hoc (detektiv) oder auch integriert (präventiv) verwendet werden.	Sofern die Risikoanalyse per Design in die Access-Management-Prozesse integriert ist, können Effizienzen auch für die Prüfungshandlungen genutzt werden. Neben der Vollständigkeit und Richtigkeit des Regelwerks ist die Verprobungsart (wie z. B. gewähltes Regelwerk und Risikoart) per Event und Prozess zu prüfen. Eingeschränkte Ausprägungsmöglichkeiten des Tools sind zu beachten.

Einflussfelder	SAP-GRC-Funktionen	Anforderungen für die Prüfungshandlungen
Zentrale Verwaltung von kritischen IT-Prozessen und Stammdaten	SAP-GRC-Komponenten ermöglichen und erfordern eine zentrale Pflege von Stammdaten, die Einfluss auf die umgesetzten Access-Management-Prozesse haben. Hierbei geht es sowohl um die Bereitstellung von Funktionen (EAM-Administration) als auch um die Aussteuerung derselben (Workflowkonfiguration). Bei SAP GRC ist zu beachten, dass Einstellungen sowohl im NetWeaver Business Client als auch im SAP-Customizing (IMG) umgesetzt werden. Während das Customizing transportierbar ist, müssen Stammdaten im NWBC pro System und Mandant:in gepflegt werden.	Aufgrund der integrierten NetWeaver-Technologie sollte der/die Auditor:in die Zusammenhänge zwischen dem GRC-Backend-Customizing und der Stammdatenpflege im NWBC kennen. Dies ist nicht nur für die Bewertung des Prozess-Designs erforderlich, sondern auch, um das Change-Management der Applikation überprüfen zu können. Insbesondere die Berechtigungseinschränkung in der produktiven GRC-Umgebung ist kritisch zu hinterfragen aufgrund der weitreichenden Auswirkung von dolosen Handlungen auf einem zentralen System.
Sicherstellung einer lückenlosen Dokumentation	Sämtliche Änderungen an Stammdaten in der NWBC-Umgebung können systemseitig und revisionssicher protokolliert werden. Zudem können teilweise auch Applikationskontrollen in Form von Pflichtfeldern hinterlegt werden, um die Vollständigkeit der Dokumentation zu unterstützen.	Die Protokollierfunktion von SAP GRC kann stark variieren und muss explizit aktiviert werden, ähnlich wie es auch bei ERP-Systemen der Fall ist. Ob und welche Applikationskontrollen für die Unterstützung der Revisionssicherheit genutzt werden, muss über Prüfungshandlungen verifiziert werden. Die meisten Protokollierfunktionen werden zentral verwaltet und können schnell auditiert werden.

10.3 Neue Anforderungen an die IT-Prüfung

10.3.1 Verlagerung der Risiken im Access-Management

Aufgrund des direkten Einflusses der GRC-Komponenten auf rechnungslegungsrelevante IT-Prozesse, im speziellen Access-Management-Prozesse, haben die Einführung und der Betrieb eines SAP GRC Access Control (oder ähnlicher Compliance-Tools) eine wesentliche Bedeutung für die Prüfungsplanung. Insbesondere bei mittelständischen Unternehmen wie auch Großunternehmen bedeutet dies ebenfalls eine Zentralisierung der Prüfungshandlungen.

Beispielsweise wird der Benutzerantragsprozess oder der Rollenpflegeprozess – je nach Design der technischen Realisierung – nicht mehr dezentral pro Zielsystem auditiert, sondern zentral über das GRC-System. Damit kann sich das Prüfenden-Team auf wesentliche Prozessrisiken fokussieren und profitiert durch die Modernisierung in der IT. Ähnlich wird dies auch bei anderen zentralen Instanzen wie dem SAP Solution Manager gehandhabt, der für die Umsetzung des Change-Managements eingesetzt werden kann.

Für die geprüfte Organisation wiederum bedeutet dies, dass Effizienz und dadurch Entlastungen durch das Audit gewährleistet werden bzw. gefordert werden können. Voraussetzung sind in jedem Fall der Scope der GRC-unterstützten Prozesse und die zentrale (wirksame) Abnahme der Prozesse und Inhalte. Wichtig zu erwähnen ist auch, dass manuelle Aktivitäten innerhalb der Benutzerverwaltung bzw. außerhalb des SAP GRC ein höheres Risiko darstellen, wenn vom vorgegebenen GRC-Prozess abgewichen wird. Änderungen mittels Transaktion SU01 (oder vergleichbarer Transaktionen) sollten von der Beurteilung des GRC-Systems und der Prozesse ausgenommen und separat beurteilt werden.

10.3.2 Neue Risiken im Access-Management

Durch den Einsatz von SAP GRC werden zum einen die Access-Management-Prozesse verlagert, zum anderen entstehen neue IT-Risiken, die in den Scope der Auditorin / des Auditors aufgenommen werden müssen. Hierbei handelt es sich um die Compliance des GRC-Systems selbst. Während die Zentralisierung der kritischen IT-Prozesse aus Sicht der Anwendung einen Mehrwert schafft, steigt durch den Single-Point-of-Failure auch das Risikoausmaß (Business-Impact) für den GRC-Betrieb.

Unternehmen sind dabei in der Nachweispflicht, dass das SAP GRC den Anforderungen als IKS-relevantes System entspricht, und müssen dies durch allgemeine IT-Kontrollen (ITGC) bestätigen. Hierbei handelt es sich u. a. um die Angemessenheit des GRC-Berechtigungskonzepts und wie kritische Zugriffsrechte sowie die Trennung von kritischen Funktionen (SoD) vermieden wird, und auch um

die Angemessenheit des GRC-Prozessdesigns (Administration der Workflows, Change-Management etc.).

10.3.3 Risikoarten beim Einsatz von SAP GRC

Folgende Risikofelder und Prüffragen können für ein erstes Scoping in der IT-Prüfung beim Einsatz von SAP GRC verwendet werden:

1. Prozessdesign (Workflow, Owner)
   - Welche Access-Management-Prozesse sind im Scope?
   - Wie ist das Prozessdesign der IKS-relevanten Prozesse?
   - Welche Zielsysteme sind im Scope, mit welchen Prozessvarianten?
   - Welche Ausnahmeprozesse gibt es (z. B. Escalation-Paths)?
   - Wird die Transaktion SU01 (oder vergleichbare Transaktionen) für manuelle Benutzerstammänderungen weiterhin verwendet oder sind diese Transaktionen deaktiviert?

2. Kritische Zugriffsrechte (Berechtigungen)
   - Gibt es eine Risikoeinschätzung der kritischen GRC-Prozesse und -Funktionen?
   - Wie werden kritische Berechtigungen identifiziert (z. B. GRC-Regelwerk)?
   - In welchen GRC-Prozessen wird das Regelwerk verwendet?

3. GRC-Stammdaten (NWBC)
   - Wie sieht das Rollenkonzept für die Stammdatenpflege im GRC aus?
   - Wie wird die Trennung hinsichtlich der Datenpflege zwischen den organisatorischen Einheiten sichergestellt?
   - Wie erfolgt der Change-Prozess zu den Stammdaten?

4. GRC-Konfiguration (SPRO, MSMP, BRF+)
   - Wie sieht das Rollenkonzept für die Konfiguration im GRC aus?
   - Wie wird die Trennung hinsichtlich der Pflege zwischen den organisatorischen Einheiten sichergestellt?
   - Wie erfolgt der Change-Prozess zum Customizing? Welche Transportwege sind erlaubt?

5. Kritische Profile/Rollen (Objektebene)
   - Welche kritischen Profile und Rollen sind identifiziert?
   - Wie ist das Monitoring in Access-Management-Prozesse eingebunden?
   - Wie wird der Einsatz dieser kritischen Rechte vermieden und überwacht?

6. Kritische Parameter (globale Konfigurationseinstellungen)

- Sind die globalen Einstellungen angemessen gesetzt?
- Wie ist der Change-Prozess zu den kritischen Parametern?

10.4 Prüfprogramm beim Einsatz von SAP GRC Access Control

Für den Aufbau des Prüfprogramms wurde ein risikoorientierter Prüfungsansatz gewählt, um ein umfassendes und effizientes Vorgehen in der Auditierung zu gewährleisten. Orientiert an den GRC-Komponenten, werden die Risiken der dadurch abgedeckten (Teil-)Prozesse analysiert (Design-Effectiveness). Für die Wirksamkeitsanalyse werden kritische Parameter wie auch kritische Zugriffe, die wesentliche Auswirkungen auf die Prozesse haben, detailliert betrachtet (Operating-Effectiveness). Somit ist eine komplette Risikoprüfung im Sinne des IKS auf Applikationsebene möglich.

Abbildung 5 Aufbau des GRC-Prüfprogramms – risikoorientierter Prüfungsansatz

10.4.1 Prüfung des Emergency-Access-Management

10.4.1.1 Prozess-Design Emergency-Access-Management

Der Einsatz von Notfallbenutzern dient der speziellen Aufgabenerfüllung aufgrund besonderer Ereignisse, die zwingend und unaufschiebbar in transaktionellen SAP-Systemen durchzuführen sind. Um zu vermeiden, dass hierbei Maßnahmen durchgeführt werden, die weder nachvollziehbar noch begründet sind, kommt in diesen Fällen das EAM von SAP GRC Access Control 12.X zum Einsatz. Es ermöglicht die zentrale Administration von ausnahmebasierten Zugängen durch die Verwendung von Firefighter-IDs oder von Firefighter-Rollen, die diversen Benutzer temporär zugeordnet werden können.

Die komplette Administration dieser zeitlich begrenzten Vergabe kritischer Rechte erfolgt auf der GRC-Plattform. Wesentlich ist der integrierte Workflow zur Protokollierung und Revision der durch die Nutzenden vorgenommenen Handlungen unter Verwendung der kritischen Berechtigungen. EAM erfüllt die Anforderungen an eine revisionssichere Nachweispflicht zur Verfolgung privilegierter Zugriffe für transaktionale SAP-Systeme.

Aus der Verwendung der Komponente und der temporären Zuweisung kritischer Rechte an Benutzer ergeben sich dringende Prüfungshandlungen, die in dem Prüfprogramm berücksichtigt wurden.

Tabelle 46 Prüfungshandlungen: Emergency-Access-Management

Nr.	Prüfungshandlungen für ein konformes Emergency-Access-Management
1	Anwendungsbereich des Notfallbenutzer-Konzepts mit EAM **Kontrollziel:** Das EAM-Szenario deckt alle kritischen Systeme ab und unterstützt den Schutz systemspezifischer Daten. **Risiko:** Es sind nicht alle kritischen Systeme und Daten durch angemessene Kontrollen gesichert.
1.1	Gibt es einen Überblick über alle an das GRC-System angebundenen Zielsysteme (Plug-In-Systeme), für die EAM angewendet wird? *Check: Transaktion SM59, alle an die/den produktive:n GRC-Mandant:in angebundenen Plug-In-Systeme und ergänzend folgenden Konfigurationspfad. SPRO > GRC > Gemeinsame Komponenteneinstellungen > Integration Framework > Verbindungseinstellungen bearbeiten. Prüfen Sie das Integration-Scenario SUPMG (Super-User-Privilege-Management), welche Konnektoren hier zugeordnet sind (Tabellen GRACCONNSTAT und GRFNCCICONNECTOR).*

Nr.	Prüfungshandlungen für ein konformes Emergency-Access-Management
	Hinweis: Für die vollständige Konfiguration von EAM auf spezifizierte Konnektoren sind weitere Einstellungen erforderlich, allerdings geben o. g. Checks bereits erste Hinweise darauf, ob ein Zielsystem EAM-relevant ist oder nicht. Auch für den dezentralen Einsatz von EAM müssen Konnektoren vorhanden sein.
2	Definition von kritischen Berechtigungen zur Aufnahme in ein dediziertes Notfallbenutzer-Konzept. **Kontrollziel:** Maßnahmen zur Identifizierung und Beschreibung von kritischen Berechtigungen sind vorhanden. **Risiko:** Kritische Zugriffe werden nicht oder nur unvollständig durch die EAM-Funktionen abgedeckt. Risikobehaftete Zugriffe sind nicht nachvollziehbar und zuordenbar, gefährden somit die Integrität der Systemdaten.
2.1	Sind Verfahrensanweisungen vorhanden, um kritische Berechtigungen aufzudecken (Risikoanalyse/Regelwerk)? Sind kritische Berechtigungen aus dem Standard in den Notfallbenutzer-Prozess mit EAM eingebunden? Gibt es Prozesse zur Neuaufnahme von neuen FFIDs und die Nominierung von adäquaten Eignern (Owner/Controller)? Hinweis: Es wird empfohlen, neben den Firefighter-Szenarien wenige Superuser weiterhin auf konventionellem Wege beizubehalten, um eine totale Abhängigkeit von GRC (GRC Shutdown) zu vermeiden. Die Notfallbenutzer sollten synchron mit dem übergreifenden Disaster-Recovery-Konzept sein.
3	Einrichtung und Änderung von Notfallbenutzern (FFIDs) **Kontrollziel:** Bei der Anlage von technischen Benutzern, hier FFIDs, und deren Eignern (hier Owner/Controller) werden Benutzer-Antragsverfahren verwendet, die angemessen sind. **Risiko:** Unangemessene Anlage und Zuordnung von Notfallbenutzern.
3.1	Wie werden FFIDs auf den Plug-In-Systemen angelegt? Wird die Einrichtung der FFIDs adäquat genehmigt? Ist der Benutzer-Kreis für die Beantragung von FFIDs entsprechend der Kritikalität eingeschränkt? Wie erfolgt die Nominierung und Benutzer-Anlage der FF-Owner? Für die Prüfung der Benutzer durch GRC selbst bitte Prüfungshandlungen aus 9.4.2.1 ARM beachten. Gibt es einen Prozess zur regelmäßigen Überprüfung der Angemessenheit aller Notfallbenutzer?

Nr.	Prüfungshandlungen für ein konformes Emergency-Access-Management
4	Genehmigung der Notfallbenutzer-Zuordnung **Kontrollziel:** Die Benennung von FF-Ownern erfolgt nachvollziehbar und zusammenhängend mit dem Risiko, das sich hinter dem Zugriff verbirgt. Es ist sichergestellt, dass Firefighter nicht ihre eigene Zuordnung genehmigen. **Risiko:** Inadäquate Genehmigung des Notfallbenutzer-Zugriffs kann zu unsachgemäßem Einsatz desselben führen.
4.1	Welche Verantwortlichen werden in den Nominierungsprozess mit eingebunden? Gibt es eine Plausibilität hinter der Ermittlung von Genehmigenden? Für die Überprüfung der systemseitigen Funktionstrennung im EAM-Prozess siehe Konfigurationseinstellungen 4013 und 4014. Stimmen die FF-Owner im GRC-NWBC mit den freigegebenen (dokumentierten) Genehmigenden überein? *Check: NWBC-Einrichtung > Notfallzugriffszuordnung > Verantwortliche (Owners) und Notfallzugriffsbearbeitung > Kontrollierende (SAP-Tabelle GRACFFCTRL)*
4.2	Wie ist sichergestellt, dass der FF-Owner in den Beantragungsprozess eingebunden ist? Wird der Genehmigungs-Workflow zur Beantragung und Zuordnung von FFIDs in ARM eingesetzt? *Check: SPRO > GRC > Access Control > Workflow für Access Control > MSMP Workflows bearbeiten > ProzessID: SAP_GRAC_ACCESS_REQUEST, Schritt 2 suche nach GRAC_MSMP_ SPM_OWNER_AGENT, Schritt 5 suche nach Firefighter-Pfad und überprüfe Genehmigenden-Stufen und Genehmigende (Bearbeitenden-ID) aus.* *Prüfen Sie über NWBC > Zugriffsverwaltung > Zugriffsanforderungsverwaltung > Anforderungen suchen, die genehmigten EAM-Anträge und validieren Sie die Angemessenheit der Genehmigenden.*
4.3	Wie ist der Prozess für den dezentralen EAM-Ansatz gelöst? Hinweis: Es können beide Ansätze parallel im Einsatz sein. Die Verwendung ist abhängig von der Anwendbarkeit im Unternehmen. Zu überprüfen ist, ob auf den dezentralen Systemen die Plug-In-Einstellungen gesetzt sind und entsprechende Berechtigungen für FF-Endbenutzer (auf dem Zielsystem) vorhanden sind.

Nr.	Prüfungshandlungen für ein konformes Emergency-Access-Management
	Check: SPRO > GRC Plug-In > Access Control > Plug-In-Konfigurationseinstellungen bearbeiten, validieren Sie Parameter: 1089, 1090, 4000, 4001, 4008, 4010 auf Angemessenheit *Check: SPRO > GRC Plug-In > Access Control > User-Exits für Plug-In-Systeme bearbeiten, validieren Sie den Parameter SAP_EXIT_USERS_SAVE auf Richtigkeit*
5	Review der Firefighter-Logs **Kontrollziel:** Der FF-Einsatz ist so konfiguriert, dass Kontrollierende zeitnah über die Verwendung informiert werden. Es ist sichergestellt, dass Firefighter nicht ihren eigenen Zugriff bestätigen. **Risiko:** Eine unvollständige oder verzögerte Prüfung der FF-Logs kann dazu führen, dass dolose Handlungen nicht oder nur verspätet aufgedeckt werden.
5.1	EAM kann systemseitig so konfiguriert werden, dass die Kontrollierenden ad hoc beim FF-Einsatz per E-Mail informiert werden und zeitnah das Log zum Review erhalten. Hierfür sind Parameter in den Konfigurationseinstellungen adäquat zu setzen. Ebenfalls wird die Funktionstrennung im EAM-Prozess systemseitig unterstützt. Siehe Konfigurationseinstellungen in Kapitel 2.4.1.2. *Hinweis: Der Versand der Log-Files zur Review durch die/den Kontrollierende:n erfolgt in Abhängigkeit von der Taktung des Batch-Jobs GRAC_SPM_LOG_SYNC_UPDATE. Dieser sollte 1h nicht übersteigen.* Hinweis: Der Versand von E-Mails ist von weiteren basisrelevanten Einstellungen abhängig, insbesondere von der SCOT-Verwaltung. Diese sollten ebenfalls beachtet werden, sind aber unabhängig vom Workflow im GRC zu sehen.

10.4.1.2 Sicherheitskritische Parameter für das Emergency-Access-Management

Die globalen Konfigurationseinstellungen sind Mandant:innen-abhängig und haben in Abhängigkeit von der GRC-Architektur eine kritische Auswirkung auf das Design der technischen GRC-Prozesse. Diese können unter folgendem Pfad validiert werden.

Check: SPRO › GRC › Access-Control › Konfigurationseinstellungen

Im Folgenden finden Sie die wesentlichen Konfigurations-Parameter für das Emergency-Access-Management. Neben dem vorkonfigurierten Standardwert wird auch eine Best-Practice-Empfehlung gegeben. Selbstverständlich ist letztere Kund:innen-individuell zu validieren.

Tabelle 47 Konfigurationsparameter – Emergency-Access-Management

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
1113	Access Control E-Mail-Absender	WF-BATCH	Kund:innen-spezifisch ausprägen	Dieser Technische Benutzer verwaltet die GRC-Workflows und muss entsprechend ausreichende Berechtigungen haben.
4000	Anwendungsart	1	1	Der Wert 1 bedeutet, dass das ID-basierte Firefighting im Einsatz ist. Es können nicht beide Varianten parallel im Einsatz sein. In Abhängigkeit von der Applikationsart entstehen neue Anforderungen an die EAM-Prozesse.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
4001	Standard-Firefighter-Gültigkeitszeit-raum (Tage)	‹empty›	1	Anzahl der Tage für die Gültigkeit der FF-Zuordnung. Hinweis: Diese Standardeinstel-lung kann im FF-Antrag durch die/den Antragstellende:n oder bei der manuellen Zuordnung durch den EAM-Administrator / die EAM-Administratorin angepasst werden.
4002	E-Mail sofort senden	YES	YES	Ad-hoc-Benachrichtigung der/des FF-Kontrollierenden, dass betroffene FFID im Einsatz ist. Hinweis: Dieser Parameter ist mit GRC 12.X obsolet.
4003	Änderungs-protokoll abrufen	YES	YES	Aktivierung der Abfrage des Change-Logs aus dem Plug-In-System.
4004	Systemprotokoll abrufen	YES	YES	Aktivierung der Abfrage des

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				System-Logs aus dem Plug-In-System.
4005	Revisions-protokoll abrufen	YES	YES	Aktivierung der Abfrage des Audit-Logs aus dem Plug-In-System.
4006	BS-Befehls-protokoll abrufen	YES	YES	Aktivierung der Abfrage des O/S-Command-Log aus dem Plug-In-System.
4007	Benachrichtigung für Protokollbericht-ausführung sofort senden	YES	YES	Sofortige Benachrichtigung des/der FF-Kontrollierenden zum Review des Log-Files Hinweis: Führend ist hier die Taktung des Jobs GRAC_SPM_LOG _ SYNC_UPDATE.
4008	Firefighter-Benutzer-anmelde-benachrichtigung senden	YES	Kund:innen-spezifisch ausprägen	Ad-hoc-Benachrichtigung des/der FF-Kontrollierenden, dass betroffene

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				FFID im Einsatz ist.
4009	Protokollbericht-ausführungs-Benachrichtigung	YES	YES	Sofortige Benachrichtigung des/der FF-Kontrollierenden zum Review des Log-Files Hinweis: Führend ist hier die Taktung des Jobs GRAC_SPM_LOG_SYNC_UPDATE.
4010	Firefighter-ID-Rollenname	ZSAP_GRAC_SMP_FFID	Kund:innen-spezifisch ausprägen	Die hier definierte Rolle muss der technischen Rolle entsprechen, die auf den Plug-In-Systemen den FFIDs zugeordnet wird.
4012	Standardbenutzer für das Weiterleiten des Revisions-protokoll-Workflows	2	2	Aufgrund der Sensibilität der Daten wird empfohlen, dass das Log-File nur innerhalb einer eingeschränkten Gruppe weitergeleitet werden kann. Hier bietet sich die Gruppe der FF-Kontrollierenden

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				an. Die Weiterleitung kann auch ausgeschlossen werden.
4013	Firefighter-ID-Verantwortliche:r kann Anforderung für ihre/seine Firefighter-ID senden	YES	NO	Sicherstellung, dass eine Funktionstrennung im EAM-Prozess gewährleistet ist.
4014	Firefighter-ID-Verantwortliche:r kann Anforderung für kontrollierte Firefighter-ID senden	YES	NO	Sicherstellung, dass eine Funktionstrennung im EAM-Prozess gewährleistet ist.
4015	Dezentrales Firefighting aktivieren	NO	Kund:innen-spezifisch ausprägen	Aufgrund der Nutzbarkeit des Access-Request-Workflows für die genehmigungs-pflichtige FFID-Zuordnung wird das zentrale Firefighting empfohlen.
4017	Access-Request-Nummer für Anzeige bei Zuordnung von Firefightern zu	YES	YES	Die Zuordnung der Access Request Nummer bei der Zuordnung von Firefightern wird

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
	Firefighter-IDs/ -Rollen aktivieren			empfohlen, weil es die Nachvollziehbar-keit erhöht.
4018	Detailprotokollie-rung (SLG1) für Firefighter-Protokoll-Synchronisie-rungsprogramme aktivieren	NO	YES	Aktivierung der Abfrage der detaillierten Logs für die Synchronisation der Firefighter-Protokolle selbst aus dem Plug-In-System.
4020	Firefighter-Protokoll für Firefighter-Sitzungen ohne Aktivität generieren	NO	YES	Aktivierung der Abfrage der Firefighter-Protokolle aus dem Plug-In-System, auch wenn keine Firefighter-Aktivität stattgefunden hat.
4021	ALV-Grid für Firefighter-Filtertransaktion verwenden	NO	Kund:innen-spezifisch ausprägen	Bei vielen Firefighter-IDs ist das ALV-Grid hilfreich.
4025	Firefighter-Gültigkeitszeit-raum während Zugriffs-anforderung einschränken	NO	Kund:innen-spezifisch ausprägen	Der Gültigkeits-zeitraum für die Zugriffsanforde-rung kann Kund:innen-spezifisch ausgeprägt werden und hilft dabei,unnötige

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				Zugriffe zu beschränken.
5033	Firefighter ohne Kontrollierende zulassen	YES	NO	Firefighter ohne Kontrollierende zuzulassen verletzt das Vier-Augen-Prinzip und wird nicht empfohlen.

10.4.1.3 Kritische Berechtigungen und Funktionstrennung im Emergency-Access-Management

Die Berechtigungen zur Steuerung der Komponente und deren wesentlicher Funktionen erfolgen über eine überschaubare Anzahl von Berechtigungsobjekten und Feldwerten. Die hierin als kritisch und prüfungsrelevant zu betrachtenden Bereiche werden im Folgenden beschrieben. Der Bezug zu den in **Fehler! Verweisquelle konnte nicht gefunden werden.** genannten Risiken wird hergestellt.

Tabelle 48 Berechtigungen – Emergency-Access-Management

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
GRAC_ ASIGN	**ACTVT** 01, 02, 06, 36, 70 **GRAC_OWN_T** FFCR, FFCU, FFID, FFRO	Über „Access-Control-Verantwortliche“ können im NWBC Mitarbeitende für Genehmigungen und Kontrollen im EAM-Umfeld ernannt werden. Dies ist nötig, um Mitarbeitende als Firefighter-Owner oder Controller zu konkreten FFIDs zuzuordnen. Das Berechtigungs-objekt GRAC_ASIGN steuert aus, zu welchen Funktionen Mitarbeitende ernannt werden können (z. B. Firefighter-Owner via GRAC_OWN_T - FFID oder Firefighter-Controller via FFCU).	Nr. 2: „Gibt es Prozesse zur Neuaufnahme von neuen FFIDs und die Nominierung von adäquaten Eignern (Owner/ Controller)?“ Überprüfung, welcher Mitarbeitende über die Rechte zur Ernennung von FF-Ownern und FF-Kontrollierenden verfügt, bspw. über die Transaktion SUIM oder via GRC-Regelwerk.
GRAC_ FFOBJ	**ACTVT** 01, 02, 06, 36	Das Objekt erlaubt die manuelle Zuordnung von Firefighter-IDs zu Endanwendenden, sofern der Workflow für die Beantragung von FFID-Zuordnungen durch die manuelle Administration ergänzt/unterstützt werden soll. Dies übersteuert den Genehmigungsprozess und sollte maximal Administrator:innen im GRC vorbehalten sein.	Nr. 4: „Welche Ver-antwortlichen werden in den Nominierungs-prozess mit eingebunden? Gibt es eine Plausibilität hinter der Genehmigenden-Ermittlung?“ Erfolgt die Zuordnung ohne Workflow, ist zu prüfen, welche Mitarbeitende über die Berechtigungen

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
			verfügen. Ein workflowunterstütz-ter Vergabeprozess ist klar zu präferieren.
GRAC_ FFOWN	**ACTVT** 01, 02, 06, 36, 70	Das Objekt erlaubt die Zuordnung Verantwortlicher zu Firefighter-IDs. Dies ist eine Funktion, die nur Administrator:innen im GRC vorbehalten sein sollte.	Nr. 4: „Welche Verantwortlichen werden in den Nominierungspro-zess mit eingebunden? Gibt es eine Plausibilität hinter der Genehmigenden-Ermittlung?“ Risiko EAM_03: „Wie erfolgt die Nominierung und Benutzeranlage der FF-Owner?“
GRAC_ OWNER	**ACTVT** 01, 02, 06, 36, 70, 78	Das Objekt erlaubt die Zuordnung von Kontrollierenden zu Firefighter-IDs. Dies ist eine Funktion, die nur Administrator:innen im GRC vorbehalten sein sollte.	Nr. 4: „Welche Verantwortlichen werden in den Nominierungspro-zess miteingebunden? Gibt es eine Plausibilität hinter der Genehmigenden-Ermittlung?“ Nach der Ernennung von Mitarbeitenden zu Firefighter-Kontrollierenden erfolgt die konkrete

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
			Zuordnung derselben zu Firefighter-IDs mit dieser Berechtigung. Nur eine stark eingeschränkte Gruppe von Mitarbeitenden darf über das Recht der FFID-Kontrollierenden-Zuordnung verfügen, um die inadäquate Ernennung von Firefighter-Kontrollierenden zu verhindern. Prüfung, welcher Mitarbeitende über die Rechte zur Zuordnung von FF-Ownern verfügt.
GRFN_USER	**ACTVT** 02	Diese Berechtigung überschreibt die meisten Berechtigungsobjekte im GRC mit der entsprechenden Aktivität und ist ausschließlich Administrator:innen vorbehalten.	Alle beschriebenen Zugriffsrisiken im EAM.

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
S_TCODE	**TCD** GRAC_EAM, GRAC_SPM (obsolete Transaktion)	Die Berechtigung erlaubt den Zugriff auf die Firefighter-Startseite. Von hier aus erfolgt der Absprung mittels FFIDs auf die angebundenen Systeme (zentralisiertes Firefighting), sofern der Zugriff auf die FFID genehmigt wurde (Workflow-gesteuerter Prozess) oder die FFID dem Benutzer zugeordnet wurde (manueller Prozess).	Nr. 3: „Ist der Benutzer-Kreis für die Beantragung von FFIDs entsprechend der Kritikalität eingeschränkt?“ Es ist eine Erhebung darüber vorzunehmen, welche Mitarbeitenden den Zugriff auf die Startseite des Firefighter-Absprungs erhalten haben (zentralisiertes Firefighting). Da in EAM kritische Berechtigungen vergeben werden, ist eine beschränkte Zuordnung des Zugriffs sicherzustellen. Hinweis: Allein die Berechtigung für die Transaktion GRAC_SPM erlaubt noch nicht den Absprung via Firefighter-ID, fungiert jedoch als Indiz für den Charakter der Firefighter-ID-Vergabe im Unter-

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
			nehmen. Erhält ein großer Anteil der Mitarbeitenden das Recht für die Transaktion GRAC_EAM, sind die EAM-Prozesse im Unternehmen zu hinterfragen.

10.4.2 Prüfung des Access-Request-Management

10.4.2.1 Prozess Design Access-Request-Management

Das Access-Request-Management stellt in SAP GRC die zentrale Komponente zur Abbildung von Antragsprozessen dar. Genauer ermöglichen Bestandteile und Funktionen von Access-Request-Management, Genehmigungsprozesse zu automatisieren. Die Workflows können übergreifend auch von den anderen GRC-Komponenten verwendet werden. Der Fokus hier liegt aber auf der Prüfung des Benutzer-Antragsprozesses.

Tabelle 49 Prüfungshandlungen: Access-Request-Management

Nr.	Prüfungshandlungen für ein konformes Access-Request-Management
6	Beantragungsprozess **Kontrollziel:** Der Zugang auf kritische Systeme oder die Auswahl der Berechtigungen ist eingeschränkt auf geeignetes Personal. Alternativ ist jede zu beantragende Berechtigung systemseitig genehmigungspflichtig, um unberechtigten Zugriff zu vermeiden. **Risiko:** Unberechtigtes Personal erhält Zugang auf kritische Systeme, möglicherweise über die automatische Zuordnung von Standardrollen.

Nr.	Prüfungshandlungen für ein konformes Access-Request-Management
6.1	Gibt es Prozessbeschreibungen zum Berechtigungsvergabeprozess mittels SAP GRC? Welche Zielsysteme sind als Konnektoren für die Provisionierung definiert? *Check: SPRO > GRC > Gemeinsame Komponenteneinstellungen > Integration Framework > Verbindungseinstellungen bearbeiten. Überprüfen Sie, welche Zielsysteme (Target Connector) für das Integration Scenario Provisioning „PROV“ hinterlegt sind* (SAP-Tabelle GRFNCONNSCNLK). Hinweis: Für die vollständige Konfiguration von ARM auf spezifizierte Konnektoren sind weitere Einstellungen erforderlich, allerdings gibt o. g. Check bereits einen ersten Hinweis darauf, ob ein Zielsystem ARM relevant ist oder nicht.
6.2	Welche Möglichkeiten gibt es generell, Benutzer (auch technische) auf der Produktion anzulegen? Welche Ausnahmen gibt es? Grundsätzlich sollten keine Dialog-, sondern nur noch vom GRC-System verwendete RFC-System-Benutzer und evtl. noch Notfallbenutzer diese Berechtigung haben. Ausnahmen sollten dokumentiert und nachvollziehbar sein. *Prüfen Sie für das jeweilige Zielsystem (ggf. auch über GRC möglich), welche Benutzer die Berechtigung zur Benutzer-Anlage haben:* *Check: Transaktion SUIM > Benutzer > Benutzer nach komplexen Selektionskriterien > Benutzer nach komplexen Selektionskriterien > S_TCODE = SU01 und S_USER_GRP mit ACTVT = 01 oder 02* Hinweis: Weitere Spezifizierung der Abfrage im Falle von vorhandenen Ausnahmen erforderlich.
7	Rollenbeantragung **Kontrollziel:** Der Zugang auf kritische Systeme oder die Auswahl der Berechtigungen ist eingeschränkt auf geeignetes Personal. Alternativ ist jede zu beantragende Berechtigung systemseitig genehmigungspflichtig, um unberechtigten Zugriff zu vermeiden. **Risiko:** Unberechtigtes Personal erhält Zugang auf das GRC-System und kann Rollen ohne Genehmigende oder fehlerhaft beantragen.

Nr.	Prüfungshandlungen für ein konformes Access-Request-Management
7.1	Wer darf Rollen für Zielsysteme via SAP GRC beantragen? Wie ist der Zugang auf das NWBC-Portal eingeschränkt? Wird das Portal als Self-Service verwendet? *Check: SPRO > GRC > Access Control > Benutzer-Erstellung > Benutzer-Anmeldung aktivieren. Überprüfen und besprechen Sie mit dem zuständigen Administrator / der zuständigen Administratorin, ob das Self-Service für das GRC-Beantragungsportal aktiviert ist.* Die Einschränkung der Antragstellenden (Requester) auf geeignetes Personal reduziert die fehlerhafte Beantragung von Rollen. Grundsätzlich muss die Beantragung jedoch nicht eingeschränkt sein, sofern sichergestellt ist, dass jeder Antrag von einem/einer Genehmigenden gesehen und bestätigt oder abgelehnt wird. Bitte beachten Sie auch den Konfigurationsparameter ARM 2033 „Alle Rollen für Anfordernde zulassen“. Hier kann die Rollenauswahl zusätzlich eingeschränkt werden.
8	Berechtigungsvergabeprozess **Kontrollziel:** Es ist sichergestellt, dass Benutzer ausschließlich über ein ordnungsgemäßes Verfahren bereitgestellt werden. Ausnahmeprozesse sind nachvollziehbar dokumentiert und unterliegen der Genehmigungspflicht. **Risiko:** Der Zugriff auf sensible Daten ist nicht angemessen geschützt. Die Zuordnung von Berechtigungen an Benutzer erfolgt nicht kontrolliert und durchgehend nachvollziehbar.
8.1	Wie ist der Genehmigungsprozess zur Rollenvergabe über SAP GRC? Validieren Sie Verfahrensbeschreibungen zum Provisionierungsprozess und überprüfen Sie die entsprechende Umsetzung im System. *Check: SPRO > GRC > Access Control > Workflow für Access Control > MSMP-Workflows bearbeiten, prüfen Sie die Ausprägung der relevanten Prozess-ID (Standard: SAP_GRAC_ ACCESS_REQUEST). Achten Sie dabei auf folgende Ausprägungen:* - Schritt 1: Betroffene Regel-ID: bildet das Mapping zur BRF+ Regel, - Schritt 5: Pfade bearbeiten: bildet die Genehmigungsstufen und -agenten pro Pfad-ID ab. - Aufgabeneinstellungen: Generelle Einstellungen wie die obligatorische Risikoanalyse, Kommentierung oder Eskalation sind pro Pfad hinterlegt.

Nr.	Prüfungshandlungen für ein konformes Access-Request-Management
8.2	BRF+ beinhaltet die betroffene Entscheidungslogik (Standard: Entscheidungstabelle) zum jeweiligen Genehmigungspfad. Möglicherweise sind Genehmigungsschritte mindestens vom Zielsystem abhängig, was man hier dann ablesen kann. Die jeweilige Pfad-ID sowie die Funktions-ID verbinden die Genehmigungs-Workflows im MSMP und die Regel BRF+. *Check 1: Transaktion BRF+, Suche die relevante Applikation und überprüfe die Funktions-ID aus der MSMP-Prozess-ID auf Übereinstimmung.* *Check 2: Validiere die Bedingungslogik (evtl. Entscheidungstabelle) über Applikation > Verwendungen > Ausdruck > <Entscheidungstabelle>* *Jede Zeile bildet eine Bedingung ab, bspw. wenn System X und Anforderungsart Y, dann initiiere die Pfad-ID (aus MSMP).*
9	Genehmigungsprozess **Kontrollziel:** Benutzeranträge werden durch geeignetes Personal angemessen genehmigt. Die Genehmigungspflicht wird systemseitig sichergestellt (erzwungen). Ausnahmen sind nachvollziehbar dokumentiert. **Risiko:** Der Zugriff auf sensible Daten ist nicht angemessen geschützt. Die Zuordnung von Berechtigungen an Benutzer erfolgt nicht kontrolliert und durchgehend nachvollziehbar.
9.1	Welche Genehmigenden-Agenten sind pro Workflow-Pfad hinterlegt? *Check: SPRO > GRC > Access Control > Workflow für Access Control > MSMP-Workflows bearbeiten. Überprüfen Sie die vorhandenen Bearbeitenden-IDs in Schritt 3 sowie die hinterlegten Bearbeitenden-IDs in Schritt 5 für den relevanten Pfad.* *Mögliche Standard-Agenten und ihre Ermittlung:* - GRAC_Manager: Vorgesetzte der Begünstigten, die aus HR-Quelldaten oder durch manuelle Eingabe im Antrag ermittelt werden - GRAC_Role Owner: Rolleneigner:innen (Role Assignment Approver) für die Provisionierung, die an der Rolle hängen und entsprechend gepflegt werden müssen (via Import-Funktion oder BRM-Rollenpflege) - GRAC_Security / GRAC_POINT_CONTACT: Sicherheitsverantwortliche:r oder Ansprechpartner:in ist eine Gruppe oder Person, die eine sekundäre Genehmigung für Zugriffsanforderungen und Prüfungen erteilen kann. Diese muss über die Access-Control-Verantwortung im NWBC gekennzeichnet werden.

Nr.	Prüfungshandlungen für ein konformes Access-Request-Management
9.2	Bitte beachten Sie auch die Auswegsbedingungen (Escape Path) und den dafür hinterlegten Pfad. Dies ist insbesondere wichtig, falls Genehmigende nicht gefunden werden, bspw. im Falle von fehlenden Rolleninhaber:innen. Hier sollte keine automatische Provisionierung erfolgen! *Check: SPRO > GRC > Access Control > Workflow für Access Control > MSMP-Workflows bearbeiten, Schritt 1, Auswegsbedingungen* Beachten Sie bitte auch den Konfigurationsparameter 2038 Rollen ohne Genehmigende automatisch genehmigen. Falls der Parameter auf YES gesetzt ist, sollte überprüft werden, wie die Ermittlung von Genehmigenden, bspw. Rolleneigner:innen, sichergestellt wird. Siehe auch Prüfungshandlung **Fehler! Verweisquelle konnte nicht gefunden werden.** für BRM.
9.3	Welche Benutzer werden, vorbei am GRC-Workflow, manuell in den Zielsystemen angelegt? *Check: Prüfung über den Report RSUSR100N in den Zielsystemen, ob andere Benutzer als der GRC-Workflow-Benutzer in einer festgelegten Prüfungsperiode aktiv waren.*

10.4.2.2 Sicherheitskritische Parameter für das Access-Request-Management

Im Folgenden finden Sie die wesentlichen Konfigurations-Parameter für das Access-Request-Management. Neben dem vorkonfigurierten Standardwert wird auch eine Best-Practice-Empfehlung gegeben. Selbstverständlich ist letztere Kund:innen-individuell zu betrachten.

Tabelle 50 Konfigurationsparameter – Access-Request-Management

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
1071	Risikoanalyse für Formularabgabe aktivieren	NO	YES	Der Parameter erzwingt die Ausführung der Risikoanalyse bei der Beantragung. So können konfliktäre Anträge bereits bei dem/der Beantragenden identifiziert und vermieden werden. Die Beantragung kann grundsätzlich trotzdem erfolgen.
1072	Minderung von kritischem Risiko vor Genehmigung von Anforderung erforderlich	NO	YES (Kund:innen-spezifisch ausprägen)	Die Kompensierung konfliktärer Benutzer-Anträge sollte grundsätzlich systemseitig ermöglicht werden. Ob dies erzwungen werden kann, sodass konfliktäre Anträge sonst nicht genehmigt werden können, ist in Abhängigkeit des Risikoappetits individuell zu bewerten.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
1302	Nur Default-Rollen mit Systemeintrag in Anforderung hinzufügen	NO	YES	Default-Rollen werden als Rollen mit geringem Risiko eingestuft und deshalb automatisch für alle Systeme hinzugefügt. Nach dem Minimalprinzip sollten Berechtigungen allerdings nur für relevante Systeme hinzugefügt werden.
2009	Default-Rollen berücksichtigen	YES	Kund:innen-spezifisch ausprägen	Die konkreten Vergabe-Kriterien von Default-Rollen müssen Kund:innen-spezifisch festgelegt werden. Das gilt im Detail auch für die Parameter 2010 bis 2013.
2014	Rollenzuordnung aktivieren	YES	Kund:innen-spezifisch ausprägen	Das Rollenmapping von Rollen untereinander kann global aktiviert und Kund:innen-spezifisch vorgenommen werden. Nach dem Minimalprinzip sollten allerdings nur relevante Rollenmappings vorgenommen werden.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
2015	Zutreffend für Rollenentfernung	YES	YES	Die automatische Rollenentfernung von automatisch gemappten Rollen wird empfohlen.
2031	Alle Rollen für Genehmigenden zulassen	YES	YES	Die Genehmigungs-fähigkeit von Rollen sollte weniger zentral eingeschränkt, sondern individuell in Abhängigkeit von der Rollenkritikalität realisiert werden.
2032	Rolleneinschrän-kungs-attribut des Genehmigenden	‹empty›	‹empty›	Falls in Parameter 2031 keine Einschränkung definiert wurde, ist dieser Parameter obsolet.
2033	Alle Rollen für Anfordernde zulassen	YES	Kund:innen-spezifisch ausprägen	Mit dem Parameter kann die Beantragung von spezifischen, insbesondere kritischen Rollen entsprechend dem Benutzerkreis eingeschränkt werden. Siehe auch Parameter 2034.
2034	Rolleneinschrän-kungsattribut des Anforderers	‹empty›	Kund:innen-spezifisch ausprägen	Entsprechend der Definition des Parameters 2033

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				wird hier das Attribut selektiert, das die Einschränkung der Rollenauswahl für die Beantragenden steuert.
2035	Rollenkommen-tare zulassen	YES	YES	Aufgrund der besseren Nachvollziehbarkeit bei der Beantragung von Rollen wird die Aktivierung von Kommentaren empfohlen.
2036	Rollenkommen-tare erforderlich	YES	YES	Aufgrund der besseren Nachvollziehbarkeit bei der Beantragung von Rollen wird die Nutzung von Kommentaren empfohlen.
2037	Abgelaufene Rollen für vorhandene Rollen anzeigen	YES	Kund:innen-spezifisch ausprägen	Ob abgelaufene Rollen bei den bestehenden Rollen angezeigt werden oder nicht, kann Kund:innen-spezifisch ausgeprägt werden.
2038	Rollen ohne Genehmigende	YES	YES	Der Parameter steuert die Möglichkeit zur

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
	automatisch genehmigen			Definition von Grundrollen (Default Roles), die Benutzer bei der Beantragung ohne Genehmigung initial erhalten. Es ist sicherzustellen, dass eine fehlerhafte Rollen-bereitstellung ohne Genehmigende aus-geschlossen ist. Siehe auch Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**.
2039	Rolle nach Transaktionen aus Backend-System suchen	NO	Kund:innen-spezifisch ausprägen	Ob Rollen nach enthaltenen Transaktionen gesucht werden können oder nicht, kann je nach Performance-Aspekten Kund:innen-spezifisch ausgeprägt werden.
2040	Zuordnungs-kommentare bei Ablehnung obligatorisch	NO	YES	Eine Ablehnung sollte im Sinne der vollständigen und nachvollziehbaren Dokumentation begründet werden. Dies wird durch den Parameter systemseitig erzwungen.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				Hinweis: Dies kann auch in den MSMP-Einstellungen in Abhängigkeit vom Workflow gesteuert werden.
2042	Sichtbarkeit von „Gültig von“ / „Gültig bis“ für Profile	0	5	Die Anzeige von „Gültig von“ / „Gültig bis“ für Profile wird empfohlen.
2043	Berechtigungs-objekt für Rollensuche – Rollendefinition und -zuordnung	GRAC_ ROLED	Kund:innen-spezifisch ausprägen	Der Parameter ermöglicht die Einschränkung der Rollenauswahl in Abhängigkeit von den Berechtigungs-objekten GRAC_ROLED und/oder GRAC_ROLEP. Ob diese Rollen-einschränkung verwendet wird, muss Kund:innen-spezifisch bewertet werden. Dies setzt allerdings voraus, dass die Beantragenden einen Benutzer auf dem GRC-System haben, was meistens nicht der Fall sein soll.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				Hinweis: Das GRC-System kann als Beantragungs-system mit Benutzerzugang ohne Berechtigungen konfiguriert werden.
2044	Profile in vorhandenen Zuordnungen, Mein Profil und Benutzervorlage anzeigen	YES	NO (Kund:innen-spezifisch ausprägen)	Die Anzeige von Profilen muss Kund:innen-spezifisch festgelegt werden. Bei der Benutzervorlage wird dies nicht empfohlen, weil es zu falschen Benut-zeranträgen führen kann.
2045	Default-Rollen-definitions- und -zuordnungsaktion nach Hinzufügen von Rollen / Profilen/FFID aus vorhandenen Zuordnungen und Mein Profil	010	009 (Kund:innen-spezifisch ausprägen)	Die konkreten Kriterien für die Suche und Zuordnung von Default-Rollen muss Kund:innen-spezifisch festgelegt werden. Das gilt im Detail auch für die Parameter 2046 bis 2048. Empfohlen wird hier sicherheitshalber der Wert 009 für „Entfernen“ als Voreinstellung.
5021	Prüfe Manager-ID für die spezifische	YES	YES	Im Falle der Geneh-migungspflicht durch

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
	User-ID			den/die Manager:in (Vorgesetzte:n) kann die Pflege im Benutzerantrag automatisiert bzw. mittels Abgleichs mit einem LDAP-/ Corporate-Directory validiert werden. Somit können Fehler in der manuellen oder automatischen Ermittlung von Manager:innen ausgeschlossen werden.

10.4.2.3 Kritische Berechtigungen im Access-Request-Management

Da die Compliance-relevante Ausgestaltung der Komponente insbesondere über die MSMP-Workflows erfolgt, kann unter den kritischen Berechtigungen zur operativen Steuerung oder Verwendung von ARM nur jene genannt werden, die den Zugriff auf die Antragsfunktion selbst ermöglicht. Hier ist insbesondere die Verwendung der Applikation im Unternehmenskontext zu betrachten. Je nach Ausgestaltung der Workflows ist es als unkritisch oder kritisch zu betrachten, wenn Zugriffe beantragt werden können.

Tabelle 51 Berechtigungen – Access-Request-Management

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
GRAC_ REQ	**ACTVT** 01, 02, 36 70	Das Berechtigungsobjekt gewährt mit dieser Ausprägung auf Aktivitätsebene einem Benutzer das Recht, Zugriffsanträge zu stellen. Je nach Ausprägung des Workflows für den Access Request (SAP_GRAC_AC-CESS_REQUEST) ist die Berechtigung als kritisch oder unkritisch zu bewerten.	Nr. 7: „Wer darf Rollen für Zielsysteme via SAP GRC beantragen?“ Die Erstellung von Anträgen für Rollen oder Benutzer wird durch das Berechtigungsobjekt GRAC_REQ gesteuert.
GRAC_ ROLEP	**ACTVT** 78	Dieses Berechtigungs-objekt steuert die Provisionierung der Benutzer und Rollen aus. Je nach Ausprägung werden Rollen zur Beantragung in Zugriffsanträgen angezeigt und können zugeordnet werden.	Nr. 8: „Wer darf Rollen in Zielsystemen via SAP GRC provisionieren?“ Die Provisionierung von Benutzern oder Rollen wird durch das Berech-tigungsobjekt GRAC_ROLEP gesteuert.

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
GRAC_ SYS	**ACTVT** 78	Mit diesem Berechtigungsobjekt können Sie den Zugriff auf bestimmte Konnektoren oder Systeme aussteuern. Je nach Ausprägung werden Systeme zur Beantragung in Zugriffsanträgen angezeigt und können zugeordnet werden.	Nr. 7: „Wer darf Rollen für Zielsysteme via SAP GRC beantragen?“ Die Zuordnung von Systemen in Benutzeranträgen wird durch das Berechtigungsobjekt GRAC_SYS gesteuert.
GRFN_USER	**ACTVT** 02	Diese Berechtigung überschreibt die meisten Berechtigungsobjekte im GRC mit der entsprechenden Aktivität und ist ausschließlich Administrator:innen vorbehalten.	Alle beschriebenen Zugriffsrisiken im ARM.

10.4.3 Prüfung des Business-Role-Management

10.4.3.1 Prozess-Design Business-Role-Management

Mit dem Rollenbau stehen u. a. die in Kapitel 6.2 genannten Risiken in Verbindung. So ist sicherzustellen, dass kritische Berechtigungen nur bedingt vergeben werden oder wesentliche technische Konzepte, die die Integrität der Anwendung erhöhen, verwendet werden (bspw. Berechtigungsgruppen von Tabellen, Konten usw.).

Die GRC-Komponente ermöglicht es, Rollen aus mehreren Systemen an einem zentralen Speicherort zu verwalten. Die Rollen können erstellt, dokumentiert, hinsichtlich SoD-Verletzungen analysiert, genehmigt und anschließend automatisch in den Entwicklungssystemen der an GRC angebundenen SAP-Systeme generiert werden. So kann u. a. die Konsistenz bei der Rollendefinition, -entwicklung, -verwaltung und bei Rollentests standardisiert sichergestellt werden.

Tabelle 52 Prüfungshandlungen: Business-Role-Management

Nr.	Prüfungshandlungen für ein konformes Business-Role-Management
10	Anwendungsbereich für den Rollenerstellungsprozess **Kontrollziel:** Die Ordnungsmäßigkeit der Rollenerstellung ist durch die Zentralisierung von Rollenpflegeoptionen sichergestellt **Risiko:** Eine zentrale Rollenpflege ist nicht sichergestellt. Somit unterstützen die zentralen Parameter und Konfigurationen kein effektives IT-IKS zur Absicherung des eingeschränkten Datenzugriffs.
10.1	Wie ist der Gesamtprozess – von der Beantragung bis zur produktiven Realisierung – zur Erstellung und Änderungen von Rollen definiert? Welche Rollenpflegemöglichkeiten gibt es? Wie sind diese Möglichkeiten eingeschränkt bzw. welche Ausnahmen gibt es hierzu? Hinweis: Der Prozess zur Beantragung von Berechtigungen zur Rollenpflege (nicht Rollenzuordnung!) erfolgt standardmäßig außerhalb der BRM-Komponente. Der Einsatz von BRM beginnt mit der Rollendefinition und anschließender technischer Ausprägung. Im Standard kann ein Genehmigungsworkflow integriert werden, allerdings ist die Rolle dann bereits im Backend angelegt! Welche Zielsysteme (Rollenpflege-Mandant:innen) sind im Anwendungsbereich für BRM hinterlegt? *Check: SPRO > GRC > Gemeinsame Komponenteneinstellungen > Integration Framework > Verbindungseinstellungen bearbeiten. Überprüfen Sie, welche Zielsysteme (Target Connector) für das Integration-Scenario Role-Management „ROLMG“ hinterlegt sind (SAP Tabelle GRFNCONNSCNLK).* *Überprüfen Sie auch die Kennzeichnung der Standard-Mandant:innen pro Konnektorgruppe. Der Absprung aus BRM ist nur auf Standard-Konnektoren systemseitig möglich.* *SPRO > GRC > Access Control > Zuordnung für Aktionen und Konnektorgruppen bearbeiten. Prüfen Sie über „Standardkonnektor der Konnektorgruppe zuordnen“, welche Standardkonnektoren pro Produktions-linie definiert sind.* *Welche Einstiegspunkte gibt es zur BRM-Komponente für die Rollenerstellung (Portal/NWBC) und wer hat darauf Zugriff? > Verweis auf kritische Berechtigungen für die Rollenpflege plus Hinweis für PFCG-Berechtigung im SAP-Backend.* *Überprüfen Sie den Parameter 3009 und 3012, dass diese adäquat gesetzt sind, sodass Transportwege nicht umgangen werden können.*
11	Rollenbereitstellung für die Provisionierung

Nr.	Prüfungshandlungen für ein konformes Business-Role-Management
	Kontrollziel: Die Rollenbereitstellung für die Provisionierung erfolgt ausschließlich über die Rollenpflege via BRM. Ausnahmen sind nachvollziehbar dokumentiert und werden nur eingeschränkt verwendet. **Risiko:** Es werden Rollen für die Benutzer-Provisionierung bereitgestellt, die nicht prozesskonform erstellt sind. Dies kann zu kritischen Zugriffen auf sensible Daten führen.
11.1	Wie erfolgt der Rollenbereitstellungsprozess für die Provisionierung via ARM (auch integrativ mit einem IdM zu berücksichtigen)? Grundsätzliche Voraussetzungen für die Bereitstellung von Rollen über BRM: - Rollenmethodologie ist vollständig abgeschlossen, Rolle ist generiert - Der Rollenstatus ist produktiv - Der Batch-Job „Repository-Objektsynchronisation“ für Rollen ist erfolgreich durchgelaufen Überprüfen Sie die Varianten der Rollenmethodologien. Der letzte Schritt sollte grundsätzlich die Rollengenerierung sein (in Ausnahmefällen gibt es noch ein Testen). Prüfen Sie hierfür die Methodikprozesse und -schritte über folgenden Pfad: *Check: SPRO > GRC > Access Control > Rollenverwaltung > Methodik-prozesse und Schritte definieren* *Prüfen Sie über „Methodikprozesse mit Bedingungsgruppe verbinden“, welche Bedingungen definiert sind, und validieren Sie diese ebenfalls mit der entsprechenden Regel BRF+. Die entsprechende Anwendung BRF+ können Sie über „Bedingungsgruppen den BRFplus-Funktionen zuordnen“ identifizieren (sofern dies angewendet wird).* *Check: Transaktion BRF+ > Suchen Sie Kund:innen-spezifische Anwendung und prüfen Sie über „Ausdruck“, welche Grundformel (bspw. Entscheidungstabelle) als Geschäftsregel hinterlegt ist.* *Prüfen Sie die Rollenstatus, die das Produktivkennzeichen haben.* *Check: SPRO > GRC > Access Control > Rollenverwaltung > Rollenstatus bearbeiten* *Prüfen Sie die Taktung und Konnektorausprägung des o. g. Batch-Jobs sowie die Kontrollaktivität hierzu. Wichtig ist die Synchronität der Rollen aus dem produktiven Zielsystem in das produktive GRC-System.* *Welche Ausnahmeprozesse gibt es zur Bereitstellung von Rollen für die Provisionierung? Wie wird die Rollenimportfunktion verwendet? Prüfen Sie auch den Parameter 3005, ob die Methodologie nach einem Import/Update erzwungen wird.*

Nr.	Prüfungshandlungen für ein konformes Business-Role-Management
	Hinweis: Die Rollenimportfunktion muss in Ausnahmefällen zur Verfügung stehen, sollte allerdings sehr restriktiv vergeben werden, da Genehmigungsprozesse und Risikoanalysen umgangen werden können. Wer hat die Berechtigung zur Durchführung von Rollen-Imports/Uploads? (siehe auch **Fehler! Verweisquelle konnte nicht gefunden werden.** kritische Berechtigungen für BRM)
12	Genehmigung in der Rollenpflege **Kontrollziel:** Es ist ein Kontrollprozess in die Rollenpflege integriert, sodass adäquate Genehmigungen im Prozess sichergestellt sind, bevor diese zur Provisionierung bereitgestellt werden. **Risiko:** Die Rollenerstellung erfolgt nicht sachgemäß entsprechend den fachlichen Anforderungen und gemäß einem 4-Augen-Prinzip zur Vermeidung von Abweichungen des Minimalprinzips.
12.1	Wie ist der Genehmigungsprozess in die Rollenpflege integriert (soweit dies über BRM abgebildet wird)? Überprüfen Sie die Varianten der Rollenmethodologien. Grundsätzlich sollte der Genehmigungsschritt integriert sein. Prüfen Sie hierfür die Methodik-prozesse und -schritte über folgenden Pfad: *Check: SPRO > GRC > Access Control > Rollenverwaltung > Methodik-prozesse und Schritte definieren. Prüfen Sie auch hier die Regel BRF+, wie oben beschrieben.* *Überprüfen Sie den Rollengenehmigungsprozess in MSMP und die entsprechende Regel BRF+ (sofern dies verwendet wird), welche Genehmigungsstufen vorhanden sind.* *Check: SPRO > GRC > Access Control > Workflow für Access Control > MSMP-Workflows bearbeiten, prüfen Sie die Prozess-ID „SAP_GRAC_ROLE_APPR“ (im Standard) oder den Kund:innen-eigenen Rollengenehmigungsprozess unter Schritt 5 „Pfade bearbeiten“, welche Pfade, Genehmigungsstufen und Bearbeitende hinterlegt sind. Im Standard sollte ein einstufiger Genehmigungsprozess über den Rolleneigner / die Rolleneigner:in (Role Content Approver) umgesetzt sein. Prüfen Sie ebenfalls die dazugehörige Regel BRF+, sofern dies verwendet wird.*

Nr.	Prüfungshandlungen für ein konformes Business-Role-Management
	Sofern der Standard verwendet wird, prüfen Sie, welche Rolleneigner:innen im NWBC (Portal) hinterlegt sind. *Check1: NWBC > Einrichtung > Zugriffsverantwortliche > Access-Control-Verantwortliche, prüfen Sie im ersten Schritt, welche Benutzer grundsätzlich als Rollenverantwortliche hinterlegt sind.* *Check2: NWBC > Einrichtung > Zugriffsverantwortliche > Rollenverantwortliche, wie das Mapping der Bedingungsgruppen aus BRF+ zu den Rolleneigner:innen umgesetzt ist.* Die Genehmigenden-Ermittlung muss lückenlos und adäquat sein. Voraussetzung für die Durchführung von Aktionen der Genehmigenden ist neben der Pflege der Rolleneigner:innen im NWBC auch die Zuordnung entsprechender Rollen im GRC-Backend.
13	Konfliktfreie Rollen in der Rollenpflege und -zuordnung **Kontrollziel:** Risiken in der Rollenerstellung werden erkannt und präventiv bereinigt. Dies erfolgt durch systemseitige Applikationskontrollen, die die Bereitstellung von konfliktären Rollen für die Benutzerzuordnung ausschließen. **Risiko:** Konflikte in der Rollenpflege werden nicht aufgedeckt bzw. ausgeschlossen; daher ist die Risikovermeidung in der Rollenzuordnung nicht oder nur schwer möglich.
13.1	Wie werden Risiken in der Rollenpflege aufgedeckt? Ist die Risikoanalyse in die BRM-Methodik integriert? Wird systemseitig ausgeschlossen, dass risikobehaftete Rollen für die Benutzer-Zuordnung bereitstehen? *Check: SPRO > GRC > Access-Control > Rollenverwaltung > Methodik-prozesse und Schritte definieren. Prüfen Sie, ob es eine BRM-Methodik gibt, die die Risikoanalyse nicht enthält. Zu beachten sind auch die Steuerungs-elemente über BRF+, sofern es Methoden ohne Risikoanalysen gibt.*
13.2	Wie wird ausgeschlossen, dass SoD-konfliktäre Rollen für die Benutzer-Provisionierung zur Verfügung stehen? Welche Maßnahmen gibt es zur Zulassung von konfliktären Rollen, bspw. für Technische Benutzer oder Notfallbenutzer? *Systemseitige Applikationskontrollen werden über die Konfigurationseinstellungen gesteuert. Prüfen Sie entsprechende Parameter 3011 sowie 3014 bis 3018.*

Nr.	Prüfungshandlungen für ein konformes Business-Role-Management
	Durch die Rollenimport- oder Rollenminderungsfunktion können risikobehaftete Rollen dennoch zugelassen werden. Wer hat diese Berechtigungen? Welche Rollen wurden im Prüfungszeitraum mitigiert? *Check: NWBC > Zugriffsverwaltung > Risikominderung auf Zugriffsebene > Risikominderung auf Rollenebene*

10.4.3.2 Sicherheitskritische Parameter für das Business-Role-Management

Im Folgenden finden Sie die wesentlichen Konfigurations-Parameter für das Business-Role-Management. Neben dem vorkonfigurierten Standardwert wird auch eine Best-Practice-Empfehlung gegeben. Selbstverständlich ist letztere Kund:innen-individuell zu betrachten.

Tabelle 53 Konfigurationsparameter – Business-Role-Management

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
3005	Bei der Änderung von Rollen-attributen Rollenmethodik zurücksetzen	YES	YES	Dieser Parameter legt fest, ob der Schritt der Rollenmethodik nach einer Massenaktualisierung auf den ersten Schritt zurückgesetzt wird (Schritt-Definition). Dies wird empfohlen, um die Erstellung von Massengenehmigungs aufträgen zu vermeiden.
3006	Hinzufügen / Löschen von Funktionen zu einer Berechtigung erlauben	YES	Kund:innen-spezifisch ausprägen	Ob der Button zum Hinzufügen/Löschen von Funktionen für Rollen angezeigt werden soll oder nicht, kann Kund:innen-spezifisch ausgeprägt werden.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
3007	Bearbeitung von Werten der Organisations-ebenen für abgeleitete Rollen erlauben	NO	Kund:innen-spezifisch ausprägen	Ob das Bearbeiten von Org-Werten für abgeleitete Rollen im BRM möglich sein soll oder nicht, kann Kund:innen-spezifisch ausgeprägt werden.
3008	Nach Berechtigungs-datenände-rungen ist eine Ticketnummer erforderlich	YES	YES	Aufgrund der besseren Nachvollziehbarkeit bei der Anpassung von Rollen wird das obligatorische Hinterlegen eines Tickets empfohlen.
3009	Löschen der Rolle vom Backend zulassen	YES	NO	Für das Löschen von Rollen wird der Transportweg empfohlen.
3010	Anhängen von Dateien zur Rollendefinition zulassen	YES	YES	Das Anhängen von Anforderungen, von Testdokumentationen oder von Freigaben an Rollen wird zu Dokumentations-zwecken empfohlen.
3011	Risikoanalyse vor Rollen-erzeugung ausführen	YES	YES	Die Risikoanalyse vor der Rollenerzeugung automatisch durchzuführen wird empfohlen.
3012	Rollenerzeu-gung für mehrere Systeme zulassen	NO	NO	Für das Verteilen von Rollen wird der Transportweg empfohlen.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
3013	Credentials des angemeldeten Benutzers für Rollen-erzeugung verwenden	NO	YES	Für mehr Transparenz bei der Erzeugung von Rollen sollte der entsprechende Benutzer sichtbar sein.
3014	Rollenerzeu-gung mit SoD-Verletzungen auf Berechti-gungsebene zulassen	NO	NO	Empfehlung: Keine SoD-Risiken auf Rollenebene erlauben.
3015	Rollenerzeu-gung mit kritischen Be-rechtigungen zulassen	NO	YES	Um technische Rollen zu generieren, sollte diese Option angeschaltet bleiben und nachträglich mitigiert werden.
3016	Rollenerzeu-gung mit SoD-Verletzungen auf Aktions-ebene zulassen	NO	NO	Empfehlung: Keine SoD-Risiken auf Rollenebene erlauben.
3017	Rollener-zeugung mit kritischen Aktionen zulassen	NO	YES	Um technische Rollen zu generieren, sollte diese Option angeschaltet bleiben und nachträglich mitigiert werden.
3018	Rollenerzeu-gung mit SoD-Verletzung bei Rollen/Profile zulassen	NO	NO	Empfehlung: Keine SoD-Risiken auf Profilebene erlauben.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
3019	Risikoanalyse-ergebnis einer Einzelrolle bei Massenrisiko-analyse überschreiben	NO	YES	Dies erfolgt individuell pro Rolle; es werden nicht alle Rollen automatisch über-schrieben.
3020	Erinnerungs-benachrich-tigung zu Rollenzertifi-zierung	10	Kund:innen-spezifisch ausprägen	Dieser Parameter legt fest, wie viele Tage vor dem Datum der nächsten Zertifizierung eine Erinnerung an die Rolleneigner:innen gesendet wird.
3021	Verzeichnis für Serverdateien des Massen-rollenimports	<empty>	<empty>	Der Import von Rollen über die Serverdateien wird nicht empfohlen.
3024	Methodik-prozess für abgeleitete Rollen bei Generierung erzwingen	YES	Kund:innen-spezifisch ausprägen	Ob abgeleitete Rollen aus anderen Stufen bei der Generierung der Master-Rolle angezeigt werden oder nicht, kann Kund:innen-spezifisch ausgeprägt werden.
3025	Selektion der Organisations-wertzuord-nungen ohne führende Organisation erlauben	NO	NO	Ein Definieren der führenden Organisa-tion für die Ableitung der Rollen wird empfohlen.
3026	Details der Rollendefinition	YES	Kund:innen-spezifisch ausprägen	Beim Kopieren der Rolle kann die

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
	und -zuord-nung beim Kopieren der Rolle sichern			Rollendefinition mitkopiert werden.
3027	Kopie der Berechtigun-gen von der Master-Rolle auf neu abge-leitete Rollen automatisieren	NO	Kund:innen-spezifisch ausprägen	Beim Erstellen der abgeleiteten Rollen können die Berech-tigungen der Master-Rolle automatisch mitkopiert werden.
3028	Abgeleitete Rollen nach anlegen/ aktualisieren generieren	NO	NO	Die explizite und nicht automatische Rollen-generierung von abgeleiteten Berech-tigungen wird empfohlen.
3029	Benutzer informieren, wenn Benutzer-Rollen-zuordnung sich ändert	NO	NO	Alle zugeordneten Benutzer einer Business-Rolle zu informieren, wenn sich eine Rollenzuordnung bei anderen Benutzern ändert, wird nicht empfohlen.
3030	Rollengeneh-migungsan-forderung initiieren mit	YES	YES	Einen Genehmigenden für den Rolleninhalt einer Business-Rolle

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
	obligato-rischem Genehmigen des Rolleninhalts			festzulegen wird empfohlen.
3040	Eine Ticketnummer ist erforderlich für alle Rollen-änderungen	NO	YES	Für eine bessere Nachvollziehbarkeit bei der Anpassung von Rollen wird das obligatorische Hinterlegen eines Tickets empfohlen. Wenn der Parameter 3040 auf YES steht, dann ist 3008 obsolet.
3041	Obligatorische Risikoanalyse während Rollenpflege durchführen	NO	YES	Die Risikoanalyse muss während der Rollenpflege verpflichtend durchgeführt werden.
3042	Rollener-zeu-gung mit Risiken nicht zulassen	NO	Kund:innen-spezifisch ausprägen	Eine Rollenerzeugung mit Risiken ist nur dann nicht zuzulassen, wenn die Generierung in Test- oder Produktiv-Systemen erfolgt und nicht über den Transportweg passiert.
4011	Technische Rollen löschen, wenn sie Teil der Business-Rollen sind	YES	NO	Die technischen Rollen einzeln zu löschen, während sie als Teil einer Business-Rolle

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				zugewiesen sind, wird nicht empfohlen.
4016	Nur die genehmigte/abgeschlossene Version der Benutzerrolle für die Rollendefinition und -zuordnung berücksichtigen	NO	YES	Nur genehmigte bzw. abgeschlossene Business-Rollen sollten Benutzer zugewiesen werden.
4019	Keine manuellen Rollenzuordnungsänderungen während der Repository-Synchronisation kopieren.	NO	NO	Aus Gründen der Transparenz wird die Synchronisation von allen Rollenzuordnungen in das GRC empfohlen.
4022	Synchronisierung zukünftiger Zuordnungen ist obligatorisch	NO	YES	Aus Gründen der Transparenz wird die Synchronisation von allen Rollenzuordnungen in das GRC empfohlen.
4023	Benutzer-Rollenzuordnungen aus IdM synchronisieren	NO	Kund:innen-spezifisch ausprägen	Wenn ein IdM genutzt wird, erlaubt dies die Synchronisation der Business-Rollen aus dem IdM in das GRC.

10.4.3.3 Kritische Berechtigungen im Business-Role-Management

Die Berechtigungen zur Steuerung der Komponente und deren wesentlicher Funktionen erfolgen über eine überschaubare Anzahl von Berechtigungsobjekten und

Feldwerten. Die hierin als kritisch und prüfungsrelevant zu betrachtenden werden im Folgenden beschrieben. Der Bezug zu den in 2.4.3.1 genannten Risiken wird hergestellt.

Tabelle 54 Berechtigungen – Business-Role-Management

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
GRAC_ ASIGN	**ACTVT** 01, 02, 06, 36, 70 **GRAC_OWN_T** ROLE	Im NWBC können mit der Funktion „Access-Control-Verantwortliche“ Mitarbeitende zu Rollenbeauftragten ernannt werden. Diese Ernennung ist verpflichtend, um Mitarbeitende in BRM als Verantwortliche spezifischen Rollen zuordnen zu können.	Nr. 10: „Wie ist der Gesamtprozess – von der Beantragung bis zur produktiven Realisierung – zur Erstellung und zu Änderungen von Rollen definiert?“ Prüfung, welcher Mitarbeitende über die Rechte zur Ernennung von Rollen-beauftragten verfügt.
GRAC_ RLMM	**ACTVT** 38 **GRAC_RLMMT** 01 (Massen-rollenimport), 02 (Massen-rollenaktualisie-rung) 03 (Massen-rollenableitung), 04 (Massen-aktualisierung abgeleiteter Rollen),	Die Berechtigung erlaubt den Zugriff auf die Massenbearbeitungs-funktionen in BRM. Die Ausprägung 06 zur Massenrollengenerie-rung erlaubt die Aktivierung mehrerer Rollen in Produktion in einem Schritt. Ist der Workflow zur genehmigungspflich-tigen Bearbeitung von Rollen (SAP_GRAC_ ROLE_APPR)	Nr. 11: „Welche Ausnahmeprozes se gibt es zur Bereitstellung von Rollen für die Provisionierung? Wie wird die Rollenimport-funktion verwendet?“ Prüfen Sie auch den Parameter 3005, ob die

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
	06 (Massenrollen-generierung)	deaktiviert, so können massenhaft auf ihre Inhalte hin ungeprüfte Rollen in Produktion begeben (Massenrollen-generierung mit GRAC_RLMMT - 06) oder massenhaft Änderungen an Rollen durchgeführt werden (GRAC_RLMMT - 02). Auch sind die Rechte zur Ausführung des Massenrollenimports, der -ableitung und der Massenaktualisierung abgeleiteter Rollen restriktiv zu betrachten.	Methodologie nach einem Import/Update erzwungen wird. Hinweis: Die Rollenimport-funktion muss in Ausnahmefällen zur Verfügung stehen, sollte allerdings sehr restriktiv ver-geben werden, da Genehmi-gungsprozesse und Risiko-analysen umgangen werden können.“ Unter anderem der Massen-import von Rollen wird mit der entsprechenden Ausprägung des Objekts GRAC_RLMM erlaubt. Eine Prüfung auf die Vergabe von Import-Rechten hat zu erfolgen. Sind die Berech-tigungen wie in den beschriebe-nen Ausnahme-prozessen restriktiv ver-geben?

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
GRAC_ MITC	**ACTVT** 01, 02, 06, 78, 88	Die Berechtigung erlaubt die Anlage, Bearbeitung und Zuordnung von mitigierenden Kontrollen zu Risiken. Mit der Berechtigung zur Bearbeitung und Zuordnung von mitigierenden Kontrollen wird im Kontext von BRM die Anpassung von Kontrollen an möglicherweise kritische Rolleninhalte ermöglicht. Dies gilt, sofern die Workflows zur genehmigungspflichtigen Änderung von mitigierenden Kontrollen (SAP_GRAC_CONTROL_MAINT) und zur genehmigungspflichtigen Zuordnung von mitigierenden Kontrollen (SAP_GRAC_CONTROL_ASGN) deaktiviert sind.	Nr. 13: „Welche Maßnahmen gibt es zur Zulassung von konfliktären Rollen, bspw. für Technische Benutzer oder Notfallbenutzer?“ Nachgelagerte Kontrollen können auch im BRM-Kontext direkt Rollen und den darin aufgedeckten Risiken zugeordnet und dokumentiert werden. Das Berechtigungsobjekt erlaubt Rückschlüsse über den Umfang der Bearbeitungs- und Zuordnungs-Rechte von mitigierenden Kontrollen.
GRAC_ ROLED	**GRAC_ACTRD** 01, 02, 06, 64, V7	Das Berechtigungsobjekt steuert die Rollenadministration im Front-End. Wird BRM genutzt, erlaubt die Vergabe der Feldwerte in GRAC_ACTRD je nach Ausprägung sowohl die Anlage als	Nr. 10: „Wie ist der Gesamtprozess – von der Beantragung bis zur produktiven Realisierung – zur Erstellung und zu

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
		auch das Generieren von Rollen. Über GRAC_ROLE findet die Aussteuerung statt, für welche Rollen die Aktivitäten der Anlage, Bearbeitung, Generierung etc. vorgenommen werden können. Dieser Feldwert eignet sich damit zur organisatorischen Eingrenzung des Rollenadministrators / der Rollenadministra-torin. Prüfen Sie, ob ausgeschlossen ist, dass derjenige/ diejenige, der/die die Rolle erstellt und bearbeitet, gleichzeitig als Rolleneigner:in zugeordnet werden kann.	Änderungen von Rollen definiert?“ Die Möglichkei-ten von der Bearbeitung der Rollen-Metadaten (Prozesse, Projekt, Name, Beschreibung, Profilname usw.), das Ableiten der Rolle bis hin zum Generieren werden über die Ausprägungen des Objekts GRAC_ROLED gesteuert. Eine Prüfung auf Feldwertebene erlaubt Rück-schluss darauf, welcher Mitarbeitende über Bearbei-tungs-, Lösch- oder Generie-rungsrechte verfügt.
GRAC_ CROLE	**ACTVT** 01, 02, 16, 78	Mit diesem Berech-tigungsobjekt können Sie den Zugriff auf SoD-kritische Rollen aus-steuern. Je nach Ausprägung dürfen SoD-kritische Rollen im BRM	Nr. 13: „Welche Maßnahmen gibt es zur Zulassung von konfliktären Rollen, bspw. für Technische Benutzer oder Notfallbenutzer?“

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
		angelegt, geändert oder zugeordnet werden. Prüfen Sie, ob ausschließlich administrativ tätige Benutzer im GRC dieses Recht haben?	Die Generierung von SoD-kritischen Rollen im BRM wird durch das Berechtigungsobjekt GRAC_CROLE gesteuert.
GRAC_ CPROF	**ACTVT** 01, 02, 16, 78	Mit diesem Berechtigungsobjekt können Sie den Zugriff auf SoD-kritische Profile aussteuern. Je nach Ausprägung dürfen SoD-kritische Profile im BRM angelegt, geändert oder zugeordnet werden. Prüfen Sie, ob ausschließlich administrativ tätige Benutzer im GRC dieses Recht haben.	Nr. 13: „Welche Maßnahmen gibt es zur Zulassung von konfliktären Rollen, bspw. für Technische Benutzer oder Notfallbenutzer?“ Die Generierung von SoD-kritischen Profilen im BRM wird durch das Berechtigungsobjekt GRAC_CPROF gesteuert.
GRFN_USER	**ACTVT** 02	Diese Berechtigung überschreibt die meisten Berechtigungsobjekte im GRC mit der entsprechenden Aktivität und ist ausschließlich Administrator:innen vorbehalten.	Alle beschriebenen Zugriffsrisiken im BRM.

10.4.4 Prüfung der Access-Risk-Analysis

10.4.4.1 Prozess-Design Access-Risk-Analysis

ARA bietet die Möglichkeit, mithilfe eines zu definierenden Regelwerks Zugriffsrisiken zu erkennen und ggf. Kontrollen zur Risikominderung zuzuordnen. Das Regelwerk als zentraler Bestandteil für alle Kernfunktionalitäten von SAP GRC Access Control bestimmt maßgeblich, inwieweit die Compliance technisch unterstützt werden kann.

Folgende Kernfunktionen stehen mit ARA zur Verfügung:

- Verwaltung des Regelwerks inklusive aller Regeln und Funktionen/ Funktionstrennungsmatrix (SoD-Matrix)
- Bereitstellung der Analysefunktion in verschiedenen Bereichen wie z. B. in der Provisionierung, im Rollenmanagement etc.
- Erstellen von Berichten über aufgetretene Konflikte für verschiedene Zielgruppen wie z. B. Management, IT, Audit etc.
- Definition von risikomindernden Kontrollen (Mitigation)

Damit ist ARA integraler Bestandteile der drei im Vorhinein vorgestellten Funktionen und Prozesse des Emergency-Access-Managements, des Access-Request-Managements und des Business-Role-Managements. Die in den Vorkapiteln vorgestellten Prüfungshandlungen beziehen damit ARA bereits zum Teil mit ein.

Die im Folgenden speziell für ARA vorgestellten Prüfungshandlungen sind technisch geprägt und beziehen sich insbesondere auf die Prozesse der Definition, Erstellung und Verwaltung jener Risiken, Regeln und Kontrollen, die integral für die Benutzer- und Rollenverwaltung sind.

Tabelle 55 Prüfungshandlungen: Access-Risk-Analysis

Nr.	Prüfungshandlungen für eine konforme Access-Risk-Analysis
14	Veränderung von Funktionen des Regelwerks **Kontrollziel:** Es ist sicherzustellen, dass Funktionsänderungen nicht ungeprüft in der Produktion erfolgen. **Risiko:** Funktionen des Regelwerks werden zulasten der Prüfung kritischer Berechtigungen und SoD verändert. Als Folge daraus werden SoD-Risiken und kritische Berechtigungen in Rollen und Benutzer neu provisioniert und für bestehende Provisionierungen nicht mehr erkannt, da die integrierte Kontrolle in BRM sowie in ARM nicht möglich ist.
14.1	Jeder/Jede Mitarbeitende im GRC, der/die Inhaber:in der Rolle zur Funktionsgenehmigung ist (im Standard: SAP_GRAC_FUNCTION_ APPROVER), kann Änderungen von Funktionen des Regelwerks

Nr.	Prüfungshandlungen für eine konforme Access-Risk-Analysis
	genehmigen. Eine solche Genehmigung hat direkte Auswirkung sowohl auf den Rollenbau-, den Provisionierungs- als auch den Mitigierungsprozess. Ist der Prozess des Funktionsbaus aktiviert? Falls ja: *Wer verfügt über die Berechtigung zur Genehmigung von Funktionsänderungen (Zuweisung einer Einzelrolle, Auflistung im Rollenkonzept)? Wer genehmigt die Änderung welcher Funktion? Überprüfung der Funktionsänderungsaufträge in der GRC-Anforderungsübersicht, Prozess-ID „Workflow zur Funktionsgenehmigung“. Stichprobenartige Überprüfung der konkreten Änderungen in der Änderungshistorie der Funktion selbst.* Falls nein: *Gibt es ein systemunabhängiges Verfahren für die Beantragung von Funktionsänderungen? Wie werden Genehmigungen nachgehalten? Überprüfung der Veränderungen anhand der Änderungshistorie und Abgleich mit dem systemunabhängigen Papierverfahren zur Funktionsänderung.* Hinweis: Da es im Standard nicht möglich ist, die Funktionen einzelnen fachlichen Expert:innen zuzuweisen, sollte die Genehmigungsstufe bei einer zentralen Compliance-Instanz liegen. Die inhaltliche Beurteilung und Freigabe einer etwaigen Funktionsänderung muss auf anderem Wege erfolgen, bspw. in einem Gremium aus Fachbereich, IT und Compliance.
15	Veränderung von Risiken des Regelwerks **Kontrollziel:** Es ist sicherzustellen, dass Risikoänderungen nicht ungeprüft in der Produktion erfolgen. **Risiko:** Risiken des Regelwerks werden zulasten der Prüfung kritischer Berechtigungen und SoD in ihrem Risikolevel herabgestuft oder in der Kombination aus relevanten Funktionen verändert. Als Folge daraus werden unter Umständen SoD-Risiken und kritische Berechtigungen Rollen hinzugefügt und Benutzer mit solchen Risiken provisioniert, da u. U. für herabgestufte Risiken geringere Anforderungen an Mitigation und Vermeidung gestellt werden.
15.1	Ist der Workflow der Risikobearbeitung und -genehmigung aktiviert? Falls ja: *Wer ist der zugeordnete Risikoverantwortliche? Wie viele unterschiedliche Risikoverantwortliche gibt es? Wurde ein 4- oder 6-Augen-*

Nr.	Prüfungshandlungen für eine konforme Access-Risk-Analysis
	Prinzip bei der Beantragung und Freigabe von Risiko-Änderungen eingehalten? Überprüfung der Risikoänderungsaufträge in der GRC-Anforderungsübersicht, Prozess-ID „Workflow zur Risikogenehmigung“. Falls nein: *Gibt es ein systemunabhängiges Verfahren für die Beantragung von Risikoänderungen? Wie werden Genehmigungen nachgehalten? Überprüfung der Veränderungen anhand der Änderungshistorie und Abgleich mit dem systemunabhängigen Papierverfahren zur Risikoänderung.*
16	Löschen des Regelwerks **Kontrollziel:** Es ist sicherzustellen, dass nur ausgewählte Mitarbeitende Zugriff auf die Upload-Funktion haben. Regelwerksänderungen unterliegen der Dokumentation und Freigabe. **Risiko:** Für die Pflege des Regelwerks in Produktion gibt es grundsätzlich zwei Möglichkeiten. Entweder erfolgt die Bearbeitung in der Entwicklung mit anschließendem Transport bis in die Produktion, oder aber die Änderungen erfolgen in der Produktion direkt durch Nutzung des NWBCs und ggf. der Upload-Funktion in der SPRO. Ein signifikantes Risiko der Löschung besteht bei Nutzung der Upload-Funktion. Eine Löschung hat temporär zur Folge, dass kein Regelwerk in Produktion zur Verfügung steht. Benutzer- und Rollenprüfungen im Hinblick auf ihr Rechteset finden dann nicht statt.
16.1	Werden Massenänderungen im Regelwerk unabhängig vom System z. B. in TXT-Details gepflegt und in die Produktion hochgeladen, erfolgt dies durch Nutzung der Zugriffsberechtigung auf die Transaktion GRAC_UPLOAD_RULES. *Erstellung einer Übersicht aller Mitarbeitenden mit Zugriff auf die Transaktion GRAC_UPLOAD_ RULES in Produktion. Wird prozessual zwischen kleinteiligen Änderungen des Regelwerks und Massenänderungen unterschieden? Gibt es für Massenänderungen einen Prozess unter Nutzung der Upload-Funktion? Wie wird sichergestellt, dass in Produktion keine Überschreibung des Regelwerks mit versehentlicher Löschung der Inhalte erfolgen kann?* Hinweis: Bei Upload des Regelwerks gibt es zwei unterschiedliche Optionen zur Wahl: Anhängen und Überschreiben. Bei Ersterem werden die hochgeladenen Regeln dem bestehenden Regelwerk hinzugefügt. Bei Auswahl

Nr.	Prüfungshandlungen für eine konforme Access-Risk-Analysis
	von „Überschreiben“ werden sämtliche bereits bestehenden Regeln gelöscht; nur die Inhalte der Upload-Datei gelangen in die Produktion.
17	Zugriff auf die Details der Prüfungslogik **Kontrollziel:** Es ist sicherzustellen, dass nur ein ausgewählter Kreis von Mitarbeitenden Zugriff auf diese Funktionen erhält. **Risiko:** SAP GRC stellt eine Funktion zur Verfügung, um das gesamte Regelwerk und somit die Prüflogik aus dem System herunterzuladen. Die Detailansicht ermöglicht Rückschlüsse darauf, gegen welche Berechtigungsrisiken geprüft wird und wie diese Prüfung umgangen werden kann. Ebenso werden Berichte zur Verfügung gestellt, die Rückschlüsse auf die implementierte Prüfungslogik zulassen. Ein irregulärer Zugriff auf die Prüfungsdetails des Systems ist zu verhindern.
17.1	Jeder/Jede Mitarbeitende im GRC, der/die Zugriff auf die Funktion zum Download des Regelwerks hat, kann die empfindlichen Informationen beziehen. Erstellung einer Übersicht der Mitarbeitenden mit Zugriff auf die Transaktion GRAC_DOWNLOAD_RULES.
18	Nachgelagerte Kontrolle von Risiken **Kontrollziel:** Bekannte und eingegangene Berechtigungsrisiken sind durch nachgelagerte Kontrollen zu mitigieren. **Risiko:** Nachgelagerte Kontrollen dienen der Mitigation von Berechtigungsrisiken, die u. a. aufgrund der organisatorischen Struktur eingegangen werden.
18.1	Ist der Workflow der Risiko-Mitigation aktiviert (also der Zuordnung von mitigierenden Kontrollen zu Risiken)?

Nr.	Prüfungshandlungen für eine konforme Access-Risk-Analysis
	Falls ja: Wie werden die Mitigations-Verantwortlichen ernannt (Überprüfung der Kontroll-Zuordnungsaufträge in der GRC-Anforderungsübersicht, Prozess-ID „Workflow für Kontrollzuordnungsgenehmigung“, Export einer Übersicht der aktuellen Mitigations-Verantwortlichen)? Wie erfolgen Anlage, Änderung und Review der Kontrollen bzw. Kontrollinhalte? Finden die Prüfaktivitäten mit einer geeigneten Frequenz statt? (Registerkarte „Berichte“ innerhalb der mitigierenden Kontrolle und hierin das Feld „Häufigkeit in Tagen“. Der Feldwert 2 bedeutet als Beispiel, dass die Kontrolle alle 2 Tage stattfindet.) *Falls nein: Wie erfolgt die Dokumentation und Beschreibung von Mitigations-Aktivitäten? Wie erfolgt die Ernennung der Verantwortlichen? Mit welcher Frequenz werden die Kontrollaktivitäten durchgeführt?*
19	Änderung nachgelagerter Kontrollen von Risiken **Kontrollziel:** Es ist sicherzustellen, dass Kontrolländerungen nicht ungeprüft in der Produktion erfolgen. **Risiko:** Nachgelagerte Kontrollen, die der Mitigation bekannter Berechtigungsrisiken dienen, werden inhaltlich zulasten der Prüf-Effektivität und -Effizienz verhindert.
19.1	Ist der Workflow der Kontroll-Bearbeitung aktiviert (also der prozessgesteuerten Anlage und Änderung von Kontrollen)? *Falls ja: Welche Kontrolländerungen erfolgten im Betrachtungszeitraum? Überprüfung der Kontroll-Bearbeitungsaufträge in der GRC-Anforderungsübersicht, Prozess-ID „Workflow zur Bearbeitung der mindernden Kontrolle“, Export der Kontrolländerungen.* *Wie wurden die Kontrolländerungen dokumentiert und freigegeben?* *Falls nein: Wie erfolgen die Beantragung, Durchführung und Freigabe von Änderungen an den Kontrollinhalten? Wer ist berechtigt, Änderungen durchzuführen?*

10.4.4.2 Sicherheitskritische Parameter für Access-Risk-Analysis

Im Folgenden finden Sie die wesentlichen Konfigurations-Parameter für die Access-Risk-Analysis. Neben dem vorkonfigurierten Standardwert wird auch eine Best-Practice-Empfehlung gegeben. Selbstverständlich ist Letztere Kund:innen-individuell zu betrachten.

Tabelle 56 Konfigurationsparameter – Access-Risk-Analysis

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
1001	Funktionsände-rungsprotokoll aktivieren	YES	YES	Die Änderungsproto-kollierung für Funktionen sollte angeschaltet sein.
1002	Risikoänderungs-protokoll aktivieren	YES	YES	Die Änderungsproto-kollierung für Risiken sollte angeschaltet sein.
1003	Organisationsregel-protokoll aktivieren	YES	YES	Die Änderungsproto-kollierung für Organisations-regeln sollte angeschaltet sein.
1004	Zusatzregelproto-koll aktivieren	YES	YES	Die Änderungsproto-kollierung für Zusatzregeln sollte angeschaltet sein.
1005	Protokoll für kritische Rolle aktivieren	YES	YES	Die Änderungsproto-kollierung für kritische Rollen sollte angeschaltet sein.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
1006	Protokoll für kritisches Profil aktivieren	YES	YES	Die Änderungs-protokollierung für kritische Profile sollte angeschaltet sein.
1007	Regelwerk-Änderungsprotokoll aktivieren	YES	YES	Die Änderungs-protokollierung für Regelwerke sollte angeschaltet sein.
1008	Rollenänderungs-protokoll aktivieren	YES	YES	Die Änderungs-protokollierung für Rollenänderungen sollte angeschaltet sein.
1011	Standardablaufzeit für Zuordnungen zu mindernden Kontrollen (in Tagen)	365	Kund:innen-spezifisch ausprägen	Die Standard-Anzahl an Tagen bis zum Ablauf einer Mitigation kann Kund:innen-spezifisch ausgeprägt werden. Sie kann jeweils bei der Zuordnung überschrieben werden.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
1012	Regel-ID auch für Minderungszuord-nung berücksich-tigen	NO	YES	Die spezifische und nicht allge-meine Mitigation von Risiken wird empfohlen.
1013	System für Minde-rungszuordnung berücksichtigen	NO	YES	Die spezifische und nicht allgemeine Mitigation von Risiken wird empfohlen.
1014	Separate Berech-tigungsprüfung für Minderung aus Zugriffsanforderung aktivieren	NO	YES	Das Zwischenspeichern der Mitigationen während Access-Requests sorgt dafür, dass die Mitigation nicht fälschlicherweise bestehen bleibt.
1015	Ungültigen Minderungsbericht aus Kurzzusam-menfassung akti-vieren	NO	Kund:innen-spezifisch ausprägen	Mit diesem Parameter können Sie die Offline-Daten aus der Tabelle Management Summary abrufen. Diese Einstellung aus Performance-Gründen kann Kund:innen-spezifisch ausgeprägt werden.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
1016	Anzahl von ungültiger Minderungsbereinigung ausgeschlossener Tage angeben	0	Kund:innen-spezifisch ausprägen	Wie lange ungültige Mitigationen von der Bereinigung ausgeschlossen werden sollen, kann Kund:innen-spezifisch ausgeprägt werden.
1021	Organisationsregeln für andere Anwendungen berücksichtigen	NO	Kund:innen-spezifisch ausprägen	Ob Organisationsregeln für andere Anwendungen berücksichtigt werden sollen oder nicht, kann Kund:innen-spezifisch ausgeprägt werden.
1022	Konnektor, für den Objekt-IDs von Groß-/Kleinschreibung abhängig bearbeitet werden können	<empty>	Kund:innen-spezifisch ausprägen	Welche Konnektoren Case-sensitive Einträge haben, muss Kund:innen-spezifisch ausgeprägt werden.
1023	Standardberichtsart für Risikoanalyse	2	1-4	Als Standard sind die Berichte 1-4 empfehlenswert.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				Um mehr als einen Eintrag vorzunehmen, muss der Parameter mehrfach gepflegt werden.
1024	Standardrisikostufe für Risikoanalyse	2	5	Es wird empfohlen alle Risikostufen bei der Risikoanalyse zu berücksichtigen.
1025	Standardregelwerk für Risikoanalyse	<empty>	Kund:innen-spezifisch ausprägen	Wenn vorhanden, sollte das zentrale Regelwerk als Standard hinterlegt werden.
1026	Standardtyp von Benutzern für Risikoanalyse	A	A	Die Dialog-Benutzer sollten als Default-Wert für die Risikoanalyse hinterlegt werden.
1027	Offline-Risikoanalyse aktivieren	NO	NO	Es wird empfohlen, die Risikoanalyse online durchzu-führen. Ein YES erfordert sonst die

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				dauerhafte Ein-planung der Batch-Risikoanalyse für aktuelle Ergeb-nisse.
1028	Abgelaufene Benutzer einschließen	NO	YES	Das standard-mäßige Einschlie-ßen von abgelau-fenen Benutzern bei der Risikoanalyse wird empfohlen.
1029	Gesperrte Benutzer einschließen	NO	YES	Das standardmäßige Einschließen von gesperrten Benutzern bei der Risikoanalyse wird empfohlen.
1030	Geminderte Risiken einschließen	NO	Kund:innen-spezifisch ausprägen	Das standardmäßige Einschließen von Risiken mit Mitigationen bei der Risikoanalyse ist nicht zwingend nötig.
1031	Kritische Rollen und Profile ignorieren	YES	NO	Die als kritisch bekannten Rollen und Profile sollten bei jeder Risikoanalyse berücksichtigt werden – speziell

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				dann, wenn diese an nicht berechtigte Benutzer vergeben werden.
1032	Bei Benutzer-analyse Referenz-benutzer einschließen	YES	YES	Es wird empfohlen, die Referenz-benutzer bei der Risikoanalyse mitzuberücksich-tigen.
1033	Rolle/Profil-mindernde Kontrollen in Risikoanalyse einschließen	YES	YES	Weil Mitigationen auf Rollenebene für ein bestimmtes Risiko alle Risiken der Benutzer mitigieren, wird empfohlen, diese bei der Risiko-analyse zu berück-sichtigen.
1034	Maximale Objektanzahl in einem Paket für Parallelverarbei-tung	100	Kund:innen-spezifisch ausprägen	Als relevantes Kriterium für die Performance muss dies Kund:innen-spezifisch ausge-prägt werden.
1035	E-Mail-Benachrichtigung an Überwacher der aktualisierten Risikominderung auf Objektebene senden	YES	YES	Für den Überwacher der Mitigation ist die Benachrichtigung bei Änderungen relevant und wird empfohlen.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
1036	Alle Objekte in der Risikoanalyse anzeigen	NO	Kund:innen-spezifisch ausprägen	Für die besseren Nachvollziehbar-keit der Ergebnisse der Risikoanalyse wird das explizite Anzeigen aller Ergebnisse empfohlen.
1037	Funktionstren-nungsergänzungs-tabelle für die Analyse verwe-nden.	YES	Kund:innen-spezifisch ausprägen	Ergänzende Regeln für die Risikoanalyse sind Kund:innen-individuell zu nutzen.
1038	FF-Zuordnungen in Risikoanalyse berücksichtigen	NO	Kund:innen-spezifisch ausprägen	Die FF-Zuordnungen können hierüber bei der Risikoanalyse berücksichtigt werden. Dies kann Kund:innen-individuell genutzt werden.
1039	Rollenzuordnung für Risikoanalyse einschließen	<empty>	<empty>	Abgelaufene und zukünftige Rollen müssen nicht zwingend bei der Risikoanalyse berücksichtigt werden.
1046	Für erweiterte Objekte aktivierter Konnektor	<empty>	Kund:innen-spezifisch ausprägen	Konnektoren für Non-SAP-Systeme werden Kund:innen-individuell verwendet.

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
1048	Betriebswirtschaf-tliche Ansicht für Risikoanalyse ist aktiviert	NO (Technical View)	Kund:innen-spezifisch ausprägen	Die Standard-Ansicht für die Risikoanalyse kann Kund:innen-individuell eingestellt werden.
1050	Standardberichts-ansicht für Risikoanalyse	Remedia-tion View	Kund:innen-spezifisch ausprägen	Die Standard-Ansicht für die Risikoanalyse kann Kund:innen-individuell eingestellt werden.
1051	Maximale Objektanzahl in einer Datei oder einem Datenbanksatz	200000	Kund:innen-spezifisch ausprägen	Die maximale Anzahl von Objekten in einer Datei oder einem Datenbanksatz muss je nach System sorgfältig ausgeprägt werden, damit Ergebnisse der Risikoanalyse richtig abgespei-chert und gelesen werden können.
1052	Ablageort der Spool-Datei	<empty>	Kund:innen-spezifisch ausprägen	Der Ort der Spool-Ergebnisse muss Kund:innen-indivi-duell eingestellt werden.
1053	Spool-Typ	D	Kund:innen-spezifisch ausprägen	Die Art der Speicherung der Risikoanalyse-Ergebnisse (Datenbank oder File-System) ist

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				maßgeblich dafür verantwortlich, ob die Risikoanalyse performant und zuverlässig läuft.
1054	Maximale Anzahl der in der Organi-sationsregel-analyse unter-stützten Über-schreitungen	500000	Kund:innen-spezifisch ausprägen	Die maximale Anzahl an Organi-sationsregeln für eine Risikoanalyse muss Kund:innen-individuell einge-stellt werden, um den Zwischen-speicher nicht zu überlasten.
1055	Konnektor aktiviert für automatische Benutzezuordnung im Repository	NO	Kund:innen-spezifisch ausprägen	Ein Konnektor wie z. B. LDAP oder Success-Factors zur automatischen Zuordnung von Benutzern muss Kund:innen-individuell eingestellt werden.
1071	Risikoanalyse auf Grundlage der Anforderungs-absendung aktivie-ren	NO	YES (Kund:innen-spezifisch ausprägen)	Der Parameter erzwingt die Ausführung der Risikoanalyse bei der Beantragung. So können konflik-täre Anträge bereits bei der/dem

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				Antragstellende:n identifiziert und vermieden werden. Die Beantragung kann grundsätzlich trotzdem erfolgen.
1072	Minderung von kritischem Risiko vor Genehmigung von Anforderung erforderlich	NO	YES (Kund:innen-spezifisch ausprägen)	Die Kompensierung von konfliktären Benutzeranträgen sollte grundsätzlich systemseitig ermöglicht werden. Ob dies erzwungen werden kann, sodass konfliktäre Anträge sonst nicht genehmigt werden können, ist in Abhängigkeit vom Risikoappetit individuell zu bewerten.
1073	Umleitung der Funktionstrennungsverletzungen bei Risiken aus vorhandenen Rollen aktivieren	NO	YES (Kund:innen-spezifisch ausprägen)	Die automatische Umleitung eines Benutzerantrags aufgrund von Risiken, die nicht durch die beantragten Rollen entstehen, kann je nach Risikoappetit

Parameter	Beschreibung	Standard-wert	Empfehlung	Kommentar
				der Organisation erfolgen.
1074	Mindernde Kontrolle in temporärer Tabelle sichern	NO	YES	Das Zwischenspeichern der Mitigationen während Access-Requests sorgt dafür, dass die Mitigation nicht fälschlicherweise bestehen bleibt.
1075	Kurzzusammen-fassung als Standardsicht in Zugriffsanforderung auswählen	NO	Kund:innen-spezifisch ausprägen	Welche Zusammenfassung als Standardsicht für Risikoanalysen in Anträgen angezeigt wird, kann Kund:innen-spezifisch ausgeprägt werden.

10.4.4.3 Kritische Berechtigungen in der Access-Risk-Analysis

Die Berechtigungen zur Steuerung der Komponente und deren wesentlicher Funktionen erfolgen über eine überschaubare Anzahl von Berechtigungsobjekten und Feldwerten. Die hierin als kritisch und prüfungsrelevant zu betrachtenden werden im Folgenden beschrieben. Der Bezug zu den in 2.4.4.1 genannten Risiken wird hergestellt.

Tabelle 57 Berechtigungen – Access-Risk-Analysis

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
GRAC_ REP	**ACTVT** 16 **GRAC_REP ID** GRAC_SOD_ MIT_CTL_REP	Die Berechtigung erlaubt das Ausführen des Berichts zu SoD-Bereinigungen mittels mitigierenden Kontrollen im NWBC. Der Bericht stellt detaillierte Informationen zur Prüflogik im Hinblick auf die Mitigation zur Verfügung.	Nr. 17: Da der Bericht sensible Informationen darüber enthält, welche kritischen Berechtigungen mitigiert werden, erlaubt der Inhalt die Ableitung doloser Handlungen, die nicht durch Kontrollen begleitet werden. Der Bericht stellt detaillierte Informationen zur Prüflogik im Hinblick auf die Mitigation zur Verfügung. Der Zugriff auf diesen Bericht ist entsprechend eingeschränkt zu vergeben.

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
S_TCODE	**GRAC_ UPLOAD_ RULES**	Die Berechtigung erlaubt den Upload des Regelwerks inklusive aller Risiken, Funktionen, Bewertungen und Feldwerte. Für die Pflege des Regelwerks in Produktion gibt es mehrere Möglichkeiten. Entweder erfolgt die Bearbeitung in der Entwicklung mit anschließendem Transport bis in die Produktion, oder die Änderungen erfolgen in der Produktion direkt durch Nutzung des NWBCs und ggf. der Upload-Funktion in der SPRO. Ein signifikantes Risiko der Löschung besteht bei Nutzung der Upload-Funktion, die insbesondere bei Massenänderungen infrage kommt. Wird als Upload-Modus „Überschreiben“ gewählt, wird die zuvor hinterlegte Prüflogik vollständig durch die Upload-Informationen ersetzt. Eine Löschung hat temporär zur Folge, dass kein Regelwerk in	Nr. 16: Mit Zugriff auf diese Transaktion erhält der Mitarbeitende die Möglichkeit, den gesamten Regel-Bestand der Produktion per Knopfdruck zu ändern oder zu löschen. Temporär stehen hierauf keine Regelverprobungen zur Verfügung. Prüfung, welcher/welche Mitarbeitende über die Rechte zum Zugriff auf die Upload-Funktion verfügt.

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
		Produktion zur Verfügung steht. Prüfungen von Benutzern und Rollen im Hinblick auf ihr Rechteset finden dann nicht statt.	
GRAC_ FUNC	**ACTVT** 01, 02, 06, 16, 64, 78, A8	Die Berechtigung erlaubt die Anlage und Bearbeitung von Regelwerks-Funktionen im NWBC sowie deren Zuordnung zu Risiken. Ist der Workflow zur genehmigungspflich-tigen Änderung von Funktionen (SAP_GRAC_FUNC_ APPR) deaktiviert, können mit dieser Berechtigung die Prüflogik beliebig verändert und dolose Handlungen ermöglicht werden.	Nr. 14: Mit der Berechtigung auf die angeführten Aktivitäten zum Berechtigungsobjekt GRAC_FUNC werden die Neuanlage und die Änderung von Funktionen ermöglicht. Damit kann auf Detailebene die Prüflogik verändert werden. Der Zugriff auf diese Berechtigung ist entsprechend einzuschränken.
GRAC_ RISK	**ACTVT** 01, 02, 06, 16, 64, 78	Die Berechtigung erlaubt die Anlage und Bearbeitung von Regelwerks-Risiken im NWBC sowie die Ernennung des Risiko-Verantwortlichen. Ist der Workflow zur genehmigungspflich-tigen Änderung von Risiken	Nr. 15: Mit der Berechtigung zu den angeführten Aktivitäten zum Berechtigungsobjekt GRAC_RISK werden die Neuanlage und die Änderung von Risiken ermöglicht. Damit kann auf Risiko-Ebene die Prüflogik verändert

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
		(SAP_GRAC_RISK_APPR) deaktiviert, können mit dieser Berechtigung Risiken in ihrer Kritikalität, in ihrer Zuordnung zu Regelwerken und in ihrer Zusammensetzung aus SoD-Funktionen verändert werden. Bewusste Veränderungen der Risiko-Inhalte können zulasten der Compliance im Hinblick auf die implementierte Prüflogik der Provisionierungs- oder Rollenpflegeprozesse erfolgen.	werden, indem z. B. relevante Funktionen aus einem definierten SoD-Risiko entfernt werden. Darüber hinaus ist es möglich, alternative Risiko-Verantwortliche zu ernennen, unabhängig von einem Genehmigungsprozess, sobald der Risiko-Änderungs-Workflow deaktiviert wurde. Der Zugriff auf diese Berechtigung ist entsprechend einzuschränken.
GRAC_ MITC	**ACTVT** 01, 02, 06, 78, 88	Die Berechtigung erlaubt die Anlage, Bearbeitung und Zuordnung von mitigierenden Kontrollen zu Risiken. Ist der Workflow zur genehmigungspflichtigen Änderung von mitigierenden Kontrollen (SAP_GRAC_CONTROL_MAINT) deaktiviert, erlaubt die Berechtigung die ungeprüfte Änderung von Kontrollinhalten. Ist der Workflow zur genehmigungspflichtigen Zuordnung von mitigierenden Kontrollen (SAP_GRAC_CONTROL_ASGN) deaktiviert, erlaubt die	Nr. 18; Nr. 19: Die Berechtigung für das Objekt GRAC_MITC erlaubt den bearbeitenden Zugriff auf mitigierende Kontrollen. Sind die Workflows für Bearbeitung und Zuordnung von mitigierenden Kontrollen aktiviert, genügt die Berechtigung zur Durchführung von Anlage und Änderungen und ist im Prozess freizugeben. Sind die Workflows deaktiviert,

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
		Berechtigung, dass ungeprüft die Zuordnung von nachgelagerten Kontrollen zu Risiken verändert werden kann. Es ist zu berücksichtigen, dass mitigierende Kontrollen sowohl den identifizierten Risiken in der Benutzerprovisio-nierung als auch zu Rollen selbst zugeordnet werden können.	kann mit dieser Berechtigung direkt und ungeprüft die Änderung der Kontrollen erfolgen.
GRAC_ ASIGN	**ACTVT** 01, 02, 06, 36, 70 **GRAC_OWN_T** MIAP, MIMO, RISK	Im NWBC können mit der Funktion „Access-Control-Verantwortliche“ Mitarbeitende für die Ausführung von Genehmigungsstufen und Kontrollen im ARA-Umfeld ernannt werden. Diese Ernennung ist verpflichtend, um Mit-arbeitende als Verant-wortliche den mitigie-renden Kontrollen zuzuordnen (GRAC_ OWN_T-MIAP), oder sie als Prüfungsdurchfüh-rende mitigierender Kontrollen (GRAC_ OWN_T-MIMO) bzw. als Risikoverantwortliche (GRAC_OWN_T-RISK) zuordnen zu können.	Nr. 18: „Wie werden die Mitigations-Verantwortlichen ernannt?“ Das Berechtigungsobjekt wird im Prozess der Zuweisung von Mitarbeitenden zur Kontrolldurchführung benötigt.
GRFN_USER	**ACTVT** 02	Diese Berechtigung überschreibt die meisten Berechtigungsobjekte	Alle beschriebenen Zugriffsrisiken im ARA.

Berechtigungs-objekt	Feldwert	Beschreibung	Mapping zu Risiko
		im GRC mit der entsprechenden Aktivität und ist ausschließlich Administrator:innen vorbehalten.	

10.5 SoD-Risiken beim Einsatz von SAP GRC Access Control

Die in den Vorkapiteln dargestellten, in sich als kritisch zu bewertenden Berechtigungen werden im Folgenden aus dem Gesichtspunkt der Funktionstrennung heraus betrachtet.

Hierzu sind teilweise die Berechtigungen aus dem Access-Request-Management, dem Emergency-Access-Management, dem Business-Role-Management sowie der Access-Risk-Analysis heranzuziehen und funktional zu gruppieren.

Im Wesentlichen werden die vorgestellten kritischen Berechtigungen in nachfolgend aufgelistete 13 Funktionen geclustert. Die Details zu den ggf. kritischen Ausprägungen der Berechtigungsobjekte sind den jeweiligen Vorkapiteln zu entnehmen

Tabelle 58 Funktionen im SAP GRC Access Control

Funktion	Inhalte
ARM:1	Benutzeranträge stellen
ARM:2	Benutzeranträge genehmigen
ARM:3	Benutzeranträge administrieren
ARA:1	Kontrollen anlegen, genehmigen, zuordnen
ARA:2	Funktionsänderungen genehmigen
ARA:3	Risiken bearbeiten

Funktion	Inhalte
BRM:1	Rollen administrieren
BRM:2	Rollen entwickeln
BRM:3	Rollen genehmigen
EAM:1	FireFighter administrieren
EAM:2	FireFighter-Logs kontrollieren
EAM:3	FireFighter-Zuweisung genehmigen
EAM:4	FireFighter einsetzen

Je nach Konfiguration des GRC-Systems kann die Kombination dieser Funktionen zu den in nachfolgender Abbildung dargestellten Risiken führen:

	ARM:1	ARM:2	ARM:3	ARA:1	ARA:2	ARA:3	BRM:1	BRM:2	BRM:3	EAM:1	EAM:2	EAM:3	EAM:4
ARM:1 Benutzer-anträge stellen		R:01	R:02			R:03							
ARM:2 Benutzer-anträge genehmigen			R:04			R:05							
ARM:3 Benutzer-anträge administrie-ren					R:06	R:07							
ARA:1 Kontrollen anlegen, ge-nehmigen, zuordnen					R:08			R:09	R:10				
ARA:2 Funktions-änderungen genehmigen						R:11							
ARA:3 Risiken bearbeiten							R:12	R:13	R:14				
BRM:1 Rollen administrie-ren								R:15	R:16				
BRM:2 Rollen entwickeln									R:17				
BRM:3 Rollen genehmigen													
EAM:1 FireFighter administrie-ren											R:18	R:19	R:20
EAM:2 FireFighter-Logs kont-rollieren												R:21	R:22
EAM:3 FireFighter-Zuweisung genehmigen													R:23
EAM:4 FireFighter einsetzen													

Abbildung 6 SoD-Risiken im GRC-System

Die gemeinsame Vergabe von Berechtigungen dieser Funktionen ist damit kritisch zu bewerten, zu hinterfragen und in die Prüfprozesse des GRC mit einzubeziehen.
Die Risiken sind aufgrund von möglichen Mitigationen im GRC, bspw. der Workflow-Komponente, in ein Kritikalitätslevel eingeordnet. Die entsprechende Kritikalität des Risikos ist trotzdem im Kontext des Unternehmens zu betrachten.

Tabelle 59 Risikobeschreibung der SoD-Risiken im GRC-System

Nr.	Titel	Beschreibung
R:01	Benutzeranträge stellen und Benutzeranträge genehmigen	Es besteht das Risiko, dass ein unbefugter Zugriff auf Zielsysteme erlangt wird, indem die/der Antragstellende ihren/seinen eigenen Antrag genehmigt. Hierbei wirken der GRC-Workflow und das damit verbundene Vier-Augen-Prinzip als mitigierende Kontrolle.
R:02	Benutzeranträge stellen und Benutzeranträge administrieren	Hier besteht das Risiko, dass ein unbefugter Zugriff auf Zielsysteme erlangt wird, indem die/der Antragstellende ihren/seinen eigenen Antrag administrativ bearbeitet.
R:03	Benutzeranträge stellen und Risiken bearbeiten	Kann eine Person Benutzeranträge stellen und die Risiken im GRC bearbeiten, so können die Risiken aus einem eigenen Antrag heruntergestuft oder deaktiviert werden. So kann ein kritischer Zugriff auf Zielsysteme ohne Risikoprüfung erlangt werden.
R:04	Benutzeranträge genehmigen und Risiken bearbeiten	Wenn eine Person Benutzeranträge genehmigen und die Risiken im GRC bearbeiten kann, dann können die Risiken aus einem zu genehmigenden Antrag heruntergestuft oder deaktiviert werden. Dies ermöglicht eine Genehmigung für kritische Zugriffe auf ein Zielsystem ohne Risikoprüfung.
R:05	Benutzeranträge genehmigen und Benutzeranträge administrieren	Es besteht das Risiko, dass ein unbefugter Zugriff auf Zielsysteme erlangt wird, indem eine/ein Genehmigende:r Anträge administrativ zu sich leitet, um sie unbefugterweise zu genehmigen.

Nr.	Titel	Beschreibung
R:06	Benutzeranträge administrieren und Funktionsänderungen genehmigen	Wenn eine Person Benutzeranträge administrieren und Funktionsänderungen genehmigen kann, dann können die Risiken aus einem Antrag verschleiert werden. Dies ermöglicht eine Umleitung und Genehmigung für kritische Zugriffe auf ein Zielsystem mit einer veränderten Risikoprüfung.
R:07	Benutzeranträge administrieren und Risiken bearbeiten	Hier besteht das Risiko, dass ein unbefugter Zugriff auf Zielsysteme erlangt wird, indem der Risikoeigner seinen eigenen Antrag administrativ bearbeitet.
R:08	Mitigierende Kontrollen anlegen, genehmigen, zuordnen und Funktions-änderungen genehmigen	Wenn Funktionsänderungen durchgeführt werden und gleichzeitig mitigierende Kontrollen zugewiesen werden, besteht das Risiko, dass neue Zugriffsrisiken sofort verschleiert werden.
R:09	Mitigierende Kontrollen anlegen, genehmigen, zuordnen und Rollen entwickeln	Kann eine Person mitigierende Kontrollen zuweisen und gleichzeitig Rollen entwickeln, so können neue Zugriffsrisiken aus den Rollen sofort verschleiert werden.
R:10	Mitigierende Kontrollen anlegen, genehmigen, zuordnen und Rollen-änderungen genehmigen	Kann eine Person mitigierende Kontrollen zuweisen und gleichzeitig Rollen entwickeln, so können neue Zugriffsrisiken aus den Rollen sofort verschleiert werden.
R:11	Funktionsänderungen genehmigen und Risiken bearbeiten	Wenn eine Person Funktionsänderungen genehmigen und die Risiken im GRC bearbeiten kann, dann kann die Kritikalität der Risiken heruntergestuft oder verschleiert werden.
R:12	Risiken bearbeiten und Rollen administrieren	Hier besteht das Risiko, dass Rollen für Zielsysteme kritische Berechtigungen erhalten, indem der Rollenadministrator / die Rollenadministratorin die Risiken aus einer Rolle deaktiviert oder verfälscht.

Nr.	Titel	Beschreibung
R:13	Risiken bearbeiten und Rollen entwickeln	Hier besteht das Risiko, dass Rollen für Zielsysteme kritische Berechtigungen erhalten, indem der Rollenentwickler / die Rollenentwicklerin die Risiken aus einer Rolle deaktiviert oder verfälscht.
R:14	Risiken bearbeiten und Rollenänderungen genehmigen	Wenn eine Person Rollenänderungen genehmigen und die Risiken im GRC bearbeiten kann, dann können die Risiken aus einer zu genehmigenden Rollenänderung heruntergestuft oder deaktiviert werden. Dies ermöglicht eine Genehmigung für kritische Zugriffe auf ein Zielsystem ohne Risikoprüfung.
R:15	Rollen administrieren und Rollen entwickeln	Es besteht das Risiko, dass ein unbefugter Zugriff auf Zielsysteme erlangt wird, indem der Rollenentwickler / die Rollenentwicklerin seine/ihre eigenen Rollenänderungen als administrativ im Workflow bearbeitet.
R:16	Rollen administrieren und Rollenänderungen genehmigen	Es besteht das Risiko, dass ein unbefugter Zugriff auf Zielsysteme erlangt wird, indem der Rollenentwickler / die Rollenentwicklerin seine/ihre eigenen Rollenänderungen administrativ im Workflow bearbeitet.
R:17	Rollen entwickeln und Rollenänderungen genehmigen	Es besteht das Risiko, dass ein unbefugter Zugriff auf Zielsysteme erlangt wird, indem der Rollenentwickler / die Rollenentwicklerin die eigenen Rollenänderungen genehmigt. Hierbei wirken der GRC-Workflow und das damit verbundene Vier-Augen-Prinzip als mitigierende Kontrolle.
R:18	FireFighter administrieren und FireFighter-Logs kontrollieren	Kann eine Person FireFighter administrieren und gleichzeitig die FireFighter-Logs kontrollieren, so können Zugriffe über den FireFighter auf Zielsysteme eingerichtet und die Nutzung verschleiert werden.

Nr.	Titel	Beschreibung
R:19	FireFighter administrieren und FireFighter-Zuweisung genehmigen	Hier besteht das Risiko, dass einer Person FireFighter zugewiesen und genehmigt werden. Dies ermöglicht einen direkten Zugriff mit kritischen Berechtigungen auf Zielsysteme des GRC-Systems und könnte erst nachträglich durch das Kontrollieren des Logs auffallen.
R:20	FireFighter administrieren und FireFighter einsetzen	Es besteht das Risiko, dass eine Person FireFighter zuweist und nutzt. Dies ermöglicht einen direkten Zugriff mit kritischen Berechtigungen auf Zielsysteme des GRC-Systems und könnte erst nachträglich durch das Kontrollieren des Logs auffallen.
R:21	FireFighter-Logs kontrollieren und FireFighter-Zuweisung genehmigen	Kann eine Person FireFighter-Logs kontrollieren und gleichzeitig FireFighter-Zuweisungen genehmigen, so können Zugriffe über den FireFighter auf Zielsysteme eingerichtet und die Nutzung verschleiert werden.
R:22	FireFighter-Logs kontrollieren und FireFighter einsetzen	Wenn eine Person FireFighter-Logs kontrollieren und FireFighter nutzen kann, dann kann sie indirekt ihre eigene Nutzung mit kritischen Berechtigungen verschleiern. Hierbei wirken die FireFighter-Zuweisung bzw. der GRC-Workflow und das damit verbundene Vier-Augen-Prinzip als mitigierende Kontrolle.
R:23	FireFighter-Zuweisung genehmigen und FireFighter nutzen	Kann eine Person FireFighter-Zuweisung genehmigen und FireFighter nutzen, so können Zugriffe über den FireFighter auf Zielsysteme eingerichtet und die Nutzung verschleiert werden. Hierbei wirken der GRC-Workflow und das damit verbundene Vier-Augen-Prinzip als nachgelagerte Kontrolle.

Impressum

Wir weisen ausdrücklich darauf hin, dass das vorliegende Dokument nicht jeglichen Regelungsbedarf sämtlicher DSAG-Mitglieder in allen Geschäftsszenarien antizipieren und abdecken kann. Insofern müssen die angesprochenen Themen und Anregungen naturgemäß unvollständig bleiben. Die DSAG und die beteiligten Autoren können bezüglich der Vollständigkeit und Erfolgsgeeignetheit der Anregungen keine Verantwortung übernehmen.

Deutschsprachige SAP® Anwendergruppe e.V.
Altrottstraße 34 a
69190 Walldorf | Deutschland
Telefon +49 6227 35809-58
Telefax +49 6227 35809-59
E-Mail info@dsag.de
dsag.de