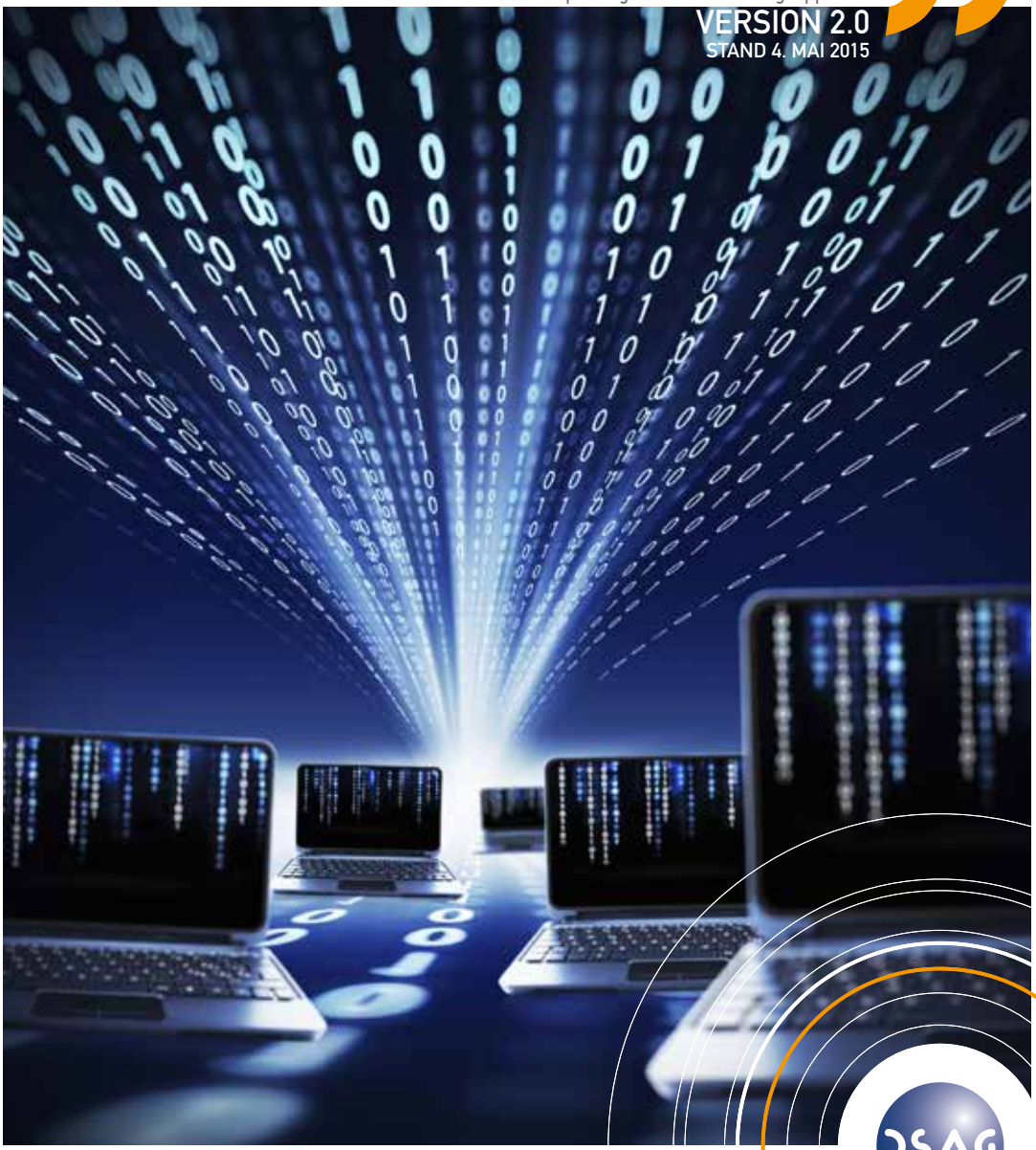
Prüfleitfaden SAP® ERP 6.0

Best-Practice-Empfehlungen des DSAG-Arbeitskreises Revision u. Risikomanagement

Deutschsprachige SAP-Anwendergruppe e.V.

VERSION 2.0

STAND 4. MAI 2015



Prüfleitfaden SAP® ERP 6.0

Best-Practice-Empfehlungen des DSAG-Arbeitskreises Revision u. Risikomanagement

VERSION 2.0
STAND 4.MAI 2015

DSAG e. V.
Deutschsprachige SAP-Anwendergruppe

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. Sämtliche Überlegungen, Vorgehensweisen und Maßnahmen hinsichtlich des Verhaltens gegenüber SAP verbleiben in der individuellen Eigenverantwortung jedes DSAG-Mitglieds. Insbesondere kann dieser Leitfaden nur allgemeine Anhaltspunkte zu vertragsrechtlichen Themen geben und keinesfalls eine individuelle Rechtsberatung bei der Verhandlung und Gestaltung von Verträgen durch IT-rechtliche Experten ersetzen.

HINWEIS:

DEUTSCHSPRACHIGE SAP® ANWENDERGRUPPE E.V.
Altrottstraße 34 a
69190 Walldorf
Deutschland
Fon +49 (0) 6227 – 358 09 58
Fax +49 (0) 6227 – 358 09 59
www.dsag.de I info@dsag.de

Die Autoren des Prüfleitfadens sind für Kritik, Änderungs- und Ergänzungswünsche dankbar (bitte als Beitrag im DSAGNet unter „AK Revision & Risikomanagement" www.dsag.de/AK-Revision melden).

Deutschsprachige
SAP® Anwendergruppe

INHALTSVERZEICHNIS

INHALTSVERZEICHNIS

EINLEITUNG

Der vorliegende Prüfleitfaden des Arbeitskreises (AK) Revision u. Risikomanagement bezieht sich im Kern auf den Releasestand SAP ERP 6.0, EHP 7, innerhalb der SAP Business Suite. Ergänzt wurde der Leitfaden um Prüfungshandlungen innerhalb der GRC Suite sowie bei SAP HANA. Der AK Revision u. 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 von SAP-Anwendungen zu geben. Er aktualisiert und erweitert den im Jahr 2009 in der Version 1.0 herausgegebenen Prüfleitfaden zu SAP ERP 6.0., dessen Teil 2 (Applikationsebene) nach wie vor Gültigkeit besitzt.

Die Prüfhinweise in diesem Leitfaden sind als Hinweise für einen mit SAP vertrauten Prüfer gedacht. Sie sind keine verbindliche Richtlinie oder Norm. Jegliche Verantwortung für Art, Umfang und Ergebnis externer und interner Prüfungen verbleibt beim Prüfer selbst. In seiner Verantwortung liegt 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).

Voraussetzung ist die Erfahrung mit dem SAP-System, insbesondere mit SAP ERP 6.0, SAP GRC, SAP HANA, 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 Schulungskurse.

Die ausgewählten Prüfprogramme vermitteln Handlungen, die dem Prüfer die Wahrnehmung der kritischen kundenspezifischen Ausprägungen, der technischen SAP-Konzepte und -Funktionen erleichtern sollen. Der notwendige Prüfungsumfang muss jeweils individuell den kundenspezifischen organisatorischen Prozessen angepasst werden.

Der Prüfleitfaden wird in Versionen fortgeschrieben.

HINWEISE ZUR HANDHABUNG DES LEITFADENS:

- Eine Prüfungshandlung auf fehlerhafte Konfiguration der SAP-Software ist in der linken Spalte mit einem „H" gekennzeichnet, wenn diese ein hohes Risiko bedeutet. Dies ist als ein Hinweis für den Prüfer gedacht. Der Prüfleitfaden bietet allerdings keine systematische Risikobewertung.

- Bei Prüfungshandlungen, die durch das SAP Audit Informationssystem (AIS) unterstützt werden, ist der betreffende AIS-Menüpfad angegeben.

- Mit der Einführung von SAP Release 4.6C wurde das AIS von einer transaktionsbasierten auf eine rollenbasierte Pflegeumgebung umgestellt. Siehe hierzu SAP-Hinweis 451960. Seit der Aufnahme des AIS in die SAP_BASIS-Komponente ist es in allen SAP-Systemen verfügbar (BW, CRM, SEM, APO etc.). Die von der SAP ausgelieferten Vorlagerollen enthalten ca. 1200 Transaktionen. Selektieren Sie hierfür im SAP-Profilgenerator nach Rollen mit dem Muster SAP*AUDITOR*.

- Prüfungshandlungen, die der SAP Security Optimization Self-Service unterstützt (http://service.sap.com/SOS), sind mit „SOS" gekennzeichnet. Text und Nummer der automatisierten Prüfung sind angegeben.

Die Autoren der einzelnen Kapitel des neuen Leitfadens sind Mitglieder des DSAG-Arbeitskreises „Revision u. Risikomanagement". Die Veröffentlichung der Kapitel erfolgt jeweils separat in unregelmäßiger Folge. Die Verantwortung für den Inhalt tragen die jeweiligen Autoren.

DIE AUTOREN DER BISHER VERÖFFENTLICHTEN KAPITEL:

Murat Böcü	Deloitte & Touche GmbH
Marcus Böhme	T-Systems International GmbH
Siegfried Filla	PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft
Falk Huber	T-Systems International GmbH
Ralf Kaib	Exagon GmbH
Vojislav Kosanovic	KPMG AG Wirtschaftsprüfungsgesellschaft
Johannes Liffers	PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft
Martin Metz	Protiviti GmbH
Christoph Nickel	KPMG AG Wirtschaftsprüfungsgesellschaft
Jan Stölting	KPMG AG Wirtschaftsprüfungsgesellschaft
Wolfgang Storm	PricewaterhouseCoopers AG, Wirtschaftsprüfungsgesellschaft
Karl Ulber	PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft

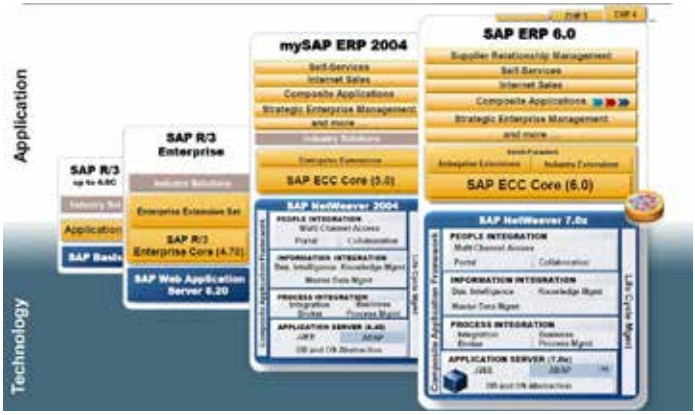
ÜBERSICHT DER VERÖFFENTLICHTEN KAPITEL:

KAPITEL	TITEL	AUTOR	STAND
	Einleitung	Siegfried Filla	01.2015
1	SAP ERP 6.0	Siegfried Filla	01.2015
2	Prüferrolle, Bestandsaufnahme von SAP-Systemlandschaft, Richtlinien u. Organisationsweisungen	Siegfried Filla	01.2015
3	Identifikation und Authentisierung (ABAP-Stack)	Ralf Kaib	03.2014
4	Autorisierung (ABAP-Stack)	Siegfried Filla, Johannes Liffers, Wolfgang Storm, Karl Ulber	02.2015
5.1	Prüfprogramm: Schutz der Batch-Input-Prozesse	Ralf Kaib	03.2014
6	Systemintegrität mit dem SAP Java-Stack	Vojislav Kosanovic	12.2013
7	Systemintegrität auf der Datenbankebene	Falk Huber	02.2015
8	Systemintegrität auf der Betriebs-systemebene	Christoph Nickel	03.2015
9	Risiken und Prüfung von SAP GRC	Murat Böcü, Martin Metz	01.2015
10	SAP HANA aus Revisionssicht	Marcus Böhme, Jan Stölting	03.2015

1. SAP ERP 6.0

Nach den Produkten SAP R/1 und SAP R/2 für die Welt der Mainframes führte SAP im Jahr 1992 SAP R/3 für die neuen Client-Server-Architekturen ein. SAP R/3 umfasste neben spezifischen Industrielösungen die SAP Basis und die verschiedenen SAP Applikationen, wie z.B. Finanzwesen, Controlling, Materialwirtschaft und Personalwirtschaft. SAP R/3 wurde in dieser Systemstruktur bis Release 4.6C ausgeliefert und dann durch das sogenannte SAP R/3 Enterprise Core (R/3 Release 4.70) mit den neuen technischen Möglichkeiten des SAP Web Application Server 6.20 im Jahre 2003 abgelöst. Ab 2004 wurde mit "mySAP ERP 2004" und danach mit „mySAP ERP 2005" ein ganzes Bündel funktionaler Erweiterungen zur Unterstützung der Unternehmensprozesse eingeführt (u.a. auch die sogenannte Enterprise Central Component "ECC 5.0" sowie „ECC 6.0" mit den Kernmodulen von SAP R/3). Durch die ergänzende Einführung von SAP NetWeaver 2004 (aktuell SAP NetWeaver 7.4) konnten jetzt u.a. auch in JAVA programmierte Lösungen eingebunden werden. Darüber hinaus dient SAP NetWeaver zur Integration und Weiterentwicklung heterogener Systemlandschaften mit dem Ziel, alle auch außerhalb eines SAP-Systems verarbeiteten Daten zu integrieren und so Prozesse systemübergreifend zu steuern.

Die nachfolgende Abbildung der SAP vermittelt einen Überblick über die Entwicklung der ERP-Lösungen bis hin zu SAP ERP 6.0 als Prüfungsobjekt dieses neuen Leitfadens.



Seit 2009 ist SAP ERP 6.0 Teil der SAP Business Suite und wird aktuell u.a. auch mit der neuen HANA-Datenbanklösung der SAP als „SAP HANA Live for ERP" angeboten. Im Verbund mit den neuen Cloud-Technologien und mobilen Applikationen ergeben sich aus Prüfersicht komplexere Risikoszenarien als noch vor einigen Jahren. Soweit möglich, haben wir diesen Entwicklungen im vorliegenden Leitfaden Rechnung getragen, insbesondere durch das Kapitel „SAP HANA aus Revisionssicht".

Aufgrund der Tatsache dass SAP die Wartung für die Kernapplikationen der SAP Business Suite 7, nämlich SAP ERP 6.0, SAP Customer Relationship Management (SAP CRM) 7.0, SAP Supply Chain Management (SAP SCM) 7.0 und SAP Supplier Relationship Management (SAP SRM) 7.0, genauso wie den Betrieb der SAP Business Suite durch SAP HANA 2013 bis Dezember 2025 verlängert hat, werden wir uns in den nächsten Jahren sicherlich mit weiteren Prüfungsherausforderungen innerhalb von SAP ERP 6.0 beschäftigen.

2. PRÜFERROLLE, BESTANDSAUFNAHME VON SAP-SYSTEMLANDSCHAFT, RICHTLINIEN U. ORGANISATIONSWEISUNGEN

2.1. GRUNDLAGEN ZUR ERSTELLUNG EINER PRÜFERROLLE

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 interne bzw. externe Prüfer generell alle Anzeigeberechtigungen, die das Prüfungsgebiet umfassen. Insofern ist die Einrichtung von Prüferrollen im Vorfeld anstehender Prüfungen empfehlenswert, damit bei Prüfungsbeginn nicht unnötige Zeit auf Anwender- und Prüferseite vertan wird. Die Prüferrollen 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.

Ist aus technischer Sicht in den Prüferrollen eine Änderungsfunktion/Änderungstransaktion unumgänglich (z.B. Zugriff auf bestimmte Customizing-Tabellen), ist diese separat nur für die Dauer des spezifischen Prüfungsschrittes zu berechtigen.

Benötigt ein Prüfer Berechtigungen (z.B. Zugriff auf Eigenentwicklungen), die denen eines Notfallusers entsprechen, ist gemäß dem vorliegenden Notfalluserkonzept zu verfahren.

2.2. BESTANDSAUFNAHME DER SAP-SYSTEMLANDSCHAFT

NR.	
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 Releasestand?
3.	Auf welchen Betriebssystemen laufen die SAP-Systeme?
4.	Welche Datenbanken unterstützen die SAP-Anwendungen?
5.	Gibt es ein detailliertes Diagramm der SAP-Systemarchitektur, das die Verbindungen der SAP-Systeme untereinander, 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.
	Welche SAP-Produkte und Module sind implementiert (Bestandsverzeichnis)?
6.	Gibt es eine Übersicht über verschlüsselte Netzverbindungen?

2.3. 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 von IT-bezogenen Richtlinien aus.

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

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 sowie der Systembetreiber?
3.	Ist die IT-Sicherheit von spezifischen Systemplattformen geregelt und dokumentiert, z.B. 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?
6.5.	› Benutzer- 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. IDENTIFIKATION UND AUTHENTISIERUNG (ABAP-STACK)

3.1. ANMELDEKONTROLLEN

Die Identifikation und Authentisierung mittels Benutzerkennung und Kennwort ist ein übliches und einfaches Verfahren. Das Verhalten des Benutzers bestimmt wesentlich die Wirksamkeit des Verfahrens. Mögliche Schwachstellen sind z.B. einfache, leicht erratbare oder auch anderen Benutzern bekannte Kennworte.

Ein weiteres für den Benutzer komfortables Verfahren ist die Anmeldung mittels Single-Sign-On. Dabei entfällt die Anmeldung mit Benutzerkennung und Passwort; die Anmeldung erfolgt über SAP-Anmeldetickets.

Mit zusätzlichen automatisierten Regeln kann Einfluss auf die Wahl des Kennworts und auf den Umgang mit dem Kennwort genommen werden. SAP bietet eine Reihe solcher möglichen Regeln über konfigurierbare Systemparameter an. Das Unternehmen muss diese gemäß den eigenen Sicherheitsvorgaben anpassen.

3.2. RISIKEN

Risiken ergeben sich vor allem aus der fehlerhaften Konfiguration der Systemeinstellungen für die Anmeldekontrollen des SAP-Systems:

- Die Systemparameter für die Anmeldekontrollen sind nicht entsprechend dem IT-Sicherheitskonzept des Unternehmens ausgeprägt. Sie sind unzureichend oder widersprüchlich gesetzt, sodass die beabsichtigte Wirkung verfehlt wird.
- Sicherheitsmechanismen, die SAP zur Unterstützung der Benutzerverwaltung bereitstellt, sind nicht angemessen umgesetzt, z.B.Vorgabe des Gültigkeitszeitraums, Nutzung von Sperrkennzeichen oder von besonderen Benutzertypen und die Zuordnung zu Benutzergruppen.
- Die Sonderbenutzer, für die SAP im Auslieferungsstand der Software bekannte Standardkennworte vorgesehen hat, sind bei der Implementierung nicht sicher konfiguriert worden.
- Sicherheitsereignisse, die ein Unterlaufen der gesetzten Anmeldekontrollen bedeuten, werden nicht erkannt und verfolgt.

3.3. KONTROLLZIELE

- Die Systemparameter für die Anmeldekontrollen sind so gesetzt, dass sie in der Verbundwirkung einen angemessenen Zugriffsschutz gewährleisten. Die gewünschte Kennwortqualität wird durch automatisierte Vorgaben sichergestellt. Ein Schutz vor Angriffen auf Kennworte wird konfiguriert. Mehrfachanmeldungen werden verhindert.
- Gültigkeitszeiträume für Benutzerkennungen sind definiert.
- Die Sonderbenutzer sind sicher konfiguriert.
- Sicherheitsmechanismen für die Verwaltung von Benutzergruppen und für besondere Benutzertypen sind aktiviert.
- Die Wirksamkeit der Anmeldekontrollen wird überwacht.

3.4. PRÜFPROGRAMM: SYSTEMPARAMETER FÜR DIE ANMELDEKONTROLLE

NR.	SYSTEMPARAMETER FÜR DIE ANMELDEKONTROLLE
	Die Systemparameter, die für die Kennwortbildung und Anmeldung relevant sind, werden wie folgt angezeigt: **AIS:** System Audit – Top Ten Security Reports – Profilparameter anzeigen (generisch über login/*) Oder Transaktion SPFPAR **AIS:** System Audit – Systemkonfiguration – Parameter – Systemparameter, Übersicht mit Historie Oder Transaktion TU02 **AIS:** System Audit – Systemkonfiguration – Parameter – Systemparameter mit Doku. Oder Transaktion RZ11 **Hinweis:** Die im Folgenden aufgeführten Vorschlagswerte für die Anmeldekontrollen sind noch einmal in der Tabelle zusammengefasst, die diesem Prüfprogramm folgt.
1.	**Kontrollziel: Die Bildung des Kennworts unterliegt Komplexitätsregeln.** **Risiko:** Das Kennwort ist einfach und kann mit wenigen Anmeldeversuchen erraten werden. Der Benutzer verwendet wiederholt dasselbe Kennwort. Er überlistet den systemseitig erzwungenen Wechsel des Kennworts, wenn keine oder eine zu kurze Passworthistorie gewählt ist.
1.1. **H**	Die Kennwortmindestlänge login/ min_password_lng ist festgelegt. Vorschlagswert: 6 Zeichen **Hinweis:** Das SAP-System lässt eine Kennwortlänge von bis zu 40 Zeichen zu. **SOS:** Minimum Password Length is Too Short (0126)
1.2. **H**	**Das Kennwort unterliegt Bildungsregeln.** Die relevanten Systemparameter sind login/ password_charset, login/ min_password_letters, login / min_password_digits und login/ min_password_specials, login/ min_password_lowercase und login/ min_password_uppercase. **Vorschlagswerte:** Kennwort muss mindestens einen Buchstaben, eine Zahl und ein Sonderzeichen enthalten. **SOS:** Required Number of Digits/Letters/Special Characters in Passwords is Too Low (0129, 0130, 0131)
1.3. **H**	Die Anzahl Zeichen ist geregelt, in denen sich ein neues Kennwort vom alten unterscheiden muss, login/ min_password_diff. **Vorschlagswert:** 3, d.h. mindestens die Hälfte der vorgeschriebenen Passwortlänge. **SOS:** Number of Characters in Which Passwords Have to Differ is Too Low (0128)
1.4. **H**	Die Größe der Passworthistorie ist vorbesetzt, login/ password_history_size. **Vorschlagswert:** 15 Kennworte bei einem Wechsel, der alle 90 Tage erzwungen wird.
1.5.	In der Tabelle USR40 sind unzulässige Kennwörter eingetragen. **Hinweis:** Wenn bereits über eine Passwortbildungsregel gefordert ist, dass mindestens ein Sonderzeichen zu wählen ist, brauchen in dieser Tabelle keine Wörter aus dem Duden, auch keine Buchstaben- oder Zahlenkombinationen eingetragen zu werden. **SOS:** Trivial Passwords Are Not Sufficiently Prohibited (0125)

NR.	SYSTEMPARAMETER FÜR DIE ANMELDEKONTROLLE
2.	**Kontrollziel: Die Gültigkeitsdauer eines Kennworts ist beschränkt.** Risiko: Benutzerkennungen verbleiben lange mit Initialkennwort. Der Benutzer kann dasselbe Kennwort monatelang verwenden. Es besteht das Risiko, dass das Initialkennwort bekannt ist oder dass das Kennwort ausgespäht worden ist.
2.1. **H**	Die Gültigkeitsdauer eines initialen Kennworts ist geregelt, login/ password_max_ idle_initial. Dieser Parameter zieht nicht für die Benutzer vom Typ Service oder System. Vorschlagswert: Die Gültigkeitsdauer überschreitet nicht drei Arbeitstage. **Hinweis:** Dieser Systemparameter ersetzt die Profilparameter login/ password_max_new_valid und login/ password_max_reset_valid aus dem SAP Web Anwendungsserver 6.20 und 6.40. **SOS:** Users with Initial Passwords Who Have Never Logged On (0009)
2.2. **H**	Der Zeitpunkt für den Kennwortänderungszwang ist vorbestimmt, login/ password_ expiration_ time. **Vorschlagswert:** Erzwungener Wechsel des Kennworts nach höchstens 90 Tagen. **SOS:** Interval for Password Change is Too Long (0127)
2.3.	Die Gültigkeitsdauer eines nicht benutzten Kennworts ist geregelt, login/ password_max_ idle_ productive. Dieser Parameter zieht nicht für die Benutzer vom Typ Service oder System. **Hinweis:** Dieser Parameter gibt die maximale Frist an, in der ein produktives vom Benutzer gewähltes Kennwort gültig bleibt, wenn es nicht benutzt wird. Nachdem diese Frist abgelaufen ist, kann das Kennwort nicht mehr zur Authentifizierung verwendet werden. Der Benutzeradministrator kann die Kennwortanmeldung durch Zuweisen eines neuen Initialkennworts wieder aktivieren.Vorschlagswert: Gültigkeitsdauer eines nicht benutzten Kennworts höher setzen als die Dauer für den erzwungenen Wechsel des Kennworts (max. 180 Tage). **SOS:** Users with Reset Passwords Who Have Never Logged On (0140) **SOS:** Users Who Have Not Logged On for an Extended Period of Time (0010)
2.4.	Der Benutzer muss sein Kennwort jederzeit ändern können. Gemäß der SAP-Mindesteinstellung ist dies einmal am Tag (Standardwert: 1) möglich, login/ password_change_waittime. **Vorschlagswert:** 1, d.h., der Benutzer muss einen Tag warten, bis er sein Kennwort wieder ändern darf.
3.	**Kontrollziel: Erschweren des Ausprobierens von Kennworten** Risiko: Kennworte fremder Benutzerkennungen können über wiederholte Anmeldeversuche ausprobiert werden.
3.1.	Die maximale Anzahl der Falschanmeldungen bis zum Abbrechen des Anmeldevorgangs ist definiert, login/ fails_to_session_end. **Vorschlagswert:** 3 als maximale Anzahl Passwortfehlversuche bis zum Abbruch des Vorgangs.
3.2. **H**	Die maximale Anzahl der Falschanmeldungen bis zur Sperre der Benutzerkennung ist bestimmt, login/ fails_to_user_lock. **Vorschlagswert:** 5 als maximale Anzahl Passwortfehlversuche bis Sperre des Benutzers. **SOS:** Too Many Incorrect Logon Attempts Allowed Before a User is Locked (0133)

NR.	SYSTEMPARAMETER FÜR DIE ANMELDEKONTROLLE
1.5.	Die automatische Freischaltung der Benutzerkennungen, die wegen Falschanmeldung gesperrt wurden, ist auf Mitternacht eingeschaltet, login/ failed_user_auto_unlock (Standardwert „0"). **Vorschlagswert:** 1, d.h. automatisches Entsperren des Benutzers über Nacht. **Hinweis:** Wenn es bei dieser Standardeinstellung bleibt, müssen zusätzlich die gesperrten Benutzerkennungen mit den Mitteln des SAP Audit Logs auf auffälliges Vorkommen im Zeitverlauf überwacht werden. **SOS:** User Locks due to Failed Logon Attempts Are Automatically Released at Midnight (0134)
4.	Kontrollziel: **Verhindern von Mehrfachanmeldungen** Risiko: Mehrere Benutzer teilen sich eine Benutzerkennung und melden sich getrennt am SAP-System an. Das ist ein Verstoß gegen die Lizenzbestimmungen von SAP.
4.1.	Mehrfachanmeldungen sind ausgeschlossen, login/ disable_multi_gui_login (Standardwert: 1). **Vorschlagswert:** 1, d.h., mehrfache Anmeldung ist nicht möglich. **Hinweis 1:** Ausnahmebenutzer wie Administratoren oder Notfallbenutzer, denen eine Mehrfachanmeldung ermöglicht werden muss, sind unter dem Systemparameter login/ multi_login_users gelistet. **Hinweis 2:** Das SAP-System protokolliert Mehrfachanmeldungen in der Tabelle USR41_ MLD. **SOS:** Multiple Logons Using the Same User Id is Not Prevented (0138)
5.	Kontrollziel: **Die unbefugte Nutzung einer offenen SAP-Sitzung durch einen anderen als den angemeldeten Benutzer wird erschwert.** Risiko: Ein Kollege nutzt die Abwesenheit des Benutzers, um an dessen Frontend einer geöffneten SAP-Sitzung nicht autorisierte Transaktionen durchzuführen.
5.1.	Ist ein passwortgeschütztes Abschalten der Bedienoberfläche des Frontend aktiviert?
5.2.	**Wird die Möglichkeit der automatischen Abmeldung der SAP-Sitzung genutzt?** Der Parameter rdisp/gui_auto_logout ist zweckentsprechend (ungleich „0") gesetzt. Er definiert die maximale Zeit in Sekunden bei ausbleibender Tätigkeit des angemeldeten Benutzers bis zum automatischen Abmeldung. Dies gilt nur für SAP-GUI-Verbindungen. Wenn der Parameter auf den Standardwert 0 gesetzt ist, erfolgt keine automatische Abschaltung. **SOS:** Interval After Which Inactive Users Are Logged Off is Too Long (0137).

3.5. TABELLE: VORSCHLAGSWERTE FÜR DIE SYSTEMPARAMETER DER ANMELDEKONTROLLE

NR.	PARAMETER	SAP-MÖGLICHE WERTE	SAP-VOREIN-STELLUNG	VORSCHLAGSWERT
1. **H**	login/ min_password_lng	6-40	6 (statt 3)	6 (Kennwortmindestlänge)
2.	login/ password_charset	0,1,2	1	1 (abwärtskompatibel)
3. **H**	login/ min_password_letters	0-40	0	1 (Kennwort muss mindestens einen Buchstabe enthalten.)
4. **H**	login/ min_password_digits	0-40	0	1 (Kennwort muss mindestens eine Zahl enthalten.)
5. **H**	login/ min_password_specials	0-40	0	1 (Kennwort muss mindestens ein Sonderzeichen enthalten.)
6.	login/ min_password_lowercase	0-40	0	optional
7.	login/ min_password_uppercase	0-40	0	optional
8. **H**	login/ min_password_diff	1-40	1	3 (mindestens die Hälfte der minimalen Kennwortlänge)
9. **H**	login/ password_history_size	1-100	5	15 Kennworte (bei einem Wechsel, der alle 90 Tage erzwungen wird)
10. **H**	login/ password_max_idle_initial	0-24.000 (Tage)	0	Gültigkeitsdauer für ein initiales Kennwort überschreitet nicht 3 Arbeitstage.
11. **H**	login/ password_expiration_time	0-999 (Tage)	0	Erzwungener Wechsel des Kennworts nach höchstens 90 Tagen.
12.	login/ password_max_idle_productive	0-24.000 (Tage)	0	Gültigkeitsdauer eines nicht benutzten Kennworts höher setzen als die Dauer für den erzwungenen Wechsel des Kennworts.
13.	login/ password_change_waittime	1-1000 (Tage)	1	1 (Benutzer muss einen Tag warten, bis er sein Kennwort wieder ändern darf.)

NR.	PARAMETER	SAP-MÖGLICHE WERTE	SAP-VOREIN-STELLUNG	VORSCHLAGSWERT
14.	login/ fails_to_session_end	1-99	3	3 (maximale Anzahl Passwortfehlversuche bis Abbruch des Vorgangs)
15. **H**	login/ fails_to_user_lock	1-99	5 (statt 12)	5 (maximale Anzahl Passwortfehlversuche bis Sperre des Benutzers)
16	login/ failed_user_auto_unlock	0 oder 1	0 (statt 1)	1 (automatisches Entsperren des Benutzers über Nacht)
17.	login/ disable_multi_gui_login	1	0	1 (mehrfache Anmeldung nicht möglich)
18.	login/ multi_login_users			Liste der Benutzer, für die eine Mehrfachanmeldung möglich ist
19.	login/ password_compliance_to_current_policy Zweck: Wenn ein bereits vergebenes Kennwort nicht mehr den inzwischen geänderten Kennwortbildungsregeln entspricht, erzwingt das System eine Änderung des Kennworts bei der Anmeldung.	0 oder 1	0	Optional
20.	login/ password_downwards_compatibility Zweck: Dieser Parameter spezifiziert den Grad der Abwärtskompatibilität z.B. der unterstützten Passwortlängen zu früheren SAP Releases. Details sind der technischen Dokumentation zu entnehmen.	Siehe SAP Dokumentation		Optional

NR.	PARAMETER	SAP-MÖGLICHE WERTE	SAP-VOREIN-STELLUNG	VORSCHLAGSWERT
21.	Tabelle USR40 Beispieleintragungen: 123456, qwertz, (oder andere Zeichenfolge auf der Tastatur) oder generisch *Montag*, *Januar*, *Sommer*, *Passwort*, *<Firmennamen>*			Abfragen auf triviale Kennworte erübrigen sich, wenn bereits komplexe Passwortbildungsregeln eingestellt sind.
22.	rdisp/ gui_auto_logout Definiert die maximale Zeit in Sekunden bei ausbleibender Tätigkeit des angemeldeten Benutzers bis zur automatischen Abmeldung. Dies gilt nur für SAP-GUI-Verbindungen. Wenn der Parameter auf den Standardwert 0 gesetzt ist, erfolgt keine automatische Abschaltung.	Jeder numerische Wert	0	Optional, aber verpflichtend, wenn keine automatische Frontend-Sperre eingerichtet ist (Bildschirmschoner mit PC-Sperre).
23.	login/password_logon_usergroup	Eine Benutzergruppe		Benutzer dieser Benutzergruppe können sich weiterhin mit Passwort anmelden.
24.	login/ticket_expiration_time	Stunden-Minuten	8:00	Ablaufzeit für das Anmeldeticket

3.6. PRÜFPROGRAMM: GÜLTIGKEITSZEITRAUM VON BENUTZERKENNUNGEN

NR.	PRÜFPROGRAMM: GÜLTIGKEITSZEITRAUM VON BENUTZERKENNUNGEN
	Wie viele Benutzer sind im Mandant registriert? **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Anzahl Benutzerstammsätze oder Tabelle USR02, keine Auswahl vornehmen, die Anzahl Treffer wird oberhalb der Ergebnisliste zwischen den Kopfzeilen des SAP-Menüs angezeigt.
1.	**Kontrollziel: Kurze Gültigkeitsdauer von Benutzerkennungen mit Initialkennwort.** **Risiko:** Ein Benutzer meldet sich unter einer fremden Benutzerkennung mit bekanntem Initialkennwort an.
1.1.	**Welche Benutzer haben sich noch nie angemeldet? Wie lange ist der Benutzer mit Initialkennwort schon angelegt?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Auswertung nach „unbenutzt" im Feld „Letzte Anmeldung" oder Tabelle USR02, Feld „letztes Login-Datum" mit „=" ‹LEER› auswählen. Das entspricht dem Feld TRDAT in der angezeigten Liste. Alternativ kann die Transaktion SUIM oder SA38 mit dem Report RSUSR200 verwendet werden. Benutzer mit Initialkennwort müssen nach Ablauf einer Frist von wenigen Arbeitstagen automatisch gesperrt werden. Dies muss über den Login-Parameter login/ password_ max_ idle_initial erzwungen sein. **SOS:** Users with Initial Passwords Who Have Never Logged On (0009) **SOS:** Users with Reset Passwords Who Have Never Logged On (0140)
1.2.	**Welche Benutzer haben seit längerer Zeit ihr Passwort nicht geändert?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Seit 180 Tagen Kennwort nicht geändert, ggf. Voreinstellung im Feld „Tage seit Kennwortänderung" überschreiben. Oder Transaktion SUIM oder SA38 mit dem Report RSUSR200. Benutzer müssen regelmäßig ihr Kennwort ändern. Dies muss über den Login-Parameter login/ password_ expiration_time erzwungen sein. **SOS:** Users Who Have Not Logged On for an Extended Period of Time (0010)
2.	**Kontrollziel: Alle Benutzer sind mit einem Gültigkeitszeitraum versehen, der dem Zeitraum des notwendigen Zugriffs auf das SAP-System entspricht.** **Risiko:** Nicht mehr benötigte Benutzerkennungen werden nicht rechtzeitig erkannt und gesperrt. Sie sind anderen Benutzern bekannt, die unter dieser fremden Benutzerkennung auf das SAP-System zugreifen können, wenn ihnen das Kennwort auf welche Weise auch immer bekannt geworden ist.
2.1.	**Für welche Benutzer ist kein Gültigkeitszeitraum oder ein zu weit gefasster Gültigkeitszeitraum eingetragen?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Benutzer nach Anmeldedatum, Auswertung nach Feld „Gültig-Bis". Oder Transaktion SUIM oder SA38 mit dem Report RSUSR002. Oder über die Tabelle USR02 ermitteln, dabei keine Auswahl vornehmen, das Ergebnis nach dem Feld GLTB, „Gültig Bis", auswerten. Abgleich mit Informationen zu den Mitarbeitern, die die Personalabteilung bereitstellt. Ist z.B. für Mitarbeiter, die Auszubildende, temporäre oder externe Mitarbeiter sind, ein solches Gültig-Bis-Datum eingetragen, das dem befristeten Arbeitsverhältnis entspricht?

NR.	PRÜFPROGRAMM: GÜLTIGKEITSZEITRAUM VON BENUTZERKENNUNGEN
3.	Kontrollziel: **Besondere Zeiträume von Aktivität oder Inaktivität werden durch flexible Handhabung und unternehmensindividuelle Kennzeichnung der Sperrung einer Benutzerkennung kontrolliert.** Risiko: Nicht aktive Benutzerkennungen sind anderen Benutzern bekannt. Diese greifen unter dieser fremden Benutzerkennung auf das SAP-System zu, wenn sie das Kennwort ausprobiert oder ausgekundschaftet haben.
3.1.	**Sind unternehmensindividuelle Varianten der Sperrargumente aktiviert?** Tabelle USR02, Feld UFLAG, „User Sperre", mit „=" ‹LEER› auswählen, das Ergebnis nach dem Inhalt von Feld UFLAG auswerten. Sind temporäre Sperren aufgrund bekannter befristeter Abwesenheit eines Mitarbeiters oder besondere Sperrkennzeichnungen für solche Mitarbeiter gesetzt, die selten die Benutzerkennung benötigen. Diese Benutzer haben i.d.R. gleichbleibende Berechtigungen für einen definierten, aber temporären Auftrag, z.B. für Aktivitäten im Rahmen von Messeveranstaltungen.
4.	Kontrollziel: **Identifikation nicht mehr benötigter Benutzerkennungen** Risiko: Benutzerkennungen ausgeschiedener Benutzer werden nicht gelöscht.
4.1.	**Welche Benutzer haben sich über einen längeren Zeitraum nicht mehr angemeldet?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – „Benutzer nach Anmeldedatum" oder „Seit 30 Tagen nicht angemeldet", Auswertung nach dem Feld „Letzte Anmeldung". Oder Transaktion SUIM oder SA38 mit dem Report RSUSR200. Oder über die Tabelle USR02 ermitteln, dabei keine Auswahl vornehmen, das Ergebnis nach dem Feld TRDAT, „letztes Login-Datum", auswerten. Abgleich mit Informationen zu den Mitarbeitern, die die Personalabteilung bereitstellt. Benutzerkennungen ausgeschiedener Mitarbeiter sind zu löschen. **SOS:** Users Who Have Not Logged On for an Extended Period of Time (0010)
4.2.	**Welche Benutzer sind gesperrt?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Benutzer nach Anmeldedatum, Auswertung nach dem Feld „Benutzer gesperrt". Oder Transaktion SUIM oder SA38 mit dem Report RSUSR002. Oder über Tabelle USR02 ermitteln, Feld UFLAG, „User Sperre", mit „=" ‹LEER› auswählen, das Ergebnis nach dem Inhalt von Feld UFLAG auswerten. Benutzerkennungen, die seit längerer Zeit gesperrt sind, können Benutzerkennungen ausgeschiedener Mitarbeiter sein, die zu löschen sind. **SOS:** Profiles on Long Time Locked Users (0089)
4.3.	**Für welche Benutzer ist der angegebene Gültigkeitszeitraum abgelaufen?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Benutzer nach Anmeldedatum, Auswertung nach dem Feld „Gültig Bis". Oder Transaktion SUIM oder SA38 mit dem Report RSUSR002. Oder über die Tabelle USR02 ermitteln, dabei keine Auswahl vornehmen, das Ergebnis nach dem Feld GLTB, „Gültig Bis", auswerten. Benutzerkennungen, deren Gültigkeitszeitraum abgelaufen ist, können Benutzerkennungen ausgeschiedener Mitarbeiter sein, die zu löschen sind.

NR.	PRÜFPROGRAMM: GÜLTIGKEITSZEITRAUM VON BENUTZERKENNUNGEN
5.	**Kontrollziel: Benutzerkennungen sind bis auf definierte Ausnahmen personenbezogen.** Risiko: Benutzerkennungen werden als Sammelbenutzer verwendet. Es gibt keine organisatorische Regelung, die in bestimmten Fällen Sammelbenutzer zulässt, oder es gibt eine organisatorische Regelung für Benutzerkennungen, der aber in der Ausprägung der Benutzerkennungen nicht gefolgt wird.
5.1.	**Welche Benutzerkennungen sind nicht aufgrund des Namens eines Benutzers gebildet oder folgen nicht der festgelegten Namenskonvention für Benutzerkennungen?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Benutzer nach Anmeldedatum, Auswertung nach dem Feld „Benutzer". Oder Transaktion SUIM. Oder über die Tabelle USR02 ermitteln, dabei keine Auswahl vornehmen, das Ergebnis nach dem Feld BNAME, „Benutzername", auswerten. Manuelles Durchsuchen der Liste auf Bezeichnungen wie AZUBI, WERK-STUDENT, LAGER, TEST, TESTUSER, TST. Benutzerkennungen, die nicht der Namenskonvention folgen, können z.B. nicht autorisierte Sammelbenutzerkennungen sein.

3.7. PRÜFPROGRAMM: SICHERE KONFIGURATION BESONDERER BENUTZERTYPEN

Übersicht über initiale Anmeldung für Sonderbenutzer in SAP-Mandanten:

MANDANT	000/001	000/001	066	NEUER MANDANT
Benutzer	SAP*	DDIC	EarlyWatch	SAP*
Initiales Kennwort	Master-Kennwort wird während der Installation gesetzt.	Master-Kennwort wird während der Installation gesetzt.	Master-Kennwort wird während der Installation gesetzt.	pass
Kennwort im früheren Release	06071992	19920706		
Mandant	000/001/alle neuen Mandanten	000		
Benutzer	SAPCPIC	TMSADM		
Initiales Kennwort	ADMIN	Master-Kennwort wird während der Installation gesetzt.		

NR.	SICHERE KONFIGURATION BESONDERER BENUTZERTYPEN
1. H	**Kontrollziel: Schutz der Sonderbenutzer vor nicht autorisiertem Zugriff** **Risiko:** Jeder kann anonym die SAP-Standardbenutzer SAP* und Early Watch über die bekannten Standardkennwörter aufrufen und darunter nicht autorisierte Aktionen durchführen. Mit SAP* können z.B. SAP-interne Kontrollen unterlaufen und SAP-interne Zwangsprotokolle manipuliert werden. **Hinweis:** In den Mandanten 000 und 001 wird bei der Installation automatisch ein Benutzerstammsatz erzeugt. Es wird gefordert, ein individuelles Kennwort für SAP* und DDIC zu vergeben. Das Kennwort beider Standardbenutzer ist nicht mehr automatisch auf das Standardkennwort aus dem Jahr 1992 gesetzt.
1.1.	**Sind in jedem Mandanten die Standardkennwörter aller SAP-Standardbenutzer geändert?** **AIS:** System Audit – Top Ten Security Reports – Kennworte der Standardbenutzer prüfen SA38 mit Report RSUSR003. **Wenn die Prüferrolle diesen Report nicht zulässt, muss der Prüfer einen der zugelassenen Systemadministratoren in seinem Beisein den Report ausführen lassen und das Ergebnis sofort prüfen.** **SOS:** User EARLYWATCH Has Default Password (0056)
1.2.	**Ist der Benutzer SAP* gegen unbefugte Nutzung geschützt (SAP-Hinweise 2 383 und 68 048)?** Sämtliche Berechtigungen im Benutzerstammsatz SAP* werden gelöscht. › Der Benutzerstammsatz SAP* wird gesperrt. › Der Benutzerstammsatz SAP* wird der Gruppe SUPER zugeordnet. › 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. › Für die Systemadministration wird ein Notfallbenutzer mit umfassenden Berechtigungen angelegt. **SOS:** User SAP* is Neither Locked nor Expired (0043) **SOS:** User SAP* is Not Assigned to the Group SUPER (0044) **SOS:** Usage of the Hard Coded User SAP* is NOT Disabled (0046)
1.3.	**Ist der Benutzer SAP* in allen Mandanten ohne Berechtigungen angelegt und gesperrt?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzer –Benutzer nach komplexen Selektionskriterien, Selektion nach Benutzer SAP*, nach Anzeige des Ergebnisses im Auswahlmenü „Rollen" oder „Profile" anklicken. Oder Transaktion SUIM oder SA38 mit dem Report RSUSR002. **SOS:** Not All Profiles Are Removed from User SAP* (0042) **SOS:** User SAP* is Neither Locked nor Expired (0043)
1.4.	**Sind die Benutzer SAP* und DDIC in allen Mandanten der Benutzergruppe SUPER zugeordnet?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzer –Benutzer nach komplexen Selektionskriterien, Selektion nach Benutzern SAP*, DDIC. Oder Transaktion SUIM oder SA38 mit dem Report RSUSR002. **SOS:** User SAP* is Not Assigned to the Group SUPER (0044)

NR.	SICHERE KONFIGURATION BESONDERER BENUTZERTYPEN
1.5.	**Welche Benutzer- und Berechtigungsadministratoren dürfen die Benutzergruppe SUPER pflegen?** Transaktion SA38 mit dem Report RSUSR002 und den Eingaben: S_TCODE = SU01 S_USER_GRP (Benutzerverwaltung) mit Aktivität 01 (Anlegen), 02 (Ändern) oder „*" und Gruppe = „*" oder = „SUPER". **SOS:** Unexpected Users Are Authorized to Change a Super User Account (0026)
1.6.	**Ist der Parameter login/ no_automatic_user_sapstar auf den Wert 1 gesetzt?** **Hinweis 1:** Mit Hilfe diese Parameters kann verhindert werden, dass sich jemand nach dem Löschen des Benutzerstammsatzes für SAP* dann unter dem systeminternen automatischen Benutzer SAP* mit dem unveränderbaren Kennwort PASS anmelden kann (Wert 1). Wenn es bei der Standardeinstellung (Wert 0) bleibt, ist immer ein erneutes Anmeldung unter diesem systeminternen Benutzer SAP* möglich. **Hinweis 2:** Soll der systeminterne automatische Benutzer SAP* wieder aktiviert werden, muss erst dieser Parameter zurückgesetzt und das System wieder gestartet werden. **SOS:** Usage of the Hard Coded User SAP* is not Disabled (0046) **SOS:** User SAP* Has Been Deleted at Least in One Client (0045).
2.	**Kontrollziel: Sichere Nutzung des Konzeptes der Referenzbenutzer** **Risiko:** Benutzerkennungen vom Typ Referenz haben Berechtigungen, die die Prinzipien der Berechtigungsvergabe verletzen (Forderung nach geringstem Berechtigungsumfang; Einhaltung der Funktionstrennung).
2.1.	**Welche Benutzerkennungen sind Referenzbenutzer (Benutzertyp „L")?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Benutzer nach Anmeldedatum, Selektion nach Benutzertyp „Referenzbenutzer". Oder Transaktion SUIM oder SA38 mit dem Report RSUSR200. Selektion auf den Benutzertyp „Referenzbenutzer" einschränken.
2.2.	**Welche Rollen und Profile sind den Referenzbenutzern zugeordnet?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzer –Benutzer nach komplexen Selektionskriterien, Selektion nach Benutzertyp „Referenzbenutzer", nach Anzeige des Ergebnisses im Auswahlmenü „Rollen" oder „Profile" anklicken. Oder Transaktion SUIM oder SA38 mit dem Report RSUSR200. Selektion auf den Benutzertyp „Referenzbenutzer" einschränken. Über den Benutzernamen kann in die SU01 verzweigt werden. Auch Referenzbenutzer dürfen nur Berechtigungen haben, die für den Arbeitsplatz notwendig sind. Es darf keine Referenzbenutzer mit weit gefassten Berechtigungen, z.B. eines Superusers, geben.
2.3.	**Welchen Benutzern sind Referenzbenutzer zugeordnet?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzer –Benutzer nach komplexen Selektionskriterien, Liste der Referenzbenutzer im Feld „Referenzbenutzer" eingeben. Oder Transaktion SUIM oder SA38 mit dem Report RSUSR002. Welchen Benutzern sind Nicht-Referenzbenutzer als Referenz zugeordnet? **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzer –Benutzer nach komplexen Selektionskriterien, Selektion auf „Nicht gleich" ‹LEER› im Feld „Referenzbenutzer", in der Ergebnisliste die Nicht-Referenzbenutzer ermitteln. Oder Transaktion SUIM oder SA38 mit dem Report RSUSR002. **Hinweis:** Die Zuordnung eines „normalen" Benutzers als Referenzbenutzer kann über einen Eintrag im Customizing grundsätzlich verhindert werden (SAP-Hinweis 513 694). **SOS:** Usage of ‚Normal' Users as Reference Users is Not Prohibited (0012)

NR.	SICHERE KONFIGURATION BESONDERER BENUTZERTYPEN
2.4.	**Wird die Zuordnung von Referenzbenutzern protokolliert?** **AIS:** System Audit – Repository/Tabellen – Tabellenaufzeichnungen – Technische Tabelleneinstellungen, letzte Zeile in der Anzeige zur Tabelle USREFUS. Transaktion SE13 mit Tabelle USREFUS.
3.	**Kontrollziel: Sichere Nutzung des Konzeptes der Benutzer vom Typ Service** **Risiko:** Benutzerkennungen vom Typ Referenz haben Berechtigungen, die die Prinzipien der Berechtigungsvergabe verletzen (Forderung nach geringstem Berechtigungsumfang; Einhaltung der Funktionstrennung).
3.1.	**Welche Benutzerkennungen sind Servicebenutzer (Benutzertyp „S")?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Benutzer nach Anmeldedatum, Selektion nach Benutzertyp „Servicebenutzer". Oder Transaktion SUIM oder SA38 mit dem Report RSUSR002, Selektion nach Benutzertyp „Servicebenutzer".
3.2.	**Welche Rollen und Profile sind den Servicebenutzern zugeordnet?** **AIS:** System Audit – Benutzer und Berechtigungen - Infosystem – Benutzer –Benutzer nach komplexen Selektionskriterien, Selektion nach Benutzertyp „Referenzbenutzer", nach Anzeige des Ergebnisses im Auswahlmenü „Rollen" oder „Profile" anklicken. Oder Transaktion SUIM oder SA38 mit dem Report RSUSR200. Selektion auf den Benutzertyp „Servicebenutzer" einschränken. Über den Benutzernamen kann in die SU01 verzweigt werden. Auch Servicebenutzer dürfen nur Berechtigungen haben, die für die Funktion notwendig sind. Es darf keine Servicebenutzer mit weit gefassten Berechtigungen, z.B. eines Superusers, geben.
4.	**Kontrollziel: Sichere Nutzung des Konzeptes der Benutzergruppe** **Risiko:** Alle Benutzeradministratoren können einzelne Benutzer pflegen. Es kann zu nicht autorisierten Berechtigungsvergaben kommen. **Hinweis:** Über die Zuordnung eines Benutzers zu einer Benutzergruppe kann gesteuert werden, welche Benutzeradministratoren diesen Benutzer pflegen können. Wenn dieser Sicherheitsmechanismus genutzt wird, muss darauf geachtet werden, dass alle Benutzer auch einer Benutzergruppe zugeordnet werden. **Hinweis:** Eine Übersicht über die existierenden Benutzergruppen geben die Tabellen USGRP(T).
4.1.	**Welche Benutzerkennungen sind keiner Benutzergruppe zugeordnet?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Benutzer nach Anmeldedatum, Selektion auf „Gleich" <LEER> im Feld „Benutzertyp (allgemein)". Oder Transaktion SUIM oder SA38 mit dem Report RSUSR002, Selektion auf „Gleich" ‹LEER› für das Feld „Gruppe für Berechtigung" Wenn der Sicherheitsmechanismus der Benutzergruppe konsequent angewendet ist, darf es keine Benutzer ohne eine Benutzergruppe geben. **SOS:** Users Are NOT Assigned to User Groups (0005)
4.2.	**Wer kann Benutzergruppen anlegen?** Report RSUSR002 mit den Eingaben: S_TCODE = SUGR S_USER_GRP (Benutzerverwaltung) mit Aktivität „*" oder 01 (Anlegen) und Gruppe = „*" oder = Gruppennamen.

NR.	SICHERE KONFIGURATION BESONDERER BENUTZERTYPEN
4.3.	**Wer kann Benutzergruppen ändern?** Report RSUSR002 mit den Eingaben: S_TCODE = SU01 S_USER_GRP (Benutzerverwaltung) mit Aktivität „*" oder 02 (Ändern) und Gruppe = „*" oder = Gruppennamen.
4.4.	**Wie sind Benutzergruppen für Administratoren eingerichtet?** Report RSUSR002 mit den Eingaben: S_TCODE = SU01 S_USER_GRP (Benutzergruppen) mit Aktivität „*" oder 02 (Ändern) und Gruppe = „*" oder = „dieselbe Gruppe, die der Benutzeradministrator angehört" Über die Zuordnung der Benutzergruppe muss verhindert werden, dass ein Administrator dem eigenen Benutzerstammsatz Rollen/Profile zuweisen kann. Auch die Änderung der Benutzergruppen Zuweisung darf im eigenen Benutzerstammsatz nicht möglich sein. **SOS:** User Administrators Are Authorized to Change Their Own User Master Record (0003)

3.8. PRÜFPROGRAMM: ÜBERWACHUNG DER WIRKSAMKEIT DES ZUGRIFFSSCHUTZES

NR.	ÜBERWACHUNG DER WIRKSAMKEIT DES ZUGRIFFSSCHUTZES
1.	**Kontrollziel: Die Zugriffe auf das SAP-System werden regelmäßig überwacht. Es ist definiert, was auffällige Ereignisse sind. Sicherheitsverstöße werden bei Verdacht auf Missbrauch untersucht.** **Risiko:** Sicherheitsereignisse, die aufgrund fehlender oder falsch eingestellter sicherheitsrelevanter Parameter auftreten, werden nicht erkannt. Ein Sicherheitsverstoß oder Missbrauch eines Benutzers wird nicht zeitnah erkannt. Bei dem Verdacht auf Missbrauch kann im Nachhinein nicht mehr auf automatisch erfolgte Systemaufzeichnungen zurückgegriffen werden, die zur Aufklärung des Vorgangs oder zur Verfolgung der Täter dienen können.
	Kontrollfragen zum Prozess: › Ist dokumentiert, dass das SAP Security Audit Log aktiviert werden muss und welche Mindesteinstellungen dabei vorgenommen werden müssen? › Ist definiert, wer für die Einrichtung und Änderung der Einstellungen des SAP Security Audit Logs und das Löschen der Protokolldateien zuständig ist? › Gibt es einen definierten Prozess für die Auswertung und Überwachung der Ereignisse, die über das SAP Security Audit Log aufgezeichnet werden? › Gibt es eine Vorgabe, wie lange die Protokolldateien im System vorgehalten werden müssen, z.B. um nachträglich noch Recherchen zu Sicherheitsereignissen durchführen zu können, die erst später und auf anderem Wege bekannt geworden sind?
1.1.	**Ist das SAP Security Audit Log aktiviert? Welche Benutzer, welche Audit-Klassen, welche Ereignisse werden protokolliert?** **AIS:** System Audit – Systemprotokolle und Statusanzeigen – Security Audit Log oder Transaktion SM19 SOS: Security Critical Events for End Users Are Not Logged in the Security Audit Log (0136) **Empfehlung 1:** Kritische Ereignisse bei den folgenden Audit-Klassen Dialog-Anmeldung RFC-/CPIC-Anmeldung RFC-Funktionsaufruf werden für **alle Benutzer** in **allen Mandanten** protokolliert. **Empfehlung 2:** Alle Ereignisse aller Audit-Klassen werden für alle Notfallbenutzer protokolliert. **Empfehlung 3:** Alle Ereignisse aller Audit-Klassen werden für alle Dialogbenutzer in der Benutzergruppe SUPER protokolliert.
1.2.	**Wer darf das SAP Security Audit Log aktivieren und die Einstellungen dazu ändern?** Report RSUSR002 mit den Eingaben: S_TCODE = SM19 S_ADMI_FCD (Systemberechtigung) mit Funktion AUDA (Audit Administration) S_C_FUNCT (direkter Aufruf von C-Kernel-Funktionen aus ABAP) mit Aktivität „16" „Ausführen" und Programmname „SAPLSECU" und C-Routine „AUDIT_SET_INFO". Diese Berechtigung ist im Produktivsystem nur für Systemadministratoren zulässig.

NR.	ÜBERWACHUNG DER WIRKSAMKEIT DES ZUGRIFFSSCHUTZES
1.3.	**Wer darf die Protokolldateien des SAP Security Audit Log auswerten?** S_TCODE = SM20 S_ADMI_FCD (Systemberechtigung) mit Funktion AUDD (Audit Anzeige) Diese Berechtigung ist im Produktivsystem nur Systemadministratoren und für die Mitarbeitern zulässig, die für die Aufgabe der Überwachung und Auswertung der Ereignisse zuständig sind.
1.4.	**Wer darf die Protokolldateien des SAP Security Audit Log löschen?** Report RSUSR002 mit den Eingaben: S_TCODE = SM18 oder SA38 oder SE38 (Report RSAUPURG) S_ADMI_FCD (Systemberechtigung) mit Funktion AUDA (Audit Administration) und ST0R (Auswerten von Traces) S_DATASET (Berechtigung zum Dateizugriff) mit Aktivität „34" und Programmname „SAPLSTUW" und Dateiname (Pfad gemäß der Angabe zu dem Profilparameter DIR_AUDIT, in dem die Protokolldateien gespeichert sind). Diese Berechtigung ist im Produktivsystem nur für Systemadministratoren zulässig.
2.	**Kontrollziel: Aufdecken von Versuchen, das Kennwort einer Benutzerkennung auszuprobieren.** **Risiko:** Ein Benutzer versucht, das Kennwort eines anderen Benutzers systematisch auszuprobieren.
2.1.	**Zu welchen Benutzerkennungen ist eine hohe Anzahl von Falschanmeldungen registriert?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Benutzer nach Anmeldedatum, Selektion auf „Benutzer mit Falschanmeldungen". Oder Transaktion SUIM oder SA38 mit dem Report RSUSR200.
2.2.	**Welche Benutzerkennungen, die seit langem inaktiv sind, haben eine Sperre wegen Falschanmeldung?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzerübersicht – Benutzer nach Anmeldedatum, Selektion auf „Benutzer mit Falschanmeldungen". Oder Transaktion SUIM oder SA38 mit dem Report RSUSR200.
2.3.	**Prüfung auf Anmeldefehler mit dem SAP Security Audit Log:** Transaktion SM20, Auswahl „Alle entf. Auditlogs", „von Datum" und „bis Datum" eingeben, Wechsel in den Expertenmodus über den Menüpunkt „Bearbeiten – Expertenmodus", Einschränkung z.B. auf folgende Meldungen: AU0, AU2, fehlgeschlagenes Login AUM, Benutzer wurde nach Falschanmeldungen gesperrt AUN, Benutzersperre wegen Falschanmeldungen wurde wieder aufgehoben. Die angezeigten Protokollsätze sind auf auffällige zeitliche Häufungen bei einer Benutzerkennung zu untersuchen. Detailinformationen können durch Doppelklick auf die Einzelmeldungen angezeigt werden. **Hinweis:** Die Texte zu allen Meldekennungen sind in der Tabelle TSL1T hinterlegt. Die für die Protokolldateien des SAP Security Audit Log relevanten Meldekennungen beginnen mit AU.

NR.	ÜBERWACHUNG DER WIRKSAMKEIT DES ZUGRIFFSSCHUTZES
2.4.	**Prüfung auf Anmeldefehler mit dem Systemlog:** Transaktion SM21, Auswahl „Alle entf. SysLogs", „von Datum" und „bis Datum" eingeben, Wechsel in den Expertenmodus über den Menüpunkt „Bearbeiten – Expertenmodus", über die Schaltfläche „Meld.kennungen" z.B. auf folgende Meldungen einschränken: › US1 „Ein Benutzer wurde auf Grund von Falschanmeldungen gesperrt." › US3 „Es wurde versucht, sich mit einem gesperrten Benutzer anzumelden." **Hinweis:** Die Texte zu allen Meldekennungen sind in der Tabelle TSL1T hinterlegt.
3.	**Kontrollziel: Aufdecken von Versuchen, sich mit einem ungültigen Anmeldeticket anzumelden.** **Risiko:** Ein Benutzer versucht systematisch, sich mit einem ungültigen Anmeldeticket anzumelden.
3.1.	**Prüfung auf Anmeldefehler mit dem Systemlog:** Transaktion SM21, Auswahl „Alle entf. SysLogs", „von Datum" und „bis Datum" eingeben, Wechsel in den Expertenmodus über den Menüpunkt „Bearbeiten – Expertenmodus", über die Schaltfläche „Meld.kennungen" z.B. auf folgende Meldungen einschränken: › USD „Der Aussteller & A des Anmeldetickets konnte nicht überprüft werden" › USE „Der Aussteller & A des Anmeldetickets ist nicht in der ACL" › USF „Es wurde ein nicht interpretierbares Anmeldeticket empfangen" **Hinweis:** Die Texte zu allen Meldekennungen sind in der Tabelle TSL1T hinterlegt.

4. AUTORISIERUNG (ABAP-STACK)

4.1. BERECHTIGUNGSVERGABE

Der Zugriff eines Benutzers auf die Funktionen und Daten des SAP-Systems wird über Berechtigungen freigeschaltet. Dabei gelten nachfolgende Vergabegrundsätze:

- Grundsätzlich sollen die Berechtigungen eines Benutzers nur diejenigen Sichten und Funktionen für die Daten freigeben, die er zur Erfüllung der Tätigkeiten an seinem Arbeitsplatz benötigt. Dies wird als das Prinzip des geringsten Berechtigungsumfangs, im englischen Sprachgebrauch als „least privilege" bezeichnet,
- sensitive Funktionen (Sensitive Access – SA) dürfen nur an einzelne, wenige Personen mit angemessener Erfahrung vergeben werden. Sensitive Funktionen beziehen sich dabei auf Funktionen, die notwendig, aber sensitiv sind (z.B. Öffnen und Schließen von Buchungsperioden im SAP System),
- neben der restriktiven Vergabe ist bei der Berechtigungsvergabe darauf zu achten, dass angemessene Anforderungen an die Funktionstrennung eingehalten werden. Eine Funktionstrennungsregel besteht dabei jeweils aus mindestens zwei Funktionen in Kombination, die nicht zusammen vergeben werden dürfen. Dieses Prinzip der Funktionstrennung hilft, Fehler und Missbrauch zu verhindern. Im englischen Sprachgebrauch wird es „principle of segregation of duties", kurz SoD, genannt.

Für die Unternehmen leiten sich die Vergabegrundsätze aus den Anforderungen an ein internes Kontrollsystem ab. Unternehmen müssen ein internes Kontrollsystem einrichten, warten, überwachen und kontinuierlich optimieren.

4.2. DIFFERENZIERUNGSMODELLE FÜR BERECHTIGUNGSKONZEPTE

Das Berechtigungskonzept samt dessen technischer Umsetzung im SAP-ECC-System muss dazu geeignet sein, die unternehmensspezifischen Anforderungen der Ablauforganisation (Abbildung einzelner Prozessschritte/Aufgaben oder ganzer Arbeitsplätze durch Berechtigungen in rollen) und der Aufbauorganisation (organisatorischer/rechtlicher Aufbau des Unternehmens) zu erfüllen.

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 klassischen SAP-ECC-Systemen werden standardmäßig rollenbasierte Berechtigungskonzepte systemseitig unterstützt.

Für die Einrichtung von rollenbasierten Berechtigungskonzepten in SAP-ECC-Systemen stehen mehrere Modelle zur Abbildung der ablauf- und aufbauorganisatorischen Unternehmensanforderungen in den Rollen zur Verfügung. Generell kann hierbei zwischen dem Kombinations- und Trennmodell unterschieden werden:

- Kombinations-Rollen-Modelle: innerhalb einer Rolle wird die ablauf- und aufbauorganisatorische Dimension kombiniert. Eine Rolle eines Kombinations-Rollen-Modells enthält insofern

immer alle technischen Berechtigungen, die zur Ausführung der in der Rolle enthaltenen Aufgaben benötigt werden. Als Beispiel: Rolle „Beleg buchen für Buchungskreis 1". Die entspricht der Ableitungsfunktion des SAP-Profilgenerators.

- Trenn-Rollen-Modelle: in diesen Modellen werden für die ablauforganisatorische Dimension einerseits und die aufbauorganisatorische Dimension andererseits eigenständig getrennte Rollen eingerichtet. Somit benötigt ein Benutzer für eine Aufgabe immer zwei Rollen, eine für den prozessualen Teil (Prozessrolle) und eine für den organisatorisch/funktionalen Teil (Differenzierungsrolle). Als Beispiel: Prozessrolle „Beleg buchen" und Differenzierungsrolle „Buchungskreis 1".

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

4.3. RISIKEN

Die Risiken liegen in der mangelhaften Umsetzung des geforderten internen Kontrollsystems, das unternehmensindividuell und risikoorientiert über die Vergabe von Berechtigungen zu realisieren ist. Beispiele für Risiken sind:

- Die Prüfbarkeit des Benutzer- und Berechtigungskonzeptes ist nicht gewährleistet, da es nicht angemessen dokumentiert ist.
- Das Berechtigungskonzept genügt nicht den gesetzlichen und unternehmensinternen Anforderungen (z.B. da es keine geeigneten Funktionstrennungsregeln beinhaltet).
- Wesentliche interne Kontrollen fehlen in der Benutzer- und Berechtigungsverwaltung (z.B. Genehmigungsregelungen).
- Organisatorische oder technische Schwachstellen ermöglichen ein Unterlaufen der beabsichtigten internen Kontrollen.
- Universelle Berechtigungen und sicherheitskritische Systemeinstellungen werden nach dem Produktiveinsatz im SAP-System nicht geändert, obwohl SAP diese nur für die Phase der Implementierung oder des Release-Wechsels vorgesehen hat. Im Produktivsystem gefährden diese aber die Systemintegrität und den ordnungsmäßigen Betrieb.
- Kritische Berechtigungen, die gegen gesetzliche und unternehmensinterne Regelungen verstoßen (internes Kontrollsystem), werden ohne Restriktionen vergeben. Es ist nicht festgelegt worden, welche Berechtigungen als kritisch einzuordnen sind, und die Bedingungen sind nicht festgelegt, unter denen sie vergeben werden dürfen.
- Technische Konzepte, die das SAP-System zur Ausprägung und Prüfung von Berechtigungen bereitstellt, werden nicht konsequent genutzt. Beispiele sind Berechtigungsgruppen von Tabellen und Programmen oder Berechtigungsprüfungen in selbst entwickelten Programmen. Somit werden Sicherheitslücken in Kauf genommen, die die Manipulation an kritischen Systemeinstellungen oder an Geschäftsdaten zulassen.
- Die eingerichteten Benutzerkennungen und die vergebenen Berechtigungen werden nicht regelmäßig geprüft und bestätigt. Möglicher Missbrauch einzelner Benutzerkennungen durch fremde Benutzer oder durch einen Benutzer, der im Zeitlauf mit umfangreichen Berechtigungen ausgestattet wurde, wird nicht verhindert.

4.4. KONTROLLZIELE

Die Kontrollziele beziehen sich in der Regel auf die effektive und effiziente Gestaltung der Prozesse der Benutzer- und Berechtigungsverwaltung:

- Ein dokumentiertes Berechtigungskonzept liegt vor, das die gesetzlichen und unternehmensinternen Anforderungen erfüllt.
- Die Organisation der Benutzer- und Berechtigungsverwaltung ist auch im SAP-System durch angemessene Autorisierung der dafür vorgesehenen Mitarbeiter gewährleistet. Insbesondere wird die Funktionstrennung im Rahmen der Benutzer- und Berechtigungsverwaltung berücksichtigt.
- Universelle SAP-Standardprofile, die nur für die Implementierung und den Release-Wechsel bereitgestellt sind, sind nicht vergeben oder durch unternehmensspezifische Berechtigungen angepasst oder abgelöst.
- Sensitive/kritische Berechtigungen sind identifiziert und die Restriktionen dokumentiert, unter denen sie zu vergeben sind. Sicherheitskritische Funktionen werden nur restriktiv und kontrolliert vergeben.
- Das in Einzelfällen notwendige Aufheben der von SAP vorgesehenen Sicherheitseinstellungen ist autorisiert und dokumentiert (z.B. Konzept für Notfallbenutzer).
- Prozesse zur Ausprägung von Berechtigungsgruppen und zur Prüfung von Berechtigungen in Eigenentwicklungen sind definiert und wirksam.
- Die Benutzer- und Berechtigungsverwaltung wird regelmäßig überwacht und die Prozesse dazu geprüft und optimiert.

4.5. PRÜFPROGRAMM: DOKUMENTIERTES BENUTZER- UND BERECHTIGUNGSKONZEPT

NR.	INHALTE EINES DOKUMENTIERTEN BERECHTIGUNGS- UND BENUTZERKONZEPTES
H	**Kontrollziel: Die Dokumentation des Berechtigungs- und Benutzerkonzeptes erfüllt die Mindestanforderungen.** **Risiko:** Gesetzliche Anforderungen an die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Berechtigungs- und Benutzerkonzeptes sind nicht erfüllt. Die Wirksamkeit eines Berechtigungs- und Benutzerkonzeptes kann nur geprüft werden, wenn das Sollkonzept dokumentiert ist.
1.	**Allgemeine Dokumentationsstandards**
1.1.	Ist einem sachkundigen Dritten ein angemessener Einstieg in die Dokumentation des Benutzer- und Berechtigungskonzeptes möglich, indem in der Einleitung die Schilderung des Inhalts und **Gegenstands** des Dokumentes dargelegt wird? *Prüfung der Einleitung darauf hin, ob Struktur und Inhalt der Dokumentation nachvollziehbar sind.*
1.2.	**Sind die mit dem Dokument erfolgten Ziele geeignet herausgearbeitet?** *Prüfung des Dokumentes auf eine ausreichende Zielerläuterung und ob die erforderlichen Compliance-Aspekte im Wesentlichen widerspiegelt werden.*

NR.	INHALTE EINES DOKUMENTIERTEN BERECHTIGUNGS- UND BENUTZERKONZEPTES
1.3.	Sind die **Adressaten** des Dokumentes ausreichend benannt? Dies sollten zumindest die aus Compliance-Gesichtspunkten relevanten Beteiligten sein. *Prüfung des Dokumentes nach einer Erläuterung der Adressaten und der mit dem Benutzer- und Berechtigungskonzept direkt oder indirekt befassten Personen. Beurteilung, ob die genannten Personenkreise mit den aus Compliance-Gründen üblicherweise mit dem Benutzer- und Berechtigungskonzept befassten Personen korrespondieren.*
1.4.	Ist die thematische und zeitliche **Gültigkeit** des Dokumentes definiert? Diese bezieht sich insbesondere auf die vom Dokument betroffenen Systeme/Mandanten sowie Module/Prozesse. *Prüfung des Dokumentes nach einer Identifizierung des Geltungsbereichs der Dokumentation.*
1.5.	Sind im Dokument externe und insbesondere **interne Anforderungen** ausreichend berücksichtigt? *Prüfung des Dokumentes nach einer Aufstellung der im Rahmen des Benutzer- und Berechtigungskonzeptes zu beachtenden externen Anforderungen (Compliance-Vorgaben) und internen Regelungen.*
1.6.	Ist im Dokument festgelegt, wer für die Pflege des Dokumentes verantwortlich ist, wer das Dokument originär abgenommen hat und wie Änderungen am Dokument zu genehmigen sind? Sind die am Dokument vorgenommenen Änderungen sowie deren Abnahme in einer **Dokumentenhistorie** festgehalten? *Prüfung des Dokumentes auf die Benennung von Dokumentenverantwortlichen und ob diese tatsächlich mit den aktuellen Verantwortlichen übereinstimmen.*
1.7.	**Ist die aktuelle Version des Dokumentes durch das zuständige Gremium abgenommen? Ist die aktuelle Version an angemessener Stelle publiziert?** *Prüfung, ob Abnahme für Dokument vorliegt und ob das Dokument entsprechend publiziert ist.*
2	**Rollen und Berechtigungen**
	a) Prozessbereiche
2.1.	Ist für alle **Prozessbereiche** des Unternehmens eine vollständige und angemessen strukturierte Übersicht der Prozessbereiche (Prozessmodell) vorhanden? *Aufnahme der für das Unternehmen vorhandenen Prozessbereiche; Abgleich und Beurteilung der Angemessenheit, Vollständigkeit und Aktualität der Dokumentation mit den erhobenen Daten.*
	b) Organisationsdimensionen
2.2.	Ist pro Prozess und -teilbereich dargestellt, welche **Organisationsdimensionen** jeweils relevant sind (rechtliche Einheit, Werk, Kostenrechnungskreis etc.)? *Prüfung des Dokumentes auf Auflistung der für das Unternehmen relevanten Organisationsdimensionen pro Prozess und -teilbereich.*

NR.	INHALTE EINES DOKUMENTIERTEN BERECHTIGUNGS- UND BENUTZERKONZEPTES
2.3.	Sind für jede Organisationseinheit die vorhandenen **Ausprägungen** aufgeführt? *Beurteilung der Vollständigkeit und Richtigkeit der in den Dokumentationen vorhandenen Aufstellungen zur Ausprägung der Organisationsdimensionen. Dies kann auch mit Verweis auf andere Dokumentationen oder direkt auf das System erfolgen. Insbesondere sollte der für die Organisationsdimensionen strukturgebende Grundgedanke erkennbar werden. Über die SAP-Tabelle AGR_1252 können die aktuell verwendeten Organisationsdimensionen pro SAP-Rolle samt Ausprägungen eingesehen werden.*
	c) Namenskonventionen
2.4.	Ist eine eindeutige Festlegung von **Namenskonventionen** für Berechtigungen vorhanden? *Beurteilung des Vorhandenseins, der Vollständigkeit und der Nachvollziehbarkeit der Namenskonvention (Anforderungen an Namenskonvention siehe nächsten Abschnitt).*
2.5.	Ist in der Namenskonvention kodiert › ob es sich um eine **Standardrolle** handelt, welche im Produktivsystem vergeben werden darf? › der **Prozessbereich**, für den die jeweilige Rolle berechtigt? › die **Organisationseinheit**, für die die jeweilige Rolle berechtigt? › der **Risikogehalt** einer Rolle? Weiterführende Informationen zur (Außen-)Gestaltung von Rollen sind in Kapitel „4.6 Prüfprogramm: Ordnungsgemäße Gestaltung von Rollen" aufgeführt. *Prüfung, ob die Namenskonvention die o.g. Punkte berücksichtigt; Prüfung, ob die im SAP-System vorhandenen Rollen der Namenskonvention laut Berechtigungskonzept entsprechen (die im SAP-System vorhandenen Rollen können über die Tabelle „AGR_Define" eingesehen werden)*
2.6.	Ist neben der Konvention für die technischen Namen ebenfalls eine Minimalkonvention für die Beschreibung und den **Langtext von Rollen** vorhanden? *Prüfung, ob ebenfalls eine Namenskonvention für den Text und die Beschreibung von Rollen vorhanden ist.*
	d) Ausnahmeregelungen
2.7.	Werden **eigenentwickelte Berechtigungsobjekte** verwendet und sind diese in den Dokumentationen angemessen beschrieben? Dies bezieht sich sowohl auf die durch die Berechtigungsobjekte geschützten betriebswirtschaftlichen Objekte als auch auf die Kriterien, über die der Zugriff gesteuert wird. *Prüfung, ob der Mandant eigene Berechtigungsobjekte erstellt hat.* *Prüfung, ob die Berechtigungsobjekte entweder im System in der Dokumentation oder außerhalb angemessen erläutert werden.*

NR.	INHALTE EINES DOKUMENTIERTEN BERECHTIGUNGS- UND BENUTZERKONZEPTES
2.8.	Werden vom Unternehmen Berechtigungsobjekte **kundenspezifisch aktiviert** und sind diese Einstellungen in den Dokumentationen angemessen beschrieben? *Prüfung, ob der Mandant Berechtigungsobjekte abweichend von den Standardeinstellungen aktiviert hat.* *Prüfung, ob die Einstellungen entweder im System in der Dokumentation oder außerhalb angemessen erläutert werden.*
	e) Verantwortlichkeiten
2.9.	Ist jede Rolle (wenn möglich über die Zuordnung zu einem Prozessbereich und einer Organisationseinheit) eindeutig einem **Datenverantwortlichen** zugeordnet? Dieser ist für Einrichtung und Änderung der Rollen sowie für die Genehmigung der Vergabe der Rollen verantwortlich. *Prüfung, ob eine eindeutige Zuordnung jeder Rolle zu einem Datenverantwortlichen möglich ist.*
2.10.	Ist jede Rolle (wenn möglich über die Zuordnung zu einem Prozessbereich und einer Organisationseinheit) eindeutig einem **Keyuser** zugeordnet? Dieser unterstützt fachlich den IT-Bereich und den Datenverantwortlichen in Fragen der Pflege und Vergabe von Rollen. *Prüfung, ob eine eindeutige Zuordnung jeder Rolle zu einem Keyuser möglich ist.*
3	**Benutzer und Rechte**
	a) Personalbereiche
3.1.	Ist eine angemessene Organisationsstruktur vorhanden, die Planstellen, Personalbereiche und Personal eines Unternehmens hierarchisch miteinander verbindet. *Aufnahme der für das Unternehmen verfügbaren Informationen zur Organisationsstruktur (im Idealfall stammt diese aus dem Organisationsmanagement des SAP). Beurteilung, ob die Unterlagen eine eindeutige Zuordnung von Vorgesetzten zu Personalbereichen ermöglichen.*
3.2.	Sind eindeutige **Zusammenhänge** zwischen den **Personalbereichen** und den **Prozessbereichen** hergestellt? Hierdurch kann die Angemessenheit von Rollen für Benutzer beurteilt werden. *Prüfung, ob eine Zuordnung von Prozessbereichen und Personalbereichen vorgenommen wurde. Sofern nicht Prüfung, ob die vorhandenen Strukturen für Prozessbereiche und Personalbereiche geeignet sind, um einen solchen Zusammenhang herzustellen.*
	b) Benutzertypen
3.3.	Liegt eine strukturierte und vollständige Definition aller in den SAP-Systemen eines Unternehmens relevanten **Benutzertypen** vor? *Prüfung, ob alle typischerweise vorkommenden Benutzertypen vollständig und zutreffend definiert sind (Dialogbenutzer, Systembenutzer etc.).*

NR.	INHALTE EINES DOKUMENTIERTEN BERECHTIGUNGS- UND BENUTZERKONZEPTES
3.4.	Werden **Benutzergruppen** verwendet, die angemessen zur Funktionstrennung genutzt werden können? *Prüfung, welche Benutzergruppen im SAP-System eingerichtet sind.* *Beurteilung, ob diese in Anlehnung an die Benutzertypen zur Differenzierung der Berechtigungen genutzt werden (Vermeidung der Eigenadministration, Differenzierung von personalisierten Benutzern und Sonderbenutzern etc.).* *Benutzergruppen können über Tabelle USGRP eingesehen werden.*
	c) Benutzerkonventionen
3.5.	Verfügt jeder Benutzer über eine eindeutige **Benutzer-ID**? Eine Person sollte soweit möglich dieselbe Benutzer-ID in allen Systemen haben. *Prüfung, ob geeignete Konventionen für die Benutzer-ID von Personen dokumentiert sind.* *Benutzer-IDs zu Benutzern können über den Report RSUSR002 eingesehen werden.*
3.6.	Sind angemessene **Mindestinformationen** für die Pflege des Benutzerstamms festgelegt? Wird systemseitig die Eingabe der Mindestinformationen erzwungen? Mindestinformationen stellen der Personalbereich zur Ableitung des Vorgesetzten sowie die Benutzergruppe dar. Sind neben den Mindestinformationen auch Festlegungen zu optionalen Informationen getroffen? *Prüfung, ob eine angemessene Vorgabe für Mindestbenutzerinformationen dokumentiert ist.* *Mindestinformationen zu Benutzern können über den Report RSUSR002 eingesehen werden.*
	d) Verantwortlichkeiten
3.7.	Ist für jeden Benutzer (intern, extern, nichtpersonalisiert) die Identifizierung eines **Verantwortlichen** möglich? Dieser ist vollumfänglich für den Benutzer, seine Daten, seine Berechtigungen und die Verwendung des Benutzers verantwortlich. *Prüfung, ob über die vorhandenen Konventionen für jeden Benutzer die Identifizierung eines Verantwortlichen möglich ist.*
	e) Sonder- und Notfallbenutzer
3.8.	Sind geeignete Regelungen für **Sonderbenutzer** und ihre Berechtigungen (wie z.B. DDIC, CPIC, SAP* etc. bei SAP-Systemen) getroffen? *Prüfung, ob Regelungen für die Berechtigungen von Sondernutzern getroffen worden sind (weiterführende Prüfungshinweise siehe Kapitel 3.7 Prüfprogramm: Sichere Konfiguration besonderer Benutzertypen).*
3.9.	Sind geeignete Regelungen für **Notfallbenutzer** und ihre Berechtigungen (Passwortschutz, Freigabeverfahren, Protokollierung, Nachkontrolle) getroffen? *Prüfung, ob die notwendigen Regelungen für die Berechtigungen, den Schutz, ein Verfahren zur Freigabe, die Protokollierung der Aktivitäten sowie für die Nachkontrolle der Aktivitäten eines Notfallbenutzers getroffen worden sind (weiterführende Prüfungshinweise siehe Kapitel 4.7 Prüfprogramm: Notfallbenutzerkonzept (ABAP-Stack)).*

NR.	INHALTE EINES DOKUMENTIERTEN BERECHTIGUNGS- UND BENUTZERKONZEPTES
3.10.	Sind u.a. im Zusammenhang mit Sonder- und Notfallbenutzer Vorgaben zur Konfiguration, Nutzung und Überwachung des **„Security Audit Log"** definiert? *Prüfung, ob Regelungen zum Security Audit Log existieren.* *Das Security Audit Log kann über die Transaktion SM20 eingesehen werden.*
	c) Vorgaben Anmeldekontrollen
3.11.	Ist definiert, welche Profilparameter für die Anmeldekontrolle relevant und konfiguriert sind? Sind Angaben für die konkrete Ausgestaltung der Parameter vorhanden? *Prüfung, ob die Profilparameter für die Anmeldekontrollen mit den Parametern aus dem Berechtigungs- und Benutzerkonzept übereinstimmen.* *Die Profilparameter sind über den Report „RSPARAM" einsehbar.* *Prüfung, ob die definierten Parameter den Mindestanforderungen nach SAP ERP Prüfleitfaden entsprechen (weiterführende Prüfungshinweise siehe Kapitel 3.5 Tabelle: Vorschlagswerte für die Systemparameter der Anmeldekontrolle).*
4	**Benutzer und Rechte**
	a) Prozess- und Risikobereiche
4.1.	Sind die Prozesse des Unternehmens nach den ihnen innewohnenden **Risiken** in Bezug auf den Jahresabschluss, aber auch ggf. auf operative Risiken bewertet? Hierzu kann auf bereits etablierte Verfahren des Risikomanagements zurückgegriffen werden. Soweit in Prozessbereichen Risiken für den Jahresabschluss identifiziert wurden, sollte beurteilt sein, ob Funktionstrennungen und die Handhabung sensitiver Funktionen zur Minderung der Risiken im Rahmen des internen Kontrollsystems genutzt werden müssen. Ist dies der Fall, sind Prozesse zur Überwachung von sensitiven Funktionen und Funktionstrennungen im Unternehmen für die betrachteten Systeme und Prozesse zu etablieren. *Prüfung, ob Prozesse und Konventionen für die Überwachung sensitiver Funktionen und Funktionstrennungen etabliert sind.*
	b) Sensitive Funktionen
4.2.	Sind Funktionen, die einen erkennbaren Einfluss auf die Integrität der Jahresabschlussinformationen (insbesondere auf deren Vollständigkeit und Richtigkeit) haben und in den SAP-Systemen gepflegt werden, im Rahmen eines Regelwerks für **Sensitive Funktionen** erfasst? Ist innerhalb des Regelwerkes zusätzlich definiert, welche Berechtigungen (Transaktionscodes und Berechtigungsobjekte) im betrachteten System zur Ausführung der Funktion erforderlich sind? *Prüfung, ob für die als risikorelevant eingestuften Prozessbereiche Regeln für sensitive Funktionen definiert sind.* *Prüfung, ob die in den Prozessbereichen definierten Regeln vollständig alle relevanten Funktionen abdecken.* *Prüfung, ob pro Funktion die dafür benötigten Berechtigungen aufgeführt sind.*

NR.	INHALTE EINES DOKUMENTIERTEN BERECHTIGUNGS- UND BENUTZERKONZEPTES
4.3.	Ist in Abhängigkeit des Einflusses der sensitiven Funktionen auf die Datenintegrität (Risiko der Funktionen) eine **Risikoeinstufung** der Funktionen erfolgt? *Prüfung, ob für die definierten sensitiven Funktionen eine Beurteilung des hiermit verbundenen Risikos vorliegt. Sinnvoll ist hierbei zumindest eine Einteilung in kritische Funktionen, die im jeweils beurteilten System aufgrund Ihres Risikos für die Integrität von Daten oder System überhaupt nicht vergeben werden sollten und restriktive Funktionen, die zwar grundsätzlich vergeben werden können, jedoch lediglich an einen mehr oder weniger eingeschränkten Personenkreis. Hier kann zur Verfeinerung eine Differenzierung in hoch, mittel und gering erfolgen.*
	c) Funktionstrennung
4.4.	Sind sensitive Funktionen im Rahmen eines **Regelwerks** für Funktionstrennungen erfasst? *Prüfung, ob für die als risikorelevant eingestuften Prozessbereiche Regeln für Funktionstrennungen definiert sind. Stellen Sie fest, ob die in den Prozessbereichen definierten Regeln vollständig alle relevanten Funktionstrennungen abdecken.*
4.5.	Sind in Abhängigkeit des Einflusses der Funktionstrennungen auf die Datenintegrität (Risiko der Funktionstrennungen) die Funktionstrennungsregeln einer **Risikoeinstufung** unterzogen worden? *Prüfung, ob für die definierten Funktionstrennungen eine Beurteilung des hiermit verbundenen Risikos vorliegt. Sinnvoll ist hierbei in hoch, mittel und gering je nach dem direkten Einfluss auf die Integrität von System und Daten.*
	d) Kompensierende Kontrollen, Namenskonvention und Verantwortung
4.6.	Sind geeignete **kompensierende Kontrollen** etabliert, soweit aufgrund geringer Kapazitäten, Urlaubsregelungen oder Ähnlichem eine Funktionstrennung oder restriktive Handhabung sensitiver Funktionen nicht möglich ist? Diese müssen geeignet gestaltet sein, um Risiken von Funktionen zu kompensieren. Sind für die kompensierenden Kontrollen definiert, für welche sensitiven Funktionen und in welchem Umfang diese eine kompensierende Wirkung entfalten? *Prüfung, ob das Unternehmen ein Standardvorgehen für die Behandlung von Funktionstrennungskonflikten festgelegt hat und ob in Ausnahmefällen Funktionstrennungsverletzungen als zulässig gelten, wenn diese kompensiert werden.* *Prüfung, ob in diesem Fall geeignete Vorgaben existieren, wie kompensierende Kontrollen zu definieren und anzuwenden sind.* *Prüfung, ob Kataloge von Kontrollen als Vorschlagswerte für die Prozessbereiche vorhanden sind, in denen diese als Lösung für Risiken aus Regelverletzungen akzeptiert werden.*
4.7.	Ist in der **Namenskonvention** einer Regel (sensitiven Funktion oder Funktionstrennung) oder einer Kontrolle der Prozessbereich kodiert, auf den die jeweilige Regel sich auswirkt? Ist ebenso durch die Namenskonvention vorgegeben, ob es sich bei einer Regel um eine Regel zur Überwachung einer sensitiven Funktion oder um eine Funktionstrennung handelt? *Prüfung, ob die Namenskonvention eine durchgängige Kodierung des einheitlich definierten Prozessbereichs berücksichtigt.*

NR.	INHALTE EINES DOKUMENTIERTEN BERECHTIGUNGS- UND BENUTZERKONZEPTES
4.8.	Kann jede Regel und Kontrolle über die Zuordnung zu einem Prozessbereich eindeutig einem **Datenverantwortlichen** zugeordnet werden? Dieser ist für Einrichtung und Änderung der Regeln und Kontrollen sowie für die Auswertung der Regelauswertungen und die Ableitung von Maßnahmen verantwortlich. *Prüfung, ob eine eindeutige Zuordnung jeder Regel und Kontrolle zu einem Datenverantwortlichen möglich ist.*
5	**Prozesse und Verantwortungen**
	a) Role Lifecycle Management (Berechtigungsadministration)
5.1.	Ist das Verfahren für Berechtigungsänderungen angemessen dokumentiert, in Kraft gesetzt und publiziert worden? Ist für die Beantragung von Berechtigungen ein **Standardformular** oder ein geeignetes Verfahren (Papier, Excel-Liste oder E-Mail) mit Minimalinformationen definiert worden? Erfolgt die originäre Antragsstellung durch einen qualifizierten Mitarbeiter (**Keyuser**), der sowohl fachliche als auch technische Aspekte der Änderung beurteilen kann? *Durchsicht der Dokumente zum Verfahren der Berechtigungsadministration und Beurteilung der Vollständigkeit und Angemessenheit.*
5.2.	Werden Änderungen an Berechtigungen mittels eines Standardformulars vom zuständigen Datenverantwortlichen genehmigt? Der Datenverantwortliche ist hierbei für die Beurteilung der Notwendigkeit verantwortlich. Wird, sofern ein Rollenantrag Änderungen enthält, die nicht mit dem Prozessbereich oder der Organisationseinheit einer Rolle korrespondieren, die Genehmigung des Dateneigners dieses rollenfremden Datenbereichs eingeholt? *Durchsicht der Dokumente, ob die Funktion eines Datenverantwortlichen benannt und für alle vorhandenen Prozessbereiche eindeutige Datenverantwortliche identifiziert sind.* *Die Einhaltung des Verfahrens kann per Aufruf Report RSSCD100_PFCG geprüft werden, indem in Stichproben Änderungsbelege von Rollen auf Vorhandensein entsprechender Freigaben durch den Datenverantwortlichen geprüft werden.*
5.3.	Werden Änderungen im **Entwicklungssystem** von den zuständigen Berechtigungsadministratoren implementiert? Wird dabei ein **Standardtransportverfahren** genutzt? Ist eine eindeutige Zuordnung zwischen Transport und Antrag durch eine gegenseitige Referenzierung möglich? Werden Änderungen vor dem Transport in das **Produktivsystem** im Testsystem von qualifizierten Keyusern der antragstellenden Fachabteilung **getestet**? Erfolgt eine **Freigabe** der Transportaufträge zum Transport in das Produktivsystem durch die verantwortlichen Transportadministratoren? Erfolgt vor der Freigabe durch die Administratoren die Prüfung, ob alle erforderlichen Dokumentationen, Freigaben und Tests vorhanden sind? *Durchsicht Dokumente, ob das Verfahren die o.g. Punkte berücksichtigt.* *Die Umsetzung des Verfahrens im SAP-System kann anhand des Tabelle E070 nachvollzogen werden.*

NR.	INHALTE EINES DOKUMENTIERTEN BERECHTIGUNGS- UND BENUTZERKONZEPTES
	b) User Lifecycle Management (Benutzeradministration)
5.4.	Ist das Verfahren für Benutzeränderungen (User Lifecycle Management) angemessen dokumentiert, in Kraft gesetzt und publiziert worden? Ist für die Beantragung von Änderungen an Benutzern und der Zuordnung und Entziehung von Berechtigungen ein **Standardformular** oder ein geeignetes Verfahren (Papier, Excel-Liste oder E-Mail) mit Minimalinformationen definiert worden? *Prüfung, ob im Rahmen der Dokumentationen von Benutzeränderungen ein geeignetes Antragsformular mit vorgegebenen Minimalinformationen definiert ist.*
5.5.	Schließt das Verfahren für Benutzeränderungen eine Genehmigung durch den **Personalverantwortlichen** (disziplinarischen Vorgesetzten) bzw. durch den Benutzerverantwortlichen (bei nicht personalisierten Benutzern) ein? Die Genehmigung schließt die Beurteilung ein, dass der Mitarbeiter die Berechtigungen benötigt und für deren Anwendung qualifiziert ist. Werden für einen Benutzer Berechtigungen beantragt, für die nicht der disziplinarische Vorgesetzte der **Dateneigner** ist, sollte das Beantragungsverfahren die Einbindung des zuständigen Datenverantwortlichen sicherstellen. *Prüfung, ob das Verfahren eine Genehmigung durch einen Personal- bzw. einen Benutzerverantwortlichen vorsieht und im SAP-System eingehalten wurde.* *Die Einhaltung des Verfahrens kann per Aufruf Report „RSUSR100" geprüft werden („von Datum" und „bis Datum" Entsprechendes bei Auswertungszeitraum eingeben, Selektion „Angelegte Benutzer" unter „Selektionskriterien zu geänderten Rechten", Auswahl von Benutzern als Stichprobe, Einsichtnahme in die Dokumentationen und Freigaben zu den angelegten Benutzern bzw. vergebenen Berechtigungen).*
5.6.	Sind für die **Sperrung**, das Ungültigsetzen und die **Löschung** von Benutzern spezifische Regelungen getroffen worden? Muss der Vorgesetzte diesen Vorgängen immer zustimmen? Dies kann bei Sperrungen jedoch auch nachgelagert erfolgen, 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.* *Selektion von Entsperrungen, bei denen eine manuelle Sperrung oder eine Sperrung aufgrund von Fehlanmeldungen erfolgt ist und Prüfung, ob für die Entsperrung eine Genehmigung durch den Vorgesetzten vorliegt.* *Die Einhaltung des Verfahrens kann per Aufruf Report „RSUSR100" geprüft werden.*
5.7.	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 einem Antrag durch Vorgesetzte, ist immer der Vorgesetzte in die Entscheidung einzubeziehen. *Prüfung, ob die speziellen Anforderungen an die Sperrung, Entsperrung und Initialisierung von Benutzern gesondert geregelt sind.* *Selektieren von Entsperrungen, bei denen eine manuelle Sperrung oder eine Sperrung aufgrund von Fehlanmeldungen erfolgt ist und Prüfung, ob für die Entsperrung eine Genehmigung durch den Vorgesetzten vorliegt.* *Die Einhaltung des Verfahrens kann per Aufruf Report „RSUSR100" geprüft werden.*

NR.	INHALTE EINES DOKUMENTIERTEN BERECHTIGUNGS- UND BENUTZERKONZEPTES
6	**Basis und übergreifende Funktionen**
	Prüfung, ob in den vorliegenden Dokumentationen angemessene Anforderungen und Verfahren für folgende übergreifende Funktionen getroffen sind: › **Pflege von Tabellen** › **Pflege von Queries** › **Ausführung von Reporten** › **Debuggen von Programmen** › **Berechtigungen auf Batch-Input-Mappen** › **Berechtigungen auf Spool-Aufträge** › **Berechtigungen auf TemSe** › **Berechtigungen auf RFC-Schnittstelle** › **Berechtigungen auf Application Link Enabling (ALE-Schnittstelle)** Empfehlungen für die Ausgestaltung der Regelungen zu den oben aufgeführten Punkten sind innerhalb des Prüfungsleitfadens der DSAG aufgeführt.

4.6. PRÜFPROGRAMM: ORDNUNGSGEMÄSSE GESTALTUNG VON ROLLEN

NR	ORDNUNGSGEMÄSSE GESTALTUNG VON ROLLEN
H	**Kontrollziel: Bei der Gestaltung von Rollen werden Mindestanforderungen beachtet.** a) Rollenklarheit: jede Einzel- und Sammelrolle ist eindeutig einem Subprozess/Prozess und einer Organisationsebene samt Organisationsebenwert zugeordnet b) Rollentransparenz: der Rollenname und der Rollenbeschreibungstext sind so gestaltet, dass der Zweck der Rolle für einen sachkundigen Dritten innerhalb angemessener Zeit nachvollziehbar ist, ohne dafür die technischen Berechtigungen der Rolle prüfen zu müssen. Ebenso sollte der Zusammenhang einer Sammelrolle mit einer Einzelrolle erkennbar sein. Zudem sollte nur eine kritische Berechtigung pro Einzelrolle enthalten sein. b) Rollenkongruenz: jede Einzelrolle beinhaltet nur die Transaktionen und Berechtigungen, die mit dem Rollennamen, der Rollenbeschreibung, der Einordnung zu einem Subprozess/Prozess und den angegebenen Organisationsebenen und -werten übereinstimmen. b) Regelkonformität: eine Einzelrolle ist frei von inhärenten Funktionstrennungskonflikten; Sammelrollen besitzen nur beabsichtigte Funktionstrennungskonflikte, die durch entsprechende Kontrollen kompensiert werden. **Risiko:** › Rollen sind in ihrer Funktion, Zweck und Umfang nicht nachvollziehbar, was das Risiko einer fehlerhaften Zuordnung von Rollen/Berechtigungen an Benutzer steigert und den Berechtigungsvergabeprozess ineffizient gestaltet. › Beim Design von Rollen werden Funktionstrennungsaspekte nicht beachtet, was zu inhärenten Funktionstrennungskonflikten in Einzelrollen führen kann.

NR.	ORDNUNGSGEMÄSSE GESTALTUNG VON ROLLEN
1	**Rollenklarheit**
1.1.	Werden neben dem technischen Namen der Rolle, dem Rollennamen sowie der Rollenbeschreibung zusätzlich die folgenden Rollenattribute verwendet? › **Prozessdimension:** ist der Prozessbereich, zu dem die Rolle gehört, ersichtlich? › **Rollentyp:** Ist ersichtlich, ob es sich um eine Einzelrolle oder Sammelrolle in Form eines Arbeitsplatzes handelt? › **Organisationsdimension:** Ist die Organisationsebene, nach der die Rolle differenziert wird (Buchungskreis, Werk usw,), ersichtlich? › **Funktion:** Sind die Funktion und die Aktivität (Anzeige-, Pflege oder Entwicklungs-/Konfigurations-Tätigkeiten) der Rolle in Form der Beschreibung eines betriebswirtschaftlichen Objektes (z.B. Kreditorenstammdaten anzeigen, Materialbelege buchen, usw.) ersichtlich? *Die im SAP-System vorhandenen Rollen können über die Tabelle „AGR_Define" eingesehen werden.*
2	**Rollentransparenz**
5.6.	Werden die Anforderungen der Rollentransparenz eingehalten? › Allgemeines Transparenzgebot (Nachvollziehbarkeit): 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. › Nachhaltigkeit: Ist die Gruppierung von Berechtigungen in Rollen so gestaltet, dass bei prozessualen Reorganisationsmaßnahmen keine erhöhten Anpassungen am Rollenkonzept notwendig werden? Dies setzt voraus, dass auf Ebene von Einzelrollen möglichst Aufgaben („Kreditorenstammdaten ändern") und keine Arbeitsplätze („Kreditorenbuchhalter") abgebildet werden. *Die im SAP-System vorhandenen Rollen können über die Tabelle „AGR_Define" eingesehen werden.*
3	**Rollenkongruenz**
3.1.	Entsprechen die technischen Berechtigungen der Rollen deren technischen Namen bzw. dem Beschreibungstext? *Die im SAP-System vorhandenen Rollen können samt den pro Rolle verwendeten Transaktionen und ausgeprägten Aktivitäten über die Tabelle „AGR_1251" eingesehen werden.*
4	**Regelkonformität**
4.1.	Werden bei der Gestaltung (mandantenspezifische) Regelwerke für Funktionstrennungskonflikte und sensitive Funktionen beachtet? Sind Einzelrollen frei von inhärenten Regelverstößen? *Prüfung, ob entsprechende Regelwerke vorliegen und diese ggf. in das SAP-System integriert sind.* *Die im SAP-System hinterlegten Regelwerke zu kritischen Kombinationen von Berechtigungen können über den Report „RSUSR008_009_NEW" eingesehen werden.*

4.7. PRÜFPROGRAMM: NOTFALLBENUTZERKONZEPT (ABAP-STACK)

NR.	NOTFALLBENUTZERKONZEPT
H	**Kontrollziel: Absicherung des Notfallbenutzers** **Risiko:** › Es gibt keinen Notfallbenutzer: Systemadministratoren arbeiten im Normalbetrieb unter dem Standardbenutzer SAP* oder zwar unter einem eigens eingerichteten Benutzer, aber mit der universalen Superuser-Berechtigung SAP_ALL. › Es gibt einen eigenen Notfallbenutzer mit der universalen Superuser-Berechtigung SAP_ALL, den sich die Systemadministratoren teilen und der jederzeit unkontrolliert eingesetzt werden kann.
1.1.	Ist für den Notfall mindestens eine Benutzerkennung eingerichtet, › die nicht der Standardbenutzer SAP* ist, › die die notwendigen weitreichenden Berechtigungen hat, › die mit einem komplexen Kennwort ausgestattet ist, › deren Kennwort an einem sicheren Ort zugriffsgeschützt aufbewahrt wird, › wobei der Zugriff auf das Kennwort im 4-Augen-Prinzip erfolgen muss.
1.2.	Werden Aktionen unter dem Notfallbenutzer dokumentiert, dann mindestens unter Angabe › des Grundes › des Zeitraums › der darunter tätigen Personen › der Tätigkeiten, die damit durchgeführt wurden.
1.3.	Werden für einen Notfallbenutzer über das SAP Security Audit Log alle Ereignisse aller Audit-Klassen zwangsprotokolliert?
1.4.	Wird nach der Notfallaktion das Kennwort des Notfallbenutzers geändert?
1.5.	Sind Notfallszenarien definiert und auf diese Notfallszenarien zugeschnittene Berechtigungen in Form von Rollen implementiert worden? Existiert nicht nur ein Notfallbenutzer, sondern pro Notfallszenario ein dedizierter Notfallbenutzer, der die für das Notfallszenario implementierten Rollen zugeordnet bekommen hat?

4.8. PRÜFPROGRAMM: NUTZUNG KRITISCHER SAP-STANDARD-PROFILE/-ROLLEN

NR.	NUTZUNG KRITISCHER SAP- STANDARDPROFILE/-ROLLEN
1	**Kontrollziel: Einschränkung der Nutzung der kritischen universellen SAP-Standard-profile/-rollen** **Risiko:** Verlust der Vertraulichkeit, Verlust der Integrität der Daten und des SAP-Systems, Verlust der Verfügbarkeit. Auf dem Produktivsystem werden – entgegen den eindeutigen Sicherheitsempfehlungen des Herstellers SAP – nach Inbetriebnahme weiterhin die sicherheitskritischen SAP-Standardprofile vergeben – nach dem Motto „Simplicity over Security": › an externe Dienstleister, z.B. für Beratung, technische Unterstützung, Wartung, › an interne Systemadministratoren, › an Benutzer aus der Fachabteilung. Damit werden das gesetzlich geforderte unternehmensinterne Interne Kontrollsystem und das SAP interne Sicherheitskontrollsystem unterlaufen. Ordnungsmäßigkeits-anforderungen werden verfehlt.
1.1.	**An welche Benutzer ist SAP_ALL vergeben?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzer –Benutzer nach komplexen Selektionskriterien, Selektion nach Profil SAP_ALL. Wie ist die Vergabe und Nutzung des Standardprofils SAP_ALL organisatorisch geregelt? Das Profil SAP_ALL ist im Produktivsystem nicht zulässig. SAP empfiehlt, dieses Profil nur dem Notfallbenutzer zuzuweisen. **Hinweis 1:** Dieses Sammelprofil enthält alle SAP-Berechtigungen. Ein Benutzer mit diesem Profil kann im SAP-System alle Aufgaben durchführen. **Risiko:** Benutzer manipulieren unter dem höchst privilegierten SAP-Standardprofil SAP_ALL beliebige Geschäftsdaten, deaktivieren installierte SAP-interne Kontrollen oder sicherheitsrelevante Systemeinstellungen oder löschen die Systemaufzeichnungen der Aktivitäten, um die Spuren erfolgter Manipulationen zu beseitigen. **Hinweis 2:** Anstatt das Profil SAP_ALL zu benutzen, können die darin enthaltenen Berechtigungen auf die entsprechenden Funktionen verteilt werden. Es sollte z.B. dem Systemadministrator nicht die Berechtigung SAP_ALL zugewiesen werden, sondern nur die für die Systemverwaltung erforderlichen Berechtigungen, also die S_*-Berechti-gungen. Dies berechtigt ihn zur Verwaltung des gesamten SAP-Systems, er kann damit jedoch keine Aufgaben in anderen Bereichen, z.B. in Anwendungen, durchführen. **Hinweis 3:** Es ist zu prüfen, ob Rollen oder Profile mit Berechtigungsumfängen analog SAP_ALL existieren. **SOS:** Users with the most Full Access Authorizations (* Field Values) (0027) **SOS:** Users with the most Roles (0028) **SOS:** 20% or max 30% of All Users That Have for the most Profiles (0029)

NR.	NUTZUNG KRITISCHER SAP-STANDARDPROFILE/-ROLLEN
1.2.	**An welche Benutzer ist SAP_NEW vergeben?** **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzer –Benutzer nach komplexen Selektionskriterien, Selektion nach Profilen der Form SAP_NEW*. **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Profile – Profile nach Profilnamen, Selektion nach Profilen der Form SAP_NEW*. Eine lange Liste von SAP_NEW-Profilen, z.B. nach mehreren Upgrades, ist ein Zeichen dafür, dass das Berechtigungskonzept zu überarbeiten und neu festzusetzen ist. **Wie ist die Vergabe und Nutzung des SAP-Standardprofils SAP_NEW organisatorisch geregelt?** Das Profil SAP_NEW ist im Produktivsystem nicht zulässig. SAP empfiehlt, die SAP_NEW_* Profile nach einem Upgrade aufzulösen und die benötigten Teilberechtigungen zu verteilen sowie SAP_NEW zu löschen. **Hinweis 1:** Dieses Sammelprofil enthält alle Profile, die mit einem Release neu hinzukommen. Nach jedem Release-Wechsel benötigt man dieses Profil, damit bestimmte Aufgaben problemlos ablaufen können. **Risiko:** Benutzer missbrauchen die privilegierten Berechtigungen des SAP-Standard-profils SAP_NEW und führen nicht autorisierte Aktivitäten durch. **SAP empfiehlt im Einzelnen:** › nach dem Upgrade die SAP_NEW_*-Profile für Releases vor der Einführung des Berechtigungskonzepts zu löschen, › die SAP_NEW_*-Profile für Releases zu löschen, in denen bereits die darin enthaltenen Profile verteilt worden sind, › den Rest der in den SAP_NEW_*-Rollen enthaltenen Profile an die entsprechenden Funktionen zu verteilen und ihre Berechtigungswerte zu pflegen, › SAP_NEW zu löschen. **SOS:** Users with Profile SAP_NEW (0031)
1.3.	**An welche Benutzer sind weitere kritische SAP-Standardprofile vergeben, ggf. noch aus alten Releaseständen? Beispiele sind:** › S_A.SYSTEM (Systemverwalter, Superuser), S_A.ADMIN (Operator), S_A.CUSTOMIZ (Customizer), S_A.DEVELOP (Alle Berechtigungen für einen Entwickler) › S_CTS_ALL, u.a. kann damit die Systemänderbarkeit gesetzt werden › S_CTS_PROJECT, u.a. kann damit ein Änderungsauftrag eines anderen Benutzers übernommen werden, indem der Name im Änderungsauftrag geändert wird › S_DATASET_AL, S_C_FUNCT_AL, S_TCD_ALL, S_TSKH_ALL › F_BUCH_ALL, Z_ANWEND **AIS:** System Audit – Benutzer und Berechtigungen – Infosystem – Benutzer – Benutzer nach komplexen Selektionskriterien, Selektion nach Profil. Sind die Vorgaben von SAP zur Vergabe und Nutzung der kritischen SAP-Standardprofile bekannt und in eine organisatorische Regelung umgesetzt? **Risiko:** Benutzer können nach dem Produktivstart oder einem Release-Wechsel diese weitreichenden SAP-Standardprofile missbrauchen, die SAP nur zur Unterstützung der Implementierungsphase bereitstellt. **SOS:** SAP Standard Roles Are Assigned to Users (0082) **SOS:** SAP Standard Profiles Are Assigned to Users (0083) **Empfehlung:** Über die Transaktion SUIM oder die Tabellen UST10S/UST12 kann zusätzlich geprüft werden, ob Profile mit analogen Inhalten zu den oben aufgeführten Profilen existieren.

4.9. PRÜFPROGRAMM: ERSETZEN KRITISCHER VORSCHLAGSWERTE IM PROFILGENERATOR

NR.	ERSETZEN KRITISCHER VORSCHLAGSWERTE IM PROFILGENERATOR
1	**Kontrollziel: Die von SAP standardmäßig gesetzten und vordefinierten Ausprägungen von Berechtigungen im Profilgenerator sind auf kritische Setzungen bewertet worden. Bei der Vergabe von Profilen werden die als kritisch erkannten Vorgaben berücksichtigt und gemäß den unternehmensspezifischen Sicherheits- und Kontrollanforderungen geändert.** **Risiko:** Die von SAP gesetzten Vorschlagswerte im Profilgenerator für die Berechtigungsprüfung werden unverändert übernommen, obwohl einige davon nicht den geforderten IT-internen Kontrollen im Produktivsystem genügen.
1.1.	**Soll jeder Benutzer auf dem Produktivsystem uneingeschränkte Entwicklungsberechtigungen erhalten?** S_DEVELOP (ABAP-Workbench) mit Aktivität „*" und Paket „*" und Objektname „*" und Objekttyp „*" und Berechtigungsgruppe „*" ist sehr kritisch. Dieses Berechtigungsobjekt darf im Produktivsystem nur mit dem Objekttyp SUSO (Berechtigungsobjekte) und der Aktivität 03 „Anzeigen" ausgeprägt sein. Risiko: Ausprägungen, die die Aktivitäten 01 „Anlegen" oder 02 „Ändern" zusammen mit einem der beiden Objekttypen DEBUG oder PROG beinhalten, verstoßen im Produktivsystem gegen Grundsätze der ordnungsmäßigen Buchführung (Radierverbot).
1.2.	**Soll jeder Benutzer die kritische Systemberechtigung zum Auswerten des Syslogs erhalten?** S_ADMI_FCD (Systemberechtigungen) mit Aktivität SM21 berechtigt, den Systemlog auszuwerten. Dieses Berechtigungsobjekt darf mit der Aktivität SM21 im Produktivsystem nicht für alle Benutzer freigeschaltet werden.
1.3.	**Soll jeder Benutzer neue Projekte generieren können?** S_PRO_AUTH (Neue Berechtigungen für Projekte) mit Aktivität 03 (Anzeigen). Dieses Berechtigungsobjekt darf im Produktivsystem nur mit der Aktivität 03 „Anzeigen" ausgeprägt werden.
1.4.	**Welche Adressgruppen können für alle Benutzer freigeschaltet werden?** S_ADRESS1 (Adresstyp1: Organisationsadressen) mit Aktivität „*" und Adressgruppe BC01 (SAP-Benutzeradressen) ist sinnvoll. Im Produktivsystem ist auf die spezifische Eingabe der Adressgruppe zu achten, insbesondere nur BC01 (SAP-Benutzeradressen) zulassen. Adressgruppen wie Geschäftspartner, BP, oder EHS-Berichtsempfänger, EHS1, dürfen wegen des Prinzips der geringsten Berechtigungsvergabe und der Gewährleistung der Vertraulichkeit nicht grundsätzlich an alle Benutzer freigegeben werden. **Risiko:** Die Vertraulichkeit von Daten ist unter Umständen nicht gewährleistet.
1.5.	**Welche Transaktionscodes können für alle Benutzer von HR freigeschaltet werden?** P_TCODE (HR Transaktionscode) mit Transaktionscode: PFCG, SUID oder SU01D ist sinnvoll. Dieses Berechtigungsobjekt darf im Produktivsystem nur für die Transaktionscodes PFCG, SUID oder SU01D freigeschaltet sein. Die im Kontext zu den Transaktionen PFCG stehenden Berechtigungsobjekte müssen gemäß der zugeordneten Aufgabe ausgeprägt sein (Administrations- oder Anzeigefunktion).

NR.	ERSETZEN KRITISCHER VORSCHLAGSWERTE IM PROFILGENERATOR
2.	**Zugriff auf Tabellen**
2.1.	**Welche Tabellengruppen dürfen von Benutzern nicht geändert werden können?** S_TABU_DIS (Tabellenpflege) mit Aktivität 03 (Anzeigen) und Berechtigungsgruppen ALE0 oder SS. Dieses Berechtigungsobjekt darf im Produktivsystem für die beiden Berechtigungsgruppen ALE0 und SS nur mit Aktivität 03 „Anzeigen" ausgeprägt werden.
2.2.	**Welche Tabellengruppen dürfen von Benutzern geändert werden können?** S_TABU_DIS (Tabellenpflege) mit Aktivität 02 oder 03 und Berechtigungsgruppe SUSR. Dieses Berechtigungsobjekt darf im Produktivsystem für die Berechtigungsgruppe SUSR nur mit den Aktivitäten 02 „Ändern" und 03 „Anzeigen" ausgeprägt werden.
3.	**Zugriff auf IDOCS**
3.1.	**Welcher Zugriff auf IDOCs kann allen Benutzern eingeräumt werden?** S_IDOCCTRL (allgemeiner Zugriff auf IDOC-Funktionen) mit Aktivität 03 und Transaktionscode „*" ist applikationsabhängig möglich. Dieses Berechtigungsobjekt darf im Produktivsystem nur die Aktivität 03 „Anzeigen" haben. Empfehlenswert ist auch Einschränkung auf nicht FI-spezifische Transaktionscodes. **Risiko:** Ansonsten können FI-spezifische IDOCs, die z.B. vertrauliche Daten beinhalten, von allen Benutzern eingesehen werden. **Hinweis:** Unter allen IDOC-Berechtigungsobjekten sollte nur das Berechtigungsobjekt S_IDOCCTRL an alle Benutzer mit den oben beschriebenen Einschränkungen berechtigt werden, falls überhaupt erforderlich.
3.2.	**Welcher Zugriff auf IDOCs kann allen Benutzern eingeräumt werden, die eine Kontrollfunktion über IDOCs benötigen?** S_IDOCMONI (Zugriff auf IDOC-Monitoring) mit Aktivität 03 und Richtung der IDOC-Übertragung 1 und 2 und Nachrichtentyp CCLONE und USERCLONE und PARTNER-NUMMER „*" und PARTNERART „LS" und TRANSAKTIONSCODE: „*" ist applikationsabhängig möglich. **Risiko:** Die Aktivität muss 03 „Anzeigen" sein. Sonst können IDOCs, die auch Änderungsbelege sind, geändert oder gelöscht werden. **Hinweis:** Die Angabe des Transaktionscodes ist dann unkritisch, wenn die anderen Felder des Berechtigungsobjekts wie oben gepflegt sind.
4.	**Benutzer- und Berechtigungsadministration**
4.1.	**Welche Administratoren sollen Benutzer und ihre Berechtigungen auf welche Weise verwalten dürfen?** S_USER_AGR (Berechtigungswesen: Prüfer für Rollen) mit Aktivität „*" und Name der Rolle „*" ist kritisch. Dieses Berechtigungsobjekt zur Benutzer- und Berechtigungsverwaltung darf im Produktivsystem nur restriktiv gemäß dem organisatorischen Konzept der Benutzer- und Berechtigungsadministration belegt werden. **Risiko:** Wenn diese von SAP vordefinierten, uneingeschränkten Freigaben („*") bestehen bleiben, kann jeder alle Aktivitäten durchführen. Insbesondere kann jeder jede Rolle anlegen. Das kann nicht gewünscht sein. **Hinweis:** Zur Einhaltung des Vieraugenprinzips müssen bei den Feldern „Aktivität" und „Name der Rolle" die 4 Funktionen „Anlegen", „Ändern", „Aktivieren" und „Zuordnen" entsprechend berücksichtigt werden.

NR.	ERSETZEN KRITISCHER VORSCHLAGSWERTE IM PROFILGENERATOR
4.2.	**Welche Administratoren sollen Benutzer und ihre Berechtigungen auf welche Weise verwalten dürfen?** S_USER_AUT (Benutzerstammpflege: Berechtigungen) mit Aktivität „*" und Berechtigungsname in Benutzerstamm „*" und Berechtigungsobjekt „*" ist kritisch. Dieses Berechtigungsobjekt zur Benutzer- und Berechtigungsverwaltung darf im Produktivsystem nur restriktiv gemäß dem organisatorischen Konzept der Benutzer- und Berechtigungsadministration belegt werden. **Risiko:** Wenn diese von SAP vordefinierten, uneingeschränkten Freigaben („*") bestehen bleiben, kann jeder alle Aktivitäten durchführen. Insbesondere kann jeder jede Rolle anlegen. Das kann nicht gewünscht sein. **Hinweis:** Zur Einhaltung des Vieraugenprinzips müssen bei den Feldern „Aktivität" und „Name der Rolle" die 4 Funktionen „Anlegen", „Ändern", „Aktivieren" und „Zuordnen" entsprechend berücksichtigt werden. Dabei sind auch die Modulverantwortlichen – sofern vorgesehen – unter den Benutzer- und Berechtigungsadministratoren zu berücksichtigen.
4.3.	**Welche Administratoren sollen Benutzer und ihre Berechtigungen auf welche Weise verwalten dürfen?** S_HIERARCH (Berechtigungsprüfungen der Hierarchiepflege) mit Aktivität „*" und Paket „*" und Strukturtyp „*" ist kritisch. Dieses Berechtigungsobjekt zur Benutzer- und Berechtigungsverwaltung darf im Produktivsystem nur restriktiv gemäß dem organisatorischen Konzept der Benutzer- und Berechtigungsadministration belegt werden. Die Möglichkeit der Einschränkung auf die verwendete Struktur zur Berechtigungsverwaltung muss genutzt werden. Dieses Berechtigungsobjekt ermöglicht das Arbeiten mit dem allgemeinen Hierarchiepflegetool oder den darauf basierenden Transaktionen. Die Berechtigung muss eingeschränkt werden über den Typ der zu bearbeitenden Struktur und über deren Paket.
4.4.	**Welche Administratoren sollen Benutzer und ihre Berechtigungen auf welche Weise verwalten dürfen?** S_USR_GRP (Benutzerstammpflege: Benutzergruppen) mit Aktivität „*" und Benutzergruppe in Benutzerstamm „*" ist kritisch. Dieses Berechtigungsobjekt zur Benutzer- und Berechtigungsverwaltung darf im Produktivsystem nur restriktiv gemäß dem organisatorischen Konzept der Benutzer- und Berechtigungsadministration belegt werden. **Risiko:** Wenn diese uneingeschränkten Freigaben („*") bestehen bleiben, kann jeder alle Aktivitäten durchführen. Dann kann jeder jede Benutzergruppe pflegen, auch sich selbst. Das kann nicht gewünscht sein. **Hinweis:** Zur Einhaltung des 4-Augen-Prinzips müssen bei der Aktivität und Name der Benutzergruppe die 4 Funktionen „Anlegen", „Ändern", „Aktivieren" und „Zuordnen" entsprechend berücksichtigt werden.

NR.	ERSETZEN KRITISCHER VORSCHLAGSWERTE IM PROFILGENERATOR
4.5.	**Welche Administratoren sollen Benutzer und ihre Berechtigungen auf welche Weise verwalten dürfen?** S_USR_PRO (Benutzerstammpflege: Berechtigungsprofil) Mit Aktivität „*" und Berechtigungsprofil im Benutzerstamm „*" ist kritisch. Dieses Berechtigungsobjekt zur Benutzer- und Berechtigungsverwaltung darf im Produktivsystem nur restriktiv gemäß dem organisatorischen Konzept der Benutzer- und Berechtigungsadministration belegt werden. **Risiko:** Wenn diese uneingeschränkten Freigaben („*") bestehen bleiben, kann jeder alle Aktivitäten durchführen. Dann kann jeder jedes Benutzerprofil pflegen. Das kann nicht gewünscht sein. **Hinweis:** Zur Einhaltung des 4-Augen-Prinzips müssen bei der Aktivität und Name des Berechtigungsprofils die 4 Funktionen „Anlegen", „Ändern", „Aktivieren" und „Zuordnen" entsprechend berücksichtigt werden.
4.6.	**Welche Administratoren sollen Benutzer und ihre Berechtigungen auf welche Weise verwalten dürfen?** S_USER_SAS (Benutzerstammpflege: Systemspezifische Zuordnungen) mit Aktivität „*", Name der Rolle „*", Benutzergruppe „*", Berechtigungsprofil im Benutzerstamm und Empfängersystem ZBV ist kritisch. Dieses Berechtigungsobjekt zur Benutzer- und Berechtigungsverwaltung darf im Produktivsystem nur restriktiv gemäß dem organisatorischen Konzept der Benutzer- und Berechtigungsadministration belegt werden. **Risiko:** Bei Vollausprägung kann jeder jede Benutzerausprägung und jede Rolle in jedem System zuweisen. **Hinweis:** Das neue Berechtigungsobjekt S_USER_SAS wird über den Eintrag mit der Id ‚CHECK_S_USER_SAS' und dem Wert ‚YES' in der Tabelle PRGN_CUST aktiviert (OSS-Hinweis 536101) und ersetzt die Berechtigungsobjekte S_USER_GRP, S_USER_AGR, S_USER_PRO und S_USER_SYS bezüglich der Zuordnung von Rollen oder Profilen zu Benutzern. Die Verwendung der erweiterten Berechtigungsprüfung ist unabhängig vom Einsatz der zentralen Benutzerverwaltung.
4.7.	**Welche Administratoren sollen Benutzer und ihre Berechtigungen auf welche Weise verwalten dürfen?** S_USR_SYS (Benutzerstammpflege: System für zentrale Benutzerpflege) spezifisches Objekt) mit Aktivität „*" und Empfängersystem ZBV ist kritisch. Dieses Berechtigungsobjekt zur Benutzer- und Berechtigungsverwaltung darf im Produktivsystem nur restriktiv gemäß dem organisatorischen Konzept der Benutzer- und Berechtigungsadministration belegt werden. **Risiko:** Bei Vollausprägung kann jeder in allen Systemen Rollen zuweisen.

NR.	ERSETZEN KRITISCHER VORSCHLAGSWERTE IM PROFILGENERATOR
4.8.	**Welche Administratoren sollen Benutzer und ihre Berechtigungen auf welche Weise verwalten dürfen?** S_USER_TCD (Berechtigungswesen: Transaktionen in Rollen) mit Transaktionscode „*" ist kritisch. Dieses Berechtigungsobjekt zur Benutzer- und Berechtigungsverwaltung darf im Produktivsystem nur restriktiv gemäß dem organisatorischen Konzept der Benutzer- und Berechtigungsadministration belegt werden. **Risiko:** Bei Vollausprägung können modul- und basisübergreifend alle Berechtigungsobjekte in Rollen aufgenommen werden.
4.9.	**Welche Administratoren sollen Benutzer und ihre Berechtigungen auf welche Weise verwalten dürfen?** S_USER_VAL (Berechtigungswesen: Feldwerte in Rollen) mit Feldname „*" und Berechtigungswert „*" und Berechtigungsobjekt „*" ist kritisch. Dieses Berechtigungsobjekt zur Benutzer- und Berechtigungsverwaltung darf im Produktivsystem nur restriktiv gemäß dem organisatorischen Konzept der Benutzer- und Berechtigungsadministration belegt werden. **Risiko:** Bei Vollausprägung können modul- und basisübergreifend alle Berechtigungsobjekte in Rollen aufgenommen werden.

4.10. PRÜFPROGRAMM: ORDNUNGSMÄSSIGE BERECHTIGUNGS- UND BENUTZERORGANISATION

NR.	ORDNUNGSMÄSSIGE BERECHTIGUNGS- UND BENUTZERORGANISATION
1.	**Kontrollziel: Einhaltung der Funktionstrennung, kein Administrator darf die folgenden drei zu trennenden Aufgaben durchführen:** **1. Benutzer verwalten** **2. Berechtigungen pflegen** **3. Berechtigungsprofile generieren** **Risiko:** Die Aufgaben des Benutzer- und Berechtigungsverwalters werden in vollem Umfang an einen oder mehrere Mitarbeiter vergeben. Eine Überwachung der Tätigkeiten eines Benutzer- und Berechtigungsverwalters gibt es nicht. Die Folgen sind: › nicht autorisierte Änderungen sind möglich, › betrügerische Handlungen können durchgeführt und die Spuren dazu zumindest verschleiert werden.
1.1.	**Sind die Möglichkeiten der Funktionstrennung bezogen auf die Ressourcen und die Sicherheitsanforderungen des Unternehmens umgesetzt?** Beispiele für die Realisierung eines 4-Augen-Prinzips und eines 6-Augen-Prinzips sind in den folgenden Übersichten aufgeführt.

NR.	ORDNUNGSMÄSSIGE BERECHTIGUNGS- UND BENUTZERORGANISATION
	Scenario 1: 4-Augen-Prinzip **Zentrale Benutzerverwaltung** › Ein Benutzerverwalter für alle Benutzer. › Unbegrenzte Berechtigungen für alle Benutzerverwaltungsaufgaben des Benutzeradministrators. **Zentrale Pflege von Rollen und Profilen** Ein Administrator übernimmt beide Rollen: › Berechtigungsdatenverwalter, › Berechtigungsprofilverwalter.
	Scenario 2: 6-Augen-Prinzip **Dezentrale Benutzerverwaltung (Produktivsystem)** Ein Benutzerverwalter für pro Anwendungsbereich (FI, MM), › berechtigt, um eine bestimmte Benutzergruppe zu pflegen, › berechtigt, um eine bestimmte Menge von Rollen/Profilen zuzuordnen, › keine weiteren Einschränkungen auf spezifische Benutzerverwaltungsaufgaben. **Zentrale Pflege von Rollen und Profilen** Trennung der Zuständigkeiten: › Berechtigungsdatenverwalter, › Berechtigungsprofilverwalter. Keine weiteren Einschränkungen auf spezifische Rollen oder Profile.
	Scenario 3: 6-Augen-Prinzip, dezentrale Benutzerverwaltung im Produktivsystem **Zentrales Anlegen und Löschen für alle Benutzer** **Dezentrale Benutzerverwaltung (Produktivsystem)** Ein Benutzerverwalter für pro Anwendungsbereich (FI, MM), › berechtigt, um eine bestimmte Benutzergruppe zu pflegen, › berechtigt, um eine bestimmte Menge von Rollen/Profilen zuzuordnen, › berechtigt für nur einige Benutzerverwaltungsaufgaben: ändern, sperren/entsperren, Kennwort zurücksetzen. **Zentrale Pflege von Rollen und Profilen** Trennung der Zuständigkeiten: › Berechtigungsdatenverwalter, › Berechtigungsprofilverwalter. Keine weiteren Einschränkungen auf spezifische Rollen oder Profile.

4.11. TABELLEN: BEISPIELSZENARIEN DER ORGANISATION EINER BENUTZER- UND BERECHTIGUNGSVERWALTUNG

4.11.1. SZENARIO 1: 4-AUGEN-PRINZIP

Zentrale Benutzerverwaltung
- Ein Benutzerverwalter für alle Benutzer
- Unbegrenzte Berechtigungen für alle Benutzerverwaltungsaufgaben des Benutzeradministrators

Zentrale Pflege von Rollen und Profilen
Ein Administrator übernimmt beide Rollen:
- Berechtigungsdatenverwalter
- Berechtigungsprofilverwalter

A. Ohne Berechtigungsobjekt S_USER_SAS

	ENTWICKLUNG		PRODUKTIV
Szenario 1	**Benutzer-administrator**	**Berechtigungs-daten- und Berechtigungsprofil-verwalter**	**Benutzerverwalter**
S_USER_GRP			
ACTVT	*	03, 08	*
CLASS	*	*	*
S_USER_AGR			
ACTVT	03, 22	*	03, 22
ACT_GROUP	*	*	*
S_USER_TCD			
TCD		*	
S_USER_VAL			
OBJECT		*	
AUTH_FIELD		*	
AUTH_VALUE		*	

	ENTWICKLUNG		PRODUKTIV
Szenario 1	**Benutzer-administrator**	**Berechtigungs-daten- und Berechtigungsprofil-verwalter**	**Benutzerverwalter**
S_USER_PRO			
ACTVT	03, 08, 22	*	03, 08, 22
PROFILE	*	*	*
S_USER_AUT			
ACTVT	03, 08	*	03, 08
OBJECT	*	*	*
AUTH	*	*	*
Bei aktiver ZBV			
S_USER_SYS			
ACTVT	03, 78		03, 78
SUBSYSTEM	*		*

B. Mit aktiviertem Berechtigungsobjekt S_USER_SAS

	ENTWICKLUNG		PRODUKTIV
Szenario 1	**Benutzer-administrator**	**Berechtigungs-daten- und Berechtigungsprofil-verwalter**	**Benutzerverwalter**
S_USER_GRP			
ACTVT		03, 08	
CLASS		*	
S_USER_AGR			
ACTVT		*	
ACT_GROUP		*	
S_USER_TCD			
TCD		*	
S_USER_VAL			
OBJECT		*	
AUTH_FIELD		*	
AUTH_VALUE		*	
S_USER_PRO			
ACTVT		*	
PROFILE		*	
S_USER_AUT			
ACTVT	03, 08	*	03, 08
OBJECT	*	*	*
AUTH	*	*	*

	ENTWICKLUNG		PRODUKTIV
Szenario 1	**Benutzer-administrator**	**Berechtigungs-daten- und Berechtigungsprofil-verwalter**	**Benutzerverwalter**
Bei aktiver ZBV wird zusätzlich das Berechtigungs-feld SUBSYSTEM gepflegt			
S_USER_SAS			
ACTVT	22		22
CLASS	*		*
SUBSYSTEM	*		*
ACT_GROUP	*		*
PROFILE	*		*

4.11.2. SZENARIO 2: 6-AUGEN-PRINZIP

Dezentrale Benutzerverwaltung (Produktivsystem)
Ein Benutzerverwalter pro Anwendungsbereich (FI, MM),
› berechtigt, um eine bestimmte Benutzergruppe zu pflegen,
› berechtigt, um eine bestimmte Menge von Rollen/Profilen zuzuordnen,
› keine weiteren Einschränkungen auf spezifische Benutzerverwaltungsaufgaben.
Zentrale Pflege von Rollen und Profilen
Trennung der Zuständigkeiten:
› Berechtigungsdatenverwalter
› Berechtigungsprofilverwalter
Keine weiteren Einschränkungen auf spezifische Rollen oder Profile.

A. Ohne Berechtigungsobjekt S_USER_SAS

	ENTWICKLUNG			PRODUKTIV	
Szenario 2	**Benutzer-administrator**	**Berechti-gungsdaten-verwalter**	**Berechti-gungspro-filverwalter**	**FI-Benutzer-verwalter**	**MM-Benutzer-verwalter**
S_USER_GRP					
ACTVT	*	03, 08	03, 22	*	*
CLASS	*	*	*	FI_USER	MM_USER
S_USER_AGR					
ACTVT	03, 22	01, 02, 03, 06	03, 64	03, 22	03, 22
ACT_GROUP	*	*	*	*	*
S_USER_TCD					
TCD		*			
S_USER_VAL					
OBJECT		*			
AUTH_FIELD		*			
AUTH_VALUE		*			
S_USER_PRO					

	ENTWICKLUNG			PRODUKTIV	
Szenario 2	**Benutzer-administrator**	**Berechti-gungsdaten-verwalter**	**Berechti-gungspro-filverwalter**	**FI-Benutzer-verwalter**	**MM-Benutzer-verwalter**
ACTVT	03, 08, 22	01, 02, 03, 06, 08	03, 07, 08	03, 08, 22	03, 08, 22
PROFILE	*	*	*	FI*	MM*
S_USER_AUT					
ACTVT	03, 08	01, 02, 03, 06, 08, 22	03, 07, 08	03, 08	03, 08
OBJECT	*	*	*	*	*
AUTH	*	*	*	*	*
Bei aktiver ZBV					
S_USER_SYS					
ACTVT	03, 78	*		03, 78	03, 78
SUBSYSTEM	*			*	*

B. Mit aktiviertem Berechtigungsobjekt S_USER_SAS

	ENTWICKLUNG			PRODUKTIV	
Szenario 2	**Benutzer-administrator**	**Berechti-gungsdaten-verwalter**	**Berechti-gungspro-filverwalter**	**FI-Benutzer-verwalter**	**MM-Benutzer-verwalter**
S_USER_GRP					
ACTVT		03, 08	03, 08		
CLASS		*	*		
S_USER_AGR					
ACTVT		01, 02, 03, 06	03, 64		
ACT_GROUP		*	*		
S_USER_TCD					
TCD		*			
S_USER_VAL					
OBJECT		*			
AUTH_FIELD		*			
AUTH_VALUE		*			
S_USER_PRO					
ACTVT		01, 02, 03, 06, 08	03, 07, 08		
PROFILE		*	*		
S_USER_AUT					
ACTVT	03, 08	01, 02, 03, 06, 08, 22	03, 07, 08	03, 08	03, 08
OBJECT	*	*	*	*	*
AUTH	*	*	*	*	*

	ENTWICKLUNG			PRODUKTIV	
Szenario 2	**Benutzer-administrator**	**Berechti-gungsdaten-verwalter**	**Berechti-gungspro-filverwalter**	**FI-Benutzer-verwalter**	**MM-Benutzer-verwalter**
Bei aktiver ZBV wird zu-sätzlich das Berechti-gungsfeld SUBSYSTEM gepflegt					
S_USER_SAS					
ACTVT	22			22	22
CLASS	*			FI_USER	MM_USER
SUBSYSTEM	*			*	*
ACT_GROUP	*			FI*	MM*
PROFILE	*			FI*	MM*

4.11.3. SZENARIO 3: 6-AUGEN-PRINZIP, DEZENTRALE BENUTZERVERWALTUNG IM PRODUKTIVSYSTEM

Zentrales Anlegen und Löschen für alle Benutzer
Dezentrale Benutzerverwaltung (Produktivsystem)
Ein Benutzerverwalter pro Anwendungsbereich (FI, MM),
› berechtigt, um eine bestimmte Benutzergruppe zu pflegen,
› berechtigt, um eine bestimmte Menge von Rollen/Profilen zuzuordnen,
› berechtigt für nur einige Benutzerverwaltungsaufgaben: ändern, sperren/entsperren, Kennwort zurücksetzen.
Zentrale Pflege von Rollen und Profilen
Trennung der Zuständigkeiten:
› Berechtigungsdatenverwalter
› Berechtigungsprofilverwalter
Keine weiteren Einschränkungen auf spezifische Rollen oder Profile

A. Ohne Berechtigungsobjekt S_USER_SAS

	ENTWICKLUNG			PRODUKTIV		
Szenario 3	**Benutzer-administ-rator**	**Berech-tigungs-datenver-walter**	**Berech-tigungs-profilver-walter**	**FI-Benutzer-verwalter**	**MM-Benutzer-verwalter**	**Zentraler Benutzer-verwalter**
S_USER_GRP						
ACTVT	*	03, 08	03, 08	02, 03, 05, 22	02, 03, 05, 22	01, 03, 06, 08
CLASS	*	*	*	FI_USER	MM_ USER	*
S_USER_AGR						
ACTVT	03, 22	01, 02, 03, 06	03, 64	03, 22	03, 22	3
ACT_GROUP	*	*	*	*	*	*
S_USER_TCD						
TCD		*				
S_USER_VAL						
OBJECT		*				
AUTH_FIELD		*				

	ENTWICKLUNG			PRODUKTIV		
Szenario 3	**Benutzer-administrator**	**Berechtigungsdatenverwalter**	**Berechtigungsprofilverwalter**	**FI-Benutzerverwalter**	**MM-Benutzerverwalter**	**Zentraler Benutzerverwalter**
AUTH_VALUE		*				
S_USER_PRO						
ACTVT	03, 08, 22	01, 02, 03, 06, 08	03, 07, 08	03, 08, 22	03, 08, 22	03, 08
PROFILE	*	*	*	FI*	MM*	*
S_USER_AUT						
ACTVT	03, 08	01, 02, 03, 06, 08, 22	03, 07, 08	03, 08	03, 08	03, 08
OBJECT	*	*	*	*	*	*
AUTH	*	*	*	*	*	*
Bei aktiver ZBV						
S_USER_SYS						
ACTVT	03, 78			03, 78	03, 78	03, 78
SUBSYSTEM	*			*	*	*

B. Mit aktiviertem Berechtigungsobjekt S_USER_SAS

	ENTWICKLUNG			PRODUKTIV		
Szenario 3	**Benutzer-administrator**	**Berechtigungsdatenverwalter**	**Berechtigungsprofilverwalter**	**FI-Benutzerverwalter**	**MM-Benutzerverwalter**	**Zentraler Benutzerverwalter**
S_USER_GRP						
ACTVT		03, 08	03, 08			
CLASS		*	*			
S_USER_AGR						
ACTVT		01, 02, 03, 06	03, 64			
ACT_GROUP		*	*			
S_USER_TCD						
TCD		*				
S_USER_VAL						
OBJECT		*				
AUTH_FIELD		*				
AUTH_VALUE		*				
S_USER_PRO						
ACTVT		01, 02, 03, 06, 08	03, 07, 08			
PROFILE		*	*			
S_USER_AUT						
ACTVT	03, 08	01, 02, 03, 06, 08, 22	03, 07, 08	03, 08	03, 08	03, 08
OBJECT	*	*	*	*	*	*
AUTH	*	*	*	*	*	*

	ENTWICKLUNG			PRODUKTIV		
Szenario 3	**Benutzer-administrator**	**Berechtigungs-datenverwalter**	**Berechtigungs-profilverwalter**	**FI-Benutzer-verwalter**	**MM-Benutzer-verwalter**	**Zentraler Benutzer-verwalter**
Bei aktiver ZBV wird zusätzlich das Berechtigungsfeld SUBSYSTEM gepflegt						
S_USER_SAS						
ACTVT	22			22	22	22
CLASS	*			FI_USER	MM_ USER	*
SUBSYSTEM	*			*	*	*
ACT_GROUP	*			FI*	MM*	*
PROFILE	*			FI*	MM*	*

4.12. PRÜFPROGRAMM: BERECHTIGUNGEN FÜR DIE BENUTZER- UND BERECHTIGUNGSVERWALTUNG

NR.	BERECHTIGUNGSVERWALTUNG: BENUTZER
1.	**Das Objekt Benutzerstammpflege, Benutzergruppen S_USER_GRP,** legt die Benutzergruppen und die zulässigen Aktivitäten fest, für die ein Benutzerverwalter berechtigt ist. Damit können Benutzer angelegt, gepflegt, ge- und entsperrt werden, insbesondere auch das Kennwort eines Benutzers geändert werden. Es kann benutzt werden, um bei einer dezentralisierten Verwaltung einem Benutzeradministrator nur die Verwaltung einer bestimmten Benutzergruppe zu ermöglichen.
1.1.	**Wer kann Benutzer anlegen?** Report RSUSR002 mit den Eingaben: S_TCODE = SU01 S_USER_GRP (Benutzergruppen) mit Aktivität „*" oder 01 (Anlegen) und Gruppe = „*" oder = Gruppennamen.
1.2.	**Wer kann Benutzereigenschaften ändern (außer den Zugriffsrechten)?** Report RSUSR002 mit den Eingaben: S_TCODE = SU01 S_USER_GRP (Benutzergruppen) mit Aktivität „*" oder 02 (Ändern) und Gruppe = „*" oder = Gruppennamen.
1.3.	**Wer kann Benutzer sperren oder löschen?** Report RSUSR002 mit den Eingaben: S_TCODE = SU01 S_USER_GRP (Benutzerverwaltung) mit Aktivität „*" oder 05 (Sperren) oder 06 (Löschen) und Gruppe = „*" oder = Gruppennamen.
2.	**Das Objekt Benutzerstammpflege, System für die zentrale Benutzerpflege S_USER_SYS,** legt fest, auf welches System ein Benutzerverwalter aus der Zentralen Benutzerverwaltung mit welchen zulässigen Aktivitäten zugreifen kann.
1.5.	**Wer kann aus der Zentralen Benutzerverwaltung Benutzer ändern?** Report RSUSR002 mit den Eingaben: S_TCODE = SU01 oder PFCG S_USER_SYS (Benutzerpflege) mit Aktivität „*" oder 02 (Ändern) und SUBSYSTEM = „*" oder = „Logisches System".
NR.	**BERECHTIGUNGSVERWALTUNG: ROLLEN**
3.	**Das Objekt Berechtigungswesen, Prüfung für Rollen S_USR_AGR** legt die Rollennamen und die zulässigen Aktivitäten fest, für die ein Berechtigungsverwalter berechtigt ist. Damit können Rollen angelegt und gepflegt werden. Es kann benutzt werden, um bei einer dezentralisierten Administration einem Berechtigungsverwalter nur Zugriff auf bestimmte Rollen zugeben, z.B. für ein Modul oder eine Organisationseinheit.
3.1.	**Wer kann Rollen anlegen (ohne Berechtigungswerte)?** Report RSUSR002 mit den Eingaben: S_TCODE = PFCG S_USER_AGR (Rollen verwalten) mit Aktivität „*", 01 (Anlegen) und Rolle = „*" oder = Rollennamen

NR.	BERECHTIGUNGSVERWALTUNG: ROLLEN
3.2.	**Wer kann Rollen ändern (ohne Berechtigungswerte)?** Report RSUSR002 mit den Eingaben: S_TCODE = PFCG S_USER_AGR (Rollen verwalten) mit Aktivität „*" oder 02 (Ändern) und Rolle = „*" oder = Rollennamen.
4.	**Das Objekt Berechtigungswesen, Transaktionen in Rollen S_USR_TCD** legt fest, welche Transaktionen ein Berechtigungsverwalter in eine Rolle aufnehmen darf. Es kann benutzt werden, um einem Berechtigungsverwalter nur die Aufnahme bestimmter Transaktionen in Rollen zu erlauben und damit die Vergabe kritischer Transaktionen zu verhindern.
4.1.	**Wer ist für S_USER_AGR berechtigt und kann Transaktionen anlegen (ohne Berechtigungswerte)?** Report RSUSR002 mit den Eingaben: S_TCODE = PFCG S_USER_AGR (Rollen verwalten) mit Aktivität „*" oder 01 (Anlegen) oder 02 (Ändern) und Rolle = „*" oder = Rollennamen. S_USER_TCD (Transaktionen in Rollen) mit Transaktionscode „*" oder = Transaktionsname.
5.	**Das Objekt Berechtigungswesen, Feldwerte für Rollen S_USR_VAL** legt fest, für welche Berechtigungsobjekte und für welche Felder ein Berechtigungsverwalter welche Feldwerte in eine Rolle eintragen darf. Es kann benutzt werden, um einem Berechtigungsverwalter nur die Vergabe bestimmter Berechtigungen in Rollen zu erlauben und damit die Vergabe kritischer Berechtigungen in Rollen zu verhindern.
5.1.	**Wer kann Rollen mit allen Berechtigungswerten ändern?** Report RSUSR002 mit den Eingaben: S_TCODE = PFCG S_USER_AGR (Rollen verwalten) mit Aktivität „*" oder 01 (Anlegen), 02 (Ändern) und Rolle = „*" oder = Rollennamen S_USER_VAL (Objektverwendung in Rollen) mit „*" in allen Feldern
NR.	**BERECHTIGUNGSVERWALTUNG: PROFILE UND BERECHTIGUNGEN**
6.	**Das Objekt Benutzerstammpflege, Berechtigungsprofil S_USR_PRO** legt die Profilnamen sowie die zulässigen Aktivitäten fest, für die ein Berechtigungsverwalter berechtigt ist. Es kann benutzt werden, um bei einer dezentralisierten Benutzerverwaltung einem Benutzerverwalter nur die Zuordnung bestimmter Profile zu ermöglichen, z.B. für ein Modul oder eine Organisationseinheit.
6.1.	**Wer kann Profile anlegen?** Report RSUSR002 mit den Eingaben: S_TCODE = SU02 S_USER_PRO (Profile verwalten) mit Aktivität „*" oder 01 (Anlegen) und Profil = „*" oder = Profilnamen.

NR.	BERECHTIGUNGSVERWALTUNG: PROFILE UND BERECHTIGUNGEN
6.2.	**Wer kann Profile ändern?** Report RSUSR002 mit den Eingaben: S_TCODE = SU02 S_USER_PRO (Profile verwalten) mit Aktivität „*" oder 02 (Ändern) und Profil = „*" oder = Profilnamen
7.	**Das Objekt Benutzerstammpflege, Berechtigungen S_USR_AUT** legt die Berechtigungsobjektnamen und die Berechtigungsnamen sowie die zulässigen Aktivitäten fest, für die ein Berechtigungsverwalter berechtigt ist. Es kann benutzt werden, um bei einer dezentralisierten Benutzerverwaltung einem Berechtigungsverwalter nur die Erstellung bestimmter Berechtigungen in Profilen zu erlauben und damit die Erstellung kritischer Berechtigungen in Profilen zu verhindern.
NR.	**BERECHTIGUNGSVERWALTUNG: ROLLEN DEN BENUTZERN ZUORDNEN**
8.1.	**Wer kann Rollen Benutzern zuordnen?** Report RSUSR002 mit den Eingaben: S_TCODE = PFCG S_USER_AGR (Rollen verwalten) mit Aktivität „*" oder 02 (Ändern) und 22 (Zuordnen) und Rolle = „*" oder = Rollennamen S_USER_GRP (Benutzerverwaltung) mit Aktivität „*" oder 22 (Zuordnen) und Gruppe = „*" oder = Gruppennamen.
8.2.	**Wer kann Benutzern Profile zuordnen und entziehen?** Report RSUSR002 mit den Eingaben: S_TCODE = SU01 oder PFCG S_USER_GRP (Benutzerverwaltung) mit Aktivität „*" oder 02 (Ändern) und Gruppe = „*" oder = Gruppennamen S_USER_PRO (Profile verwalten) mit Aktivität"*" oder 22 (Zuordnen) und Profil = „*" oder = Profilnamen.
8.3.	**Wer kann Benutzern Rollen oder Profile zuordnen und entziehen?** Report RSUSR002 mit den Eingaben: S_TCODE = SU01 S_USER_GRP (Benutzerverwaltung) mit Aktivität „*" oder 02 (Ändern) und Aktivität 22 (Zuordnen) und Gruppe = „*" oder = Gruppennamen S_USER_PRO (Profile verwalten) mit Aktivität „*" oder 22 (Zuordnen) und Profil = „*" oder = Profilnamen S_USER_AGR (Rollen verwalten) mit Aktivität „*" oder 22 (Zuordnen) und Rolle = „*" oder = Rollennamen.

4.13. PRÜFPROGRAMM: SICHERHEITSMECHANISMEN ZUR AKTIVIERUNG DER PRÜFUNG VON BERECHTIGUNGEN

1.1.	**Berechtigungsverwaltung: Wer kann Berechtigungsobjekte deaktivieren?** Report RSUSR002 mit den Eingaben: S_TCODE = AUTH_SWITCH_OBJECTS S_USER_OBJ (Objekte verwalten) mit Aktivität 02 (Ändern) und 07 (Aktivieren) und Objekt = „*" oder = „Objektnamen". Diese Berechtigung ist restriktiv an Systemadministratoren zu vergeben. Das Deaktivieren von Berechtigungsobjekten muss freigegeben und dokumentiert werden. **Hinweis:** Mit der Transaktion AUTH_ SWITCH_ OBJECTS können Berechtigungsobjekte global ausgeschaltet werden. › Für ausgeschaltete Berechtigungsobjekte fügt der Profilgenerator keine Berechtigungen in die generierten Profile ein. › Beim Wiedereinschalten eines Objektes muss daher eventuell eine große Anzahl von Rollen bzw. Profilen bearbeitet werden. Das Abschalten von Objekten wird auch aus diesem Grund nicht empfohlen. › Berechtigungsobjekte, die mit S_ und P_ beginnen (Bereiche Basis und HR), lassen sich grundsätzlich nicht global ausschalten. › Ein Überblick über global ausgeschaltete Objekte kann mit der Transaktion AUTH_DISPLAY_OBJECTS angezeigt werden. › Im Anwendungsprotokoll (Transaktion SLG1) wird unter dem Objektnamen PRGN_LOG_OBJ das globale Ein- und Ausschalten von Objekten protokolliert.
1.2.	**Ist der Profilgenerator aktiviert?** **AIS:** System Audit - Top Ten Security Reports – Profilparameter anzeigen (auth/*) **AIS:** System Audit – Systemkonfiguration – Parameter – Systemparameter, Übersicht mit Historie Seit Version 4.6C ist der Profilparameter auth/no_check_in_some_cases auf den Wert Y (Defaultwert) gesetzt.
1.3.	**Wer kann die Prüfkennzeichen und Vorschlagswerte des Profilgenerators pflegen?** Report RSUSR002 mit den Eingaben: S_TCODE = SU24 S_DEVELOP (Anwendungsentwicklung) mit Aktivität 02 (Ändern) und Objekttypen › SUSK (Zuordnung Transaktion zu Berechtigungsobjekt im Kundenstamm, USOBX_C und USOBT_C) › SUST (Zuordnung Transaktion zu Berechtigungsobjekt in SAP-Systemen, USOBX und USOBT und Objektname = „*" (alle Transaktionen) oder = „Name einer Transaktion, die zu bearbeiten ist". Diese Berechtigung ist restriktiv an Systemadministratoren zu vergeben. Die Pflege der Prüfkennzeichen und Vorschlagswerte des Profilgenerators muss freigegeben und dokumentiert werden.

1.4.	**Werden indirekte Transaktionsaufrufe einer Berechtigungsprüfung unterzogen?** Ist in der Tabelle TCDCOUPLES im Feld OKFLAG bei den aufgeführten Transaktionspaaren ein „X" gesetzt? **Hinweis:** Wird eine Transaktion indirekt, d.h. von einer anderen Transaktion aufgerufen, so wird keine Berechtigungsprüfung vorgenommen. So werden z.B. Berechtigungen nicht geprüft, wenn eine Transaktion eine andere mit der Anweisung CALL TRANSACTION aufruft (SAP-Hinweis 358 122).
1.5.	**Ist bei Transaktionsaufrufen die Berechtigungsprüfung deaktiviert?** Ist in der Tabelle USOBX_C im Feld OKFLAG ein „N" und im Feld MODIFIED ein „X" gesetzt? **Hinweis:** Ist die Berechtigungsprüfung für ein Berechtigungsobjekt einer Transaktion über die SU24 deaktiviert worden, ist dies in der Tabelle USOBX_C nachvollziehbar. Für deaktivierte Berechtigungsobjekte ist zu prüfen, ob eine entsprechende Freigabe vorliegt.

5. SYSTEMINTEGRITÄT AUF DER ANWENDUNGSEBENE

5.1. PRÜFPROGRAMM: SCHUTZ DER BATCH-INPUT-PROZESSE

NR.	SCHUTZ DER BATCH-INPUT-PROZESSE
1.	**Kontrollziel: Die ordnungsmäßige Verarbeitung der Geschäftsdaten und des Buchungsstoffs ist sichergestellt.** 1. Die Vollständigkeit, Richtigkeit und Zeitgerechtigkeit der Verarbeitung ist sicherzustellen, insbesondere bei Daten der Buchhaltung. 2. Über Arbeitsanweisungen ist sichergestellt, dass die Vollständigkeit der Verarbeitung überwacht wird und die notwendigen Maßnahmen zur Nachbearbeitung von Belegen durchgeführt werden. 3. Das interne Kontrollsystem verlangt eine Funktionstrennung zwischen planender, ausführender und überwachender Stelle. **Risiko:** Belege werden nicht verarbeitet. Fehlerhafte oder nicht vollständige Belege werden nicht korrigiert. Die gleichen Belege werden mehrfach eingelesen. Belege werden in falscher Reihenfolge bearbeitet, z.B. Stammdatenänderungen nach Buchungen, die diese Stammdatenänderungen zur Voraussetzung hatten. Fehler- und Verarbeitungsprotokolle werden gelöscht, bevor sie als Hinweise für notwendige Korrekturen oder als Nachweise der ordnungsmäßigen Verarbeitung verwendet worden sind.
1.1.	**Kontrollfragen zum Prozess:** › Gibt es eine Übersicht über alle Batch-Input-Schnittstellen, z.B. mit den folgenden Angaben: abgebendes Arbeitsgebiet, Dateninhalt, Dateiname, Periode, Mappenname, Verarbeitungsjob, relevante Tabellen, Abstimmkreis, Verantwortlichkeit? › Welche Anwender dürfen welche Mappen erstellen, starten, korrigieren oder löschen? › Gibt es eine Übersicht, welche Mappennamen für welche Abteilung reserviert sind? › Wer stimmt den Buchungsstoff der verarbeiteten Mappen ab? › Wer kontrolliert, dass die Daten aus den Vorsystemen vollständig, richtig und zeitgerecht übernommen werden? Wird insbesondere ein mehrfaches Einlesen der gleichen Belege verhindert? Werden die Dateien nach dem Einlesen gesichert und gelöscht? › Sind die internen Kontrollen zwischen Vorsystemen und dem Zielsystem gewahrt, in dem die Mappen abgespielt werden?
1.2.	Analyse der Batch-Input-Mappen **AIS:** System Audit – Hintergrundverarbeitung – Batch-Input-Monitoring Oder Transaktion SM35
1.3.	**Wer darf alle Batch-Input-Mappen uneingeschränkt verwalten?** Report RSUSR002 mit den Eingaben: S_TCODE = SM35 S_BDC_MONI (Batch-Input-Berechtigung) mit Aktivität „*" und Mappennamen = „*" oder speziell auf alle kritischen Verwaltungsaktionen bezogen: S_BDC_MONI (Batch-Input-Berechtigung) mit Aktivitäten ABTC (Hintergrundverarbeitung), FREE (Freigeben), LOCK (Ent-/Sperren), DELE (Löschen) und REOG (Reorganisieren) und Mappennamen = „*". Diese Berechtigung ist nur an Systemadministratoren zu vergeben.

NR.	SCHUTZ DER BATCH-INPUT-PROZESSE
1.4.	**Wer kann Batch-Input-Mappen freigeben?** Report RSUSR002 mit den Eingaben: S_TCODE = SM35 S_BDC_MONI (Batch-Input-Berechtigung) mit Aktivität FREE (Mappen freigeben) und Mappennamen = *. Hierbei ist die Funktionstrennung (4-Augen-Prinzip) einzuhalten.
1.5.	**Wer kann Batch-Input-Mappen und Protokolle analysieren?** Report RSUSR002 mit den Eingaben: S_TCODE = SM35 S_BDC_MONI (Batch-Input-Berechtigung) mit Aktivität ANAL (Mappen und Protokolle analysieren) und Mappennamen = *. Hierbei ist die Funktionstrennung (4-Augen-Prinzip) einzuhalten.
1.6.	**Wer kann Batch-Input-Mappen im Dialogbetrieb oder im Hintergrund verarbeiten?** Report RSUSR002 mit den Eingaben: S_TCODE = SM35 S_BDC_MONI (Batch-Input-Berechtigung) mit Aktivität ABTC (Mappen für die Hintergrundverarbeitung übergeben) oder AONL (Mappen im Dialogbetrieb abspielen) und Mappennamen = *. **Risiko:** Im Dialogbetrieb können Werte in Eingabefeldern überschrieben werden.
1.7.	**Wer kann Batch-Input-Mappen (ent-)sperren?** Report RSUSR002 mit den Eingaben: S_TCODE = SM35 S_BDC_MONI (Batch-Input-Berechtigung) mit Aktivität LOCK (Mappen sperren oder entsperren) und Mappennamen = *. Hierbei ist die Funktionstrennung (4-Augen-Prinzip) einzuhalten.
1.8.	**Wer kann Batch-Input-Mappen und Protokolle reorganisieren?** Report RSUSR002 mit den Eingaben: S_TCODE = SM35 S_BDC_MONI (Batch-Input-Berechtigung) mit Aktivität REOG (Mappen und Protokolle reorganisieren) und Mappennamen = *. **Risiko:** Verarbeitungsnachweise können über einen Reorganisationslauf gelöscht werden. Hierbei ist die Funktionstrennung (4-Augen-Prinzip) einzuhalten.
1.9.	**Wer kann Batch-Input-Mappen löschen?** Report RSUSR002 mit den Eingaben: S_TCODE = SM35 S_BDC_MONI (Batch-Input-Berechtigung) mit Aktivität DELE (Mappen löschen) und Mappennamen = *. **Risiko:** Mappen z.B. mit relevantem Buchungsstoff können vor der Weiterverarbeitung gelöscht werden. Hierbei ist die Funktionstrennung (4-Augen-Prinzip) einzuhalten.
1.A	**Ist die Übergabedatei über geeignete Dateizugriffsrechte geschützt?** Transaktion AL11 – Attribute der Übergabedatei **Risiko:** Die Übergabedatei kann vor der Verarbeitung manipuliert werden. Eine Protokollierung findet nicht statt. Die Datenintegrität über Systemgrenzen ist nicht mehr gewährleistet.

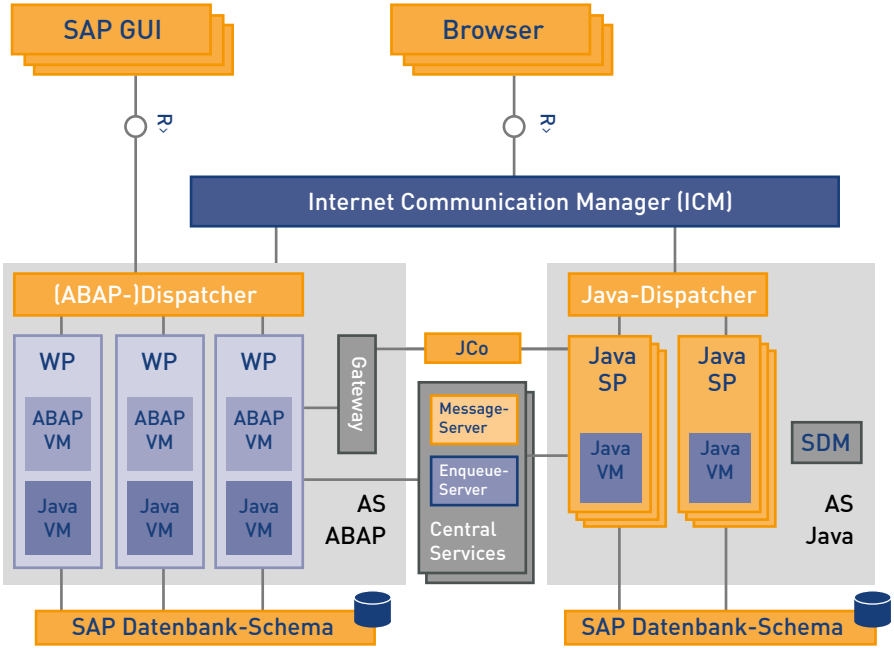
NR.	SCHUTZ DER BATCH-INPUT-PROZESSE
2.	**Kontrollziel: Gewährleistung des ordnungsmäßigen Programmeinsatzes und der Datenintegrität, wenn beim Direct-Input-Verfahren die Daten mit reduzierten Plausibilitätsprüfungen direkt in die Datenbank geschrieben werden.** Risiko: Es ist möglich, vorhandene Datenbestände unprotokolliert zu verändern. Bei einer fehlerhaften Anwendung ist die Datenintegrität des Systems gefährdet. Auf die Verwendung der Transaktion LSMW oder den direkten Aufruf der jeweiligen Reports sollte aus Gründen der Datenintegrität verzichtet werden. Nur die Transaktion bietet einen Wiederaufsetzmechanismus.
2.1.	**Wird das Verfahren des Direct-Input genutzt?** Prüfen über die Transaktion BMV0 (Verwaltung von Datenübernahmen).
2.2.	**Kontrollfragen zum Prozess:** › Ist der Einsatz des Direct-Input-Verfahrens dokumentiert? › Wird der Einsatz eines Direct-Input-Ablaufs vor dem produktiven Einsatz im Testsystem getestet und nach dem 4-Augen-Prinzip freigegeben? › Gibt es eine Verfahrensanweisung, wie der Prozess des Direct-Input überwacht und wie fehlerhafte Abläufe behandelt werden?
2.3.1.	**Wer kann einen Direct-Input-Job definieren?** Report RSUSR002 mit den Eingaben: *S_TCODE = BMV0* *S_TABU_DIS mit ACTVT 02 und DICBERCLS SS.* Hierbei ist die Funktionstrennung (4-Augen-Prinzip) einzuhalten.
2.3.2.	**Wer kann einen Direct-Input-Job definieren?** Report RSUSR002 mit den Eingaben: *S_TCODE = SXDA* *S_TABU_DIS mit ACTVT 02 und DICBERCLS SS.* *S_DX_MAIN mit TCD SXDA und ACTVT 03* *S_DX_PROJ mit TCD SXDA und ACTVT 16* Hierbei ist die Funktionstrennung (4-Augen-Prinzip) einzuhalten.
2.4.1.	**Wer kann einen Direct-Input-Job starten, wiederaufsetzen, verwalten?** Report RSUSR002 mit den Eingaben: *S_TCODE = BMV0* *S_BDC_MONI mit BDCACTI ABTC oder REOG* *S_BTCH_JOB mit Jobaction RELE* *S_DATASET mit ACTVT 33 und Program* RMDATIND RM06EEI0 RM06EEI1 RSTXLITF RVINVB10 RFBIBL00 RCCLBI03 RAALTD11 RCPTRA02 RM60IN00 RCRAPDX2 RFVIMEDI RFVIMVDI RIIBIP00 RSADRLSM02 Hierbei ist die Funktionstrennung (4-Augen-Prinzip) einzuhalten.

NR.	SCHUTZ DER BATCH-INPUT-PROZESSE
2.4.2.	**Wer kann einen Direct-Input-Job starten, wiederaufsetzen, verwalten?** Report RSUSR002 mit den Eingaben: S_TCODE = SXDA *S_BDC_MONI mit BDCACTI ABTC oder REOG* *S_BTCH_JOB mit Jobaction RELE* *S_DX_MAIN mit TCD SXDA und ACTVT 03* *S_DX_PROJ mit TCD SXDA und ACTVT 16 oder 02* *S_DATASET mit ACTVT 33 und Program* RMDATIND RM06EEI0 RM06EEI1 RSTXLITF RVINVB10 RFBIBL00 RCCLBI03 RAALTD11 RCPTRA02 RM60IN00 RCRAPDX2 RFVIMEDI RFVIMVDI RIIBIP00 RSADRLSM02 Hierbei ist die Funktionstrennung (4-Augen-Prinzip) einzuhalten.
2.4.3.	**Wer kann einen Direct-Input-Job starten, wiederaufsetzen?** Report RSUSR002 mit den Eingaben: *S_TCODE = LSMW* *B_LSMW mit ACTVT 16 und TCD LSMW* *B_LSMW_PRO mit Project <variabel>* *S_DATASET mit ACTVT 33 und Program* RMDATIND RM06EEI0 RM06EEI1 RSTXLITF RVINVB10 RFBIBL00 RCCLBI03 RAALTD11 RCPTRA02 RM60IN00 RCRAPDX2 RFVIMEDI RFVIMVDI RIIBIP00 RSADRLSM02 Hierbei ist die Funktionstrennung (4-Augen-Prinzip) einzuhalten.

6. SYSTEMINTEGRITÄT MIT DEM SAP JAVA-STACK

6.1. ÜBERBLICK

Im Jahr 2004 hat SAP die NetWeaver-Technologie eingeführt und erstmalig den sogenannten „Java-Stack" (SAP AS Java) implementiert. Die Technologieplattform NetWeaver dient als Grundlage für eine serviceorientierte Architektur, um durchgängige Prozesse mit Anwendungen der SAP Business Suite zu gewährleisten. Das aktuelle Release 7.4 kann als eigenständige Installation oder im sogenannten „Dual-Stack" mit einem ABAP-System betrieben werden. SAP stellt den Java-Stack auf einem Anwendungsserver gemäß der Spezifikation J2EE (Java 2 Enterprise Edition) bzw. Java EE Standard bereit. Der Leitfaden zielt auf die Absicherung und Beschreibung von Kontrollen des SAP AS Java sowohl für eine reine Java-Instanz als auch für einen parallelen Betrieb mit dem AS ABAP. Zudem ist eine Mischung von ABAP/Java-Komponenten im AS ABAP möglich, auf die in diesem Abschnitt nicht eingegangen wird. Risiken bei der Verwendung von Java im AS ABAP müssen über Kontrollen im AS ABAP behandelt werden.



6.2. RISIKEN

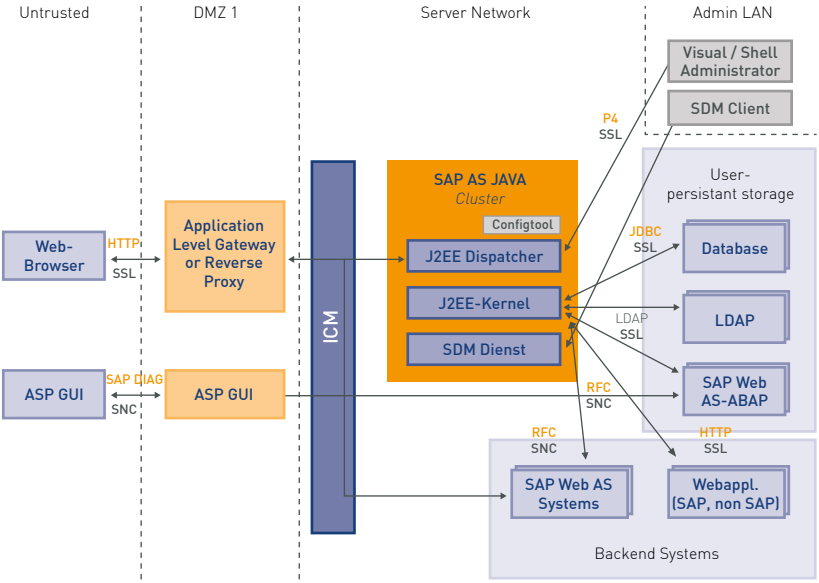
- Die Sicherheitsanforderungen der Java-Architektur sind nicht bekannt, ermittelt und umgesetzt.
- Schwächen in der Konfiguration ermöglichen den unautorisierten Zugriff auf Daten.
- Unsichere Passwörter von Standardbenutzern gefährden die Sicherheit und Integrität von Daten.
- Ein geregeltes Softwareänderungs- und Einsatzverfahren ist nicht umgesetzt. Es besteht das Risiko, dass schwachstellenbehaftete und nicht autorisierte Java-Anwendungen betrieben werden. Die Vertraulichkeit, Integrität und Verfügbarkeit von Daten kann nicht gewährleistet werden.

6.3. KONTROLLZIELE

- Die Sicherheitsempfehlungen von SAP zur sicheren Konfiguration der Java-Architektur sind umgesetzt.
- Standardbenutzer verfügen über sichere Passwörter. UME-Rollen sind gemäß IKS-Anforderungen eingerichtet.
- Die Anforderungen an ein geregeltes Softwareänderungs- und Einsatzverfahren sind mit den Mitteln von SAP unterstützt (SDM, SPML und CMS).
- Portaldienste und Anwendungen sind ausreichend vor Webrisiken abgesichert.

6.4. SAP AS JAVA SYSTEMARCHITEKTUR

Zum Verständnis der Kontrollen, Risiken und der Durchführung der Kontrollhandlungen ist ein grundlegendes Verständnis der AS-Java-Architektur notwendig. Folgende Abbildung stellt relevante Komponenten der Architektur von AS Java dar:



Die einzelnen Komponenten und AS-Java-Tools werden in den beiden folgenden Tabellen kurz vorgestellt.

TABELLE 1: SAP-PROGRAMMBESCHREIBUNGEN

	PROGRAMM	BESCHREIBUNG
1	SAP J2EE Engine (AS Java)	Die SAP J2EE Engine unterstützt unterschiedliche Ablagen zum Sichern von Benutzerinformationen. Standardmäßig ist die User Management Engine (UME) die aktive Benutzerablage; alternativ dazu kann die J2EE-eigene DBMS-Benutzerablage verwendet werden.
2	User Management Engine (UME)	Die User Management Engine dient allen Java-Applikationen als Benutzer-Directory und ist fähig, Benutzer aus mehreren Quellen zu bearbeiten. J2EE SAP Engine der SAP WEB AS Java integriert die UME als zentralen Benutzer-Manager und kann UME mithilfe des eigenen Administrationstools warten.
3	Internet Commu-nication Manager (ICM)	Der Internet Communication Manager gewährleistet die Kom-munikation zwischen dem SAP-System (SAP Web Application Server) mit der Außenwelt über die Protokolle HTTP, HTTPS und SMTP. In der Serverrolle kann er Anfragen aus dem Internet bearbeiten, die mit URLs mit der Server/Port-Kombination, auf die der ICM hört, ankommen. Abhängig von der URL ruft der ICM dann den entsprechenden lokalen Handler auf.

	PROGRAMM	BESCHREIBUNG
4	SAP Web Dispatcher	Der SAP Web Dispatcher steht zwischen dem Internet und dem SAP-System (SAP Web AS). Er ist der Einstiegspunkt für HTTP(S)-Request. Als „Software-Web-Switch" kann er Verbindungen abweisen oder annehmen und nimmt dann die Request-Verteilung für eine gleichmäßige Serverauslastung vor (Lastausgleich).
5	ICF Modul (Internet Communication Framework)	Das Internet Communication Framework (ICF) ist integriert in den SAP Web Application Server. Es bietet eine Umgebung zur Behandlung von HTTP Requests in ABAP-Prozessen. ICF dient als Server oder Client für SAP WEB AS HTTP Requests.
6	AS ABAP	ABAP-Anwendungsprogramme werden in der Programmiersprache ABAP erstellt und laufen in der ABAP-Anwendungsschicht des SAP NetWeaver Application Server ABAP.
7	Service Provisioning Markup Language (SPML)	Die Service Provisioning Markup Language (SPML) ist ein XML-basiertes Framework für den Austausch von Benutzer-, Ressourcen- und Service-Provisioning-Informationen zwischen kooperierenden Organisationen. „Service Provisioning" beschreibt generell die Vorbereitung von bestimmten (IT-) Aktivitäten.
8	Software Deployment Manager Client (SDM)	Der Software Deployment Manager (SDM) ist ein Werkzeug, mit dem Softwarepakete, die SAP verteilt, verwaltet und deployed werden können. SDM hat nur einen Benutzer mit einem Passwort.

TABELLE 2: AS JAVA PROGRAMME UND TOOLS

	PROGRAMM	BESCHREIBUNG	PORT
1	SAP NetWeaver Administrator (NWA)	Nachfolger des Visual Adminstrator Tools und webbasiertes Werkzeug für die Administration, Konfiguration und Monitoring der J2EE-Instanzen. Nutzt die User Management Engine (UME). SAP bietet standardmäßig die folgenden vordefinierten Rollen innerhalb der UME: Release 7.0 SAP_JAVA_NWADMIN_LOCAL SAP_JAVA_NWADMIN_LOCAL_READONLY SAP_JAVA_NWADMIN_CENTRAL SAP_JAVA_NWADMIN_CENTRAL_READONLY Release 7.1 NWA_READONLY NWA_SUPERADMIN Pfad: http://‹Host›:‹port›/irj/nwapi	5 ‹Java_ instance_ number› 00

	PROGRAMM	BESCHREIBUNG	PORT
2	SAP Enterprise – Config Tool	Eigenständiges Werkzeug zur Offline-Konfiguration und Administration von Cluster-Elementen des Web AS Java. Kann ohne Eingabe eines Passwortes durch den Administrator gestartet werden und wird insbesondere dann verwendet, wenn der Visual Administrator nicht verfügbar ist. Mit dem Config Tool können sowohl lokale als auch globale Konfigurationseinstellungen vorgenommen werden. Im Gegensatz zum Visual Admin arbeitet das Config Tool direkt auf der Datenbank. ‹Verzeichnis der J2EE-Installation› Ordner: ‹SID›\‹Instanzname›/j2ee\configtool\ configtool. [sh|bat]	-
3	Visual Administrator	Der Visual Admin dient als GUI, mit dem alle Cluster-Elemente und alle Module des J2EE Engine administriert werden können. Es kann allgemeine Informationen über Services, Manager, Schnittstellen und Libraries des Java-Systems abrufen sowie Einstellungen und administrative Aufgaben an den Services, Managern und Schnittstellen vornehmen. Ebenfalls sind Änderungen von globalen Einstellungen des Java Servers möglich. Pfad (local): \usr\sap\‹SAPSID›\‹Instanzname›/ j2ee\admin\go. [sh|bat]	5 ‹J2EE instance_ number› 04
4	SAP Management Console (SAP MC)	Überwachung, Start, Stopp und Restart von SAP-Systemen und Instanzen. Anzeige der SAP-Protokoll- und Trace-Dateien, der Start-Profile, Instanzparameter, der System- und SAP-Umgebung und der Statistik des Internet Communication Manager (ICM). Pfad: http://‹Application-server-of-the-SAP-instance›:‹port›	5 ‹J2EE instance_ number› 13
5	Shell Administrator (Telnet)	Für den Fall, dass der Visual Admin nicht zur Verfügung steht, ist es möglich, über Telnet zu administrieren. Dies ist aus Sicherheitsgründen nicht empfohlen.	50008
6	SDM Client	Tool zum Verwalten des SDM Dienstes.	

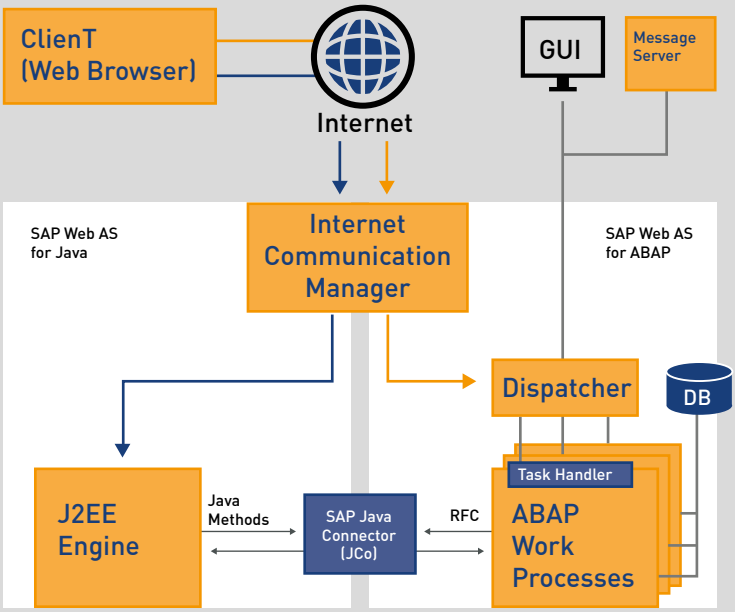
6.5. PRÜFPROGRAMM: SICHERE KONFIGURATION DES SAP JAVA-STACK

NR.	SICHERE KONFIGURATION DES SAP JAVA-STACK
1.	**Kontrollziel: Sichere Konfiguration des SAP Java-Stack** **Risiko:** Sicherheitsrisiken im Betrieb eines SAP Java-Stacks sind nicht beurteilt und abgestellt. **Hinweis:** Der SAP Java-Stack bleibt in dem ungesicherten Zustand nach erfolgter Standardinstallation.
1.1.	**Werden überhaupt Java-basierte Produkte oder Anwendungen eingesetzt?** **Hinweis:** Falls dies nicht zutrifft, können alle Dienste des Java-Stack deaktiviert werden.
1.2.	**Sind nicht benötigte Dienste abgeschaltet? Ist der folgende SAP-Hinweis bekannt und umgesetzt worden?** **SAP-Hinweis:** 871 394, „Dispensable functions with impact on security".
1.3.	**Ist der http-Dienst gesichert?** › Ist die Verzeichnisanzeige unterbunden? › Sind nicht benötigte Alias deaktiviert? › Ist das Hochladen von Daten ausgeschlossen (http PUT)? **SAP-Hinweis:** 604 285, „Security vulnerability by unprotected http PUT method". **SOS:** HTTP Based Browsing IEX (0780) **SOS:** Restriction of HTTP PUT Method IEX (0779)
1.4.	**Ist die kryptografische Funktionsbibliothek konfiguriert?** **Hinweis 1:** Die Datei IAIK_JCE.JAR muss manuell in das Verzeichnis ‹SAPj2eeEngine_install_dir› / admin / lib kopiert oder nachträglich durch Deployment der SAP Java Cryptographic Toolkit SDA konfiguriert werden. **Hinweis 2:** Per default wird die SAP J2EE Engine nur mit der Exportversion des Sicherheitswerkzeugkastens ausgeliefert. Diese enthält nur die Funktionen für die digitale Verschlüsselung, nicht aber die Verschlüsselungsfunktion, um HTTPS zu unterstützen. **SOS:** Installation of the SAPcryptolib IEX (0871)
1.5.	**Sind die Betriebssystemdateien mit den streng vertraulichen Anmeldeinformationen stark verschlüsselt?** **Hinweis 1:** Die J2EE Engine speichert standardmäßig sichere Daten in der Datei \usr\sap\‹SID›\SYS\global\security\data\SecStore.properties im Dateisystem. Diese Datei wird während der Installation erstellt und die J2EE Engine benutzt sie, um vertrauliche Verbindungsdaten zu speichern. Diese Verbindungsdaten vom Datenbankbenutzer SAP‹SID›DB enthalten z.B. sein Passwort, die Datenbankbasis sowie Informationen über den Benutzeradministrator und dessen Passwort. Die Verschlüsselung für Secure-Storage-Daten kann mit dem Paramter „$internal/mode = z.B. encrypted" in der SecStore.properties geprüft werden. **Hinweis 2:** Zur Verschlüsselung der Passwörter des Datenbankbenutzers SAP‹SID›DB und des Administrator-Benutzers sollte die SAP Java Cryptographic Library aktiviert sein. Wenn die SAP Java Cryptographic Library genutzt wird, werden die Passwörter mit dem Triple-DES-Verfahren verschlüsselt, anstatt mit dem base64-Verfahren codiert. **Hinweis 3:** Der Schlüssel für die Datei \usr\sap\‹SID›\SYS\global\security\data\SecStore.properties befindet sich in \usr\sap\‹SID›\SYS\global\security\data\SecStore.key. Der Lese- und Schreibzugriff auf beide Dateien sollte stark eingeschränkt werden. **Hinweis 4:** Die Installation der SAP Note 1619539 wird empfohlen. **SOS:** Strong Encryption for the Secured Storage in the File System IEX (0882)

NR.	SICHERE KONFIGURATION DES SAP JAVA-STACK
1.6.	**Welche Benutzer sind in der Standardbenutzergruppe „Administrators"?** **Hinweis:** Benutzer der Gruppe „Administrators" haben uneingeschränkte Administrator-Privilegien auf den Java-Anwendungsserver. Sie haben die Berechtigung, alle anderen Benutzer zu verwalten, einschließlich anderer Benutzer mit Administrator-Privilegien. Sie können alle Sicherheitseinstellungen verändern. Es gibt außerhalb dieser Gruppe keine anderen Benutzer, die für die Benutzer- und Sicherheitsadministration zuständig sind. Nur Systemadministratoren dürfen in der Standardbenutzergruppe „Administrators" sein. **SOS:** Users of Standard User Group „Administrators" IEX (0893)
1.7.	**An welche Benutzer ist die Sicherheitsrolle „telnet_login" vergeben?** **Hinweis 1:** Sie darf nur an die Administratoren der J2EE Engine vergeben sein. **SOS:** J2EE Server Remote Administration with Telnet IEX (0775) **Hinweis 2:** Der netzwerkseitige Zugriff auf den Telnet-Dienst kann über den Parameter „BIND" im Configtool auf „localhost" oder „127.0.0.1" eingeschränkt werden. Anmeldungen aus dem Netzwerk werden hierdurch unterbunden.
1.8.	**Werden sicherheitsrelevante Java Notes regelmäßig eingespielt?** **Hinweis 1:** SAP Notes bzw. Java Notes, die eine hohe Risikoklassifizierung (priority 1 und 2) besitzen, sollten monatlich eingespielt werden. SAP veröffentlicht jeden zweiten Dienstag im Monat neue sicherheitsrelevante Updates (SAP Security Notes).
2.	**Kontrollziel: Sichere Einstellung von Security Logs von UME und ICM** **Risiko:** Die Security Logs vom UME und ICM bieten bei einer unzureichenden Konfiguration keine ausreichenden Nachweise bei unautorisierten Änderungen oder Zugriffen. Logdateien können durch eine nicht revisionssichere Speicherung unauthorisiert gelöscht oder manipuliert werden. **Hinweis:** 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. Eine Auslagerung der Protokolldateien auf einen dedizierten Log-Host kann die Sicherheit erhöhen. Im ICM Security Log werden Incidents aus der Netzwerkkommunikation aufgezeichnet. Sofern der Zugriffsschutz im UME vom Java-Stack eingerichtet ist, werden sicherheitsrelevante Ereignisse im UME-Security Log aufgezeichnet. Der Zugriff durch die Administratoren sollte daher restriktiv vergeben werden.
2.1.	**Werden die eingehenden Verbindungen geloggt?** **Hinweis:** Parameter ist zu finden unter „icm/HTTP/logging_‹xx›". Bei Anwendungen mit entsprechenden Schutzbedarf zu aktivieren. Hier ist zu beachten, dass vertrauliche und personenbezogene Daten aufgezeichnet werden können und evtl. datenschutzrechtliche Aspekte beachtet werden müssen.
2.2.	**Werden die ausgehenden Verbindungen geloggt?** **Hinweis:** Parameter ist zu finden unter „icm/HTTP/logging_client_‹xx›". In Absprache mit den Applikationsverantwortlichen sollte geklärt werden, ob eine Überwachung der ausgehenden Daten erforderlich ist. Unter Umständen kann hier eine Data-Leakage-Funktionalität eingebunden werden.

NR.	SICHERE KONFIGURATION DES SAP JAVA-STACK
2.4.	**Sind die Sicherheitslogs von ICM und SAP Web Dispatcher konfiguriert?** **Hinweis 1:** Parameter „icm/security_log" kontrolliert die Ausgabe von ICM und SAMP Web Dispatcher und hat folgenden Einstellungen: LOGFILE=dev_icm_sec,LEVEL=2, MAXSIZEKB=500 **Hinweis 2:** Der Trace-Level sollte auf produktiven Systemen nicht den Wert 3 besitzen und Traces, die für administrative Zwecke angelegt wurden, müssen nach der Tätigkeit vom produktiven System entfernt werden.
2.5.	**Ist das Sicherheitslog von UME gesichert?** **Hinweis:** Speicherort im Log Viewer: ./log/system/security.log Speicherort im Dateisystem: /usr/sap/‹SID›/‹instance_number›/j2ee/cluster/server‹X›/log/system/security.log Diese Datei enthält alle Änderungen an Benutzerstammdaten, Anmeldungen sowie weitere UME-Meldungen. Die Berechtigung auf die Dateien ist einzuschränken. Die Protokolle sollten zyklisch auf einem zentralen Log-Host abgelegt werden.

6.6. PRÜFPROGRAMM: SICHERHEIT DES ICM

NR.	PRÜFPROGRAMM: SICHERHEIT DES ICM
1.	**Kontrollziel: Absicherung des ICM** **Risiko:** Ungesicherte (Web-)Schnittstellen im WebAS- und J2EE-Umfeld können die Vertraulichkeit und Sicherheit von Daten gefährden. **Hinweis:** ICM Web-Anfragen werden vom ICF-Modul (Internet Communication Framework) verarbeitet. Hierzu werden in einem zentralen Repository alle registrierten Dienste gespeichert, wodurch der ICF entscheiden kann, an welchen dahinterliegenden Service er den Web-Request leitet. Anfragen für den Java-Stack durchlaufen ebenfalls den ICM. Daher müssen Schnittstellen im ICM angemessen abgesichert und eine Verschlüsselung zum Benutzer und gegebenenfalls zu internen Schnittstellen eingerichtet werden.  *Abbildung 2: Integration des ICM zwischen ABAP- und Java-Stack* Ausnahmen sollten dokumentiert und nur in Abstimmung mit dem Sicherheitsmanagement eingerichtet werden.
1.1.	**Werden interne Versionsangaben im Header angezeigt?** **Risiko:** Angaben über interne Komponenten liefern Angreifern wertvolle Informationen, die für weiterführende Angriffsszenarien genutzt werden können. **Hinweis:** „http.properties:UseServerHeader" definiert, ob Versionsinformationen in einem HTTP-Header angezeigt werden. Der Vorschlagswert ist „false".

NR.	PRÜFPROGRAMM: SICHERHEIT DES ICM
1.2.	**Ist die maximale Größe von Web-Anfragen eines Benutzers definiert?** **Hinweis:** Eingehende Anfragen sollten über den Parameter „icm/‹PROT›/max_request_size_KB" auf maximal 2048 KB (2MB) eingeschränkt werden. Mit diesem Parameter kann der Applikationsserver vor einer Denial of Service Attacke (DOS) mit großen Anfragepaketen geschützt werden.
1.3.	**Ist die Administrationsoberfläche mithilfe von Verschlüsselung geschützt?** **Hinweis:** Die Administrationsoberfläche ist mit folgenden Parametern zu konfigurieren: icm/HTTP/admin_‹xx› Mit ‹xx› als port=https, HOST=interne Admin Rechner Dabei ist nur auf HTTPS Ports zu setzen icm/server_port_2 ‹yy› Mit ‹yy› als PROT=HTTPS, PORT=443, TIMEOUT=15, PROCTIMEOUT=45, VCLIENT=2
1.4.	**Werden HTTP(S) Request gefiltert?** **Hinweis:** Parameter „icm/HTTP/auth_‹xx›" sollte geprüft werden. Mit diesem Parameter kann der HTTP-Request anhand von verschiedenen Kriterien abgeblockt werden. Wenn aktiviert, wird dieser Filter bei jedem HTTP(S) Request zum ICM oder Web Dispatcher durchlaufen, bevor der Request zu einem anderen HTTP-Handler (Dateizugriff, Cache Administration, Redirect) oder zum Backend-System (ABAP oder J2EE Engine) weitergeleitet wird. Bei der Benutzung von PERMFILE sollten Whitelists zum Einsatz kommen. Die Whitelist ist pro Anwendung zu definieren.
1.5.	**Ist das Verhalten von ICM im Fehlerfall eingestellt?** **Hinweis:** Parameter „icm/HTTP/error_templ_path" soll gesetzt werden. Der Parameter dient zur Einstellung des ICM im Fehlerfall.
1.6.	**Sind die Dateizugriffe auf statische Webinhalte eingeschränkt?** **Hinweis:** Parameter „icm/HTTP/file_access_‹xx›" sollte gesetzt werden. Dieser Parameter bestimmt, für welches URL-Präfix statische Dateizugriffe erlaubt sind und in welchem Verzeichnis die statischen Dateien gespeichert sind. BROWSEDIR=0 (aus) DOCROOT darf keine schützenswerten Inhalte enthalten! Vor jeder Inbetriebnahme sollte dieses Verzeichnis auf gültige Dateien geprüft werden!
1.7.	**Ist die Kommunikation des ICM mit der J2EE Engine festgelegt und ist eine Verschlüsselung eingerichtet?** **Hinweis:** Parameter „icm/HTTP/j2ee_‹xx› " sollte geprüft werden. Mit diesem Parameter wird die Kommunikation des ICM mit der J2EE Engine festgelegt. Syntax: icm/HTTP/j2ee_‹xx› = PREFIX=‹uri-prefix›, [HOST=‹host›,] PORT=‹port›, CONN=‹Anzahl Verbindungen› [, SSLENC=‹n›, TYPE=‹t›, CRED=‹file›, SPORT=‹HTTPS-port› icm/HTTP/j2ee_0 = PREFIX=/, CONN=0-10, PORT=50000,SPORT=50003, SSLENC=1, TYPE=2,CRED=‹Credential›.pse
1.8.	**Werden Benutzer explizit verifiziert?** **Hinweis:** Parameter „icm/HTTPS/verify_client" sollte geprüft werden. Dieser Parameter spezifiziert, ob der Client ein Zertifikat vorweisen muss oder nicht. Es gibt insgesamt drei Stufen der Verifikation (0-2): 2, wenn Zertifikat erforderlich sein soll; mindestens 1, wenn keine Client Authentication verwendet werden soll.

NR.	PRÜFPROGRAMM: SICHERHEIT DES ICM
1.9.	**Sind der Service/Port und der Keepalive-Timeout spezifiziert?** **Hinweis:** Service/Port und der Keepalive-Timeout werden mit folgenden Parameter konfiguriert: Parameter „icm/server_port_‹xx›" soll gesetzt werden. Mit ‹xx›=PROT=HTTPS, PORT=‹HTTPS_Port›, TIMEOUT=900, wobei HOST=internes Interface
1.10.	**Ist HTTPS für den Zugriff auf den Web Dispatcher im Standard eingerichtet?** **Hinweis:** Der Parameter „icm/ssl_config_‹xx›" ist nur relevant für HTTPS-Konfigurationen von ICM bzw. Web Dispatcher (Kommunikation über HTTPS). Insbesondere beim Web Dispatcher spielt HTTPS eine große Rolle, da dieser in der DMZ steht und als Einstiegspunkt für Anfragen aus dem Internet dient.
1.11.	**Ist die Standardfehlermeldung konfiguriert?** **Hinweis:** Der Parameter „is/HTTP/show_detailed_errors" bestimmt die Form der HTTP-Fehlermeldungen, die der Server im Standard erzeugt und an den Client schickt. „is/HTTP/show_detailed_errors" sollte auf „FALSE" gesetzt werden.
1.12.	**Ist der Server-Headerfeld Verhalten bei HTTP-Nachrichten konfiguriert?** **Hinweis:** Der Parameter „is/HTTP/show_server_header" bestimmt, ob das Server-Headerfeld bei HTTP-Nachrichten eingefügt werden soll oder nicht. „is/HTTP/show_server_header" soll auf „FALSE" gesetzt werden.
1.13.	**Ist der Server-Port gesetzt?** **Hinweis:** Der Parameter „ms/https_port" ist obselet und sollte nicht mehr benutzt werden. Benutzen Sie stattdessen den Parameter „ms/server_port_‹xx› „mit ‹xx› als die Portnummer.
1.14.	**Ist die Kommunikation mit dem Message-Server gesichert?** **Hinweis:** Die Verbindungen zum Message-Server sollten durch HTTPS verschlüsselt werden. Folgende Parameter sollten daher eingestellt werden. › rdisp/mshost=‹message_server_host› › ms/https_port=‹message_server_HTTPS_Port› (wenn Verschlüsselung erforderlich ist) › ms/http_port=‹message_server_HTTP_Port› (wenn keine Verschlüsselung erforderlich ist)
1.15.	**Sind die ausgehenden Verbindungen gesichert?** **Hinweis:** Die ausgehenden Verbindungen sollen mittels HTTPS verschlüsselt werden. Folgende Parameter sollten eingestellt werden. wdisp/ssl_encrypt=‹0,1,2› wdisp/ssl_auth=‹0,1,2› wdisp/ssl_cred=‹File_name_of_client_PSE›
1.16.	**Sind administrative Verbindungen gesichert?** **Hinweis:** HTTPS für LDAP unter „Global server configuration/configuration/cfg/services/com.sap.security.core.ume.service.properties" und für P4 unter „Global dispatcher configuration/configuration/cfg/services/p4.properties" sollten auf „TRUE" gesetzt sein.

NR.	PRÜFPROGRAMM: SICHERHEIT DES ICM
2.	**Kontrollziel: Sichere Einstellung und Verwendung eines Webfilters** **Risiko:** Risiko- oder schwachstellenbehaftete Dienste können bei einen unautorisierten Zugriff auf Anwendungen und Daten missbraucht werden. Die Integrität und Vertraulichkeit von Daten ist nicht gewährleistet. **Hinweis:** Um nicht autorisierte Zugriffe auf kritische Funktionalitäten (z.B. SPML-Dienste) zu schützen, sollten Webfilter aktiviert werden. Alternativ kann ein externer Webfilter (z.B. Web Application Firewall) verwendet werden. Es sollten nur für Benutzer freigegebene Webseiten freigeschaltet werden. Alle von SAP intern genutzt URLs sind auf dem produktiven Interface zum Endbenutzer zu filtern. Der SAP Web Dispatcher und das ICM-Modul können als URL-Filter konfiguriert werden. Dazu können mittels einer Whitelist nur bestimmte Dienste, die auf den SAP-Systemen angeboten werden, erreichbar gemacht werden. Außerdem können Dienste, die aus dem Internet nicht erreichbar sein sollen, mittels des Parameters D blockiert werden. Mit Hilfe eines externen Webfilters (z.B. Web Application Firewall) kann diese Funktionalität erweitert bzw. ersetzt werden.
2.1.	**Sind die Pfade, welche Informationen über die Infrastruktur und Konfiguration liefern, gesetzt?** **Hinweis 1:** Verwenden Sie den Web Dispatcher als URL-Filter mit Whitelists. Folgende URLs liefern Informationen über die Infrastruktur und Konfiguration und sollen auf Parameter „wdisp\permission_table = ‹ptabfile›" gesetzt werden: D /sap/public/icman/* D /sap/public/ping D /sap/public/icf_info/* **Hinweis 2:** Den Zugriff auf die interne Infoseite sollte durch folgenden Eintrag in der URI-Permission-Tabelle gesperrt werden: D /sap/wdisp/info
2.2.	**Ist die Standardprofildatei bei SAP Netweaver 7.1 und höher (siehe Security Note 1616058) konfiguriert?** Hinweis: Der Modification-Handler wird im Standardprofil „DEFAULT.PFL" festgelegt. Folgende Parameter müssen gepflegt werden: icm/HTTP/mod_0 = PREFIX=/,FILE=$(DIR_GLOBAL)/security/data/icm_filter_rules.txt Filterregeln können entsprechend eingesehen und ausgewertet werden.
3.	**Kontrollziel: Filterung unsicherer Webservices** **Risiko:** Risiko- oder schwachstellenbehaftete Dienste können bei einen unautorisierten Zugriff auf Anwendungen und Daten missbraucht werden. Die Integrität und Vertraulichkeit von Daten ist nicht gewährleistet. **Hinweis:** Unsichere Protokolle bieten keinen ausreichenden Schutz für die Vertraulichkeit und Integrität von Daten.

NR.	PRÜFPROGRAMM: SICHERHEIT DES ICM
3.1.	Werden unverschlüsselte Dienste für den Zugriff aus potenziell unsicheren Netzwerken durch eine Firewall oder Webproxy gesperrt? **Hinweis:** Folgende Dienste werden im Betrieb des Java-Stack eingerichtet. **Dienst** — **Port Nummer** — **Standard** — **Range** HTTP — 5NN00 — 50000 — 50000–59900 HTTPS — 5NN01 — 50001 — 50001–59901 IIOP Initial context — 5NN02 — 50002 — 50002–59902 IIOP over SSL — 5NN03 — 50003 — 50003–59903 P4 — 5NN04 — 50004 — 50004–59904 P4 over HTTP tunneling — 5NN05 — 50005 — 50005–59905 P4 over SSL — 5NN06 — 50006 — 50006–59906 Internet Inter-Orb Protocol IIOP — 5NN07 — 50007 — 50007–59907 Telnet — 5NN08 — 50008 — 50008–59908 Java Message Service (JMS) — 5NN10 — 50010 — 50010–59910 Server Join Port — 5NN20 + x × 5 — 50020 — 50020–59995 Server Debug Port — 5NN21 + x × 5 — 50021 — 50021-59996 Dienste mit SSL oder HTTPS können eine Verschlüsselung sicherstellen.
3.2.	Sind unverschlüsselte Dienste nur auf die Kommunikation im lokalen Netzwerksegment eingeschränkt?

6.7. PRÜFPROGRAMM: AUTHENTISIERUNG UND AUTORISIERUNG (JAVA-STACK)

NR.	AUTHENTISIERUNG UND AUTORISIERUNG BEI NUTZUNG DES SAP JAVA-STACK
1.	**Kontrollziel: Sichere Authentisierung und Autorisierung des SAP Java-Stacks** **Risiko:** Sicherheitsparameter sind nicht oder fehlerhaft konfiguriert. Die Passwortregeln und Anmeldekontrollen sind nicht, widersprüchlich oder unzureichend gesetzt, dadurch ist eine wirksame Kontrolle von Zugriffen auf Funktionen und Dateien nicht möglich. Die protokollierten Sicherheitsereignisse aus der Anmeldung oder aus der Benutzer- und Berechtigungsverwaltung werden nicht regelmäßig überwacht.
1.1.	Gibt es ein Benutzer- und Berechtigungskonzept speziell für den SAP Java-Stack?
1.2.	**Wie ist der Benutzerpersistenzspeicher konfiguriert?** **Hinweis:** Es gibt zwei technische Möglichkeiten, um Benutzer und ihre Zugriffsrechte zu verwalten, entweder über die Nutzung des J2EE Java Authentication und Authorization Service (JAAS) oder über die darauf aufbauende SAP-spezifische User Management Engine (UME). Die UME lässt wiederum drei Optionen zu, wie die Stamm- und Anmeldedaten gespeichert werden: › in der eigenen J2EE-Datenbank › in Anbindung an ein LDAP-Verzeichnis › im SAP WEB-Anwendungsserver SAP (ABAP-Stack).

NR.	AUTHENTISIERUNG UND AUTORISIERUNG BEI NUTZUNG DES SAP JAVA-STACK
1.3.	**Wie sind die Authentisierungsmodule konfiguriert?** **Hinweis:** Es gibt drei technische Möglichkeiten, um die Anmeldung beim Zugriff auf den Java-Stack zu regeln (Authentisierungsverfahren): › Benutzernamen und Passwort-Verfahren › Zertifikate › Single-Sign-On-Tickets. Weitere Verfahren können aktiviert werden, indem z.B. Bibliotheken von Drittherstellern installiert werden, die dem Java-Standard der JAAS-Schnittstelle genügen.
1.4.	**Werden sowohl der J2EE Java Authentication und Authorization Service (JAAS) als auch die SAP-spezifische User Management Engine (UME) zur Administration von Benutzern und Berechtigungen eingesetzt?** Risiko: Benutzer- und Berechtigungsadministration erfolgt über zwei unterschiedliche Anwendungen, auch wenn UME softwaretechnisch auf JAAS aufgesetzt ist. Nicht autorisierte oder konkurrierende Einrichtung von Benutzern und deren Berechtigungen werden dadurch begünstigt.
1.5.	**Ist das Java-Stack Single-Sign-On sicher konfiguriert?** Sind der HTTPS Service Provider und das HTTPS Server Zertifikat angegeben? Ist der startup Modus auf „Always" gesetzt, sodass der HTTPS-Dienstleister aktiviert ist? **SOS:** Start of the SSL Service Provider IEX (0872) Ist für CN=localhost das default Server Certificate ersetzt? **SOS:** Default SSL Server Certificate IEX (0873) **Hinweis 1:** Wird Single-Sign-On über die Header-Variablen realisiert, muss über wirksam konfigurierte Netzwerkfilter oder eine HTTPS-Verbindung zwischen Authentifizierungs-Server und dem SAP-Portal sichergestellt werden, dass der Authentifizierungsserver nicht umgangen und eine direkte Verbindung zwischen Web Clients und SAP Enterprise Portal hergestellt werden kann. **Hinweis 2:** Wird die J2EE Engine mit Windows-Authentifizierung genutzt, muss auf das SPNegoLoginModule umgeschaltet werden.
1.6.	**Ist eine verschlüsselte Übertragung zwischen der UME im Java-Stack und dem ABAP-System eingerichtet?** **Hinweis:** Diese Kontrolle betrifft nur die Java-Installationen, die ihre Benutzerverwaltung weitestgehend im ABAP-Stack betreiben. In diesen Fällen kann eine sichere Übertragung von Passwörtern nur mittels SNC erfolgen. Hierbei müssen folgende Parameter gesetzt werden: › ume.r3.connection.‹adapterID›.snc_mode = 1 › ume.r3.connection.‹adapterID›.snc_qop = 3
2.	Kontrollziel: **Sicherheit der Standardbenutzer im Java-Stack** Risiko: Sicherheitsparameter sind nicht oder fehlerhaft konfiguriert. Die Passwortregeln und Anmeldekontrollen sind nicht, widersprüchlich oder unzureichend gesetzt, um eine wirksame Kontrolle auf die Zugriffe auszuüben. Die protokollierten Sicherheitsereignisse aus der Anmeldung oder aus der Benutzer- und Berechtigungsverwaltung werden nicht regelmäßig überwacht.

NR.	AUTHENTISIERUNG UND AUTORISIERUNG BEI NUTZUNG DES SAP JAVA-STACK
2.1.	**Sind die Standardbenutzer durch sichere Passwörter geschützt?** **Hinweis:** Folgende Tabelle stellt alle relevanten Standardbenutzer dar. **Tabelle 3: Standardbenutzer im Java-Stack** **Benutzer** / **Beschreibung** / **Zuständigkeit** ‹SID›_ADMIN (Unix) SAPService‹SID› (Windows) / Betriebssystembenutzer SAP / Betriebssystem Betrieb ‹SID›ADM / OS-Benutzer SAP / Betriebssystem Betrieb superdba / Local J2EE database user / DBA SAP‹SID›DB / DB-Benutzer J2EE (intern) / DBA Administrator / Administrator UME/LDAP / SAP Basis SDM Administrator / Administrator für den Zugriff auf das SDM / SAP Basis Visual Administrator / Visual Administrator / SAP Basis SAPJSF / Technischer Benutzer / SAP Basis J2EE_ADMIN / Schnittstellenbenutzer J2EE ‹-› ABAP / SAP Basis SLDDSUSER / Standardkommunikationsuser für den Zugriff auf das SLD / SAP Basis Die Passwörter werden während der Installation des SAP-Systems eingerichtet. Diese sollten den unternehmensweit gültigen Anforderungen an ein sicheres Administratorenpasswort genügen.
2.2.	Sind Regelungen zum Umgang mit den Passwörtern im Berechtigungskonzept hinterlegt? Sind angemessene Kontrollen, z.B. 4-Augen-Prinzip, berücksichtigt worden?
	User Management Engine (UME) Anmeldekontrollen
3.	**Kontrollziel: Die Bildung der Benutzerkennung und des Kennworts unterliegt Komplexitätsregeln.** **Risiko:** › Systemtechnische Benutzerkennungen oder die der Administratoren sind aufgrund der Funktion, für die sie eingerichtet werden, leicht zu erraten, sodass Kennwortattacken gezielt auf die erratenen Benutzerkennungen vorgenommen werden können. › Das Kennwort ist einfach und kann mit wenigen Anmeldeversuchen erraten werden. › Der Benutzer verwendet wiederholt dasselbe Kennwort. Er überlistet den systemseitig erzwungenen Wechsel des Kennworts, wenn keine oder eine zu kurze Passworthistorie gewählt ist.
3.1.	**Sind Passwortregeln für Benutzerkennungen der UME-Benutzer im Java-Stack konfiguriert?** **Hinweis:** In Tabelle 2 sind die für die UME-Benutzer relevanten Passwortrichtlinien zusammengefasst. Bewerten Sie die aktuellen Einstellungen anhand der Vorschlagswerte bzw. der unternehmensweiten Richtlinien.
3.2.	**Sind Passwortregeln für Benutzerkennungen der ABAP-Benutzer im AS ABAP konfiguriert?** **Hinweis:** Benutzer in AS Java können im AS ABAP führend verwaltet werden. In diesen Fällen stellt der AS ABAP die Richtlinien für die Verwaltung der Passwörter fest.

NR.	AUTHENTISIERUNG UND AUTORISIERUNG BEI NUTZUNG DES SAP-JAVA-STACK
6.	**Kontrollziel: Zugriff auf die J2EE-Tokens absichern** Risiko: J2EE-Token werden in der Web-Kommunikation meist in sogenannte Cookies gespeichert. Es ist sicherzustellen, dass Cookies verschlüsselt übertragen werden und Sicherheitsmerkmale im Browser gesetzt sind (z.B. das „secure" Flag), um unautorisierte Zugriffe durch Angreifer zu verhindern.
6.1.	**Sind die Sessions IP-beschränkt?** **Hinweis:** „SessionIPProtectionEnabled" sollte „TRUE" eingestellt sein (unter „Global server configuration/configuration/cfg/services/servlet_jsp.properties"), damit die IP-Beschränkung von Session IDs eingestellt ist.
6.2.	**Sind die J2EE-Token geschützt?** **Hinweis 1:** „SystemCookiesDataProtection" sollte auf „TRUE" eingestellt sein, damit die Tokens in den Cookies vor Cross-Site-Scripting geschützt werden. **Hinweis 2:** Der Parameter „ume.logon.httponlycookie" bewirkt, dass das „httpOnly" Flag für SAP Logon Tickets gesetzt wird. Dadurch kann das Cookie nicht mehr durch JavaScript ausgelesen werden, wodurch Cross-Site-Scripting Angriffe erschwert werden.
6.3.	**Ist die Übertragung von Session-Cookies gesichert?** **Hinweis 1:** „SystemCookiesHTTPSProtection" sollte „TRUE" eingestellt sein (unter „Global server configuration/configuration/cfg/services/http.properties"), damit die Übertragung der Cookies verschlüsselt ist. **Hinweis 2:** Der Parameter „ume.logon.security.enforce_secure_cookie" bewirkt, dass das „secure" Flag für SAP Logon Tickets gesetzt wird. Dadurch wird dieses Cookie nur noch über verschlüsselte Verbindungen versendet.

NR.	AUTHENTISIERUNG UND AUTORISIERUNG BEI NUTZUNG DES SAP-JAVA-STACK
	User Management Engine (UME) Benutzer- und Berechtigungsverwaltung
7.	**Kontrollziel: Rollen- und aufgabenspefische Vergabe von Administrationsberechtigungen** **Risiko:** Derselben Administratorkennung sind unterschiedliche Rollen der Benutzer- und Berechtigungsverwaltung zugewiesen. Der Grundsatz der Funktionstrennung ist nicht eingehalten. Administrationsberechtigungen sind auch an nicht autorisierte Benutzer vergeben, wodurch die Anforderungen gemäß IKS unterlaufen werden. **Hinweis:** Die Vergabe von Rollen und Berechtigungen sollte die IKS-Anforderungen sowie die jeweils gültigen regulatorischen Anforderungen des untersuchten Systems erfüllen.

	Super Administrators	Administrators		Business Users
		All	Company-Specific	Profile-Specific
User	Manage_All Read_All	Manage_All_Companies Manage_All_User_ Passwords	Manage_Users Manage_User_Pass- words	Manage_My_Profile Read_My_Profile Manage_My_Password
Groups		Manage_Groups		
UME Roles		Manage_Roles		
Specific Functions		Import and Export Batch_Admin		Self-Registration Selfregister_User
Portal-Specific	Manage_All AclSuperUser		Manage_Role_ Assignments	

UME Actions According to Principal and Role

Abbildung 3: Standard-UME-Rollen

Der Umgang mit privilegierten Benutzern, insbesondere dem Notfallbenutzer, muss im SAP-Berechtigungskonzept geregelt werden.

7.1.	**Welche Benutzer sind der Rolle „Administrators" zugeordnet (Benutzergruppe im UME-Benutzerspeicher)?** **Hinweis:** Der UME Web Admin und der Visual Admin, haben die „Administrators"- Rolle zugeordnet. Sie können alle Benutzerdaten uneingeschränkt pflegen. Nur Benutzer- und Berechtigungsadministratoren dürfen in der UME-Benutzergruppe „Administrators" sein. Sofern möglich, sollten diese Benutzer nur im Rahmen des Notfallbenutzerkonzepts verwendet werden. **SOS:** Users of UME User Group „Administrators" IEX (0793)

NR.	AUTHENTISIERUNG UND AUTORISIERUNG BEI NUTZUNG DES SAP-JAVA-STACK
7.2.	**Welche der folgenden Administrationsberechtigungen sind an welche Benutzer vergeben?** **Hinweis:** *1 UME.Manage_User_Passwords* *2 UME.Manage_All* *3 UME.Manage_Users* *4 UME.Manage_All_Companies* *5 UME.Manage_Groups* *6 UME.Manage_Roles* *7 UME.Batch_Admin.* Diese Administrationsberechtigungen sind restriktiv nur an die zuständigen Sachbearbeiter zu vergeben. Im Rahmen des IKS sollten angemessene Funktionstrennungen beachtet werden.
7.3.	**Wird das Protokoll über Sicherheitsereignisse (Security Logging) regelmäßig überwacht?** **Hinweis:** Protokolldatei über den Log Viewer: ./log/system/security.log Protokolldatei im Dateisystem: /usr /sap /‹SID› /‹instance_number› /j2ee /cluster / server‹X› /log /system /security.log Diese Protokolldatei enthält die Aufzeichnung relevanter Sicherheitsereignisse wie erfolglose Anmeldungen oder das Anlegen oder Ändern von Benutzern, Gruppen oder Rollen. **Im Einzelnen:** *user.create* und *useraccount.create* — Benutzer neu angelegt *role.create* — Anlegen von Rollen *role.modify* — Ändern von Rollen *islocked* — Benutzer gesperrt/entsperrt *login.error* — Fehlgeschlagene Anmelde-versuche *(IP-Adresse* wird mit geloggt.)
7.4.	**Sind die Berechtigungen des Kommunikationsbenutzers zwischen der UME und den angebundenen SAP-Systemen angemessen vergeben?** **Hinweis:** Standardmäßig wird der Benutzer SAPJSF verwendet. SAP liefert die Rollen *SAP_BC_JSF_COMMUNICATION* (Schreibrechte auf Benutzerkonten) und *SAP_BC_JSF_COMMUNICATION_RO* (Lesezugriff auf Benutzerkonten) aus. Der Kommunikationsbenutzer muss vom Typ System und darf nicht vom Typ Service oder Dialog sein, da keine Online-Anmeldung erlaubt ist.

NR.	AUTHENTISIERUNG UND AUTORISIERUNG BEI NUTZUNG DES SAP-JAVA-STACK
7.5.	**Wird der Java-Benutzer SAP* als Notfallbenutzer eingesetzt?** **Hinweis:** Der Benutzer SAP* in Java-Systemen ist nicht zu verwechseln mit dem in ‚klassischen' SAP-Systemen. Er verfügt über volle Administrationsberechtigungen und wird in der UME als Notfallbenutzer eingesetzt. Er verfügt über kein Standard-Kennwort. Dieses wird über eine UME-Eigenschaft gesetzt. Durch Aktivierung des Benutzers SAP* als Notfallbenutzer werden nach dem Neustart des Java-Anwendungsservers alle anderen Benutzer deaktiviert. ume.superadmin.activated — aktiviert bzw. deaktiviert den Benutzer als Notfallbenutzer TRUE/FALSE) ume.superadmin.password — enthält das Kennwort des Notfallbenutzers Diese Einstellung darf nur in einem tatsächlichen Notfall gesetzt werden.
7.6.	**An welche Benutzer ist die Sicherheitsrolle „telnet_login" vergeben?** **Hinweis:** Sie darf nur an die Administratoren der J2EE Engine vergeben sein. **SOS:** J2EE Server Remote Administration with Telnet IEX (0775)

6.8. TABELLE: VORSCHLAGSWERTE FÜR DIE SYSTEMPARAMETER DER UME-ANMELDEKONTROLLE

PARAMETER	BESCHREIBUNG	VORSCHLAGS-WERT
ume.logon.security_policy.auto_unlock_time	Zeitspanne in Minuten, die das System gesperrt wird, für den Fall mehrfacher fehlerhafter Loginversuche.	0
ume.logon.security_policy.enforce_policy_at_logon	Das Passwort wird während des Anmeldens gegen die Sicherheitsrichtlinie überprüft. Sollte es nicht mehr ausreichend sein, wird der Benutzer aufgefordert, ein neues Passwort zu setzen.	TRUE
ume.logon.security_policy.lock_after_invalid_attempts	Anzahl fehlerhafter Loginversuche, bevor der Nutzer gesperrt wird.	5
ume.logon.security_policy.oldpass_in_newpass_allowed	Definiert, ob das neue Passwort Teile des alten Passworts enthalten darf. Dafür überprüft UME die Passwörter während des Änderns.	FALSE
ume.logon.security_policy.password_alpha_numeric_required	Minimale Anzahl an Buchstaben und Zahlen in einem Passwort. Ist diese Zahl z.B. auf 3 gesetzt, muss das Passwort mindestens drei Buchstaben und drei Zahlen enthalten.	1
ume.logon.security_policy.password_change_allowed	Definiert, ob Benutzer-Passwörter geändert werden können.	TRUE
ume.logon.security_policy.password_expire_days	Zeitspanne in Tagen, die ein Passwort gültig ist.	35
ume.logon.security_policy.password_history	Die UME kann die Hash-Werte alter Passwörter speichern. Dieses verhindert, das Benutzer alte Passwörter wiederverwenden. Der Wert legt fest, wie viele alte Passwörter gespeichert werden.	10
ume.logon.security_policy.password_impermissible	Eine durch Kommata getrennte Liste, welche Ausdrücke und Zeichen enthalten, welche nicht Teil eines Passworts sein dürfen.	Gemäß den Einträgen aus der USR40 anzupassen.
ume.logon.security_policy.password_last_change_date_default	Wenn ein Benutzer niemals sein Passwort mithilfe der AS Java verändert hat, zählt dieses Datum als Datum der letzten Änderung. Das Format ist MM/DD/YYYY Siehe auch: ume.logon.security_policy.password_expire_days	

PARAMETER	BESCHREIBUNG	VORSCHLAGS-WERT
ume.logon.security_policy.password_max_idle_time	Zeitspanne in Tagen nach dem letzten erfolgreichen Login mit Benutzer-ID und Passwort, bevor UME das Passwort sperrt.	35
ume.logon.security_policy.password_max_length	Maximale Passwortlänge	
ume.logon.security_policy.password_min_length	Minimale Passwortlänge	8
ume.logon.security_policy.password_mix_case_required	Minimale Anzahl an Groß- und Kleinbuchstaben in einem Passwort. Ist diese Zahl auf 3 gesetzt, muss das Passwort mindestens drei große und drei kleine Buchstaben enthalten.	1
ume.logon.security_policy.password_special_char_required	Minimale Anzahl an Sonderzeichen in einem Passwort.	1
ume.r3.connection.‹adapterID›.snc_mode	Wenn die UME mit dem ABAP-System kommuniziert, sollte SNC zur Verschlüsselung der Zugangsdaten aktiviert werden.	1
ume.r3.connection.‹adapterID›.snc_qop	Wenn die UME mit dem ABAP-System kommuniziert, sollte SNC zur Verschlüsselung der Zugangsdaten aktiviert werden.	3
ume.superadmin.activated	Aktivierung bzw. Deaktivierung des UME Notfallusers SAP*.	FALSE
ume.superadmin.password	Festlegung des Kennworts für den Notfalluser SAP*	Im 4-Augen-Prinzip bzw. nur im Rahmen des Notfalluserkonzepts anzuwenden.
ume.logon.security_policy.userid_digits	Minimale Anzahl an Zahlen in einer Benutzer-Login-ID Value ‹ 0: Zahlen sind nicht erlaubt. Value = 0: Zahlen sind erlaubt. Value › 0: Zahlen sind erforderlich.	1
ume.logon.security_policy.userid_in_password_allowed	Definiert, ob das Passwort Teile der Benutzer, ID enthalten darf.	FALSE

PARAMETER	BESCHREIBUNG	VORSCHLAGS-WERT
ume.logon.security_policy.userid_special_char_required	Minimale Anzahl an Sonderzeichen in einer Benutzer-Login-ID Value ‹ 0: Sonderzeichen sind verboten. Value = 0: Sonderzeichen sind erlaubt. Value › 0: Sonderzeichen sind erforderlich	0
ume.logon.security_policy.useridmaxlength	Maximale Länge der Benutzer-ID: Dieser Wert wird automatisch auf 12 gesetzt, wenn die Kombination AS Java und AS für ABAP installiert ist. Wenn eine Datenbank als Quelle für Benutzer-daten verwendet wird, muss dieser Wert kleiner bzw. gleich 200 sein.	Default
ume.logon.security_policy.useridminlength	Minimale Länge der Benutzer-ID.	4
login/ min_password_lng	Minimale Passwortlänge	6
login/ password_charset	Das Passwort muss mindestens einen Buchstaben, eine Zahl und ein Sonderzeichen enthalten.	1
login/ min_password_letters,	Anzahl von Buchstaben in einem Passwort	0
login / min_password_digits und login	Anzahl von Zahlen in einem Passwort	0
min_password_specials, login	Anzahl von Sonderzeichen in einem Passwort	0
min_password_lowercase und login	Anzahl Kleinbuchstaben in einem Passwort	0
min_password_uppercase	Anzahl Großbuchstaben in einem Passwort	0
login/ min_password_diff	In wie vielen Zeichen muss sich ein neues von einem alten Passwort unterscheiden	3
login/ password_history_size	Die Hash-Werte alter Passwörter können gespeichert werden. Dieses verhindert, dass Benutzer alte Passwörter wiederverwendet. Der Wert legt fest, wie viele alte Passwörter gespeichert werden.	15
Tabelle USR40	Liste mit unzulässigen Passwörtern	

PARAMETER	BESCHREIBUNG	VORSCHLAGS-WERT
login/ password_max_ idle_initial.	Zeitspanne in Tagen, nach denen das Initial-passwort geändert werden muss. **Hinweis:** Dieser Systemparameter ersetzt die Profilparameter login/ password_max_new_valid und login/ password_max_reset_valid aus dem SAP Web Anwendungsserver 6.20 und 6.40. **SOS:** Users with Initial Passwords Who Have Never Logged On (0009)	3
login/ password_ expiration_ time	Zeitspanne in Tagen, nach dem ein Passwort geändert werden muss.	90
login/ password_max_ idle_ productive	Gültigkeitszeitspanne in Tagen, nach denen ein nicht benutztes Passwort gesperrt wird. Dieser Parameter bezieht sich nicht auf die Benutzer vom Typ Service oder System.	Gültigkeits-dauer eines nicht benutzten Kennworts höher setzen als die Dauer für den erzwungenen Wechsel des Kennworts (max. 90 Tage).
login/ password_change_waittime.	Der Benutzer muss sein Kennwort jederzeit ändern können.	Standard: einmal am Tag
login/ fails_to_session_ end	Anzahl Login-Fehlversuche bis zum Abbruch des Vorgangs.	3
login/ fails_to_user_lock	Anzahl Login-Fehlversuche bis zum Sperren des Benutzers.	5
login/ failed_user_auto_ unlock	Automatische Freischaltung der durch Login-Fehlversuche gesperrten Benutzer.	1(= Freischaltung über Nacht)
login/ disable_multi_ gui_login	Ist die gleichzeitige Anmeldung von verschiedenen Systeme durch einen Benuter möglich.	1 (= mehrfache Anmeldung ist nicht möglich)
rdisp/gui_auto_logout	Zeitspanne in Sekunden bei keiner Benutzer-aktion bis zum automatischen Abmelden des Benutzers. Bei o erfolgt kein automatischer Logout.	0
login/ password_compliance_ to_current_policy	Wenn ein bereits vergebenes Kennwort nicht mehr den inzwischen geänderten Kennwort-bildungsregeln entspricht, erzwingt das System eine Änderung des Kennworts bei der Anmeldung.	0

6.9. PRÜFPROGRAMM: SAP-JAVA-STACK-SOFTWAREVERTEILUNG

NR.	SICHERE ANWENDUNG DER SAP–JAVA-STACK-SOFTWAREVERTEILUNG
1.	**Kontrollziel: Sichere Konfiguration der SAP-Java-Stack-Softwareverteilung** **Risiko:** Entwickler importieren ohne Auftrag geänderte Software selbst in das Produktivsystem. Test- und Freigabeschritte sind nicht vorgegeben oder werden umgangen. Nicht autorisierte Änderungen an den Einstellungen des Change Management Service (CMS) und an den Transportdaten selbst sind möglich. Schwächen im SDM-Service können ausgenutzt werden, um kritische Funktionsbausteine unter Umgehung der systemseitigen Schutzmechanismen aufzurufen.
1.1.	Gibt es ein Konzept für die SAP-Softwareverteilung, das auf die SAP-Java-Stack-Umgebung zugeschnitten ist?
1.2.	Sind die getrennten Zuständigkeiten in den Phasen der Entwicklung, des Testens und der Abnahme geregelt?
1.3.	**Wer darf Softwareverteilungen direkt aus einer Entwicklungsumgebung in ein Produktivsystem vornehmen?** **Risiko:** Software kann aus der Entwicklungsumgebung unmittelbar in den Java-Stack geladen werden.
1.4.	**Wie ist der Software Deployment Manager SDM-Dienst (Software Deployment Manager) Dienst konfiguriert?** › Ist das Standardkennwort des SDM-Administrators bei der Installation geändert worden? › Ist das neue Kennwort nach restriktiven Passwortregeln vergeben worden? › Wie vielen Benutzern ist das neue Kennwort zur Erfüllung ihrer Aufgaben mitgeteilt worden? › Wird der Dienst nur während des Deployments aktiviert? › Wird das Passwort in Start- und Stop-Skripten gespeichert? **Risiko:** Die Rolle der SDM-Administration kann nicht vergeben werden. Nur der SDM-Administrator selbst kann verwendet werden. Ein Zurückverfolgen, wer diesen Benutzer für welche Aktivität genutzt hat, ist erschwert, wenn nicht unmöglich. Nach einem Patch-Upgrade wird systemseitig keine Änderung des Kennworts des SDM-Administrators erzwungen.
1.5. H	**Ist die Netzwerkverbindung zwischen SDM-Client und SDM-Server für Produktivsysteme gesichert?** **Hinweis:** SAP empfiehlt, für die Softwareverteilung auf produktive Zielsysteme eine gesicherte VPN-Verbindung oder einen IP-Filter einzurichten und zu nutzen. Beachten Sie hierzu die SAP Note 1616058.

6.10. SAP ENTERPRISE PORTAL

Das SAP Enterprise Portal stellt Java-Anwendungen gemäß der J2EE bzw. Java EE als Standard-Java-Container zur Verfügung. Hierfür werden sogenannte fertige Build-Pakete durch die Entwicklung erstellt und auf die produktiven Web- und EJB-Container übertragen. Die Inbetriebnahme von Java-Builds wird auch als Deployment bezeichnet.

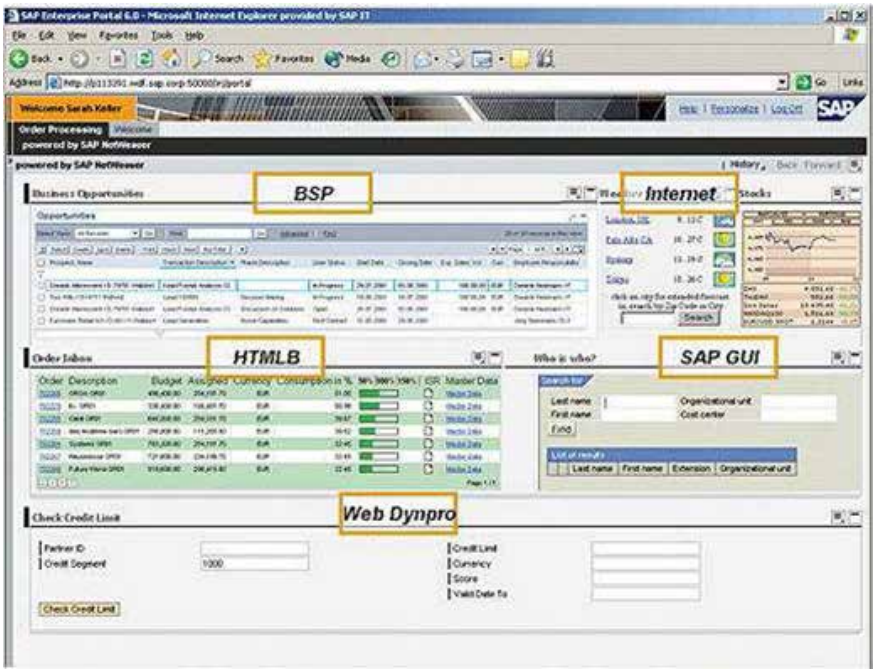


Abbildung 4: Mögliche Komponenten einer Portalanwendung

Jedes Build verfügt über eine Konfigurationsdatei, die vom Java-Container gelesen und für den Betrieb des Java-Programms genutzt wird. In SAP-Portalanwendungen können Inhalte aus diversen SAP-Quellen integriert werden. Selbst aus dem ABAP stammende Webkomponenten (z.B. SAP GUI oder Web Dynpro) können über das Enterprise Portal beliebig zusammengefasst und dargestellt werden (siehe Abbildung 4). Die hier eingesetzten Komponenten basieren auf Web-Technologien, die im produktiven Einsatz eine ausreichende Systemhärtung sicherstellen müssen. Schwachstellen in der Konfiguration können die Sicherheit der Anwendung erheblich beeinträchtigen und alle betriebenen Anwendungen gefährden. Die in diesem Abschnitt beschriebenen Maßnahmen sind zwingend umzusetzen, um eine Grundlage für einen sicheren Betrieb und die Wirksamkeit eines IKS-Systems für Java-Anwendungen zu schaffen.

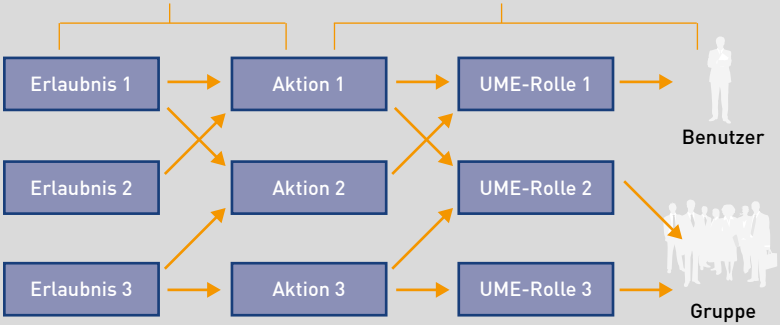
6.11. PRÜFPROGRAMM: SAP-JAVA-STACK-SOFTWAREVERTEILUNG

NR.	SICHERE ANWENDUNG DES SAP ENTERPRISE PORTALS
1.	**Kontrollziel: Deaktivierung des Invoker Servlets** **Risiko:** Geschützte Portalanwendungen und Java-Klassen können ohne Authentifizierung aufgerufen werden. Unbefugte Dritte können den administrativen Zugang zum System erlangen und eingerichtete Schutzmechanismen umgehen.
1.1. H	**Ist das Invoker Servlet global deaktiviert?** **Risiko:** Sollte der genannte Parameter auf TRUE stehen oder nicht vorhanden sein, besteht ein erhebliches Sicherheitsrisiko. Über schwachstellenbehaftetete Systemschnittstellen, z.B. die CTC-Komponente, kann bspw. ohne Anmeldung auf Systemressourcen zugegriffen werden. Die Vertraulichkeit und Integrität von Daten kann nicht wirksam gewährleistet werden. **Hinweis 1:** Das Invoker Servlet sollte deaktiviert und kritische Java-Klassen vor unautorisierten Zugriffen geschützt werden. Ein globales Abschalten des „Invoker Servlet" kann durch ein „False" im Parameter „EnableInvokerServletGlobally" in der „Global server configuration/configuration/cfg/services/servlet_jsp.properties" erreicht werden. **Hinweis 2:** Die SAP Notes 1467771 und 1445998 beschreiben die versionsabhängigen Voraussetzungen.
1.2. H	**Ist der Klassenaufruf eines Servlets deaktiviert?** **Hinweis:** Deaktivieren Sie den Aufruf eines Servlets durch Klassen-Namen unter Global server configuration/configuration/persistent/servlet_jsp/global-web.xml.
2.	**Kontrollziel: Absicherung des Portal-Tokens** **Risiko:** Portal-Token können durch Angreifer über potenzielle Cross-Site-Scripting oder Cross-Site-Request-Forgery-Sicherheitslücken kompromittiert werden. Hierdurch erhalten Angreifer den unautorisierten Zugang zum System. **Hinweis:** Analog zum J2EE-Token muss auch das Portal-Token angemessen vor potenziellen Webrisiken geschützt werden. Beide Token bilden die zentralen Authentifizierungsmerkmale des Benutzers während einer Sitzung für das J2EE und das Enterprise Portal.
2.1.	**Ist eine maximale Gültigkeit des Tokens bei Inaktivität gesetzt?** **Hinweis:** Lebensdauer des „Logon Tickets" kann unter „Global server configuration/configuration/cfg/services/com.sap.security.core.ume.service.properties" ausgewertet werden. Beachten Sie, dass anwendungsbezogene Tokens eine eigene Laufzeit besitzen können.
2.2.	**Ist der Zugriff auf das Cookie mittels Javascript gesperrt?** **Hinweis:** Bewirkt, dass das „httpOnly" Flag für SAP Logon Tickets gesetzt wird. Dadurch kann das Cookie nicht mehr durch JavaScript ausgelesen werden, wodurch Cross-Site-Scripting Angriffe erschwert werden.
2.3.	**Werden Cookies ausschließlich über HTTPS übertragen?** **Hinweis:** Bewirkt, dass das „secure" Flag für SAP Logon Tickets gesetzt wird. Dadurch wird dieses Cookie nur noch über verschlüsselte Verbindungen versendet. Gängige Browser speichern das Cookie nur im Arbeitsspeicher und erzeugen keine lokale Kopie im Cache.

NR.	SICHERE ANWENDUNG DES SAP ENTERPRISE PORTALS
3.	**Kontrollziel: Härtung der Portalanwendungen** **Risiko:** Das Enterprise Portal stellt umfangreiche Einstellungsmöglichkeiten zur Verfügung, die bei einer nicht sachgerechten Konfiguration Schutzmechanismen deaktivieren können. Angreifern können somit Zugriffe auf vertrauliche Daten ohne Zugangsdaten ermöglicht werden. **Hinweis:** Webanwendungen verfügen im J2EE über eine eigene Konfiguration, die im Zusammenwirken mit globalen Systemeinstellungen funktioniert. Daher müssen die lokalen Konfigurationsdateien ausreichend sicher implementiert werden, um eine ausreichende Betriebssicherheit zu gewährleisten.
3.1. H	**Ist der Schutz vor Cross-Site Request Forgery aktiviert?** **Hinweis:** Schutz vor Cross-Site Request Forgery (Parameter „xsrf.protection.enabled") unter „Global server configuration/configuration/cfg/services/servlet_jsp.properties" aktivieren.
3.2.	**Ist die Nutzung von ActiveX im Enterprise Portal unterbunden?** **Hinweis:** ActiveX kann über die Parametrisierung „a-ra:/applications/com.sap.portal.ui.uiservice/services/ui" deaktiviert werden. Sofern möglich, sollte auf ActiveX generell verzichtet werden.
3.3. H	**Ist das Directory Listing deaktiviert?** **Hinweis:** Directory Listing sollte grundsätzlich deaktiviert werden. Die Einstellungen können je nach Version wie folgt ausgewertet werden: SAP J2EE engine 6.20: DirList=false in server/services/http/properties and server/services/servlet_jsp/properties SAP J2EE Engine 6.40: Visual Administrator -› ServerID -› Services -› Http Provider. On the tab Runtime -› Virtual Hosts -› General (which is shown by default) there's a check box 'Directory List'
3.4. H	**Sind alle selbst entwickelten Anwendungen mit einer ausreichenden Security Zone ausgestattet?** **Risiko:** Verfügen Anwendungen über die Security Zone „No Safety", lassen sie sich direkt über die URL aufrufen, z.B. über „/irj/servlet/prt/portal/prtroot/‹iView_ID›". Je nach Applikation kann unter Umständen auf vertrauliche Daten zugegriffen werden. **Hinweis:** Bewerten Sie Applikationen mit der Security Zone „No Safety" im Hinblick auf den Schutzbedarf.

NR.	SICHERE ANWENDUNG DES SAP ENTERPRISE PORTALS
3.5.	**Werden interne Fehler durch eine eigene Fehlerseite unterdrückt?** Risiko: Fehlertexte liefern Angreifern wertvolle Informationen über zentrale Komponenten und Daten. Diese können wertvolle Information für weiterführende Angriffswege liefern. Datenbankfehler können Daten direkt in Fehlerseiten ausgeben und die Vertraulichkeit der Daten gefährden. **Hinweis:** Interne Fehler sollten abgefangen und nicht in den Content der Webseite weitergegeben werden. In der WEB.XML lässt sich über den Parameter „‹error-page›" das Verhalten bei internen Fehlern konfigurieren. Beispielsweise leitet der folgende Auszug die Fehlernummer 500 auf eine eigene Fehlerseite um: ‹error-page› ‹error-code›500‹/error-code› ‹location›/path/to/error.jsp‹/location› ‹/error-page› ‹error-page› ‹exception-type›java.lang.Throwable‹/exception-type› ‹location›/path/to/error.jsp‹/location› ‹/error-page›
3.6. H	**Wenn alle HTTP-Methoden, die nicht benötigt werden, deaktiviert werden, wie unterbindet man dann kritische Handlungen im System?** Risiko 1: Wenn die Methode HEAD erlaubt ist, kann mittels HTTP Verb Tampering eine Schwachstelle ausgenutzt werden, um zugriffsgeschützte Funktionen im Portal ohne Anmeldung auszuführen. Dies kann u.a. zum Anlegen von Benutzern oder zur Erweiterung von Berechtigungen ausgenutzt werden. Risiko 2: Die Methode TRACE kann potenzielle Cross-Site-Scripting-Angriffe begünstigen. **Hinweis 1:** Alle HTTP-Methoden, die nicht benötigt werden, sollten in der WEB.XML explizit deaktiviert werden (löschen aller ‹http-method› Einträge). Zugriff auf kritische Anwendungen sollte nur mit gültiger Authentifizierung möglich sein (‹security-constraint›). **Hinweis 2:** SAP Notes 1503579,1616259,1589525 und 1624450 sollten implementiert sein.
3.7. H	**Wurde die WEB.XML von allen lokalen Invoker Servlet Aktivierungen bereinigt?** **Hinweis:** Alle „‹param›InvokerServletLocallyEnabled‹/param›" müssen aus der WEB.XML gelöscht werden, um ein lokales Aktivieren des Invoker Servlets zu verhindern.
3.8.	**Laufen Sitzungen bei Inaktivität ab?** **Hinweis:** Sitzungen sollten über den „‹session-timeout›"-Parameter in der WEB.XML gemäß den Sicherheitsvorgaben für inaktive Sitzungen eingestellt sein.
3.9.	**Wird die Übertragung von Session-IDs in der URL verhindert?** Risiko: Die Anzeige der Token oder Session-IDs in der URL kann in diversen Caches oder Proxy- und Browser-Historien aufgezeichnet werden. Fremde können auf diese gespeicherten Einträge u.U. zugreifen und die Sitzung eines aktiven Benutzers übernehmen. **Hinweis:** Der Parameter „‹tracking-mode›" sollte auf „COOKIE" gesetzt werden, um die Session-ID als Cookie und nicht innerhalb der URL zu übergeben.

NR.	SICHERE ANWENDUNG DES SAP ENTERPRISE PORTALS
3.10.	**Erfordert die Nutzung der Anwendung HTTPS?** **Hinweis:** Der Parameter „‹transport-guarantee›" sollte auf „CONFIDENTIAL" gestellt sein, um HTTPS zu nutzen.
3.11. H	**Ist der Schutz vor Cross-Site-Scripting-Attacken (XSS) via EPCF eingerichtet?** **Hinweis:** Beachten Sie die SAP Note 1656549.
3.12. H	**Ist der Schutz vor XML-External-Entity-Attacken (XXE) eingerichtet?** **Hinweis:** Beachten Sie die SAP Note 1619539.
3.13. H	**Wurden die Filter im Knowledge Management aktiviert, um das Hochladen bösartiger Dateien zu verhindern?** **Hinweis:** › Prüfen Sie die Dateierweiterungen in „File Extension" und Dateigrößen Filter unter „System Administration > System Configuration > Content Management > Repository > Filters > Show Advanced Options > File Extension and Size Filter" › Prüfen Sie die Filter in „Malicious Script Filter" unter „System Administration > System Configuration > Content Management Repository > Filters > Show Advanced Options > Malicious Script Filter" › Ist der Parameter „Forbidden Scripts" aktiviert? › Ist die Option „Send E-Mail to Administrator" aktiviert?
3.14. H	**Wurde die Validierung der Pfade im Knowledge Management System installiert?** **Risiko:** Wenn nicht erlaubte Pfade akzeptiert werden, können Phishing-Angriffe begünstigt werden. **Hinweis:** Beachten Sie die SAP Note 1630293.

NR.	SICHERE ANWENDUNG DES SAP ENTERPRISE PORTALS
4.	**Kontrollziel: Berechtigungsmanagement im Enterprise Portal** **Risiko:** Wenn Aktionen falsch zugewiesen werden, erhalten Portalbenutzer unautorisierten Zugriff auf geschützte Anwendungen und Daten. Die Wirksamkeit des IKS und Berechtigungskonzepts wird somit unterlaufen. **Hinweis:** UME setzt auf einen programmatischen Berechtigungskonzeptansatz, indem der Entwickler Anwendungsrechte (Permissions) in der Anwendung definiert und diese in der Datei actions.xml zu Aktionen bündelt. Jede Aktion wird gegen eine Rolle im UME gemappt. Vor diesem Hintergrund muss jede einzelne Aktion im Portal dahingehend untersucht werden, ob die in der UME eingerichtete Rolle sachgerecht zugewiesen wurde. User aus dem ABAP-System sind als solche in der UME sichtbar und können sich am AS Java authentifizieren. **Zuordnung** › durch Entwickler › in der Datei actions.xml **Zuordnung in der UME-Konsole**  *Abbildung 5: Abhängigkeit Portal- und UME-Rollen* Die ABAP-Rollen erscheinen in der UME als UME-Gruppen. Im ABAP-System erhält der Nutzer seine Berechtigungen aus dem zur Rolle gehörenden Profil. Seine Java-Berechtigungen bekommt er aus der UME-Rolle, die der UME-Gruppe zugeordnet wird.
4.1.	Existiert ein Regelprozess für die Prüfung der „actions.xml" bei der Einführung oder Änderung von Portalanwendungen?
4.2.	Sind die eingerichteten Rollen und Zuweisungen in einem Berechtigungskonzept definiert?

NR.	SICHERE ANWENDUNG DES SAP ENTERPRISE PORTALS
4.3.	**Sind administrative Rollen (siehe) in selbstentwickelten Portalanwendungen gemappt?** **Hinweis:** Standardrollen sollten nicht in Eigenentwicklungen verwendet werden. Wenn einzelne administrative Funktionsbausteine benötigt werden, sollten angepasste Rollen erzeugt und ausgerollt werden.
5.	Kontrollziel: **Deaktivieren von nicht benötigten Diensten** Risiko: Aktivierte Funktionsbausteine können bei der Veröffentlichung von Schwachstellen die Systemsicherheit erheblich gefährden und wirksame Zugriffsschutzmechanismen umgehen. **Hinweis:** In der Auslieferung und Standardinstallation werden einige hundert Java-Funktionsaufrufe installiert. Ein Großteil der Funkionen wird nicht genutzt und muss explizit durch die Administratoren im VisualAdmin Tool deaktiviert werden. Dieses Verfahren entspricht dem Vorgehen gemäß SICF-Transaktion im ABAP-Stack.
5.1.	Existiert ein Standardprozess zum Deaktivieren von Standard-Diensten beim Einrichten neuer SAP-Instanzen?
5.2.	**Entsprechen die aktivierten Dienste den Anforderungen der fachlich benötigten Services?** **Hinweis:** Im VisualAdmin kann eine Liste von aktivierten Diensten erzeugt und geprüft werden.

7. SYSTEMINTEGRITÄT AUF DER DATENBANKEBENE

7.1. INTERNE UND EXTERNE ANFORDERUNGEN

Die Daten eines SAP-Systems werden in einer proprietären Datenbank gehalten, z.B. Oracle. Auf alle Daten eines SAP-Systems kann über das Datenbanksystem zugegriffen werden. Dabei können auch Daten geändert werden – unabhängig vom Zugriffsschutz, der über die SAP-Anwendungen realisiert ist.

Die Datenbank ist ein eigenes System, das implementiert, konfiguriert, betrieben, verwaltet und überwacht werden muss. Dabei sind die allgemeinen Sicherheitsanforderungen zur Gewährleistung von Verfügbarkeit, Zugriffsschutz, Integrität und Vertraulichkeit umzusetzen.

Spezielle Sicherheitsanforderungen ergeben sich zum einen aus dem SAP-spezifischen Einsatz der Datenbank, zum anderen aus der proprietären Ausprägung der Funktionen der Datenbank.

Deshalb sind sowohl die Hinweise von SAP zu den Datenbank-Plattformen im SAP NetWeaver Security Guide zu berücksichtigen als auch die Security White Paper des Herstellers der Datenbank.

Prüfungsstandards zum Einsatz von Informationstechnologie fordern insbesondere die Prüfung der Datenbank eines ERP-Systems.

7.2. RISIKEN

Risiken können sich zum einen daraus ergeben, dass die Sicherheitsempfehlungen von SAP nicht umgesetzt sind, zum anderen, dass die Datenbank konkurrierend zur Nutzung durch SAP genutzt wird:

- Die SAP-Systembenutzer, der Datenbank-Systembenutzer oder zusätzlich eingerichtete Administratoren nutzen noch das Initialkennwort des Auslieferungsstandes der Software. Dies ermöglicht auch nicht autorisierten Dritten das unbefugte Anmelden an die Datenbank.
- Benutzer aus der Fachabteilung können sich an die Datenbank anmelden und sind berechtigt, mit den Funktionen der Datenbank Änderungen in den Datenbanktabellen durchzuführen, die konkurrierend auch von SAP-Benutzern geändert werden.
- Angreifer können über nicht benötigte Datenbankbenutzer eine Sicherheitsschwachstelle im Datenbanksystem nutzen, um privilegierten Zugriff auf die Datenbank zu erlangen.
- Die Datenbank lässt beliebige Anmeldeversuche über das Netz zu.
- Anmeldungen an die Datenbank werden nicht protokolliert und überwacht.
- Die Daten in der Datenbank sind nicht verschlüsselt und werden auch nicht verschlüsselt übertragen.
- Sicherheitsempfehlungen des Herstellers der Datenbank sind nicht umgesetzt.

7.3. KONTROLLZIELE

- Die Sicherheitsempfehlungen von SAP zur sicheren Konfiguration und zum ordnungsmäßigen Betrieb der Datenbank sind umgesetzt.
- Eine zur SAP-Anwendung konkurrierende Nutzung der Datenbank ist nicht implementiert, die Änderungen an den gleichen Datenbanktabellen zulässt, die schon SAP verwaltet.
- Anmeldungen von beliebigen Clients aus nicht vertrauenswürdigen Netzwerksegmenten an der Datenbank sind verhindert.
- Die technischen Möglichkeiten, dass ein Benutzer sich von seinem Client aus direkt an der Datenbank anmelden kann, sind entweder ausgeschlossen oder auf den notwendigen Umfang eingeschränkt und gegen unbefugte Nutzung abgesichert (ODBC-Zugriff).
- Nicht benötigte Datenbankbenutzer sind gesperrt oder gelöscht.
- Die Funktionen zur Anmeldekontrolle werden genutzt, die das proprietäre Datenbanksystem bereitstellt. Insbesondere werden Fehlversuche bei der Anmeldung protokolliert und überwacht.
- Die Daten in der Datenbank werden entsprechend ihrem Schutzbedarf verschlüsselt gespeichert und übertragen.
- Zusätzliche Sicherheitsempfehlungen des Herstellers der Datenbank sind umgesetzt.

7.4. PRÜFPROGRAMM: ABSICHERUNG VON ORACLE UNTER UNIX

NR.	AUTHENTISIERUNG MIT ORACLE UNTER UNIX
1.	**Kontrollziel: Angemessene Zugriffskontrolle für Oracle unter UNIX** **Risiko:** Beliebige Benutzer können sich Remote an der Datenbank unter einem der Standard-Datenbankbenutzer mit dem Standardkennwort anmelden, können alle Tabelleninhalte einsehen und nicht autorisierte Änderungen durchführen.
1.1.	**Welche Benutzer sind in der Datenbank eingerichtet?** *SQL> SELECT * FROM all_users;* *Klären, welche Benutzer zu welchem Zweck eingerichtet sind.* Nicht benötigte Datenbankbenutzer, z.B. Gast- oder Demo-Benutzer, sind zu sperren oder zu entfernen.
1.2. **H**	**Ist der SAP-Datenbankbenutzer SAPR3/SAP‹SAPSID› gegen unbefugten Zugriff geschützt?** 1. Durch regelmäßigen Wechsel des Kennworts für ‹SAPSID›ADM? 2. Durch Deaktivieren des Dienstes rlogin? 3. Durch Deaktivieren anderer hostbasierter Authentifizierungen, z.B. über SSH (HostbasedAuthentication)? 4. Durch angemessene Nutzung des Valid-Node-Checking-Mechanismus der sqlnet.ora-Datei, der Quell-IP-Adressen zulässt oder aussperrt? (Siehe 4.1.)

NR.	AUTHENTISIERUNG MIT ORACLE UNTER UNIX
1.3. **H**	**Sind die Standardkennwörter der Standard-Datenbankbenutzer geändert?** - SAP‹SAPSID› oder SAPR3 (Kennwort: SAP) - SYS (Kennwort: CHANGE_ON_INSTALL) - SYSTEM (Kennwort: MANAGER). **Sind noch Default-Passwörter der Oracle-Default-Accounts vorhanden?** *SQL>select * from dba_users_with_defpwd; (ab 11g)* *Austesten, ob eine Anmeldung mit den Standardkennworten bzw. Benutzername=Passwort möglich ist.* Die Kennwörter sind während der Installation zu ändern. Komplexe Kennwörter sind zu wählen.
1.4.	**Werden Systemereignisse wie An- und Abmeldungen an der Datenbank protokolliert?** *SQL>select * from DBA_AUDIT_SESSION;* *SQL>show parameter audit;* Wird die Protokolldatei regelmäßig archiviert und gelöscht, um zu verhindern, dass es zu einem Überlauf der SYS.AUD$-Tabelle kommt? Haben nur Systemadministratoren Zugriffsrechte auf die Einstellungen für die Protokolldatei und auch die Protokolldatei selbst?
2.	**Kontrollziel: Die Bildung des Kennworts unterliegt Komplexitätsregeln.** **Risiko:** Das Kennwort ist einfach und kann mit wenigen Anmeldeversuchen erraten werden.
2.1.	**Wurde eine Passwort-Policy-Prüfungsfunktion für alle relevanten Nutzerprofile hinterlegt?** *SQL>select * from dba.profiles;* Prüfung, ob ein Wert für PASSWORD_VERIFY_FUNCTION angegeben ist. Prüfung, ob die angegebene Funktion den Anforderungen an sichere Passworte genügt.
2.2.	**Ab wie vielen Anmeldeversuchen wird ein Account gesperrt (FAILED_LOGIN_ATTEMPTS) und wie lange wird ein Account gesperrt (PASSWORD_LOCK_TIME)?** *SQL>select * from dba.profiles;* Die Einstellungen müssen einen Brute-Force-Angriff erschweren, dürfen aber nicht zu einer dauerhaften Deaktivierung von Accounts führen.
2.3.	**Sind Passwörter Case-Sensitiv? (ab 11g)** *SQL>show parameter sec_case_sensitive_logon;* Sind noch Accounts mit case-insensitivem Passwort vorhanden? *SQL>select username, password_versions from dba.dba_users;*
3.	**Kontrollziel: Zugriff auf die Datenbank ist exklusiv für SAP-Anwendungen und gemäß den Vorgaben von SAP installiert.** **Risiko:** Konkurrierende Datenbankänderungen durch weitere Datenbankanwendungen auf den SAP-Tabellen führen zur Dateninkonsistenz.
3.1.	**Sind die Zugriffsrechte für Oracle-Verzeichnisse und -Dateien unter UNIX so gesetzt, wie es von SAP vorgesehen ist und bei der Standard-Installation durchgeführt wird?** Insbesondere die Daten-Dateien, Log- und Trace-Dateien und die Konfigurations-Dateien müssen vor dem unbefugten Auslesen oder gar Verändern geschützt sein.

NR.	AUTHENTISIERUNG MIT ORACLE UNTER UNIX
3.2.	**Nutzt exklusiv das SAP-System die Datenbank oder werden auch andere Anwendungen auf der Datenbank betrieben?** Auf der Datenbank für das SAP-System dürfen keine anderen Anwendungen ablaufen, insbesondere dürfen keine Verknüpfungen zwischen den Tabellen des SAP-Systems und anderen Datenbanken eingerichtet sein.
3.3.	Ist der Oracle Listener sicher konfiguriert? Ist ein Kennwort für den Oracle Listener vergeben?
3.4.	Sind weitere Nutzer in der OS-Gruppe dba außer ‹sid›adm und personalisierten Administratoren?
3.5.	**Sind unnötige Datenbank-Links definiert?** *SQL>select * from dba_db_links;* Sind diese public? Welchen Schutzbedarf haben die Systeme im Vergleich zum geprüften System?

NR.	REDUZIERUNG DER ANGRIFFSFLÄCHE VON ORACLE UNTER UNIX
4.	**Kontrollziel: Um die Angriffsfläche zu verringern, dürfen nur die notwendigen Services und Einstiegsmöglichkeiten gegeben und erreichbar sein.** **Risiko:** Mit jeder unnötigen Komponente erhöht sich die Wahrscheinlichkeit, dass Schwachstellen im System ausgenutzt werden können.
4.1. **H**	**Können sich Benutzer über eine Client-Software an der Datenbank anmelden?** **Ist der Remote-Datenbankzugriff eingeschränkt und kontrolliert?** › Sind in der sqlnet.ora-Datei die IP-Adressen der zugelassenen Clients (Management-Konsolen) eingetragen (tcp.invited.nodes)? Ist der Zugriff auf die Datenbank über eine Firewall geregelt (Oracle Listener auf dem Port TCP/IP 1521)?
4.2.	**Sind Komponenten des Oracle-DBMS aktiv, welche nicht benötigt werden?** **Zum Beispiel:** Apache-HTTP-Server, Enterprise Manager, APEX, OLAP, Ultrasearch, Java
4.3.	**Werden auf der Betriebssysteminstanz weitere Datenbanken oder andere Dienste betrieben?** Angriffe auf diese zusätzlichen Systeme können sich auch auf die Datenbank auswirken. Nur absolut notwendige Dienste sollten auf dem Server betrieben werden.
4.4.	**Sind nicht-benötigte externe Prozeduren definiert?** „PROGRAM=extproc" in der listener.ora

7.5. PRÜFPROGRAMM: ABSICHERUNG VON ORACLE UNTER WINDOWS

NR.	AUTHENTISIERUNG MIT ORACLE UNTER WINDOWS
1.	**Kontrollziel: Angemessene Zugriffskontrolle für Oracle unter Windows** **Risiko:** Beliebige Benutzer können sich Remote an der Datenbank unter einem der Standard-Datenbankbenutzer mit dem Standardkennwort anmelden, können alle Tabelleninhalte einsehen und nicht autorisierte Änderungen durchführen.
1.1.	**Welche Benutzer sind in der Datenbank eingerichtet?** *SQL> SELECT * FROM all_users;* *Klären, welche Benutzer zu welchem Zweck eingerichtet sind.* Nicht benötigte Datenbankbenutzer, z.B. Gast- oder Demo-Benutzer, sind zu sperren oder zu entfernen.
1.2.	**Wird der OPS-Mechanismus korrekt genutzt?** *SQL> select * from OPS$<SID>ADM.SAPUSER* SAP empfiehlt, nur OPS$-Benutzer für die Windows Benutzer zu definieren, die für den Betrieb des SAP-Systems erforderlich sind. Normalerweise sind das die Benutzer SAPService‹SID› und ‹SID›ADM. Weitere Informationen über das Anlegen von OPS$-Benutzern unter Windows finden sich im SAP-Hinweis 50 088.
1.3. **H**	**Sind die SAP-Datenbankbenutzer SAPR3/SAP‹SAPSID› und ‹SAPSID›ADM gegen unbefugten Zugriff geschützt?** 1. Durch regelmäßigen Wechsel des Kennworts für ‹SAPSID›ADM? 2. Durch angemessene Nutzung des Valid-Node-Checking-Mechanismus der sqlnet.ora-Datei, der Quell-IP-Adressen zulässt oder aussperrt? (Siehe 4.1.)
1.4. **H**	**Sind die Standardkennwörter der Standard-Datenbankbenutzer geändert?** - SAP‹SAPSID› oder SAPR3 (Kennwort: SAP) - SYS (Kennwort: CHANGE_ON_INSTALL) - SYSTEM (Kennwort: MANAGER). **Sind noch Default-Passwörter der Oracle-Default-Accounts vorhanden?** *SQL>select * from dba_users_with_defpwd; (ab 11g)* *Austesten, ob eine Anmeldung mit den Standardkennworten bzw. Benutzername=Passwort möglich ist.* Die Kennwörter sind während der Installation zu ändern. Komplexe Kennwörter sind zu wählen.
1.5.	**Werden Systemereignisse wie An- und Abmeldungen an der Datenbank protokolliert?** *SQL>select * from DBA_AUDIT_SESSION;* *SQL>show parameter audit;* Wird die Protokolldatei regelmäßig archiviert und gelöscht, um zu verhindern, dass es zu einem Überlauf der SYS.AUD$-Tabelle kommt? Haben nur Systemadministratoren Zugriffsrechte auf die Einstellungen für die Protokolldatei und auch die Protokolldatei selbst?
2.	**Kontrollziel: Die Bildung des Kennworts unterliegt Komplexitätsregeln.** **Risiko:** Das Kennwort ist einfach und kann mit wenigen Anmeldeversuchen erraten werden.
2.1.	**Wurde eine Passwort-Policy-Prüfungsfunktion für alle relevanten Nutzerprofile hinterlegt?** *SQL>select * from dba.profiles;* Prüfung, ob ein Wert für PASSWORD_VERIFY_FUNCTION angegeben ist. Prüfung, ob die angegebene Funktion den Anforderungen an sichere Passworte genügt.

NR.	AUTHENTISIERUNG MIT ORACLE UNTER WINDOWS
2.2.	**Ab wie vielen Anmeldeversuchen wird ein Account gesperrt (FAILED_LOGIN_ ATTEMPTS) und wie lange wird ein Account gesperrt (PASSWORD_LOCK_TIME)?** *SQL>select * from dba.profiles;* Die Einstellungen müssen einen Brute-Force-Angriff erschweren, dürfen aber nicht zu einer dauerhaften Deaktivierung von Accounts führen.
2.3.	**Sind Passworter Case-Sensitiv? (ab 11g)** *SQL>show parameter sec_case_sensitive_logon;* Sind noch Accounts mit case-insensitivem Passwort vorhanden? *SQL>select username, password_versions from dba.dba_users;*

NR.	INTEGRITÄTSWAHRUNG MIT ORACLE UNTER WINDOWS
3.	**Kontrollziel: Zugriff auf die Datenbank ist exklusiv für SAP-Anwendungen und gemäß den Vorgaben von SAP installiert.** Risiko: Konkurrierende Datenbankänderungen durch weitere Datenbank-anwendungen auf den SAP-Tabellen führen zur Dateninkonsistenz.
3.1.	**Sind die Zugriffsrechte für ORACLE-Verzeichnisse und -Dateien unter Windows so gesetzt, wie es von SAP vorgesehen ist und bei der Standard-Installation durchgeführt wird?** Um die ORACLE-Dateien zu schützen, müssen folgende Zugriffsrechte vergeben sein: - der lokalen Gruppe SAP_‹SID›_LocalAdmin und dem lokalen Benutzer SYSTEM müssen die Zugriffsrechte Full control für alle ORACLE-Dateien zugewiesen sein. - anderen Gruppen oder Benutzern dürfen keine Zugriffsrechte für die ORACLE-Dateien vergeben sein. **Die folgende Tabelle gibt die Dateien und die zugehörenden notwendigen Zugriffsrechte an:**
3.2.	**Nutzt exklusiv das SAP-System die Datenbank oder werden auch andere Anwendungen auf der Datenbank betrieben?** Auf der Datenbank für das SAP-System dürfen keine anderen Anwendungen ablaufen, insbesondere dürfen keine Verknüpfungen zwischen den Tabellen des SAP-Systems und anderen Datenbanken eingerichtet sein.

ORACLE VERZEICHNISSE	ZUGRIFFSRECHT	BENUTZER ODER GRUPPE
%ORACLE_HOME%	Full Control	SYSTEM, Administrators, SAP_‹SAPSID›_GlobalAdmin (domain installation), SAP_‹SAPSID›_LocalAdmin (local installation)
‹drive›:\oracle\‹dbsid›	Full Control	SYSTEM, Administrators, SAP_‹SAPSID›_GlobalAdmin (domain installation), SAP_‹SAPSID›_LocalAdmin (local installation)

NR.	INTEGRITÄTSWAHRUNG MIT ORACLE UNTER WINDOWS
3.3. **H**	Ist der Oracle Listener sicher konfiguriert? Ist ein Kennwort für den Oracle Listener vergeben?
3.4.	**Sind unnötige Datenbank-Links definiert?** *SQL>select * from dba_db_links;* Sind diese public? Welchen Schutzbedarf haben die Systeme im Vergleich zum geprüften System?

NR.	REDUZIERUNG DER ANGRIFFSFLÄCHE VON ORACLE UNTER WINDOWS
4.	**Kontrollziel: Um die Angriffsfläche zu verringern, dürfen nur die notwendigen Services und Einstiegsmöglichkeiten gegeben und erreichbar sein.** **Risiko:** Mit jeder unnötigen Komponente erhöht sich die Wahrscheinlichkeit, dass Schwachstellen im System ausgenutzt werden können.
4.1. **H**	**Können sich Benutzer über eine Client-Software an der Datenbank anmelden?** **Ist der Remote-Datenbankzugriff eingeschränkt und kontrolliert?** - Sind in der sqlnet.ora-Datei die IP-Adressen der zugelassenen Clients (Management-Konsolen) eingetragen (tcp.invited.nodes)? Ist der Zugriff auf die Datenbank über eine Firewall geregelt (Oracle Listener auf dem Port TCP/IP 1521)?
4.2.	**Sind Komponenten des Oracle-DBMS aktiv, die nicht benötigt werden?** **Zum Beispiel:** Apache-HTTP-Server, Enterprise Manager, APEX, OLAP, Ultrasearch, Java
4.3.	**Werden auf der Betriebssysteminstanz weitere Datenbanken oder andere Dienste betrieben?** Angriffe auf diese zusätzlichen Systeme können sich auch auf die Datenbank auswirken. Nur absolut notwendige Dienste sollten auf dem Server betrieben werden.
4.4.	**Sind nicht-benötigte externe Prozeduren definiert?** „PROGRAM=extproc" in der listener.ora

7.6. PRÜFPROGRAMM: SICHERES DATENBANKMANAGEMENT MIT ORACLE

NR.	DATENBANKMANAGEMENT
1.	**Kontrollziel: Implementierung eines Risikomanagement-Prozesses** **Risiko:** Durch unentdeckte und unbewertete Risiken kann der Sicherheitszustand der Datenbank nicht definiert werden und somit keine Maßnahmen getroffen werden.
1.1.	Wurden sämtliche Sicherheitsvorgaben konsolidiert und dokumentiert?
1.2.	Wurden anhand von Datenklassifizierung, Infrastruktur und bereits implementierten Sicherungsmaßnahmen Risiken erfasst und bewertet?
1.3.	Wurden anhand der fehlenden Umsetzung von Sicherheitsvorgaben und den erfassten Risiken Maßnahmen dokumentiert, priorisiert und mit Umsetzungsterminen versehen?
1.4.	Wurden Verantwortliche ernannt, welche den Status der Umsetzung überwachen?

NR.	DATENBANKMANAGEMENT
1.5.	Werden regelmäßige Konfigurationsprüfungen und Bestandsaufnahmen durchgeführt, um sicherzustellen, dass die einmal vorgenommenen Härtungen weiterhin vorzufinden sind? Werden dabei auch Erkenntnisse aus aktuellen Bedrohungen, Sicherheitsvorfällen und bekannten Schwachstellen berücksichtigt?
2.	**Kontrollziel: Es existiert ein angemessenes und funktionierendes Datenbank-sicherungs- und Disaster-Recovery-Konzept** **Risiko:** Ein nicht funktionsfähiges Datensicherungskonzept könnte zum Verlust von Daten führen und damit ggf. die Vollständigkeit des Buchungsstoffes gefährden.
2.1.	Besteht ein Datenbanksicherungskonzept und wie ist dieses ausgeprägt?
2.2.	Wie ist sichergestellt, dass keine Daten verloren gehen bzw. unvollständige Daten-sicherungen erkannt werden?
2.3.	Besteht ein Disaster-Recovery-Konzept und wie ist dieses ausgeprägt?
2.4.	Liegen Nachweise vor, die die Funktionsfähigkeit des Datenbanksicherungs- und Disaster-Recovery-Konzeptes belegen?
3.	**Kontrollziel: Es besteht ein angemessener und funktionierender Patch Management-Prozess** **Risiko:** Wesentliche sicherheitsrelevante Patches von Oracle sind nicht installiert, sodass Angreifer bekannte Sicherheitsschwachstellen ausnutzen können.
3.1. **H**	Befindet sich die eingesetzte Produktversion in der „Premier Support"- oder „Extended Support"-Phase? Wird die Version also weiterhin mit Sicherheitspatches beliefert?
3.2.	Wird die Datenbank mit von SAP freigegebenen Sicherheits-Patches (CPU – critical patch updates) auf dem neusten Stand gehalten?
3.3.	Gibt es einen geregelten und dokumentierten Prozess zur Freigabe und Installation von Patches?
4.	**Kontrollziel: Wahrung der Vertraulichkeit und Integrität der Daten durch Verschlüs-selung** **Risiko:** Sensible Daten können aus der Kommunikation mitgelesen und manipuliert werden. Daten können von Systemadministratoren ausgelesen werden.
4.1.	Wird entsprechend der System- und Datenklassifizierung Verschlüsselung für die Kommunikation und die Datenhaltung in der Datenbank vorgenommen?
4.2.	**Ist die Transport-Verschlüsselung und Integritätsprüfung obligatorisch?** **Sqlnet.ora:** *SQLNET.ENCRYPTION_CLIENT = required* *SQLNET.CRYPTO_CHECKSUM_CLIENT = required*
4.3.	**Wird entsprechend den aktuellen Crypto-Bewertungen eine sichere Verschlüsselungs- und Hashfunktion verwendet?** **Sqlnet.ora:** *SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT* *SQLNET.ENCRYPTION_TYPES_CLIENT*
4.4.	**Werden für administrative Zugriffe verschlüsselte Kommunikationswege verwendet?** Wenn auf Listener-Verschlüsselung verzichtet wird, da die Kommunikation in einem abgesicherten Netzsegment stattfindet, sollte der administrative Zugriff auf den Listener z.B. nur über einen SSH-Tunnel stattfinden anstelle von einem unverschlüsselten direkten Zugriff.

8. SYSTEMINTEGRITÄT AUF DER BETRIEBSSYSTEMEBENE

8.1. INTERNE UND EXTERNE ANFORDERUNGEN

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 über das Netzwerk oder das Dateisystem. 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.

Es sind sowohl die Hinweise von SAP zu den Betriebssystem-Plattformen im SAP NetWeaver Security Guide zu berücksichtigen als auch die Security Guides der jeweiligen Betriebssystemhersteller.

8.2. 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 Administratoren sind noch auf dem Standard der Auslieferung oder lassen sich leicht erraten und ermöglichen das unautorisierte Anmelden an das Betriebssystem.
- 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.
- Aufgrund von unzureichend gesetzten Zugriffsprivilegien können beliebige Anwender auf ein Verzeichnis mit streng vertraulichen Informationen oder ausführbaren SAP-Programmen zugreifen, das über das Netz nur für eine bestimmte Benutzergruppe bereitgestellt sein soll.
- Anmeldungen an das Betriebssystem werden nicht protokolliert und überwacht.
- Das Betriebssystem hat eine bekannte Sicherheitsschwachstelle, die ein Angreifer über das Netz erkennen und ausnutzen kann. Dieses kann zur Offenlegung von sensiblen Daten oder der 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 von systemrelevanten Dateien wird nicht erkannt.

8.3. 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 Netz auf das Betriebssystem ist restriktiv gesetzt und sicher konfiguriert.
- Network Shares sind mit restriktiven Zugriffsrechten nur für die zugelassene Benutzergruppe gesetzt. Sie werden auf fehlerhafte Zugriffsvergaben (Windows: EVERYONE, UNIX: weltweites Lese- oder Schreibrecht) 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.

8.4. PRÜFPROGRAMM: SYSTEMINTEGRITÄT VON UNIX/LINUX

NR.	PHYSISCHER SCHUTZ
1.	**Kontrollziel: Angemessener physischer Schutz des Systems** › Nur wenige autorisierte Personen sollten physischen Zugriff zu dem System besitzen. › Das unkontrollierte Neustarten eines Systems 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.	Welche Personen haben physischen Zugang zu dem System? Sind diese Personen für den Zugang zu den Rechnerräumen oder Rechenzentren autorisiert?
1.2.	Welche Maßnahmen wurden gegen eine physische Sabotage oder Manipulation ergriffen?
1.3.	Werden regelmäßige Kontrollen zur Überprüfung der jeweiligen Hardware durchgeführt?

NR.	ZUGRIFFSPRIVILEGIEN UND -KONTROLLEN
2.	**Kontrollziel: Angemessene Zugriffsprivilegien und -kontrollen auf UNIX/Linux-Ebene** › Der Zugriff personenbezogener Benutzer auf das Betriebssystem ist auf wenige Systemadministratoren beschränkt. › Benutzer aus Fachabteilungen haben keinen Zugriff auf das 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 Benutzern sind Standardumgebungen, z.B. login shell, eingerichtet, die zu weit reichende automatische Rechtevergaben beinhalten. Unbefugte Aktionen auf der Betriebssystemebene sind möglich. Die Integrität der System- und Datendateien des SAP-Systems ist gefährdet.
2.1.	**Wird ein sicheres Authentifizierungsverfahren eingesetzt? Nutzt dieses Verfahren modernste Verschlüsselungsverfahren? Werden Zugangsdaten durch ein zentrales Anmeldesystem verwaltet?** Im Unix besteht die Möglichkeit, sichere Anmeldeverfahren wie z.B. TACAC+ oder LDAP zu verwenden. Hierdurch können Administratoren zentral und systemübergreifend verwaltet werden. Zudem werden schützenswerte Zugangsdaten zentral abgelegt und systemübergreifend bereitgestellt. Eine lokale Speicherung auf dem Host ist nicht erforderlich.
2.2.	**Welche Benutzer sind auf dem System eingerichtet? Sind neben den Standardsystembenutzern auch personenbezogene Benutzer vergeben? Welche Aufgaben haben diese eingerichteten personenbezogenen Benutzer?** Die Benutzer root, ‹sid›adm und ‹db›‹sid› sollten neben wenigen Spezialsystembenutzern die einzigen Benutzer auf den Anwendungsservern und der Hauptinstanz sein. Nach der Installation kann ‹db›‹sid› auf den Anwendungsservern gesperrt werden. **Hinweis:** Die Standardbenutzer sind in der Systemdokumentation des Herstellers und von SAP aufgeführt.
2.3.	**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-Feldes der Datei /etc/passwd zeigt an, dass das gehashte Passwort in der /etc/shadow Datei hinterlegt ist.
2.4.	Sind für alle Benutzer Passwörter vergeben?
2.5.	**Welche Gruppen sind auf dem System eingerichtet? Sind neben den Standardgruppen auch unternehmensspezifische Gruppennamen vergeben? Welche Benutzer sind den unternehmensspezifischen Gruppen zugeordnet? Welche Rechte wurden den jeweiligen Gruppen zugeordnet?** **Hinweis:** Die Standardgruppen sind in der Systemdokumentation des Herstellers aufgeführt.

NR.	ZUGRIFFSPRIVILEGIEN UND -KONTROLLEN
2.6.	**Sind Regeln für die Bildung und Änderung des Passwortes aktiviert?** 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. **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.
2.7.	**Werden Anmeldungen von Benutzern, insbesondere fehlerhafte Anmeldungen automatisch, protokolliert und überwacht?** Bei Linux werden verhaltensrelevante Ereignisse durch den Syslog in sogenannten Logfiles 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.
2.8.	**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:** Folgende Zugriffsprivilegien werden bei der Installation automatisch gesetzt:

SAP Verzeichnis oder Datei	Zugriffsrecht	Besitzer	Gruppe
/‹sapmnt›/‹SAPSID›/exe	755	‹sapsid›adm	sapsys
/‹sapmnt›/‹SAPSID›/exe/saposcol	4755	root	sapsys
/‹sapmnt›/‹SAPSID›/global	700	‹sapsid›adm	sapsys
/‹sapmnt›/‹SAPSID›/profile	755		
/usr/sap/‹SAPSID›	751		
/usr/sap/‹SAPSID›/‹Instance ID›	755		
/usr/sap/‹SAPSID›/‹Instance ID›/*	750	‹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	755	‹sapsid›adm	sapsys
‹home directory of ‹sapsid›adm›	700	‹sapsid›adm	sapsys
home directory of ‹sapsid›adm›/*	700	‹sapsid›adm	sapsys

2.9.	**Welche UMASK-Definitionen sind in den relevanten Dateien, z.B. in .login, .cshrc, .profile, /etc/profile vergeben?** 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.

NR.	ZUGRIFFSPRIVILEGIEN UND -KONTROLLEN
2.10.	**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 des Benutzers bzw. der Gruppe ausgeführt, der diese Datei gehört. Normalerweise werden diese Bits bei Dateien verwendet, die als Superuser „root" ausgeführt werden müssen, um auf Systemressourcen, die erweiterte Berechtigungen benötigen, zuzugreifen. Risiko: Diese Dateien sind beliebte Ziele von Angreifern, um erweiterte Privilegien, z.B. des Superusers, zu erhalten.

NR.	KONFIGURATION VON DIENSTEN UND NETZWERKZUGRIFFEN
3.	Kontrollziel: **Sichere Konfiguration von Diensten und Netzwerkzugriffen** Schwachstellen in der Konfiguration eines Dienstes bzw. innerhalb des Dienstes selber 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 Dienstes 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.
3.1.	Sind die Sicherheitshinweise des UNIX/Linux-Distributors zum Härten des Systems, z.B. Hinweise zum Deaktivieren nicht benötigter Dienste, bekannt und umgesetzt?
3.2.	Wird das Betriebssystem mit den vom UNIX/Linux-Distributor freigegebenen Sicherheits-Patches auf dem neusten Stand gehalten?
3.3.	**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 die Sicherheit der gesamten SAP-Landschaft und erleichtert die Verwaltung und Wartung der Regelwerke. SAP bietet Zertifizierungen für Sicherheitslösungen an; eine Liste von zertifizierten Herstellern können im SAP-Portal frei eingesehen werden.
3.4.	**Werden zur Wartung des Systems Remote-Werkzeuge eingesetzt? Sind diese sicher konfiguriert?** Es sollte vermieden werden, Programme/Protokolle wie ftp, telnet oder rlogin/rsh zu verwenden, da diese die Daten unverschlüsselt übertragen und somit ein Abfangen der Daten ermöglichen. Daher wird der Einsatz von sicheren Alternativen wie ssh, scp oder sftp empfohlen. **Hinweis:** Die sicherere Konfiguration des jeweiligen Dienstes kann entsprechenden Sicherheitshandbüchern entnommen werden.
3.5.	**Ist das Network Information System (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 Netzwerkes eingesetzt.

NR.	KONFIGURATION VON DIENSTEN UND NETZWERKZUGRIFFEN
3.6.	**Administrative Fernzugriffe auf das Betriebssystem sind durch sichere Verfahren abzusichern, d.h., sind die Standardkennwörter durch komplexe Kennwörter ersetzt, wird eine sichere Verschlüsselung genutzt und sind Härtungsmaßnahmen für Web-Schnittstelle getroffen worden? Werden alternative Zugriffsmöglichkeiten, wie z.B. Terminalserver, genutzt?** **Risiko:** Bei der Installation eines UNIX/Linux-Betriebssysteme kann standardmäßig ein Remote-Zugriff der Systemadministratoren implementiert werden, ohne dass dies bei der Installation bekannt oder wahrgenommen wird. Angreifer aus dem Netzwerk können die dabei vergebenen Standardkennworte oder Sicherheitsschwachstellen in der Version des betreffenden Web-Servers ausnutzen, um unbefugte Aktionen auf der Ebene des Betriebssystems auszuführen.
3.7.	Ist der X-Windows Service im Einsatz? Wird er tatsächlich benötigt? Ist er gemäß den Sicherheitsempfehlungen des UNIX/Linux-Herstellers installiert?
3.8.	**Ist das Network Filesystem (NFS) restriktiv und kontrolliert eingesetzt?** Über NFS dürfen keine Verzeichnisse mit vertraulichen Daten exportiert werden. Über NFS dürfen keine Home-Verzeichnisse – von welchen Benutzern auch immer – mit Schreibberechtigung exportiert werden. Verzeichnisse dürfen nur an vertrauenswürdige Systeme exportiert werden. **Risiko:** Die über NFS exportierten Verzeichnisse können vertrauliche Daten, die für alle Benutzer im Netz lesbar sind, enthalten. 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.

NR.	SICHERHEITSRICHTLINIEN UND VORGEHENSWEISEN
4.	**Kontrollziel: Sicherheitsrichtlinien und Vorgehensweisen** › Welche Maßnahmen sind eingerichtet, um die Integrität sowie den Schutz der Vertraulichkeit des Systems sicherzustellen und zu überwachen? **Risiko:** › Bei unzureichenden Maßnahmen können die Integrität sowie der Schutz der Vertraulichkeit des Systems nicht ausreichend gewährleistet sein.
4.1.	**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 Loghost gespeichert? Werden regelmäßige Auswertungen auf verdächtige Aktivitäten durchgeführt?** 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 berechtige Benutzer sollten daher Zugriff auf die Dateien erhalten. Eine Auslagerung der Protokolldateien auf einen dedizierten Log-Server kann die Sicherheit erhöhen. Betriebspersonal hat keinen Zugriff auf die zentralen Log-Dateien. In der Praxis können sogenannte SIEM-Systeme (Security Incident & Event Management Systeme) klassische Log-Hosts ersetzen. Intelligente Abfragen unterstützen dabei die Analyse von verdächtigen Vorgängen.

NR.	SICHERHEITSRICHTLINIEN UND VORGEHENSWEISEN
4.2.	**Wird ein Back-up des Systems auf einem dedizierten Medium (separater Back-up Server) durchgeführt?** Ein Back-up kann einerseits dabei helfen, gelöschte oder beschädigte Daten wieder herzustellen. 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 Back-up-Medium in einer sicheren Umgebung aufbewahrt wird, sodass dass es gegen Manipulation geschützt ist.
4.3.	Unterstützt das UNIX/Linux-Betriebssystem Integritätsprüfungen oder sogenannte Host based Intrusion Detection Software (HIDS) für Systemdateien? Wird diese Möglichkeit genutzt?
4.4.	**Gibt es eine Richtlinie, wie Daten auf stillgelegten Systemen oder von nicht mehr verwendeten Datenmedien gelöscht werden?** Werden Systeme stillgelegt bzw. Datenmedien nicht mehr verwendet, müssen die darauf enthaltenen sensiblen Daten so gelöscht werden, dass diese nicht wieder hergestellt werden können. Um dieses zu erreichen, können sogenannte Wipe Tools eingesetzt werden.

8.5. PRÜFPROGRAMM: SYSTEMINTEGRITÄT VON WINDOWS

NR.	PHYSISCHER SCHUTZ
1.	**Kontrollziel: Angemessener physischer Schutz des Systems** › Nur wenige autorisierte Personen sollten physischen Zugriff zu dem System besitzen. › Das unkontrollierte Neustarten eines Systems 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.	Welche Personen haben physischen Zugang zu dem System? Sind diese Personen für den Zugang zu den Rechnerräumen oder Rechenzentren autorisiert?
1.2.	Welche Maßnahmen wurden gegen eine physische Sabotage oder Manipulation ergriffen?
1.3.	Werden regelmäßige Kontrollen zur Überprüfung der jeweiligen Hardware durchgeführt?

NR.	ZUGRIFFSPRIVILEGIEN UND -KONTROLLEN
2.	**Kontrollziel: Angemessene Zugriffsprivilegien und -kontrollen auf Windows-Ebene** › Der Zugriff personenbezogener Benutzer auf das Betriebssystem ist auf wenige Systemadministratoren beschränkt. › Benutzer aus Fachabteilungen haben keinen Zugriff auf das 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 Usern sind zu weit reichende Rechte vergeben. Unbefugte Aktionen auf Betriebssystemebene sind möglich. Die Integrität der System- und Dateien des SAP-Systems ist gefährdet.
2.1.	**Ist das SAP-System auf einem Windows-Domänencontroller installiert?** **Hinweis:** Ein auf einem Domänencontroller definiertes lokales Benutzerrecht ist auf allen Domänencontrollern gültig. SAP empfiehlt, SAP-Systeme nicht auf einem Domänencontroller zu installieren.

2.2.	**Werden insbesondere bei großen Systemlandschaften die SAP Systeme durch eine separate Domäne von den Unternehmensdaten getrennt?**
	SAP empfiehlt, zwei getrennte Domänen für die SAP-Systeme anzulegen.
	› In der Unternehmens-Domäne sind die Domänenbenutzer, einschließlich der SAP-Systembenutzer, und der Unternehmens-Domänenadministrator eingerichtet.
	› In der davon getrennten SAP-Domäne sind die SAP-System-Server, Dienste und Administratoren eingerichtet. Dazu zählen:
	  › SAP-System-Anwendungsserver und -Datenbankserver
	  › SAP-System- oder Datenbank-Dienste
	  › SAP-Systemadministratoren
	  › Windows-Administratoren
	  › Administratoren der SAP-Domäne

2.3.	**Welche Vertrauensbeziehungen sind zwischen anderen Windows-Domänen und der Windows-Domäne für die SAP-Systeme definiert?** **Hinweis 1:** In den Standard-Installationsvorgehensweisen empfiehlt SAP, getrennte Domänen einzurichten. Zu beachten ist jedoch, dass bestimmte SAP-spezifische Funktionen und Windowsspezifische 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 2:** Wenn das SAP-System standardmäßig installiert wird, implementiert das Installationswerkzeug, SAPinst genannt, automatisch alle notwendigen Maßnahmen, die relevant sind, um das SAP-System gegen nicht autorisierten Zugriff zu schützen.

NR.	ZUGRIFFSPRIVILEGIEN UND -KONTROLLEN
2.4.	**Welche Gruppen sind auf den SAP-Servern registriert (Windows-Domäne)? Sind neben den Standardgruppen auch unternehmensspezifische Gruppennamen vergeben? Welche Benutzer sind den unternehmensspezifischen Gruppen zugeordnet? Welche Rechte wurden den jeweiligen Gruppen zugeordnet?** Es sollten keine anderen Gruppen als die Windows-Standardgruppen und die SAP-System- und Datenbankgruppen definiert sein. **Hinweis 1:** Globale Benutzergruppen sind innerhalb einer Windows-Domäne gültig, nicht nur auf einem Server. SAP empfiehlt, die Domänenbenutzer nach Aufgaben in verschiedenen Aktivitätsgruppen zu bündeln. Der Domänenadministrator kann die Aktivitätsgruppen in andere Domänen exportieren, sodass der entsprechende Benutzer auf alle zur Verwaltung des SAP-Systems erforderlichen Ressourcen zugreifen kann. **Hinweis 2:** Standardmäßig ist die globale Gruppe für SAP-Administratoren als SAP_‹SID›_GlobalAdmin definiert.
2.5.	**Welche Gruppen sind auf den SAP-Servern registriert (lokaler SAP-Server)? Sind neben den Standardgruppen auch unternehmensspezifische Gruppennamen vergeben? Welche Benutzer sind den unternehmensspezifischen Gruppen zugeordnet? Welche Rechte wurden den jeweiligen Gruppen zugeordnet?** **Hinweis 1:** Lokale Benutzergruppen (und lokale Benutzer) liegen lokal auf einem Server vor. Bei der Installation werden Benutzerrechte lokalen Benutzern anstelle von Gruppen zugeordnet. Z.B. erhält der Benutzer <SID>ADM das Benutzerrecht „Logon on as a service". SAP empfiehlt, um die Benutzerverwaltung zu vereinfachen, Serverressourcen lokalen Gruppen anstelle von einzelnen Benutzern zuzuordnen. Entsprechende globale Benutzer und globale Gruppen können dann der lokalen Gruppe zugeordnet werden. Dadurch kann besser kontrolliert werden, wer zu welcher Gruppe gehört und welche Aufgaben er besitzt. **Hinweis 2:** Standardmäßig ist die lokale Gruppe für SAP-Administratoren als SAP_‹SID›_LocalAdmin definiert. Diese lokale Gruppe enthält die Domänen-Gruppe SAP_‹SID›_GlobalAdmin.
2.6.	**Welche Benutzer sind auf dem System eingerichtet? Sind neben den Standardsystembenutzern auch personenbezogene Benutzer vergeben? Welche Aufgaben haben diese eingerichteten personenbezogenen Benutzer?** **Hinweis:** Die Standardbenutzer sind in der Systemdokumentation des Herstellers und von SAP aufgeführt.
2.7.	**Ist der Benutzeradministrator gesichert?** **Hinweis:** Der in Windows eingebaute Administrator hat unbeschränkten Zugriff auf alle Windows-Ressourcen. Der Administrator 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 Benutzername muss geändert und das Kennwort geheim gehalten werden. Für Verwaltungsaufgaben sollten andere Benutzer angelegt und deren Rechte auf die Aufgaben, für die sie verwendet werden, z.B. Benutzeradministrator, Sicherungs- und Serveroperatoren, beschränkt sein.

NR.	ZUGRIFFSPRIVILEGIEN UND -KONTROLLEN
2.8.	**Ist der Benutzer ‹SID›ADM gesichert?** **Hinweis 1:** ‹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 instanzspezifischen 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: › sein Kennwort regelmäßig zu ändern. › seine Zugriffsrechte auf instanzenspezifische Ressourcen für das SAP-System zu beschränken. **Hinweis 2:** Wenngleich ‹SID›ADM auf SAP-System-Dateien zugreifen kann, wird das SAP-System von einem anderen Benutzer (SAPService‹SID›) gestartet.
2.9.	**Ist der Benutzer SAPService‹SID› gesichert?** **Hinweis 1:** SAPService‹SID› wird bei der Installation des SAP-Systems angelegt. Der Benutzer wird normalerweise als ein Domänenbenutzer, der das SAP-System ausführt und Datenbankressourcen verwaltet, angelegt. 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 2:** SAPService‹SID› verwaltet auch die SAP-System- und Datenbankressourcen innerhalb des Computing Center Management System (CCMS). Der Benutzer braucht daher vollen Zugriff auf alle instanzen- und datenbankspezifischen Ressourcen wie Dateien, Shares, Peripheriegeräte und Netzwerkressourcen. **Hinweis 3:** Das Kennwort dieses Windows-Service-Benutzers zu ändern, ist relativ schwierig, da hierfür der Service somit auch das SAP-System gestoppt werden muss. SAP empfiehlt, folgende Vorkehrungen treffen, um SAPService‹SID› zu schützen: › das Benutzerrecht „Log on locally" und „Log on through Terminal Services" aufzuheben › seinen Zugriff auf instanz- und datenbankspezifische Ressourcen zu beschränken
2.10.	Ist der Benutzer-Gast gesperrt oder gelöscht?
2.11.	Sind für alle Benutzer Passwörter vergeben?
2.12.	**Sind Regeln für die Bildung und Änderung des Passwortes aktiviert?** 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. **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.
2.13.	**Werden Anmeldungen von Benutzern, insbesondere fehlerhafte Anmeldungen automatisch, protokolliert und überwacht?** Damit fehlerhafte Logins innerhalb der Ereignisanzeige angezeigt werden, müssen diese in der Überwachungsrichtlinie der lokalen Computerkonfiguration aktiviert sein.

NR.	ZUGRIFFSPRIVILEGIEN UND -KONTROLLEN
2.14.	Wer darf das SAP-System starten oder stoppen?
2.15.	Sind die Zugriffsprivilegien auf die SAP Datei- und Systemverzeichnisse so gesetzt, wie es von SAP vorgesehen ist und bei der Installation standardmäßig durchgeführt wird?
2.16.	**Wer hat Zugriff auf das Shared Memory?** **Hinweis:** Der gemeinsame Speicher wird vom SAP-System-Dispatcher und den Work-prozessen für bestimmte Aktivitäten verwendet, z.B. zur Zwischenspeicherung oder für den Austausch von Verwaltungsinformationen. Diese Prozesse nutzen die Access Contol Lists (ACL) ihrer eigenen ausführbaren Datei (z.B. für den Dispatcher: disp+work.exe) dazu ihre angelegten oder hinzugefügten Shared-Memory-Segmente zu schützen. Das bedeutet, Benutzer, die nur die Rechte Read, List Content und Execute besitzen, können keine Shared-Memory-Segmente erzeugen bzw. in sie hineinschreiben.
2.17.	**Sind die Schutzmaßnahmen für dynamisch erzeugte Dateien wirksam?** **Hinweis:** Eine von ABAP erstellte Datei erhält die Zugriffsrechte des Ordners, in dem sie erstellt wurde. Nur der Besitzer der Dateien oder der Administrator kann diese Zugriffsrechte ändern. Wenn ABAP-Anweisungen die Dateien anlegen, gehören sie dem SAP-System (‹SID›ADM oder SAPService‹SID›).

NR.	KONFIGURATION VON DIENSTEN UND NETZWERKZUGRIFFEN
3.	**Kontrollziel: Sichere Konfiguration von Diensten und Netzwerkzugriffen** Schwachstellen in der Konfiguration eines Dienstes bzw. innerhalb des Dienstes selber 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, welches nicht installiert ist, kann durch einen Angreifer nicht verwendet werden. Daher sollte das System auf die Bereitstellung eines Dienstes beschränkt sein. Unterschiedliche Dienste sollten auf separaten Systemen eingerichtet sein. Risiko: Schwachstellen in Programmen bzw. Diensten können zur Offenlegung von sensiblen Daten bzw. zur Kompromitterung des Systems führen.
3.1.	**Sind die Sicherheitshinweise von Microsoft zum Härten des Systems, z.B. Hinweise zum Deaktivieren nicht benötigter Dienste, bekannt und umgesetzt?** **Hinweis:** Als Referenz können hier die von Microsoft bereitgestellten Dokumente „Security Guide for SAP on SQL Server 2012" oder „SAP Hardening and PatchManagement Guide for Windows Server" dienen.
3.2.	Wird das Betriebssystem mit den von Microsoft freigegebenen Sicherheits-Patches auf dem neusten Stand gehalten?
3.3.	**Wird eine Firewall oder eine Paketfilterung eingesetzt, die nur autorisierten Netz-werkverkehr zulässt?** **Hinweis:** Eine Liste von Ports, die durch SAP-Software genutzt werden, wird von SAP bereitgestellt. Eine zentrale, netzwerkbasierte Paketfilterung erhöht die Sicherheit der gesamten SAP-Landschaft und erleichtert die Verwaltung und Wartung der Regelwer-ke. SAP bietet Zertifizierungen für Sicherheitslösungen an; eine Liste von zertifizierten Herstellern können im SAP-Portal frei eingesehen werden.

NR.	KONFIGURATION VON DIENSTEN UND NETZWERKZUGRIFFEN
3.4.	**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. Zudem sollten für eine verstärkte Sicherheit des Systems die dynamisch erzeugten administrativen Freigaben deaktiviert werden.
3.5.	Administrative Fernzugriffe auf das Betriebssystem sind durch sichere Verfahren abzusichern, d.h., sind die Standardkennwörter durch komplexe Kennwörter ersetzt, wird eine sichere Verschlüsselung genutzt und sind Härtungsmaßnahmen für Web-Schnittstelle getroffen worden? Werden alternative Zugriffsmöglichkeiten, wie z.B. Terminalserver, genutzt?

NR.	SICHERHEITSRICHTLINIEN UND VORGEHENSWEISEN
4.	**Kontrollziel: Sicherheitsrichtlinien und Vorgehensweisen** › Welche Maßnahmen sind eingerichtet, um die Integrität sowie den Schutz der Vertraulichkeit des Systems sicherzustellen und zu überwachen? **Risiko:** › Bei unzureichenden Maßnahmen können die Integrität sowie der Schutz der Vertraulichkeit des Systems nicht ausreichend gewährleistet sein.
4.1.	**Wird das System z.B. durch einen Eventlog-Dienst durchgängig überwacht? Ist der Zugriff auf die Log-Dateien restriktiv vergeben und werden die Log-Dateien revisionssicher auf einem zentralen Loghost gespeichert? Werden regelmäßige Auswertungen auf verdächtige Aktivitäten durchgeführt?** 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 berechtige Benutzer sollten daher Zugriff auf die Dateien erhalten. Eine Auslagerung der Protokolldateien auf einen dedizierten Log-Server kann die Sicherheit erhöhen. Betriebspersonal hat keinen Zugriff auf die zentralen Log-Dateien. In der Praxis können sogenannte SIEM-Systeme (Security Incident & Event Management Systeme) klassische Log-Hosts ersetzen. Intelligente Abfragen unterstützen dabei die Analyse von verdächtigen Vorgängen.
4.2.	**Wird ein Backup des Systems auf einem dedizierten Medium (separater Back-up-Server, Tape) durchgeführt?** Ein Back-up kann einerseits dabei helfen, gelöschte oder beschädigte Daten wieder herzustellen. 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 Back-up-Medium in einer sicheren Umgebung aufbewahrt wird, sodass es gegen Manipulation geschützt ist.
4.3.	Unterstützt das Windows-Betriebssystem Integritätsprüfungen oder sogenannte Host based Intrusion Detection Software (HIDS) für Systemdateien? Wird diese Möglichkeit genutzt?
4.4.	**Gibt es eine Richtlinie, wie Daten auf stillgelegten Systemen oder von nicht mehr verwendeten Datenmedien gelöscht werden?** Werden Systeme stillgelegt bzw. Datenmedien nicht mehr verwendet, müssen die darauf enthaltenen sensiblen Daten so gelöscht werden, dass diese nicht wieder hergestellt werden können. Um dieses zu erreichen, können sogenannte Wipe Tools eingesetzt werden.

9. RISIKEN AUS DEM EINSATZ VON SAP GRC

Durch die verstärkte Sensibilisierung von Daten und Systemen hinsichtlich der Zugriffsrisiken haben die meisten vor allem größeren Unternehmen bereits Maßnahmen getroffen, um diesen entgegenzuwirken. Oftmals ist es unumgänglich, auf bewährte Compliance-Tools zurückzugreifen, um Kontrollen zu automatisieren. Diese unterstützen Organisationen bei der Schaffung von Transparenz, Bewertung und angemessenem Umgang mit Zugriffsrechten. Die Umsetzung und Überwachung von Revisionsaufgaben werden idealerweise von zentralen Stabsstellen umgesetzt. Ähnliches gilt auch für den Einsatz von Compliance-Tools. SAP GRC Access Control ist eines der Tools, das Unternehmen ganzheitlich in der Sicherstellung von IT-Compliance im Access Management unterstützt. Da es wesentliche Abweichungen in den unterschiedlichen Releases des GRC-Tools gibt, beziehen wir uns hier auf die aktuellen SAP GRC Access Control 10.X-Funktionen. Die Annahme zur Beschreibung von Prüfungshandlungen für SAP GRC ist die Nutzung als Standalone-Lösung, bspw. ohne die Integration von IDM-Systemen.

9.1. ACCESS-MANAGEMENT-PROZESSE

Um ein einheitliches Verständnis über IT-Prozesse zu erhalten, die durch den Einsatz von SAP GRC Access Control 10.X unterstützt werden, soll dies mit der Hilfe folgender Darstellung beschrieben werden.

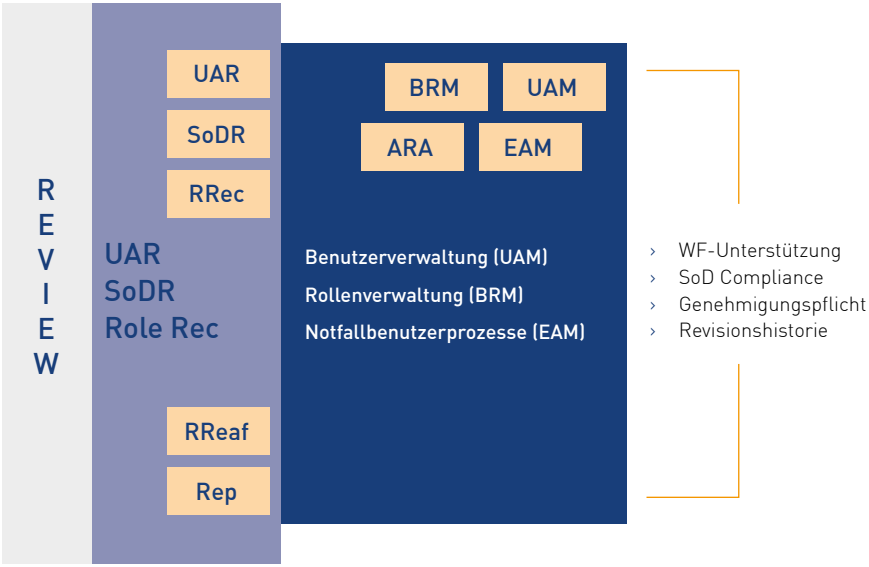


Abbildung 1: Access-Management-Prozesse

Im Kontext des IT-Audits hat die Einführung von SAP GRC oder ähnlichen Tools Auswirkung auf die Benutzerverwaltung, die Rollenverwaltung und die Notfallbenutzerprozesse (Primärprozesse). Diese können vollständig über das GRC-Tool unterstützt werden. Darüber hinaus können diese durch Reviewprozesse (Sekundärprozesse) unterstützt werden und gewährleisten somit ein Continuous Control im Access-Management. Diese Sekundärprozesse substituieren weniger, sondern kompensieren primär die Compliance-Prozesse und sollten bei der Gesamtbeurteilung des IKS berücksichtigt werden. Durch den vollständigen Einsatz und der adäquaten Ausprägung der Funktionen können die Prozesse durch die Workflow-Unterstützung, die SoD Compliance, die Genehmigungspflichten und Revisionshistorien wesentlich zur IKS-Optimierung beisteuern.

Relevante Komponenten/Funktionen des SAP GRC Access Control 10.X:

- User Access Management (UAM)
- Business Role Management (BRM)
- Emergency Access Management (EAM)
- Access Risk Analysis (ARA)
- User Access Review (UAR)
- SoD Review (SoDR)
- Role Recertification (RRec)
- Role Reaffirm (RReaf)
- Access Risk Reporting (Rep)

9.2. ANPASSUNG VON PRÜFUNGSHANDLUNGEN BEIM EINSATZ VON SAP GRC ACCESS CONTROL 10.X

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 Auditoren. Folgende Aspekte sollen mögliche Eingriffsfelder beim Einsatz der Tools aufzeigen und eine erste Abwägung für Auditoren erlauben, in welchem Kontext eine Anpassung der Prüfungshandlungen erfolgen muss.

- Einflussfelder im Access Management und Auswirkungen auf Prüfungshandlungen:
  - Konsolidierung/Zentralisierung von Kontrollaktivitäten
  - Automatisierung von kritischen Genehmigungs-Workflows
  - Automatische Ermittlung von adäquaten Genehmigern
  - Präventive Vermeidung von kritischen Zugriffen (Risikoanalyse)
  - Zentrale Verwaltung von kritischen IT-Prozessen/Stammdaten
  - Sicherstellung einer lückenlosen Dokumentation (Logs/Pflichtfelder)

EINFLUSSFELDER	SAP-GRC-FUNKTIONEN	ANFORDERUNG FÜR PRÜFUNGS-HANDLUNGEN
Konsolidierung/ Zentralisierung von Kontrollaktivitäten	Durch die Einführung von SAP-GRC-Funktionen werden dezentrale Prozesse wie die Benutzerprovisionierung 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 ist die Identifizierung von Prozessen/ Systemen im Scope, die durch das zentrale Tool gesteuert werden, und der Ausschluss der Umgehung dieser zentralen Prozesse.
Automatisierung von kritischen Genehmigungs-WF	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 diverser Faktoren wie der SystemID und/oder des Geschäftsprozesses variiert werden. Die Realisierung erfolgt mit Hilfe der integrierten Komponenten MSMP und/oder BRF+.	Der Auditor sollte ähnlich wie bei manuell durchgeführten Prozessen das Design der Umsetzung auf Angemessenheit überprüfen. Sofern dieser automatisierte Prozess für die Prozesse im Scope nicht umgangen werden kann, ist eine eingeschränkte Funktionsprüfung ausreichend.
Automatische Ermittlung von adäquaten Genehmigern	In Kombination mit den Workflow-Komponenten MSMP und BRF+ können Access-Management-Prozesse soweit automatisiert werden, dass selbst die Genehmiger systemseitig ermittelt werden können. Dies erfolgt bspw. über die Einbindung von Entscheidungstabellen.	Der Einsatz von Entscheidungstabellen zur systemseitigen Ermittlung von adäquaten Genehmigern ermöglicht es auch dem Prüfer durch wenige Checks, die Angemessenheit der hinterlegten Logik zu verstehen und zu validieren. Hierbei gibt es technische Voraussetzungen, die gegeben sein müssen, die überprüft werden sollten. Dabei handelt es sich u.a. um die gepflegten Access Control Owner im System (potenzielle Genehmiger) als auch um Eskalationspfade (Escape Conditions).

EINFLUSSFELDER	SAP-GRC-FUNKTIONEN	ANFORDERUNG FÜR PRÜFUNGS-HANDLUNGEN
Präventive Vermeidung von kritischen Zugriffen (Risikoanalyse)	Die Basis für das SoD-Management und sämtlicher Compliance-Funktionen ist das hinterlegte SoD-Regelwerk. Sofern ein technisches Regelwerk systemisch hinterlegt ist, kann diese Risikoanalyse ad hoc/detektivisch 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.
Zentrale Verwaltung von kritischen IT-Prozessen/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 dieser (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 gepflegt werden.	Aufgrund der integrierten NetWeaver-Technologie sollte der Auditor 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 variiert sein 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.

9.3. NEUE ANFORDERUNGEN AN DIE IT-PRÜFUNG

9.3.1. VERLAGERUNG DER RISIKEN IM ACCESS MANAGEMENT

Aufgrund des direkten Einflusses der GRC-Komponenten auf rechnungslegungsrelevanten ITGC-Prozessen, hier: Access-Management-Prozesse, hat die Einführung und der Betrieb eines SAP GRC Access Control (oder ähnliche Compliance Tools) eine wesentliche Bedeutung auf die Prüfungsplanung. Insbesondere bei Mittelständischen wie auch Großunternehmen bedeutet dies ebenfalls eine Zentralisierung der Prüfungshandlungen.

Bspw. 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 Prüferteam auf wesentliche Prozessrisiken fokussieren und profitiert durch die Modernisierung in der IT.

Ähnlich ist dies auch bei anderen zentralen Instanzen wie dem SolMan hinsichtlich der Umsetzung des Change Management.

Für die geprüfte Organisation wiederum bedeutet dies, dass Effizienz und dadurch Entlastungen durch das Audit gewährleistet wird bzw. gefordert werden kann. Voraussetzung ist in jedem Fall der Scope der GRC-unterstützten Prozesse und die zentrale (wirksame) Abnahme der Prozesse und Inhalte.

9.3.2. 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 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, für das SAP GRC als IKS-relevantes System die Einhaltung der ITGC-Anforderungen zu bestätigen. Hierbei handelt es sich u.a. um die Angemessenheit des GRC-Berechtigungskonzeptes hinsichtlich der Einschränkung von kritischen Zugriffsrechten sowie Trennung von kritischen Funktionen (SoD) und auch um die Angemessenheit des GRC-Prozessdesigns (z.B. die Provisionierung des GRC-Systems, Administration der Workflows, Change Management hinsichtlich der Stammdaten).

9.3.3. 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, BRF+/MSMP, Owner)**
   - Welche Access-Management-Prozesse sind im Scope?
   - Wie ist das Prozessdesign der IKS-relevanten Prozesse?
   - Welche Zielsysteme (PlugIn-Systeme) sind im Scope, mit welchen Prozessvarianten?
   - Welche Ausnahmeprozesse gibt es? (Escape Conditions/Escalation Paths)
2. **Kritische Zugriffrechte > Berechtigungen**
   - Gibt es eine Risikoeinschätzung hinsichtlich kritischer GRC-Prozesse/-Funktionen?
   - Wie werden kritische Berechtigungen identifiziert? Gibt es ein GRC-Regelwerk?
   - In welchen GRC-Prozessen wird das Regelwerk präventiv und integriert verwendet?
   - 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 Standard- und kundeneigenen Profile/Rollen sind identifiziert?
   - Wie wird das Monitoring hierzu in die Access-Management-Prozesse eingebunden?
   - Wie wird der Einsatz dieser kritischen Rechte vermieden und/oder überwacht?
6. **Kritische Parameter (globale Konfigurationseinstellungen)**
   - Sind die globalen Einstellungen angemessen gesetzt?
   - Wie ist der Change Prozess zu den kritischen Parametern?

9.4. 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.

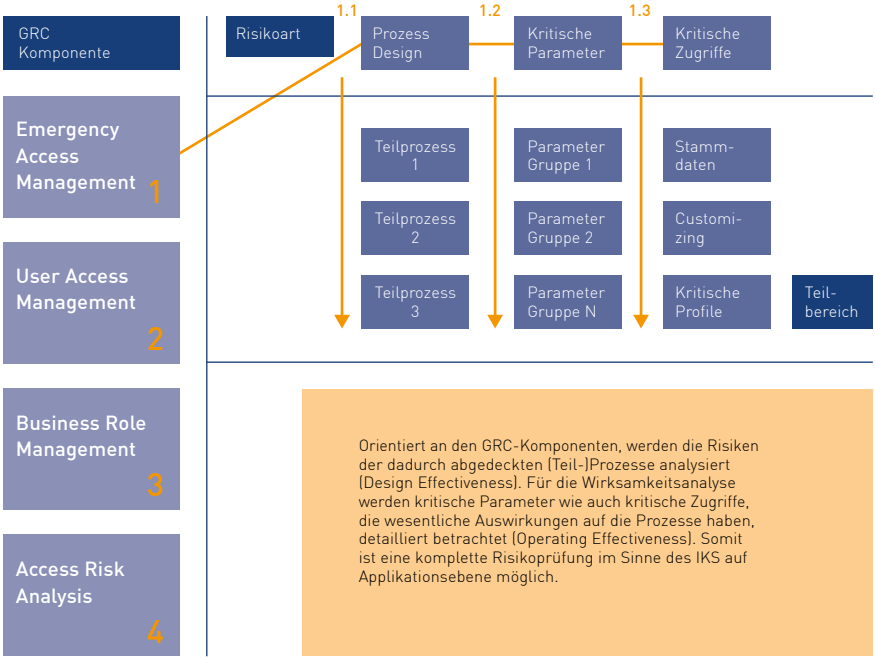


Abbildung 2: Aufbau des GRC-Prüfprogramms - risikoorientierter Prüfungsansatz

9.4.1. PRÜFUNG DES EMERGENCY ACCESS MANAGEMENT

9.4.1.1. Prozess Design Emergency Access Management

Der Einsatz von Notfallbenutzern dient zur 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 unbegründet sind, kommt in diesen Fällen das EAM von SAP GRC Access Control 10.X zum Einsatz. Es ermöglicht die zentrale Administration von ausnahmebasierten Zugängen durch die Verwendung von Firefighter-IDs (Benutzer vom Typ Service), die von mehreren Benutzern – nicht parallel – verwendet oder von Firefighter-Rollen, die diversen Benutzern 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 Nutzer vorgenommenen Handlungen unter Verwendung der kritischen Berechtigungen. EAM erfüllt die Anforderungen an eine revisionssichere Nachweispflicht zur Verfolgung von privilegierten Zugriffen 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.

NR.	PRÜFUNGSHANDLUNGEN FÜR EIN COMPLIANT EMERGENCY ACCESS MANAGEMENT
1.	**Anwendungsbereich des Notfallbenutzerkonzepts 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 (PlugIn-Systeme), für die EAM angewendet wird?** ***Check:*** *Transaktion SM59, alle an den produktiven GRC-Mandanten angebundenen PlugIn-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.* **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.

NR.	PRÜFUNGSHANDLUNGEN FÜR EIN COMPLIANT EMERGENCY ACCESS MANAGEMENT
2.	**Definition von kritischen Berechtigungen zur Aufnahme in ein dediziertes Notfallbenutzerkonzept** **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 Notfallbenutzerprozess 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/Änderung von neuen/existierenden Notfallbenutzern (FFIDs)** **Kontrollziel: Bei der Anlage von technischen Benutzern, hier FFIDs, und deren Eignern (hier Owner/Controller) werden Benutzerantragsverfahren verwendet, die angemessen sind.** Risiko: Unangemessene Anlage und Zuordnung von Notfallbenutzern.
3.1.	Wie werden technische Benutzer, insbesondere FFIDs auf den PlugIn-Systemen angelegt? Wird die Einrichtung der FFIDs adäquat genehmigt? Ist der Benutzerkreis für die Beantragung von FFIDs entsprechend der Kritikalität eingeschränkt? Wie erfolgt die Nominierung und Benutzeranlage der FF-Owner? Für die Prüfung der Benutzer durch GRC selbst bitte Prüfungshandlungen aus 9.4.2.1 UAM beachten. Gibt es einen Prozess zur regelmäßigen Überprüfung der Angemessenheit aller Notfallbenutzer?
4.	**Genehmigung der Notfallbenutzer-Zuordnung** **Kontrollziel: Die Benennung von FF-Ownern erfolgt nachvollziehbar und zusammenhängend zu dem Risiko, das sich hinter dem Zugriff verbirgt. Es ist sichergestellt, dass Firefighter nicht ihre eigene Zuordnung genehmigen.** Risiko: Inadäquate Genehmigung des Notfallbenutzerzugriffs kann zu unsachgemäßem Einsatz dieser führen.
4.1.	Welche Verantwortlichen werden in den Nominierungsprozess mit eingebunden? Gibt es eine Plausibilität hinter der Genehmigerermittlung? 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) Genehmigern überein? ***Check:*** *NWBC-Einrichtung > Notfallzugriffszuordnung > Verantwortliche (Owners) und Notfallzugriffsbearbeitung > Kontrolleure*

NR.	PRÜFUNGSHANDLUNGEN FÜR EIN COMPLIANT EMERGENCY ACCESS MANAGEMENT
4.2.	Wie ist sichergestellt, dass der FF-Owner in den Beantragungsprozess eingebunden ist? Wird der Genehmigungsworkflow zur Beantragung/Zuordnung von FFIDs in UAM 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 Genehmigerstufen und Genehmiger (Bearbeiter-ID) aus.* *Prüfen Sie über NWBC > Zugriffsverwaltung > Zugriffsanforderungsverwaltung > Anforderungen suchen, die genehmigten EAM-Anträge und validieren die Angemessenheit der Genehmiger*
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 PlugIn-Einstellungen gesetzt sind und entsprechende Berechtigungen für FF-Endbenutzer (auf dem Zielsystem) vorhanden sind. ***Check:*** *SPRO > GRC PlugIn > Access Control > PlugIn-Konfigurationeinstellungen bearbeiten, validieren Sie Parameter: 1089, 1090, 4000, 4001, 4008, 4010 auf Angemessenheit* *Check: SPRO > GRC PlugIn > Access Control > User-Exits für PlugIn-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 Kontrolleure 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 Kontrolleure 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 Logfiles zur Review durch den Kontrolleur erfolgt in Abhängigkeit der Taktung des Batchjobs 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.

9.4.1.2. Sicherheitskritische Parameter für das Emergency Access Management

Die globalen Konfigurationseinstellungen sind mandantenabhängig 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 kundenindividuell zu validieren.

PARA-METER-ID	BESCHREIBUNG	STANDARD-WERT	BEST-PRACTICE-EMPFEHLUNG	KOMMENTAR
1113	Access Control E-Mail-Absender	WF-BATCH	kunden-spezifisch auszuprägen	Dieser technische Benutzer verwaltet die GRC-Workflows und muss entsprechend ausreichende Berechti-gungen 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 der Ap-plikationsart entstehen neue Anforderungen an die EAM-Prozesse.
4001	Standard-Firefighter-Gültigkeitszeitraum (Tage)	‹blank›	1	Anzahl der Tage für die Gültigkeit der FF-Zuordnung. **Hinweis:** Diese Stan-dardeinstellung kann im FF-Antrag (via UAM) durch den Antragsteller oder bei der manuellen Zuordnung durch den EAM-Administrator angepasst werden.

PARA-METER-ID	BESCHREIBUNG	STANDARD-WERT	BEST-PRACTICE-EMPFEHLUNG	KOMMENTAR
4002	E-Mail sofort senden	JA	JA	Ad hoc Benachrichtigung des FF-Kontrolleurs, dass betroffene FFID im Einsatz ist.
4003	Änderungs-protokoll abrufen	JA	JA	Aktivierung der Abfrage des Change Logs aus dem PlugIn-System
4004	Systemprotokoll abrufen	JA	JA	Aktivierung der Abfrage des System Logs aus dem PlugIn-System
4005	Revisionsprotokoll abrufen	JA	JA	Aktivierung der Abfrage des Audit Logs aus dem PlugIn-System
4006	BS-Befehls-protokoll abrufen	JA	JA	Aktivierung der Abfrage des O/S Command Log aus dem PlugIn-System
4007	Benachrichtigung für Protokoll-berichtausführung sofort senden	JA	JA	Sofortige Benachrich-tigung des FF-Kontrol-leurs zum Review des Log Files **Hinweis:** Führend ist hier die Taktung des Jobs GRAC_SPM_LOG_ SYNC_UPDATE.
4008	Firefighter-Benutzeranmelde-benachrichtigung senden	JA	JA	Ad hoc Benachrichtigung des FF-Kontrolleurs, dass betroffene FFID im Einsatz ist.
4009	Protokollbericht-ausführungs-Benachrichtigung	JA	JA	Sofortige Benachrich-tigung des FF-Kontrol-leurs zum Review des Log Files **Hinweis:** Führend ist hier die Taktung des Jobs GRAC_SPM_LOG_ SYNC_UPDATE.

PARA-METER-ID	BESCHREIBUNG	STANDARD-WERT	BEST-PRACTICE-EMPFEHLUNG	KOMMENTAR
4010	Firefighter-ID-Rollenname	SAP_ GRAC_ SMP_FFID	kunden-spezifisch auszuprägen	Die hier definierte Rolle muss der technischen Rolle entsprechen, die auf den PlugIn-Systemen den FFIDs zugeordnet wird.
4012	Standardbenutzer für das Weiterleiten des Revisionspro-tokoll-Workflows	2	2	Aufgrund der Sensi-bilität der Daten wird empfohlen, dass das Log File nur innerhalb einer eingeschränkten Gruppe weitergeleitet werden kann. Hier bietet sich die Gruppe der FF-Kontrolleure an. Die Weiterleitung kann auch ausgeschlossen werden.
4013	Firefighter-ID-Ver-antwortlicher kann Anforderung für seine Firefighter-ID senden	JA	NO	Sicherstellung, dass eine Funktions-trennung im EAM-Prozess gewährleistet ist.
4014	Firefighter-ID-Ver-antwortlicher kann Anforderung für kontrollierte Fire-fighter-ID senden	JA	NO	Sicherstellung, dass eine Funktions-trennung im EAM-Prozess gewährleistet ist.
4015	Dezentrales Fire-fighting aktivieren	NO	kunden-spezifisch auszuprägen	Aufgrund der Nutzbar-keit des Access Request Workflows für die genehmigungspflichtige FFID-Zuordnung wird das zentrale Firefighting empfohlen. Allerdings ist auch der dezentrale Ansatz zuläs-sig, sofern sichergestellt ist, dass die Genehmi-gung und Zuordnung der FFIDs angemessen ausgeprägt ist.

9.4.1.3. 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 2.4.1.1 genannten Risiken wird hergestellt.

BERECHTIGUNGSOBJEKT	FELDWERT	BESCHREIBUNG	MAPPING ZU RISIKO
GRAC_ ASIGN	ACTVT - 01 ACTVT - 02 ACTVT - 06 ACTVT - 70 GRAC_OWN_T - FFCR GRAC_OWN_T - FFCU GRAC_OWN_T - FFID GRAC_OWN_T - FFRO	Im NWBC können mit der Funktion „Access Control Verantwortliche" Mitarbeiter für die Ausführung von Genehmigungsstufen und Kontrollen im EAM-Umfeld ernannt werden. Diese Ernennung ist verpflichtend, um Mitarbeiter zu Firefighter-Ownern oder Firefighter-Kontrolleuren zu definieren und hierzu konkreten FFIDs zuzuordnen. Das Berechtigungsobjekt GRAC_ASIGN steuert aus, zu welchen Funktionen Mitarbeiter ernannt werden können (bspw. Firefighter-Owner via GRAC_OWN_T - FFID oder Firefighter-Kontrolleur via GRAC_OWN_T - FFCU).	Nr. 2: „Gibt es Prozesse zur Neuaufnahme von neuen FFIDs und die Nominierung von adäquaten Eignern (Owner/Controller)?" Überprüfung, welcher Mitarbeiter über die Rechte zur Ernennung von FF-Ownern und FF-Kontrolleuren verfügt, bspw. über die Transaktion SUIM oder via GRC-Regelwerk.
GRAC_ FFOBJ	ACTVT - 01 ACTVT - 02 ACTVT - 06	Das Objekt erlaubt die manuelle Zuordnung von Firefighter-IDs zu Endanwendern, sofern der Workflow für die Beantragung von FFID-Zuordnungen durch die manuelle Administration ergänzt/unterstützt werden soll.	Nr. 4: „Welche Verantwortlichen werden in den Nominierungsprozess mit eingebunden? Gibt es eine Plausibilität hinter der Genehmigerermittlung?" Erfolgt die Zuordnung ohne Workflow, ist zu prüfen, welche Mitarbeiter über die Berechtigungen verfügen. Ein workflowunterstützter Vergabeprozess ist klar zu präferieren.

BERECHTIGUNGS-OBJEKT	FELDWERT	BESCHREIBUNG	MAPPING ZU RISIKO
GRAC_ FFOWN	ACTVT - 01 ACTVT - 02 ACTVT - 06 ACTVT - 70	Das Objekt erlaubt die Zuordnung Verantwortlicher zu Firefighter-IDs.	Nr. 4: „Welche Verantwortlichen werden in den Nominierungsprozess mit eingebunden? Gibt es eine Plausibilität hinter der Genehmigerermittlung?" **Risiko EAM_03:** „Wie erfolgt die Nominierung und Benutzeranlage der FF-Owner?" Nach der Ernennung von Mitarbeitern zu Firefighter-Verantwortlichen erfolgt die konkrete Zuordnung derer zu Firefighter-IDs mit dieser Berechtigung. Nur eine stark eingeschränkte Gruppe von Mitarbeitern darf über das Recht der FFID-Owner-Zuordnung verfügen, um die inadäquate Ernennung von Firefighter-Verantwortlichen zu verhindern. Prüfung, welcher Mitarbeiter über die Rechte zur Zuordnung von FF-Ownern verfügt.
GRAC_ OWNER	ACTVT - 01 ACTVT - 02 ACTVT - 06 ACTVT - 70 ACTVT - 78	Das Objekt erlaubt die Zuordnung von Kontrolleuren zu Firefighter-IDs.	Nr. 4: „Welche Verantwortlichen werden in den Nominierungsprozess miteingebunden? Gibt es eine Plausibilität hinter der Genehmigerermittlung?" Nach der Ernennung von Mitarbeitern zu Firefighter-Kontrolleuren erfolgt die konkrete Zuordnung derer zu Firefighter-IDs mit dieser Berechtigung. Nur eine stark eingeschränkte Gruppe von Mitarbeitern darf über das Recht der FFID-Kontrolleur-Zuordnung verfügen, um die inadäquate Ernennung von Firefighter-Kontrolleuren zu verhindern. Prüfung, welcher Mitarbeiter über die Rechte zur Zuordnung von FF-Ownern verfügt.

BERECHTIGUNGS-OBJEKT	FELDWERT	BESCHREIBUNG	MAPPING ZU RISIKO
S_TCODE	S_TCODE – GRAC_SPM	Die Berechtigung erlaubt den Zugriff auf die Firefighter-Startseite. Von hieraus erfolgt der Absprung mittels FFIDs auf die angebundenen Systeme (zentralisiertes Firefighting), sofern der Zugriff auf die FFID genehmigt wurde (workflowgesteuerter Prozess) oder die FFID dem Benutzer zugeordnet wurde (manueller Prozess).	Nr. 3: „Ist der Benutzerkreis für die Beantragung von FFIDs entsprechend der Kritikalität eingeschränkt?" Es ist eine Erhebung darüber vorzunehmen, welche Mitarbeiter 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 Unternehmen. Erhält ein großer Anteil der Mitarbeiter das Recht für die Transaktion GRAC_SPM, sind die EAM-Prozesse im Unternehmen zu hinterfragen.

9.4.2. PRÜFUNG DES USER ACCESS MANAGEMENT

9.4.2.1. Prozess Design User Access Management

Das User Access Management stellt in SAP GRC die zentrale Komponente zur Abbildung von Antragsprozessen dar. Genauer ermöglichen Bestandteile und Funktionen von User Access 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 Benutzerantragsprozesses.

NR.	PRÜFUNGSHANDLUNGEN FÜR EIN COMPLIANT USER ACCESS 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 kritischen Systemen, möglicherweise über die automatische Zuordnung von Standardrollen.
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.* **Hinweis:** Für die vollständige Konfiguration von UAM auf spezifizierte Konnektoren sind weitere Einstellungen erforderlich, allerdings gibt o.g. Check bereits einen ersten Hinweis darauf, ob ein Zielsystem UAM 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 – 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 Benutzeranlage haben:* ***Check:** Tcode SUIM > Benutzer > Benutzer nach komplexen Selektionskriterien > Benutzer nach komplexen Selektionskriterien > S_Tcode = SU01* **Hinweis:** Weitere Spezifizierung der Abfrage im Falle von vorhandenen Ausnahmen erforderlich.

NR.	PRÜFUNGSHANDLUNGEN FÜR EIN COMPLIANT USER ACCESS MANAGEMENT
7.	**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 Genehmiger oder fehlerhaft beantragen.
7.1.	Wer darf Rollen für Zielsysteme via SAP GRC beantragen? Wie ist der Zugang auf das NWBC-Portal eingeschränkt? Wird das Portal als Selfservice verwendet? ***Check:*** *SPRO > GRC > Access Control > Benutzererstellung > Benutzeranmeldung aktivieren. Überprüfen und besprechen Sie mit dem zuständigen Administrator, ob das Selfservice für das GRC-Beantragungsportal aktiviert ist.* Die Einschränkung der Antragssteller (Requester) auf geeignetes Personal reduziert die fehlerhafte Beantragung von Rollen. Grundsätzlich muss die Beantragung jedoch nicht eingeschränkt sein, sofern sichergestellt ist, dass jeder Antrag genehmigungspflichtig ist. Bitte beachten Sie auch die Konfigurationsparameter für UAM 2033. Alle Rollen für Anforderer 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 zugehörigen Regel BRF+.* ***- 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.*
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 Genehmigungsworkflows im MSMP und die Regel BRF+. ***Check 1:*** *Tcode 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)*

NR.	PRÜFUNGSHANDLUNGEN FÜR EIN COMPLIANT USER ACCESS MANAGEMENT
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 Genehmigeragenten sind pro Workflow-Pfad hinterlegt?** ***Check:*** *SPRO > GRC > Access Control > Workflow für Access Control > MSMP-Workflows bearbeiten. Überprüfen Sie die vorhandenen Bearbeiter-IDs in Schritt 3 sowie die hinterlegten BearbeiterIDs 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 (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: Sicherheitsverantwortlicher oder der Ansprechpartner ist eine Gruppe oder Person, die eine sekundäre Genehmigung für Zugriffsanforderungen und Prüfungen erteilen kann. Dieser muss über die Access-Control-Verantwortung im NWBC gekennzeichnet werden.*
9.2.	Bitte beachten Sie auch die Auswegsbedingungen (Escape Path) und den dafür hinterlegten Pfad. Dies ist insbesondere wichtig, falls Genehmiger nicht gefunden werden, bspw. im Falle von fehlenden Rolleninhabern. 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 Ja gesetzt ist, sollte überprüft werden, wie die Ermittlung von Genehmigern, bspw. Rolleneigner, sichergestellt wird. Siehe auch Prüfungshandlung 2.4.3.1 für BRM.

9.4.2.2. Sicherheitskritische Parameter für das User Access Management

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

PARA-METER-ID	BESCHREIBUNG	STANDARD-WERT	BEST-PRACTICE-EMPFEHLUNG	KOMMENTAR
1071	Risikoanalyse für Formularabgabe aktivieren	NO	JA	Der Parameter erzwingt die Ausführung der Risikoanalyse bei der Beantragung. So können konfliktäre Anträge bereits beim Beantrager identifiziert und vermieden werden. Die Beantragung kann grundsätzlich trotzdem erfolgen.
1072	Minderung von kritischem Risiko vor Genehmigung von Anforderung erforderlich	NO	JA (kundenspe-zifisch auszu-prägen)	Die Kompensierung von konfliktären Benutzer-anträgen sollte grund-sätzlich systemseitig ermöglicht werden. Ob dies erzwungen werden kann, sodass konfliktäre Anträge sonst nicht ge-nehmigt werden können, ist in Abhängigkeit des Risikoappetits individuell zu bewerten.
2031	Alle Rollen für Genehmigenden zulassen	JA	JA	Die Genehmigungs-fähigkeit von Rollen sollte weniger zentral eingeschränkt, sondern individuell in Abhängig-keit der Rollenkritikalität realisiert werden.
2032	Rolleneinschrän-kungsattribut des Genehmigenden	‹empty›	‹empty›	Falls in 2031 keine Einschränkung definiert wurde, ist dieser Parameter obsolet.

PARA-METER ID	BESCHREIBUNG	STANDARD-WERT	BEST-PRACTICE-EMPFEHLUNG	KOMMENTAR
2033	Alle Rollen für Anforderer zulassen	JA	kunden-spezifisch auszuprägen	Mit dem Parameter kann die Beantragung von spezifischen, insbesondere kritischen Rollen entsprechend des Benutzerkreises eingeschränkt werden. Siehe auch 2034.
2034	Rolleneinschränkungsattribut des Anforderers	‹empty›	kunden-spezifisch auszuprägen	Entsprechend der Definition in 2033 wird hier das Attribut selektiert, das die Einschränkung der Rollenauswahl für die Beantragenden steuert.
2038	Rollen ohne Genehmigende automatisch genehmigen	JA	JA	Der Parameter steuert die Möglichkeit zur Definition von Grundrollen (Default Roles), die Benutzer bei der Beantragung ohne Genehmigung initial erhalten. Es ist sicherzustellen, dass eine fehlerhafte Rollenbereitstellung ohne Genehmiger ausgeschlossen ist. Siehe auch Kapitel 2.4.3.1
2040	Zuordnungskommentare bei Ablehnung obligatorisch	NO	JA	Eine Ablehnung sollte im Sinne der vollständigen und nachvollziehbaren Dokumentation begründet werden. Dies wird durch den Parameter systemseitig erzwungen. **Hinweis:** Dies kann auch in den MSMP-Einstellungen in Abhängigkeit des Workflows gesteuert werden.

PARA-METER-ID	BESCHREIBUNG	STANDARD-WERT	BEST-PRACTICE-EMPFEHLUNG	KOMMENTAR
2043	Berechtigungs-objekt für Rollen-suche – Rollen-definition und -zuordnung	BOTH	kunden-spezifisch auszuprägen	Der Parameter ermöglicht die Einschränkung der Rollenauswahl in Abhängigkeit der Berechtigungsobjekte GRAC_ROLED und/oder GRAC_ROLEP. Ob diese Rolleneinschränkung verwendet wird, muss kundenspezifisch bewertet werden. Dies setzt allerdings voraus, dass die Beantragenden einen Benutzer auf dem GRC-System haben, was meistens nicht der Fall sein soll. **Hinweis:** Das GRC-System kann als Beantragungssystem mit Benutzerzugang ohne Berechtigungen konfiguriert werden.
5021	Prüfe Manager-ID für die spezifische User-ID	JA	JA	Im Falle der Genehmigungspflicht durch den Manager (Vorgesetzten) kann die Pflege im Benutzerantrag automatisiert bzw. mittels Abgleich mit einem LDAP/Corporate Directory validiert werden. Somit können Fehler in der manuellen oder automatischen Ermittlung von Manager ausgeschlossen werden.

9.4.2.3. Kritische Berechtigungen im User Access 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 UAM 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.

BERECHTIGUNGS-OBJEKT	FELDWERT	BESCHREIBUNG	MAPPING ZU RISIKO
GRAC_REQ	ACTVT – 01 ACTVT – 02	Das Berechtigungsobjekt gewährt mit dieser Ausprägung auf Aktivitätsebene einem Benutzer das Recht, um Zugriffsanträge zu stellen. Je nach Ausprägung des Workflows für den Access Request (SAP_GRAC_ACCESS_REQUEST) ist die Berechtigung als kritisch oder unkritisch zu bewerten.	Nr. 7: „Wer darf Rollen für Zielsysteme via SAP GRC beantragen?" Die Beantragung von Rollen wird durch das Berechtigungsobjekt GRAC_REQ gesteuert.

9.4.3. PRÜFUNG DES BUSINESS ROLE MANAGEMENT

9.4.3.1. Prozess Design Business Role Management

Mit dem Rollenbau stehen u.a. die in Kapitel 4.4 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.

NR.	PRÜFUNGSHANDLUNGEN FÜR EIN COMPLIANT 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 zur 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 (Rollenpflegemandanten) 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.* *Überprüfen Sie auch die Kennzeichnung der Standard-Mandanten 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 Produktionslinie 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** **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 Benutzerprovisionierung bereitgestellt, die nicht prozesskonform erstellt sind. Dies kann zu kritischen Zugriffen auf sensible Daten führen.

NR.	PRÜFUNGSHANDLUNGEN FÜR EIN COMPLIANT BUSINESS ROLE MANAGEMENT
11.1.	**Wie erfolgt der Rollenbereitstellungsprozess für die Provisionierung via UAM (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 Batchjob „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 > Methodikprozesse 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: Tcode BRF+ > Suche kundenspezifische 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. Batchjobs 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.* **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 9.4.3.3. 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 eines 4-Augen-Prinzips zur Vermeidung von Abweichungen des Minimalprinzips.

NR.	PRÜFUNGSHANDLUNGEN FÜR EIN COMPLIANT BUSINESS ROLE MANAGEMENT
12.1.	**Wie ist der Genehmigungsprozesse 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 Methodikprozesse und -schritte über folgenden Pfad: ***Check:*** *SPRO > GRC > Access Control > Rollenverwaltung > Methodikprozesse und Schritte definieren. Prüfen Sie auch hier die Regel BRF+, wie oben beschrieben.* *Überprüfen Sie den Rollengenehmigungsprozess in MSMP und 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 kundeneigenen Rollengenehmigungsprozess unter Schritt 5 „Pfade bearbeiten", welche Pfade, Genehmigungsstufen und Bearbeiter hinterlegt sind. Im Standard sollte ein einstufiger Genehmigungsprozess über den Rolleneigner (Role Content Approver) umgesetzt sein. Prüfen Sie ebenfalls die dazugehörige Regel BRF+, sofern dies verwendet wird.* *Sofern der Standard verwendet wird, prüfen Sie, welche Rolleneigner 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 Rolleneignern umgesetzt ist.* Die Genehmigerermittlung muss lückenlos und adäquat sein. Voraussetzung für die Durchführung von Genehmigeraktionen ist neben der Rolleneignerpflege 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 ausschließt.** 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 Benutzerzuordnung bereitstehen? ***Check:*** *SPRO > GRC > Access Control > Rollenverwaltung > Methodikprozesse und Schritte definieren. Prüfen Sie, ob es eine BRM Methodik gibt, die die Risikoanalyse nicht enthält. Zu beachten sind auch die Steuerungselemente über BRF+, sofern es Methoden ohne Risikoanalysen gibt.*

NR.	PRÜFUNGSHANDLUNGEN FÜR EIN COMPLIANT BUSINESS ROLE MANAGEMENT
13.2.	Wie wird ausgeschlossen, dass SoD konfliktäre Rollen für die Benutzerprovisionierung 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.* 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*

9.4.3.2. 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 kundenindividuell zu betrachten.

PARA-METER-ID	BESCHREIBUNG	STANDARD-WERT	BEST-PRACTICE-EMPFEHLUNG	KOMMENTAR
3005	Bei der Änderung von Rollenattributen Rollenmethodik zurücksetzen	Nein	Nein	
3009	Löschen der Rolle vom Backend zulassen	JA	Nein	
3010	Anhängen von Dateien zur Rollendefinition zulassen	JA	JA	
3011	Risikoanalyse vor Rollenerzeugung ausführen	JA	JA	
3012	Rollenerzeugung für mehrere Systeme zulassen	Nein	Nein	

PARA-METER-ID	BESCHREIBUNG	STANDARD-WERT	BEST-PRACTICE-EMPFEHLUNG	KOMMENTAR
3013	Credentials des angemeldeten Benutzers für Rollenerzeugung verwenden	Nein	JA	
3014	Rollenerzeugung mit Berechtigungsebenenüberschreitungen zulassen	Nein	Nein	Empfehlung: Keine SoD-Risiken auf Rollenebene erlauben.
3015	Rollenerzeugung mit kritischen Berechtigungsüberschreitungen zulassen	Nein	JA	
3016	Rollenerzeugung bei Verletzung der Aktionsebene zulassen	Nein	Nein	Empfehlung: Keine SoD-Risiken auf Rollenebene erlauben.
3017	Rollenerzeugung bei Verletzung der kritischen Aktion zulassen	Nein	JA	
3018	Rollenerzeugung bei Verletzung kritischer Rollen/Profile zulassen	Nein	Nein	
3019	Risikoanalyseergebnis einer Einzelrolle bei Massenrisikoanalyse überschreiben	Nein	JA	Hinweis: Dies erfolgt individuell pro Rolle, es werden nicht alle Rollen automatisch überschrieben.
3020	Erinnerungsbenachrichtigung zu Rollenzertifizierung	10	kundenspezifisch auszuprägen	

9.4.3.3. 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.

BERECHTIGUNGS-OBJEKT	FELDWERT	BESCHREIBUNG	MAPPING ZU RISIKO
GRAC_ ASIGN	ACTVT - 01 ACTVT - 02 ACTVT - 06 ACTVT - 70 GRAC_OWN_T - ROLE	Im NWBC können mit der Funktion „Access Control Verantwortliche" Mitarbeiter zu Rollenbeauftragten ernannt werden. Diese Ernennung ist verpflichtend, um Mitarbeiter 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 Änderungen von Rollen definiert." Prüfung, welcher Mitarbeiter über die Rechte zur Ernennung von Rollenbeauftragten verfügt.
GRAC_ RLMM	ACTVT - 38 GRAC_RLMMT - 01 (Massenrollenimport) GRAC_RLMMT - 02 (Massenrollenaktualisierung) GRAC_RLMMT - 03 (Massenrollenableitung) GRAC_RLMMT - 04 (Massenaktualisierung abgeleiteter Rollen) GRAC_RLMMT - 06 (Massenrollengenerierung)	Die Berechtigung erlaubt den Zugriff auf die Massenbearbeitungsfunktionen in BRM. Die Ausprägung 06 zur Massenrollengenerierung erlaubt die Aktivierung mehrerer Rollen in Produktion in einem Schritt. Ist der Workflow zur genehmigungspflichtigen Bearbeitung von Rollen (SAP_GRAC_ROLE_APPR) deaktiviert, so können massenhaft auf ihre Inhalte hin ungeprüfte Rollen in Produktion begeben (Massenrollengenerierung 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.	Nr. 11: „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 erzwingen wird. **Hinweis:** Die Rollenimportfunktion muss in Ausnahmefällen zur Verfügung stehen, sollte allerdings sehr restriktiv vergeben werden, da Genehmigungsprozesse und Risikoanalysen umgangen werden können." U.a. der Massenimport 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 Berechtigungen im Maße der beschriebenen Ausnahmeprozesse restriktiv vergeben?

BERECHTIGUNGSOBJEKT	FELDWERT	BESCHREIBUNG	MAPPING ZU RISIKO
GRAC_ROLED	GRAC_ROLE - * GRAC_ACTRD - 01 (Anlage) GRAC_ACTRD - 02 (Änderung) GRAC_ACTRD - 06 (Löschung) GRAC_ACTRD - 64 (Generieren) GRAC_ACTRD - V7 (Bestätigen)	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 auch das Generieren von Rollen. Über GRAC_ROLE findet die Aussteuerung statt, für welche Rollen die Aktivitäten der Anlage, Bearbeitung, Generierung etc. vorgenommen werden kann. Dieser Feldwert eignet sich damit zur organisatorischen Eingrenzung des Rollenadministrators. Prüfen Sie, ob ausgeschlossen ist, dass derjenige, der die Rolle erstellt und bearbeitet, gleichzeitig als Role Owner zugeordnet werden kann?	Nr. 10: „Wie ist der Gesamtprozess – von der Beantragung bis zur produktiven Realisierung – zur Erstellung und Änderungen von Rollen definiert." Die Möglichkeiten von der Bearbeitung der Rollen-„Meta-Daten" (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 Rückschluss darauf, welcher Mitarbeiter im Einzelnen bspw. über Bearbeitungs-, Lösch- oder Generierungsrechte verfügt.
GRAC_RLMM	ACTVT - 01 (Anlegen) ACTVT - 02 (Ändern) ACTVT - 06 (Löschen) ACTVT - 78 (Zuordnen)	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.

9.4.4. PRÜFUNG DES ACCESS RISK ANALYSIS

9.4.4.1. Prozess Design Access Risk Analysis

ARA bietet die Möglichkeit, mit Hilfe eines zu definierenden Regelwerkes 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/Funktionstrennungs-matrix (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 der Emergency Access Managements, des User Access Managements und des Business Role Managements. Die in den Vorkapiteln vorgestellten Prüfungshandlungen beziehen damit ARA bereits im 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.

NR.	PRÜFUNGSHANDLUNGEN FÜR DIE 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 Benutzern neu provisioniert und für bestehende Provisionierungen nicht mehr erkannt, da die integrierte Kontrolle in BRM sowie in UAM nicht möglich ist.
14.1.	Jeder Mitarbeiter im GRC, der Inhaber der Rolle zur Funktionsgenehmigung ist (im Standard: SAP_GRAC_FUNCTION_APPROVER), kann Änderungen von Funktionen des Regelwerks 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 Experten zuzuweisen, sollte die Genehmigungsstufe bei einer zentralen Compliance-Instanz liegen. Die inhaltliche Beurteilung und Freigabe einer etwaigen Funktionsänderung muss auf anderem Wege bspw. in einem Gremium aus Fachbereich, IT und Compliance erfolgen.
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 u.U. 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.

NR.	PRÜFUNGSHANDLUNGEN FÜR DIE ACCESS RISK ANALYSIS
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-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 Mitarbeiter 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 bspw. in den TXT-Details gepflegt und in die Produktion hochgeladen, erfolgt dies durch Nutzung der Zugriffsberechtigung auf die Transaktion GRAC_UPLOAD_RULES. *Erstellung einer Übersicht aller Mitarbeiter 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 Set hinzugefügt. Dieses wird erweitert. Bei Auswahl von „Überschreiben" werden sämtliche bereits bestehenden Regeln gelöscht, nur die Inhalte der Upload-Datei gelangen in die Produktion.

NR.	PRÜFUNGSHANDLUNGEN FÜR DIE ACCESS RISK ANALYSIS
17.	**Zugriff auf die Details der Prüfungslogik** **Kontrollziel: Es ist sicherzustellen, dass nur ein ausgewählter Kreis von Mitarbeitern Zugriff auf diese Funktionen erhält.** **Risiko:** SAP GRC stellt eine Funktion zur Verfügung, um das gesamte Regelwerk und somit die Prüflogik aus dem System runterzuladen. 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 Mitarbeiter im GRC, der Zugriff auf die Funktion zum Download des Regelwerks hat, kann die empfindlichen Informationen beziehen. Erstellung einer Übersicht der Mitarbeiter 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)?** ***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:** **Risiko:** Nachgelagerte Kontrollen, die der Mitigation bekannter Berechtigungsrisiken dienen, werden inhaltlich zu Lasten der Prüf-Effektivität und -Effizienz verhindert.

NR.	PRÜFUNGSHANDLUNGEN FÜR DIE ACCESS RISK ANALYSIS
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 Bearbeiung der mindernden Kontrolle", Export der Kontrolländerungen.* *Wie wurden die Kontrolländerungen dokumentiert und freigegeben?* ***Falls nein:*** *Wie erfolgt die Beantragung, Durchführung und Freigabe von Änderungen an den Kontrollinhalten? Wer ist berechtigt Änderungen durchzuführen?*

9.4.4.2. Sicherheitskritische Parameter für das Access Risk Analysis

Im Folgenden finden Sie die wesentlichen Konfigurations-Parameter für das Access Risk Analysis. Neben dem vorkonfigurierten Standardwert wird auch eine Best-Practice-Empfehlung gegeben. Selbstverständlich ist letztere kundenindividuell zu betrachten.

PARA-METER-ID	BESCHREIBUNG	STANDARD-WERT	BEST-PRACTICE-EMPFEHLUNG	KOMMENTAR
1001	Funktionsänderungs-protokoll aktivieren	JA	JA	
1002	Risikoänderungsproto-koll aktivieren	JA	JA	
1003	Organisationsregelproto-koll aktivieren	JA	JA	
1004	Zusatzregelprotokoll aktivieren	JA	JA	
1005	Protokoll für kritische Rolle aktivieren	JA	JA	
1006	Protokoll für kritisches Profil aktivieren	JA	JA	
1007	Regelwerk-Änderungs-protokoll aktivieren	JA	JA	
1008	Rollenänderungs-protokoll aktivieren	JA	JA	

PARA-METER-ID	BESCHREIBUNG	STANDARD - WERT	BEST-PRACTICE-EMPFEHLUNG	KOMMENTAR
1011	Standardablaufzeit für Zuordnungen zu mindernden Kontrollen (in Tagen)	365	Kunden-spezifisch auszuprägen	Die Standard-Anzahl an Tagen bis zum Ablauf einer Risikomitigation. Diese Anzahl kann bei der Zuordnung über-schrieben werden.
1012	Regel-ID auch für Minderungszuord-nung berücksich-tigen	Nein	JA	
1013	System für Minde-rungszuordnung berücksichtigen	Nein	JA	
1021	Organisations-regeln für andere Anwendungen berücksichtigen	Nein	JA	
1023	Standardberichts-art für Risiko-analyse	2	1-4	Um mehr als einen Eintrag vorzunehmen, muss der Parameter mehrfach ausgewählt und gepflegt werden
1024	Standardrisikostufe für Risikoanalyse	3	Alle (*)	
1025	Standardregelwerk für Risikoanalyse	‹blank›	Kundenspe-zifisch auszu-prägen	Wenn vorhanden, sollte das zentrale Regelwerk als Standard hinterlegt werden
1026	Standardbenutzer-typ für Risiko-analyse	A	A	
1027	Offline-Risiko-analyse aktivieren	Nein	Nein	Erfordert die Aktualisie-rung von Risikoanalyse-ergebnissen in Bezug auf Berechtigungen, Rollen und Benutzer
1028	Abgelaufene Be-nutzer einschließen	Nein	Nein	

PARA-METER-ID	BESCHREIBUNG	STANDARD - WERT	BEST-PRACTICE-EMPFEHLUNG	KOMMENTAR
1029	Gesperrte Benutzer einschließen	Nein	Nein	
1030	Geminderte Risiken einschließen	Nein	Nein	
1031	Kritische Rollen und Profile ignorieren	JA	JA	
1032	Bei Benutzeranalyse Referenzbenutzer einschließen	JA	JA	
1033	Rolle/Profil-min-dernde Kontrollen in Risikoanalyse einschließen	JA	JA	Mitigierte Rollen in der Benutzeranalyse
1035	E-Mail-Benachrichti-gung an Überwacher der aktualisierten Risikominderung auf Objektebene senden	JA	JA	
1036	Alle Objekte in der Risikoanalyse anzeigen	Nein	JA	Diese Einstellung bezieht sich auf die SoD-Batch-Risk-Analyse. Zudem werden bei der Ad-hoc-Analyse alle geprüften Objekte mit angezeigt, unabhängig vom Ergebnis.
1037	Funktionstrennungs-ergänzungstabelle für die Analyse verwenden.	JA	JA	Bei Bedarf auszu-wählen
1038	FF-Zuordnungen in Risikoanalyse berücksichtigen	JA	Nein	

9.4.4.3. Kritische Berechtigungen im 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.

BERECHTIGUNGS-OBJEKT	FELDWERT	BESCHREIBUNG	MAPPING ZU RISIKO
GRAC_REP	ACTVT - 16 GRAC_REP - 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.

BERECHTIGUNGSOBJEKT	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 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, die insbesondere bei Massenänderungen in Frage 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 Produktion zur Verfügung steht. Benutzer- und Rollenprüfungen im Hinblick auf ihr Rechteset finden dann nicht statt.	Nr. 16: Mit Zugriff auf diese Transaktion erhält der Mitarbeiter die Möglichkeit, den gesamten Regel-Bestand der Produktion per Knopfdruck zu ändern oder zu löschen. Temporär stehen hierauf keine Regelverprobungen zur Verfügung. Prüfung, welcher Mitarbeiter über die Rechte zum Zugriff auf die Upload-Funktion verfügt.
GRAC_ FUNC	ACTVT - 01 ACTVT - 02 ACTVT - 06 ACTVT - 16 ACTVT - 78	Die Berechtigung erlaubt die Anlage und Bearbeitung von Regelwerks-Funktionen im NWBC sowie deren Zuordnung zu Risiken. Ist der Workflow zur genehmigungspflichtigen 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 wird die Neuanlage und Änderung von Funktionen ermöglicht. Damit kann auf Detailebene die Prüflogik verändert werden. Der Zugriff auf diese Berechtigung ist entsprechend einzuschränken.

BERECHTIGUNGSOBJEKT	FELDWERT	BESCHREIBUNG	MAPPING ZU RISIKO
GRAC_RISK	ACTVT - 01 ACTVT - 02 ACTVT - 06 ACTVT - 16 ACTVT - 78	Die Berechtigung erlaubt die Anlage und Bearbeitung von Regelwerks-Risiken im NWBC sowie die Ernennung des Risiko-Verantwortlichen. Ist der Workflow zur genehmigungspflichtigen Änderung von Risiken (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 zu Lasten der Compliance im Hinblick auf die implementierte Prüflogik der Provisionierungs- oder Rollenpflegeprozesse erfolgen.	Nr. 15: Mit der Berechtigung auf die angeführten Aktivitäten zum Berechtigungsobjekt GRAC_RISK wird die Neuanlage und Änderung von Risiken ermöglicht. Damit kann auf übergeordneter Risiko-Ebene die Prüflogik verändert werden, indem bspw. 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 ACTVT - 02 ACTVT - 06 ACTVT - 16 ACTVT - 78	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 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 Benutzerprovisionierung als auch zu Rollen selbst zugeordnet werden können.	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, kann mit dieser Berechtigung direkt und ungeprüft die Änderung der Kontrollen erfolgen.

BERECHTIGUNGS-OBJEKT	FELDWERT	BESCHREIBUNG	MAPPING ZU RISIKO
GRAC_ ASIGN	ACTVT - 01 ACTVT - 02 ACTVT - 06 ACTVT - 70 GRAC_OWN_T - MIAP GRAC_OWN_T - MIMO GRAC_OWN_T - RISK	Im NWBC können mit der Funktion „Access Control Verantwortliche" Mitarbeiter für die Ausführung von Genehmigungsstufen und Kontrollen im ARA-Umfeld ernannt werden. Diese Ernennung ist verpflichtend, um Mitarbeiter als Verantwortliche den Mitigierenden Kontrollen zuzuordnen (GRAC_OWN_T-MIAP), sie als Prüfungsdurchführende Mitigierender Kontrollen (GRAC_OWN_T-MIMO) oder 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 Mitarbeitern zur Kontrolldurchführung benötigt.

9.5. 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 Emergency Access Management, dem Business Role Management sowie der Access Risk Analysis heranzuziehen und funktional zu clustern. Die Berechtigungen zum User Access Management lösen im Zusammenspiel mit weiteren Rechten aus GRC keine Funktionstrennungskonflikte aus, da es sich hierbei um eine reine Workflow-Komponente handelt.

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

FUNKTION	INHALTE	BERECHTIGUNGSOBJEKTE
ARA_1	Upload und Download von Regelwerksinhalten, Bearbeitung von Funktionen und Risiken im Frontend	S_TCODE (mit GRAC_UPLOAD_RULES und GRAC_DOWNLOAD_RULES) GRAC_FUNC GRAC_RISK
ARA_2	Erstellung, Änderung und Zuordnung von Mitigierenden Kontrollen	GRAC_MITC GRAC_ASIGN
BRM_1	Anlegen und Ändern von Rollen	GRAC_ROLED
BRM_2	Administrationsaufgaben, Rollenimport, Rollenvergleich, Kontrollzuordnung	GRAC_RLMM GRAC_MITC GRAC_ASIGN
EAM_1	Zuordnung von FF-Verantwortlichen und Kontrolleuren in AC-Verantwortliche, Zuordnung von Verantwortlichen und Kontrolleuren zu Firefighter-IDs, Ausführen des Berichts zu SoD-Bereinigungen mittels Mitigierenden Kontrollen	GRAC_FFOBJ GRAC_ASIGN GRAC_FFOWN GRAC_OWNER GRAC_REP
EAM_2	Nutzung der Firefighter-Funktionalität als Endanwender	S_TCODE (mit GRAC_SPM oder /GRCPI/GRIA_EAM; Zentraler oder Dezentraler Ansatz)

Die drei Kern-Komponenten BRM, ARA und EAM sind aus Sicht der Berechtigungsvergabe und der Vermeidung von Funktionstrennungskonflikten inhaltlich in je zwei Funktionen zu unterscheiden. Jedes der nun aufgeführten Risiken ist jedoch dezidiert vor dem Hintergrund der organisatorischen Ausgestaltung und der Verwendung der Konfigurationsparameter zu betrachten. Je nach Aussteuerung kann die Kombination dieser Funktionen zu den in nachfolgender Abbildung dargestellten Risiken führen:

SOD MATRIX GRC REGELWERK	ARA_1	ARA_2	BRM_1	BRM_2	EAM_1	EAM_2
ARA_1: Administrationsaufgaben, Upload und Download von Regelwerksinhalten, Bearbeitung von Funktionen und Risiken im Frontend			Hoch			
ARA_2: Erstellung, Änderung und Zuordnung von Mitigierenden Kontrollen			Mittel			
BRM_1: Anlegen und Ändern von Rollen	Hoch	Mittel		Hoch		
BRM_2: Administrationsaufgaben, Rollenimport, Role Mining, Kontrollzuordnung			Hoch			
EAM_1: Nutzung der Firefighter-Funktionalität als Endanwender						Mittel
EAM_2: Administration: Zuordnung von FF-Ownern und Kontrolleuren, Ausführen der Berichts- zu SoD-Bereinigungen mittels Mitigierenden Kontrollen					Mittel	

Abbildung 3: SoD-Risiken im GRC

Die vier wesentlichen Risiken sind auch im Hinblick auf ihr Kritikalitätslevel spezifisch im Kontext des Unternehmens zu betrachten.

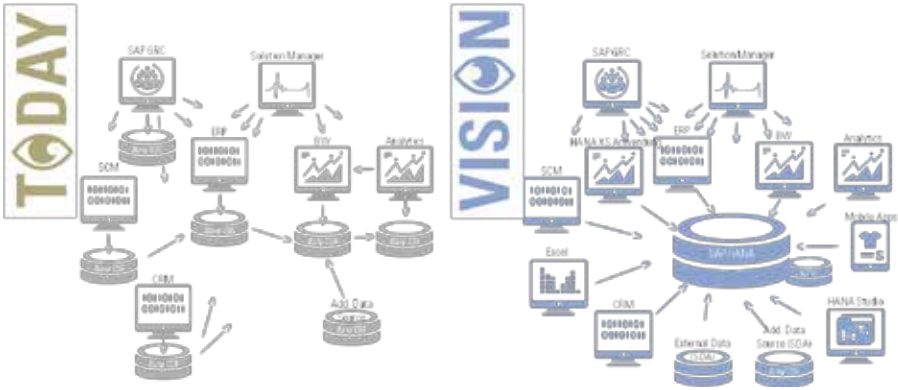
NR.	LEVEL	TITEL	BESCHREIBUNG
01	Hoch	ARA-Administration und Rollenpflege	Die direkte Bearbeitung des definierten Regelwerks und gleichzeitige Vergabe der Berechtigung zur operativen Rollenadministration erlaubt die Manipulation der Prüfroutinen zugunsten der Implementierung möglicherweise unzulässiger Rolleninhalte.
02	Mittel	ARA-Kontrollpflege und Rollenpflege	Die Funktion zur Zuordnung Mitigierender Kontrollen steht neben der Benutzeradministration auch der Rollenpflege zur Verfügung. Durch die Zuordnung von Kontrollen werden damit Risiken aus dem Rollenbau kompensiert. Die gemeinsame Vergabe der Berechtigungen zur Bearbeitung und Zuordnung solcher Kontrollen einerseits und der operativen Rollenadministration andererseits ist eine unzulässige Funktionsüberschreitung.
03	Hoch	BRM-Administration und Rollenadministration	Werden Berechtigungen beider Funktionscluster zusammen vergeben, eröffnen sich administrative BRM-Prozesse für operative Rollenadministratoren. Die u.U. erzwungene Risikoanalyse oder Genehmigung der Rollen kann so vom Rollenadministrator bspw. durch die Nutzung des Rollenimports umgangen werden. Risikobehaftete Rollen würden so nach einer Provisionierung in das produktive System gelangen.
04	Mittel	EAM-Administration und Firefighter-Endanwender	Findet eine Vermengung administrativer und operativer Rechte des Emergency Access Managements statt, können Kontrollmechanismen umgangen, möglicherweise unberechtigte Notfallzugriffe ermöglicht und inadäquate Prüfroutinen der durchgeführten Zugriffe implementiert werden.

Die gemeinsame Vergabe von Berechtigungen dieser Funktionen ist damit kritisch zu bewerten, zu hinterfragen und in die Prüfprozesse des GRCs mit einzubeziehen.

10. SAP HANA AUS REVISIONSSICHT

Neben den Datenbanken anderer Anbieter, wie z.B. Oracle, stellt SAP mit HANA eine eigene Datenbank für SAP-Anwendungen zur Verfügung. In-Memory-Technologie und spaltenorientierte Speichertechniken sorgen für enorme Geschwindigkeitsvorteile und versprechen gleichzeitig neue Anwendungsszenarien. SAP HANA bietet letztlich die Chance, wesentlich größere Datenmengen in wesentlich kürzerer Zeit zu verarbeiten. Umgekehrt werden mit den technologischen Möglichkeiten aber auch bestimmte Risiken stärker betont.

Grundsätzlich lassen sich ähnliche bzw. dieselben Risiken wie bei anderen Datenbankmanagementsystemen identifizieren. Darüber hinaus sollten beim Einsatz von SAP HANA weitere Risiken beleuchtet werden. Die Betrachtung der Risiken wird durch zwei wesentliche architektonische Änderungen bestimmt, die sich durch den Einsatz von SAP HANA in der Systemlandschaft ergeben (siehe Grafik unten). Neben potenziellen schnelleren Verarbeitungszeiten von Transaktionen sorgt die Speichertechnologie insbesondere für enorme Geschwindigkeitsvorteile bei analytischen Datenauswertungen. SAP HANA bietet damit die Möglichkeiten, in Echtzeit Analysen auf den transaktionalen Daten der SAP Business Suite durchzuführen. Die klassische Trennung zwischen Online-Analytical-Processing-Systemen (OLAP) (wie SAP ECC) und Online-Transaction-Processing-Systemen (OLTP) (wie SAP Business Objects) wird aufgelöst und auf einer Plattform zusammengeführt. Insgesamt ist es Ziel der SAP, dass SAP HANA als zentrale Datenplattform dient, über die Unternehmensanwendungen wie die Business Suite, SAP BW, BI-Anwendungen, Office-Anwendungen integriert werden. Dabei findet die Integration in der Regel schrittweise statt. Unternehmen starten bspw. mit SAP BW on HANA und sukzessive werden andere SAP-Systeme (und nicht SAP) auf einer (oder mehreren) zentralen SAP-HANA-Plattform betrieben (siehe exemplarische Abbildung unten).



Die zweite wesentliche architektonische Änderung ist, dass die architektonische Trennung zwischen Datenbank- und Anwendungsschicht (teilweise) aufgelöst wird. Die Verarbeitung und damit auch die Entwicklung wird zunehmend von der Anwendungs- in die Datenbank-Ebene verlagert, insbesondere um die Geschwindigkeitsvorteile der In-Memory-Technologie zu nutzen. Im Rahmen des Einsatzes von HANA XS wird die Trennung nahezu komplett aufgehoben, da Anwendungs- und Datenbankserver auf einer HANA-Plattform integriert sind.

Die architektonischen Änderungen haben auch entsprechende Implikationen auf die Sicherheit der Plattform. Wie der Abbildung zuvor zu entnehmen ist, gibt es deutlich mehr Schnittstellen und Kommunikationswege gegenüber einer klassischen SAP-Datenbank. Zudem erfolgt die Entwicklung und Modellierung zunehmend direkt auf der HANA-Plattform. Gleichzeitig greifen neben den bisher administrativ tätigen Benutzern abhängig vom Anwendungsszenario auch Entwickler oder Anwender der Fachbereiche, also in der Summe deutlich mehr Anwender, auf die Plattform zu. Beispielsweise ist es möglich, dass Anwender das ERP-Schema aus HANA in Excel einbinden und mit den Daten in der lokalen Anwendung arbeiten. Um eine entsprechende Zugriffskontrolle auf die Daten zu implementieren und bspw. zu verhindern, dass Gehaltsdaten gelesen werden können, muss ein Zugriffsschutz für die Anwender direkt in SAP HANA implementiert werden. Insgesamt gelten in einem solchen Szenario dieselben Sicherheitsanforderungen, die bisher eher auf SAP-Anwendungsebene gestellt wurden, analog für SAP HANA. Dies betrifft insbesondere die Zugriffskontrollen, die Transportkette (Entwicklungs-, Qualitätssicherungs- und Produktiv-Datenbankserver) sowie das Change-Management-Verfahren von Programmänderungen und Entwicklungen. Es ist dringend zu empfehlen, zunächst ein Verständnis über Zweck und Nutzungsszenarien von SAP HANA sowie deren Einbettung in die IT-Landschaft zu erlangen, um die beschriebenen Implikationen auf Sicherheit und Compliance zu verstehen, potenzielle Risiken zu identifizieren und daraus den Prüfungsfokus ableiten zu können.

10.1. RISIKEN

- Standard-Datenbankbenutzer haben noch das Initialkennwort des Auslieferungsstandes des SAP HANA Hardware Providers. Dies ermöglicht auch nicht autorisierten Dritten das unbefugte Anmelden an der Datenbank mit den bekannten Passwörtern.
- Schwachstellen der Anmeldekontrolle ermöglichen das unbefugte Anmelden an der Datenbank.
- Bei der Rollenkonzeption werden Funktionstrennungskonflikte nicht berücksichtigt.
- Endanwender erhalten unautorisierten Zugriff auf Unternehmensinformationen in SAP HANA.
- Benutzer besitzen Berechtigungen für Änderungen in der Produktion.
- Die Vergabe kritischer Berechtigungen erlaubt es, das interne Kontrollsystem zu umgehen.
- Das Berechtigungskonzept genügt nicht den gesetzlichen und unternehmensinternen Anforderungen.
- Technische Schnittstellen-Benutzer sind unzureichend abgesichert und ermöglichen unautorisierte Zugriffe auf SAP HANA.
- Die Kommunikation mit SAP HANA ist unzureichend abgesichert und erlaubt das unautorisierte Lesen oder Manipulieren von Daten im Transfer.
- Schwachstellen in der Betriebssystemkonfiguration ermöglichen unautorisierte Zugriffe auf die SAP-HANA-Server.

- Mangelnde Kontrollen im Transportwesen sorgen für nicht freigegebene Änderungen in der Produktion oder direkte Änderungen in der Produktionsumgebung.
- Nicht funktionsfähige Datensicherungskonzepte und Disaster-Recovery-Konzepte gefährden die Datenintegrität, Vertraulichkeit und Verfügbarkeit der Daten.
- Wesentliche sicherheitsrelevante Patches für SAP HANA sind nicht installiert, sodass Angreifer bekannte Sicherheitsschwachstellen ausnutzen können.
- Sicherheitsrelevante Systemereignisse werden nicht protokolliert und überwacht. Angriffe oder Sicherheitsverletzungen werden nicht erkannt und verfolgt.
- Es gibt keine Maßnahmen, die Sicherheitsschwachstellen identifizieren und beheben.

10.2. KONTROLLZIELE

- Die Standard-Datenbankbenutzer sind angemessen abgesichert.
- Die Funktionen zur Anmeldekontrolle sind sicher implementiert und werden regelmäßig kontrolliert.
- Es liegt ein formales und freigegebenes Berechtigungskonzept vor, das gesetzliche und unternehmensinterne Vorgaben angemessen berücksichtigt.
- Die Vergabe von Berechtigungen erfolgt rollen- und aufgabenspezifisch, dabei werden wesentliche Prinzipien der Funktionstrennung und der minimalen Rechtevergabe beachtet.
- Für Anwender der Fachbereiche sind angemessene Zugriffskontrollen in SAP HANA definiert.
- Benutzer haben keine Entwicklungsrechte in der Produktion. Rechte zum Ändern der produktiven Tabellen der SAP-Applikation sollten restriktiv und ausschließlich für Performancetuning- und Wartungszwecke vergeben werden.
- Die Nutzung kritischer Berechtigungen erfolgt eingeschränkt und angemessen.
- Die Kommunikation mit SAP HANA ist verschlüsselt und die Nutzung von Hashverfahren sichert die Integrität der Daten im Transfer.
- Die Schnittstellen-Benutzer sind angemessen abgesichert.
- Der Zugriff auf das Betriebssystem ist sicher implementiert.
- Es besteht ein ordnungsmäßiges und sicher implementiertes Software-Änderungs- und Entwicklungs-Verfahren.
- Es besteht ein funktionierendes Datenbanksicherungs- und Disaster-Recovery-Konzept.
- Es besteht ein funktionsfähiger Patch-Management-Prozess.
- Sicherheitsrelevante Ereignisse werden protokolliert und überwacht. Kritische Sicherheitsverstöße werden nachverfolgt.
- Regelmäßige Sicherheits-Prüfungen der Plattform identifizieren Sicherheitsschwachstellen und leiten kompensierende Maßnahmen ein.

10.3. PRÜFPROGRAMM: AUTHENTISIERUNG UND AUTORISIERUNG MIT SAP HANA

Prüfungshandlungen zur Beurteilung der Angemessenheit der Zugangs- und insbesondere Zugriffskontrollen sind auf das Einsatzszenario, die genutzten Anwendungen zur Kommunikation mit der Datenbank sowie die unternehmensspezifischen Anforderungen abzustimmen.
Die unten stehende abstrahierende Abbildung veranschaulicht potenzielle Zugriffspfade auf die SAP-HANA-Datenbank, abhängig vom geplanten Nutzungsszenario (basierend auf SAP HANA SP8 Rev. 82). Wesentliche Erkenntnis ist, dass
a) administrative und technische Schnittstellen-Benutzer
und abhängig vom Einsatzszenario zusätzlich Endanwender, also
b) Entwickler und Transportbenutzer zur Steuerung des Transports von Änderungen sowie
c) Anwender aus den Fachbereichen
direkt auf die Datenbank zugreifen können. Die Implementierung von Zugriffskontrollen für Endanwender stellt in Abhängigkeit vom Einsatzszenario eine wesentliche zusätzliche Sicherheitsanforderung dar und kann aus verschiedenen Gründen notwendig sein. Es besteht der Bedarf, dass Entwickler Informationsmodelle und andere Entwicklungsobjekte in der SAP-HANA-Datenbank erstellen, um analytische Auswertungen auf den Daten zu ermöglichen oder die Verarbeitung bestehender Transaktionen und Reports zu beschleunigen. Auch Benutzer der Fachbereiche können direkten Zugriff auf SAP HANA benötigen, bspw. zur Auswertung der Daten mittels geeigneter Analyse-Tools wie SAP Business Objects oder Microsoft Excel. Im Rahmen dessen kann es sinnvoll und notwendig sein, die Zugriffskontrollen für Endanwender direkt in SAP HANA zu implementieren, statt einen technischen Benutzer zur Kommunikation mit SAP HANA zu nutzen und diesen zu berechtigen. So lässt sich bspw. über entsprechende Berechtigungen in SAP HANA der Datenzugriff dergestalt steuern, dass Anwender nur auf Daten einer spezifischen Region oder eines bestimmten Buchungskreises zugreifen können. Eine Abbildung entsprechender Zugriffsregeln in SAP HANA abstrahiert dabei vom zugreifenden System, sodass die Zugriffskontrollen unabhängig von der zugreifenden Anwendung wirksam sind.
Die Notwendigkeit angemessener Zugriffskontrollen wird umso stärker betont, wenn transaktionale und analytische Systeme die SAP-HANA-Plattform gemeinsam nutzen.

Zusammenfassend ist zu empfehlen, zunächst ein Verständnis über die Nutzungsszenarien von SAP HANA sowie deren Einbettung in die IT-Landschaft zu erlangen, um potenzielle Risiken zu identifizieren und daraus den Prüfungsfokus ableiten zu können. Wichtige generelle Fragestellungen, die es vorab zu klären gilt, sind etwa:

- Welche Ziele werden mit dem Einsatz von SAP HANA verfolgt?
- Welche Nutzungsszenarien kommen zum Einsatz?
- Wie bettet sich SAP HANA generell in die Systemlandschaft ein?
- Welche Anwendungen kommunizieren mit der Datenbank?
- Erfolgt die Benutzeradministration anwendungs-/systemübergreifend über ein zentrales Tool oder dezentral mittels SAP HANA Studios? Für welche Zwecke wird das SAP HANA Studio genutzt?

NR.	AUTHENTISIERUNG UND AUTORISIERUNG MIT SAP HANA
1.	**Kontrollziel: Angemessene Absicherung von Standardbenutzern** **Risiko:** Beliebige Benutzer können sich Remote an der Datenbank unter einem der Standard-Datenbankbenutzer mit dem Standardkennwort des SAP-HANA-Hardware-Providers anmelden, können alle Tabelleninhalte einsehen und nicht autorisierte Änderungen durchführen.
1.1.	Sind die Standardkennwörter des Standard-Datenbankbenutzers SYSTEM entsprechend den Vorgaben aus dem internen Kontrollsystem und gängigen Best Practices geändert, Test, ob eine Anmeldung mit den Standardkennworten möglich ist. **Hinweis:** Im Betriebsmodell „Tailored Data Center" werden die Standardkennwörter durch den Provider der Appliance gesetzt. Leider ist derzeit kein Report verfügbar, der es ermöglicht, die Nutzung von Standard-Passwörtern zu identifizieren. Auch die Definition eines eigenen Reports ist derzeit nicht möglich, da die Passwörter als Hash-Werte abgespeichert sind und diese Werte sich für jede HANA-Instanz unterscheiden. Insofern empfiehlt es sich, nach entsprechenden Richtlinien der Anbieter zu fragen, in denen die Standardbenutzer und Passwörter beschrieben sind. Die Kennwörter sollten während der Installation geändert und im Key Store hinterlegt werden. Die Passwortwahl sollte sich an gängigen Standards und Empfehlungen orientieren.
1.2.	Gibt es eine Verfahrensanweisung, die den Umgang mit dem SYSTEM-Benutzer regelt?
2.	**Kontrollziel: Die Anmeldekontrolle über Verfahren sind sicher implementiert. (Anwendbar beim Einsatz von SSO-Lösungen Single-Sign-On für die Anmeldekontrolle)** **Risiko:** Schwachstellen in den genutzten Authentifizierungsmechanismen ermöglichen es, Zugriffskontrollen auszuhebeln.
2.1.	**Gibt es Benutzer, die sich parallel mit unterschiedlichen Authentifizierungsmechanismen an der Datenbank anmelden können?** *SQL> SELECT * FROM "SYS"."USERS"* *WHERE LENGTH(IS_PASSWORD_ENABLED||* *IS_KERBEROS_ENABLED || IS_SAML_ENABLED||IS_X509_ENABLED)<19;* *Klären, wieso verschiedene Mechanismen genutzt werden.*
2.2.	**Gibt es unterschiedliche Benutzer mit derselben External ID (Kerberos ID)?** *SQL> SELECT * FROM "SYS"."USERS" WHERE EXTERNAL_IDENTITY IN (* *SELECT EXTERNAL_IDENTITY FROM "SYS"."USERS"* *WHERE EXTERNAL_IDENTITY IS NOT NULL* *GROUP BY EXTERNAL_IDENTITY* *HAVING COUNT(*)>1* *);* ***Risiko:*** *SAP HANA prüft lediglich die External ID. Somit kann sich ein Benutzer mit unterschiedlichen SAP-HANA-Benutzern anmelden und Funktionstrennungen aushebeln.*
2.3.	Sind Kontrollen implementiert, die eine Mehrfachzuweisung der External ID für unterschiedliche Benutzer verhindern oder zumindest erkennen?

NR.	AUTHENTISIERUNG UND AUTORISIERUNG MIT SAP HANA
3.	**Kontrollziel: Die Bildung des Kennworts unterliegt Komplexitätsregeln. (Anwendbar beim Einsatz von Benutzernamen und Passwort zur Authentisierung und Authentifizierung an der Datenbank)** **Risiko:** Das Kennwort ist einfach und kann mit wenigen Anmeldeversuchen erraten werden. Der Benutzer verwendet wiederholt dasselbe Kennwort. Er überlistet den systemseitig erzwungenen Wechsel des Kennworts, wenn keine oder eine zu kurze Passworthistorie gewählt ist.
3.1.	Die Kennwortmindestlänge *minimal_password_length* ist festgelegt. Vorschlagswert: 8–10 Zeichen *SQL> SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE* *LOWER(PROPERTY) = 'minimal_password_length' AND VALUE < '8'('10')* (Das SQL-Statement zeigt einen Verstoß gegen den Vorschlagswert an.)
3.2.	Das Kennwort unterliegt Bildungsregeln. Der relevante Systemparameter ist *password_layout.* **Vorschlagswert:** Kennwort sollte mindestens einen Groß- und Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten (A1a$). *SQL> SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE* *LOWER(PROPERTY) = 'password_layout' AND VALUE != 'A1a$'* (Das SQL-Statement zeigt einen Verstoß gegen den Vorschlagswert an.) **Hinweis:** A1a$ kann variieren, indem andere Werte aus den Bereichen gewählt wurden, z.B. Z7x#
3.3.	Die Länge der Passworthistorie *last_used_passwords* ist vorbesetzt. **Vorschlagswert:** 15 Kennworte bei einem Wechsel, der alle 90 Tage erzwungen wird. *SQL> SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE* *(LOWER(PROPERTY) = 'last_used_passwords' AND VALUE < '15') OR* *(LOWER(PROPERTY) = 'maximum_password_lifetime' AND VALUE < '90')* (Das SQL-Statement zeigt einen Verstoß gegen den Vorschlagswert an.)
4.	**Kontrollziel: Die Gültigkeitsdauer eines Initialkennworts ist beschränkt. (Anwendbar beim Einsatz von Benutzernamen und Passwort zur Authentisierung und Authentifizierung an der Datenbank)** **Risiko:** Das Initialkennwort ist unbegrenzt gültig oder über einen zu langen Zeitraum. Das Initialkennwort ist bekannt oder es wird regelmäßig das gleiche Initialpasswort genutzt. Neu angelegte Benutzerkonten werden durch einen nicht autorisierten oder fremden Mitarbeiter genutzt.
4.1.	Die Gültigkeitsdauer *maximum_unused_initial_password_lifetime* eines initialen Kennworts ist definiert. **Vorschlagswert:** Die Gültigkeitsdauer überschreitet nicht fünf Tage. *SQL> SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE* *LOWER(PROPERTY) = 'maximum_unused_inital_password_lifetime' AND VALUE > '5'* (Das SQL-Statement zeigt einen Verstoß gegen den Vorschlagswert an.)

NR.	AUTHENTISIERUNG UND AUTORISIERUNG MIT SAP HANA
4.2.	Der Zeitpunkt für den Kennwortänderungszwang ist definiert (*maximum_unused_initial_password_lifetime*). **Vorschlagswert:** Erzwungener Wechsel des Kennworts nach mindestens 90 Tagen. *SQL> SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE (LOWER(PROPERTY) = 'maximum_password_lifetime' AND VALUE < '90')* (Das SQL-Statement zeigt einen Verstoß gegen den Vorschlagswert an.)
4.3.	Die Gültigkeitsdauer eines nicht benutzten Kennworts ist geregelt (*maximum_unused_productive_password_lifetime*). **Hinweis:** Dieser Parameter gibt die maximale Frist an, in der ein produktives, vom Benutzer gewähltes Kennwort gültig bleibt seit dem letzen erfolgreichen Login, wenn es nicht benutzt wird. Nachdem diese Frist abgelaufen ist, kann das Kennwort nicht mehr zur Authentifizierung verwendet werden. Der Benutzeradministrator kann die Kennwortanmeldung durch Zuweisen eines neuen Initialkennworts wieder aktivieren. **Vorschlagswert:** Gültigkeitsdauer eines nicht benutzten Kennworts höher setzen als die Dauer für den erzwungenen Wechsel des Kennworts (max. 180 Tage). *SQL> SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE LOWER(PROPERTY) = 'maximum_unused_productive_password_lifetime' AND VALUE > '180';* (Das SQL-Statement zeigt einen Verstoß gegen den Vorschlagswert an.)
4.4.	Der Benutzer muss warten, bis er sein Kennwort wieder ändern kann *(minimum_password_lifetime).* **Vorschlagswert:** 1, d.h. der Benutzer muss einen Tag warten, bis das Kennwort wieder durch den Benutzer geändert werden darf. *SQL> SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE LOWER(PROPERTY) = 'minimum_password_lifetime' AND VALUE <'1';* (Das SQL-Statement zeigt einen Verstoß gegen den Vorschlagswert an.)
5.	Kontrollziel: **Erhöhung des Zugriffsschutzes durch Benutzersperre nach mehrmaliger Falscheingabe. (Anwendbar beim Einsatz von Benutzernamen und Passwort zur Authentisierung und Authentifizierung an der Datenbank)** Risiko: Kennworte fremder Benutzerkennungen können über wiederholte Anmeldeversuche ausprobiert werden.
5.1.	Die maximale Anzahl der Falschanmeldungen bis zur Sperre der Benutzer ist definiert *(maximum_invalid_connect_attempts).* **Vorschlagswert:** Maximal 3 Passwortfehlversuche bis zur Sperre des Benutzers. *SQL> SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE LOWER(PROPERTY) = 'maximum_invalid_connect_attempts' AND VALUE > '3';* (Das SQL-Statement zeigt einen Verstoß gegen den Vorschlagswert an.)

NR.	AUTHENTISIERUNG UND AUTORISIERUNG MIT SAP HANA
5.2.	Die automatische Freischaltung der Benutzerkennungen ist definiert und führt zu einer automatischen Sperrung des Benutzers (*password_lock_time*). **Vorschlagswert:** *maximum_unused_productive_password_lifetime* * 1440 Minuten (erzwingt die faktische Sperrung des Benutzers. Entsprechend der Empfehlung in 4.3 ergibt sich ein Wert von 180*1440 = 259200 Minuten; Vorschlagswert der SAP ist 1440 Minuten, d.h., der Benutzer wird nach einem Tag entsperrt.) *SQL> SELECT PROPERTY, VALUE FROM M_PASSWORD_POLICY WHERE LOWER(PROPERTY) = 'password_lock_time' AND VALUE > '259200';* (Das SQL-Statement zeigt einen Verstoß gegen den Vorschlagswert an.) **Hinweis:** Aus betrieblichen Gründen kann es eine Notwendigkeit geben, den Wert runter oder auf 0 zu setzen, um technische Benutzerverbindung im Angriffsfall nicht zu sperren. Fehlversuche sollten über kompensierende Kontrollen identifiziert werden.
6.	**Kontrollziel: Es liegt ein dokumentiertes Berechtigungskonzept vor, das die gesetzlichen und unternehmensinternen Anforderungen berücksichtigt.** **Risiko:** › Es besteht kein formales Konzept. Das Berechtigungskonzept genügt nicht den gesetzlichen und unternehmensinternen Anforderungen.
6.1.	Liegt ein formales Berechtigungskonzept für SAP HANA oder ein Konzept, welches SAP HANA berücksichtigt, vor?
6.2.	**Berücksichtigt das Berechtigungskonzept gesetzliche und unternehmensinterne Anforderungen?** › Dokumentationsstandards › Rollen und Privilegien › Benutzer und Rechte › Risiken und Regeln › Prozesse, Kontrollen und Verantwortlichkeiten Offizielles Inkrafttreten des Dokuments
6.3.	**Sind folgende Informationen der Unternehmensorganisation verfügbar?** › Definition der Arbeitsplätze und Aufgaben › Definition der Zugriffselemente (Rollen, Profile) und die Zuordnung von Arbeitsplätzen zu Zugriffselementen in Form einer Matrix?
6.4.	Findet in regelmäßigen Abständen eine Rezertifizierung der Benutzer und vergebenen Berechtigungen (Kontrolle) statt und ist diese nachvollziehbar?

NR.	AUTHENTISIERUNG UND AUTORISIERUNG MIT SAP HANA
7.	**Kontrollziel: Die Vergabe von Berechtigungen erfolgt rollen- und aufgabenspezifisch, dabei werden wesentliche Prinzipien der Funktionstrennung und der minimalen Rechtevergabe beachtet.** **Risiko:** Beim Design der Rollen werden wesentliche Grundsätze nicht beachtet, wodurch inhärente Funktionstrennungskonflikte resultieren. Administrationsberechtigungen sind auch an Benutzer der Fachbereiche vergeben. Benutzer besitzen Berechtigungen zur Entwicklung und Freigabe von Änderungen in der Produktion. Der Zugriff auf Daten ist nicht angemessen eingeschränkt. **Hinweis:** Einen guten Einstiegspunkt für das Verständnis sowie die Modellierung unternehmensspezifischer SAP HANA Rollen bietet das folgende SAP Dokument: https://scn.sap.com/docs/DOC-53974
7.1.	Sind die Möglichkeiten der Funktionstrennung und zur minimalen Rechtevergabe umgesetzt?
7.2.	**Wie erfolgt der Zugriff von Benutzern auf Schema, Tabellen und Daten?** **Hinweis 1:** Erfolgt ein direkter Zugriff der Anwender auf die Datenbank, entstehen erweiterte Sicherheitsanforderungen. So ist sicherzustellen, dass Zugriffskontrollen definiert sind, die den Zugriff der Anwender auf die Datenbank steuern (siehe Einführung Kapitel 11.4). **Hinweis 2:** Endanwender sollten keine administrativen Berechtigungen (SYSTEM PRIVILEGES) und keine Berechtigung zur Änderung an SAP-Anwendungsobjekten haben. Für den lesenden Zugriff sind in der Regel analytische Privilegien auf Views, Privilegien auf _SYS_BI und _SYS_BIC (enthalten Metadaten und Daten über Views) sowie grundsätzliche Rechte für das Repository notwendig.
7.3.	**Wie wird der Zugriff von Administratoren auf die Datenbank gesteuert?** **Hinweis:** SYSTEM-Privilegien (die in der Regel mit ADMIN enden) sind Berechtigungen für den administrativen Zugriff auf die Datenbank. INIFILE ADMIN erlaubt beispielsweise die Änderungen der wesentlichen Systemkonfigurationen. Einen generellen lesenden Zugriff auf die Administrationskonsole ist mit der Berechtigung CATALOG READ möglich.

NR.	AUTHENTISIERUNG UND AUTORISIERUNG MIT SAP HANA
7.4.	**Wie erfolgt die Zugriffsteuerung für Entwicklung, Test, Freigabe und den Transport von Änderungen in die Produktion?** **Hinweis 1:** Der Transport von Entwicklungsobjekten wird über Transportartefakte (Delivery Units) sichergestellt. Diese Objekte müssen zur Nutzung in einer Umgebung manuell über das HANA Studio importiert oder über CTS+ transportiert werden. In der Regel ist der Import auch gleichzeitig mit einer Aktivierung und damit einer Freigabe für die Nutzung der Objekte in der Umgebung verbunden. Zum Zeitpunkt der Erstellung des Leitfadens hat SAP den SAP HANA Application Lifecycle Manager (HALM) für den Transport von Entwicklungsobjekten eingeführt. Mit Hilfe dieses Tools soll der automatische Import der Transportartefakte zwischen zwei HANA-Systemen möglich sein. Dadurch sollten auch die bis dato für die Produktion notwendigen Import (REPO.IMPORT, CREATE SCENARIO) und separaten Aktivierungsrechte (REPO.ACTIVATE_IMPORTED_OBJECTS, REPO.ACTIVATE_NATIVE_OBJECTS) für das Repository obsolet werden, da das HALM implizit in den SYS_REPO-Benutzer wechselt und die Änderungen vornimmt. Ein ändernder Zugriff auf das Repository der produktiven Umgebung sollte somit für den normalen Betrieb nicht notwendig sein, wodurch sich gleichzeitig das Risiko von unautorisierten Änderungen weiter reduziert. Insofern ist zu vermuten, dass der Einsatz des HALMs empfehlenswert ist. Inwiefern das Tool ein sicheres und ordnungsmäßiges Transportwesen unterstützt, konnte jedoch zum Zeitpunkt der Erstellung des Leitfadens nicht geprüft werden. **Hinweis 2:** Wesentliche Entwicklungsberechtigungen sind DEVELOPMENT (vordefinierte SAP HANA Rolle) oder REPO.EDIT_IMPORTED_OBJECTS, REPO.EDIT_NATIVE_OBJECTS, REPO.MAINTAIN_IMPORTED_PACKAGES und REPO.MAINTAIN_NATIVE_PACKAGES sowie Lese-Berechtigungen in den benötigten Schemas. Benutzer zum Import und Freigabe von Entwicklungsobjekten müssen in allen nachgelagerten Systemen angelegt sein (außer beim Einsatz des HALM, siehe Hinweis 1). Wesentliche Berechtigungen sind REPO.IMPORT, CREATE SCENARIO und möglicherweise noch REPO.ACTIVATE_IMPORTED_OBJECTS und REPO.ACTIVATE_NATIVE_OBJECTS für die nachträgliche Aktivierung von Entwicklungsobjekten. **Hinweis 3:** In SAP HANA SP8 ist es nicht möglich, den Entwickler auf dedizierte Repository-Objekte einzuschränken. So kann dieser sowohl Rollen als auch Schemas anlegen, ohne ROLE ADMIN und SCHEMA ADMIN Berechtigungen zu besitzen. Entwickler sollten, damit sie sich nicht eigene Rollen erweitern können, auf diese keine REPO.EDIT_*_OBJECTS und auch REPO.ACTIVATE_*_OBJECTS haben.
8.	**Kontrollziel: Die Nutzung kritischer Berechtigungen, Standard-Rollen und -Benutzer erfolgt eingeschränkt und angemessen.** **Risiko:** Benutzer besitzen kritische Berechtigungen, die es erlauben. Zugriffskontrollen auszuhebeln. Eine Übersicht aller Berechtigung eines Benutzers und Auflösung der Rollen sind in dem View *SQL> SELECT ** *FROM "SYS"."EFFECTIVE_PRIVILEGES"* *WHERE USER_NAME="<USERNAME>";* zu finden.

NR.	AUTHENTISIERUNG UND AUTORISIERUNG MIT SAP HANA
8.1.	**Kommt der SYSTEM-Benutzer zum Einsatz und in welchem Kontext?** **Hinweis:** Der SYSTEM-Benutzer besitzt nahezu Vollzugriff auf die Datenbank. Insofern sollte die Nutzung des SYSTEM-Benutzers im Regelbetrieb nicht möglich sein. Den SYSTEM-Benutzer benötigt man höchstens im Rahmen der initialen Konfiguration der Datenbank oder bei Datenbank-Upgrades. SAP empfiehlt, den Benutzer zu deaktivieren. **Die letzte Nutzung des Benutzers kann geprüft werden über:** *SQL> SELECT LAST_SUCCESSFUL_CONNECT* *FROM "PUBLIC"."USERS"* *WHERE USER_NAME='SYSTEM';* **Die Prüfung, ob der Benutzer deaktiviert ist:** *SQL> SELECT USER_DEACTIVATED* *FROM "PUBLIC"."USERS"* *WHERE USER_NAME='SYSTEM';*
8.2.	**Werden SAP HANA Standard-Rollen an Benutzer vergeben?** *SQL> SELECT GRANTEE_TYPE, GRANTEE, PRIVILEGE* *FROM "PUBLIC"."GRANTED_PRIVILEGES"* *WHERE PRIVILEGE IN ('CONTENT ADMIN')* *ORDER BY GRANTEE_TYPE, GRANTEE* *SQL> SELECT ROLE_NAME, GRANTEE FROM "PUBLIC"."GRANTED_ROLES"* *WHERE ROLE_NAME IN ('MONITORING')* *ORDER BY ROLE_NAME, GRANTEE* **Hinweis:** Es ist kritisch zu hinterfragen, ob vor dem Hintergrund des Prinzips der minimalen Rechtevergabe die Vergabe von SAP HANA Standard-Rollen angemessen ist. Die Standard-Rollen enthalten vielfach über den intendierten Nutzungskontext hinausgehende Berechtigungen. SAP empfiehlt deshalb, eigene Rollen zu definieren und die Standard-Rollen als Orientierungshilfe für die Ausprägung zu nutzen. Beispiele für solche Standard-Rollen bilden MODELING und CONTENT ADMIN zur Erstellung von Informationsmodellen und MONITORING zur betrieblichen Überwachung der Datenbank.

NR.	AUTHENTISIERUNG UND AUTORISIERUNG MIT SAP HANA
8.3.	**Ist die Berechtigung ROLE ADMIN in der Produktion vergeben?** *SQL> SELECT GRANTEE_TYPE, GRANTEE, PRIVILEGE* *FROM "PUBLIC"."GRANTED_PRIVILEGES"* *WHERE PRIVILEGE IN ('ROLE ADMIN', 'USER ADMIN')* *ORDER BY GRANTEE_TYPE, GRANTEE* **Hinweis:** ROLE ADMIN ermöglicht es, Rollen in der Produktion zu erstellen. Die Rollen können zum Zeitpunkt der Speicherung sofort produktiv genutzt werden. Somit können existierende Zugriffskontrollen ausgehebelt werden. Insbesondere da höchstwahrscheinlich für die Rollenerstellung mittels ROLE ADMIN auch weitergehende Berechtigungen auf Privilegien (mit GRANT OPTION) vergeben sein werden, um die Rollenverwaltung vornehmen zu können. Im Endeffekt besteht auch die Gefahr, dass bestehende und zugewiesene Rollen direkt verändert werden können, ohne dass Änderungen einer Kontrolle unterliegen. Anstatt ROLE ADMIN für die Rollenverwaltung zu nutzen, ist es empfehlenswert, Rollen als Design-Time-Objekte zu erstellen, sodass ein Transport der Rollen unterstützt und Funktionstrennungen implementiert werden können. Bei einer konsequenten Rollendefinition als Design-Time-Objekte ist damit die Nutzung von ROLE ADMIN zur Erstellung von Rollen obsolet. Dies entspricht auch dem empfohlenen Vorgehen der SAP (siehe: https://scn.sap.com/docs/DOC-53974) **Hinweis 2:** Für die Erstellung von SLT Schemas wird derzeit noch die Berechtigung ROLE ADMIN benötigt, um die SLT-Standardrollen durch den Hintergrundprozess erstellen zu lassen. Die Einbindung von SLT-Schemas ist jedoch keine Regelaktivität.
8.4.	**Sind Entwicklungsberechtigungen DEVELOPMENT, REPO.EDIT_IMPORTED_OBJECTS oder REPO.EDIT_NATIVE_IMPORTED_OBJECTS an Benutzer in der Produktion vergeben?** **Hinweis:** REPO.EDIT_IMPORTED_OBJETCS / REPO.EDIT_NATIVE_OBJECTS erlaubt die Änderung von Entwicklungsobjekten z.B. von Informationsmodellen, Stored Procedures oder Rollen. Benutzer mit diesen Berechtigungen können insbesondere über die „SAP HANA Development"-Perspektive ausbrechen und im Kontext eines technischen Benutzers (z.B. _SYS_REPO) beliebige Änderungen an Repository-Objekten durchführen.
8.5.	**Ist die Berechtigung DEBUG und ATTACH DEBUGGER an Benutzer in der Produktion vergeben?** **Hinweis:** Die Debug-Funktion sollte in der Regel nicht in der Produktion vergeben werden. Eine zeitlich beschränkte Verwendung von DEBUG im Produktivsystem sollte zwingend durch den Einsatz des SAP HANA Auditing protokolliert werden.
8.6.	**Ist die Berechtigung SYS_BIC_ALL in der Produktion vergeben?** **Hinweis:** Die Vergabe der Berechtigung _SYS_BI_CP_ALL in Verbindung mit der Vergabe von Lese-Berechtigungen auf ein Schema erlaubt es, sämtliche Views eines Schemas auszuführen und damit sämtliche Daten in diesem View zu lesen. Somit können implementierte Kontrollen zur Beschränkung des Zugriffs auf einzelne Views ausgehebelt werden. Insofern ist die Vergabe der Berechtigung kritisch zu hinterfragen.

NR.	AUTHENTISIERUNG UND AUTORISIERUNG MIT SAP HANA
8.7.	**Ist die Berechtigung DATA ADMIN in der Produktion vergeben?** **Hinweis:** Die Berechtigung DATA ADMIN erlaubt es, jegliche Daten in System Views zu lesen und jegliche DDL-Kommandos (Data Definition Language) in der Datenbank abzusetzen. Dies ermöglicht es, Änderungen an wesentlichen Tabellen und Views vorzunehmen. Insofern ist die Vergabe von DATA ADMIN kritisch zu hinterfragen. Notwendige DDL-Kommandos in der Produktion bspw. zum Reorganisieren von Tabellen können auch über eigene Rollen explizit auf ein Schema gesetzt werden.
9.	**Kontrollziel: Es ist ein formales Notfallbenutzerkonzept definiert. Der Notfallbenutzer ist angemessen abgesichert.** **Risiko:** › Es gibt keinen eigenen Notfallbenutzer: Systemadministratoren arbeiten im Normalbetrieb unter dem Standardbenutzer SYSTEM oder nutzen den Standardbenutzer SYSTEM als Notfallbenutzer. › Es gibt einen eigenen Notfallbenutzer, der nicht angemessen abgesichert ist.
9.1.	Ist für den Notfall mindestens eine Benutzerkennung eingerichtet, › die nicht der Standardbenutzer SYSTEM ist, › die die notwendigen weitreichenden Berechtigungen hat, › die mit einem komplexen Kennwort ausgestattet ist, › deren Kennwort an einem sicheren Ort zugriffsgeschützt aufbewahrt wird, wobei der Zugriff auf das Kennwort im 4-Augen-Prinzip erfolgen muss?
9.2.	Werden Aktionen unter dem Notfallbenutzer dokumentiert mindestens unter Angabe › des Grundes › des Zeitraums › der darunter tätigen Personen der Tätigkeiten, die damit durchgeführt wurden?
9.3.	Werden für einen Notfallbenutzer über das SAP HANA Auditing alle Ereignisse aller Audit-Klassen zwangsprotokolliert?
9.4.	Wird nach der Notfallaktion das Kennwort des Notfallbenutzers geändert?

10.4. PRÜFPROGRAMM: SICHERE KONFIGURATION DER SCHNITTSTELLEN VON SAP HANA

NR.	SICHERE KONFIGURATION DER SCHNITTSTELLEN VON SAP HANA
1.	**Kontrollziel: Die Kommunikation mit den SAP-HANA-Servern ist verschlüsselt und die Nutzung von Hashverfahren sichert die Integrität der Daten im Transfer.** **Risiko:** Die Datenübertragung erfolgt unverschlüsselt. Ein Angreifer (Man-in-the-Middle) kann die Kommunikation abhören und Passwörter abfangen und/oder Geschäftsdaten lesen und manipulieren.
1.1.	Erfolgt die Kommunikation mit unterschiedlichen Systemen (z.B. SAP HANA Studio, Replikationsserver, Solution Manager, Business Suite, SAP BI etc.) und der SAP-HANA-Datenbank sowie innerhalb von HANA-Servern bspw. im Scale-Out-Szenario oder für HANA-Disaster-Recovery-Server verschlüsselt? Generelle Einstellung zur verschlüsselten Kommunikation. *SQL> SELECT * FROM M_INIFILE_CONTENTS WHERE SECTION='communication' AND FILE_NAME='global.ini'* Der Cryptoprovider kann über den Parameter (KEY) sslcryptoprovider abgeleitet werden, sslkeystore und ssltrustore geben den Dateinamen und Pfad für den trust store und key store auf der HANA appliance an. Ist der Parameter sslenforce (KEY) mit TRUE (VALUE) gesetzt, akzeptiert SAP HANA ausschließlich verschlüsselte Datenbankverbindungen. Stichprobenprüfung der Verbindungseinstellungen von Benutzern im HANA Studio und/oder mittels einer Abfrage auf die View SYS.M_CONNECTIONS. Diese View führt alle aktiven und ruhenden Verbindungen zum HANA-Server auf. *SQL> SELECT CONNECTION_TYPE, IS_ENCRYPTED, COUNT(*)* *FROM "SYS"."M_CONNECTIONS"* *GROUP BY CONNECTION_TYPE, IS_ENCRYPTED* *ORDER BY IS_ENCRYPTED DESC* Das Ergebnis zeigt, ob und wie viele verschlüsselte und unverschlüsselte Verbindungen (aktiv und ruhend) existierten. **Hinweis 1:** Jegliche Verbindungen zur Datenbank und XS-Engine lassen sich beispielsweise mittels der Nutzung von OpenSSL oder CommonCrypto (TLS 1.0) verschlüsseln. Insbesondere sollten Verbindungen aus nicht vertrauenswürdigen Netzsegmenten verschlüsselt werden und solche, bei denen die Daten ein hohes Schutzniveau besitzen. **Hinweis 2:** Da laut SAP ab Rev74 nur noch die CommonCrypto unterstützt wird, sollte eine Implementierung entsprechend mit Hilfe dieser von SAP entwickelten Bibliothek erfolgen.
1.2.	**Sind Netzwerkkontrolle implementiert, die die Nutzung von Diensten einschränkt?** **Hinweis:** Aus Sicherheitsgründen empfiehlt es sich, nicht genutzte Ports weitreichend einzuschränken.

NR.	SICHERE KONFIGURATION DER SCHNITTSTELLEN VON SAP HANA
2.	**Kontrollziel: Die Schnittstellen-Benutzer sind angemessen abgesichert.** **Risiko:** Technische Schnittstellen-Benutzer sind unzureichend abgesichert, sodass Zugriffskontrollen mit den entsprechenden Benutzern ausgehebelt werden können.
2.1.	**Unterliegt der SAP‹SID› Benutzer, die für die Kommunikation und den Zugriff von SAP Anwendungen auf SAP HANA notwendig sind, Passwortkomplexitätsregeln?** **Hinweis:** Der SAP‹SID› Benutzer ist der technische Benutzer zum Zugriff von SAP Anwendungen wie SAP ECC, SAP BW etc. auf die Datenbank. Die Applikationsebene implementiert dabei die Zugriffskontrollen auf Applikationsebene. Nichtsdestotrotz muss der SAP‹SID› Benutzer separat in SAP HANA berechtigt werden. Eine direkte Anmeldung mit dem Benutzer ist derzeit technisch möglich und kann nicht unterbunden werden (SAP HANA SP7).
2.2.	Erfolgt die Berechtigungsvergabe an den SAP‹SID› Benutzer nach dem Prinzip der minimalen Rechtevergabe?
2.3.	**Welche weiteren technischen Benutzer sind zur Kommunikation mit anderen Systemen in HANA eingerichtet und welche Berechtigungen besitzen diese Benutzer?** **Hinweis:** Für die Kommunikation mit anderen Systemen wie etwa dem Solution Manager oder dem DBA Cockpit liefert SAP Standard-Rollen aus (in diesem Fall die Rolle DBA-COCKPIT). Deren Angemessenheit sollte jedoch kritisch geprüft werden, da bspw. die Rolle DBACOCKPIT die Konfiguration der Datenbank erlaubt (INIFILE ADMIN). Es ist möglich, eigene Rollen für die Benutzer zu definieren. Dies gilt im Übrigen auch für den SAP-OSS-Benutzer. Eine direkte Anmeldung mit diesen Benutzern an der Datenbank ist möglich. Seit SPS 8 steht ein neuer User Typ „Restricted User", der sich nicht direkt an der Datenbank anmelden kann, sondern nur über HANA XS, wenn die entsprechende XS-basierte Applikation ihm entsprechende Rollen zugewiesen hat. Eine Prüfung der Wirksamkeit dieses Mechanismus war im Rahmen der Erstellung des Leitfadens leider nicht möglich.

10.5. PRÜFPROGRAMM: ABSICHERUNG VON SAP HANA UNTER LINUX

SAP-HANA-Server werden auf Basis unterschiedlicher Modelle ausgeliefert und betrieben. Das derzeit gängigste Modell ist das des Tailored Data Centers, d.h., ein zertifizierte Partner liefert SAP HANA als Appliance aus. Vereinfacht ausgedrückt bedeutet dies, dass Hardware, Betriebssystem und Software vorkonfiguriert durch den Hardware-Lieferanten bereitgestellt werden.Die folgenden Ausführungen in diesem Kapitel beziehen sich lediglich auf dieses Auslieferungsmodell, da den Autoren keine Erfahrungen mit anderen Auslieferungsmodellen vorliegen.

Für die Sicherheit der Systeme bedeutet der Betrieb einer Appliance zunächst, dass Härtungsregeln zur Absicherung des Betriebssystems derzeit nur eingeschränkt umgesetzt werden können. SAP erlaubt es seinen Kunden zwar, inzwischen Betriebssystemeinstellungen zu ändern – es sei denn, SAP hat eine bestimmte Änderung explizit ausgeschlossen (siehe auch SAP Notes: 1730999: Configuration changes in HANA appliance, 1731000: Unrecommended configuration changes). Dennoch müssen Unternehmen Änderungen von Betriebssystemeinstellungen immer auch mit dem jeweiligen Hardware-Partner abstimmen. Insofern sind die Unternehmen auch auf die Härtung durch den Anbieter angewiesen. Dennoch können die Prüfungshandlungen zur Prüfung der Systemintegrität auf der Betriebssystemebene prinzipiell analog zum Kapitel Systemintegrität auf Betriebssystemebene durchgeführt werden. Darüber hinaus können einige weitere Prüfungen durchgeführt werden.

NR.	ABSICHERUNG VON SAP HANA UNTER LINUX
1.	**Kontrollziel: Angemessene Zugriffskontrollen unter Linux** **Risiko:** Schwachstellen in der Betriebssystemkonfiguration ermöglichen den nicht-autorisierten Zugriff auf die SAP-HANA Server.
1.1.	**Sind die Standard-Kennwörter des Appliance Providers der Standard-Benutzer des Betriebssystems nach einer Systeminstallation vor Produktivstellung geändert worden (*root, <SID>adm* und weitere Benutzer zur Verwaltung der Hardware/Appliance)?** *Test, ob eine Anmeldung mit den Standardkennwörtern möglich ist.* **Hinweis 1:** Die Standardkennwörter werden durch den Provider der Appliance gesetzt. Insofern empfiehlt es sich, nach entsprechenden Richtlinien der Anbieter zu fragen, in denen die Standardbenutzer und Passwörter beschrieben sind. Die Kennwörter sollten während der Installation geändert und im Key Store hinterlegt werden. Komplexe Passwörter sind zu wählen.
1.2.	Erfolgt die Anmeldung am Betriebssystem personalisiert und mittels starker Authentisierungsmechanismen?
1.3.	Ist die direkte Nutzung von root und *<SID>adm* per ssh deaktiviert?
1.4.	Ist der Zugriff auf das HOME-Verzeichnis sowie die Dateien eingeschränkt?
1.5.	Werden Benutzer-Kennwörter in Skripten zur automatisierten Durchführung administrativer Tätigkeiten im Klartext gespeichert oder wird durchgehend auf die Mechanismen des hdbuserstore zugegriffen?

NR.	ABSICHERUNG VON SAP HANA UNTER LINUX
1.6.	**Sind nicht benötigte Dienste abgeschaltet?** *Plausibilisieren der Liste aller offenen Ports* Bash› set IID=`cat /usr/sap/${SID}/SYS/global/hdb/install/config/sapprofile.ini | grep "SAPSYSTEM=" | awk -F "=" '{print $2}'`; \ netstat -apntu \ \| egrep -v "(ESTABLISHED\|CLOSE_WAIT)" \ \| egrep -v "(:3${IID}07|:3${IID}08)" \ \| egrep -v "(:3${IID}10)" \ | egrep -v "(:3${IID}01)" \ \| egrep -v "(:3${IID}02)" \ | egrep -v "(:3${IID}03\|:3${IID}15)" \ | egrep -v "(:3${IID}05\|:3${IID}17)" \ | egrep -v "(:64998|:64999|:65000|:80${IID})" \ \| egrep -v "(:5${IID}13)" \ | egrep -v "(:3${IID}00)" \ | egrep -v "(:1128 |:1129)" \ | egrep -v "(0.0.0.0:22 |:::22)" \ | egrep -v "(127.0.0.1:25 |::1:25)" \ | egrep -v "(:123)" \ | egrep -v "(:111)" \ | egrep -v "(:199)" \ | egrep -v "(:161)" \ | egrep -v "(:80)" \ | egrep -v "(:2301 |:2381)" \ | egrep -v "(:25375 |:25376 |:25393)" \ | egrep -v "(:681)"; \ unset IID Ergebnis zeigt zusätzlich geöffnete Ports
1.7.	Die SAP HANA Server sind im Standard gehärtet und garantieren ein äquivalentes Schutzniveau zu den Empfehlungen von SUSE Linux (siehe Link https://www.suse.com/documentation/sles11/singlehtml/book_hardening/book_hardening.html) bzw. den unternehmensspezifischen Unternehmen Härtungsregeln für SUSE Linux?

10.6. PRÜFPROGRAMM: SICHERES DATENBANKMANAGEMENT MIT SAP HANA

NR.	DATENBANKMANAGEMENT
1.	**Kontrollziel: Es besteht ein ordnungsmäßiges und sicher implementiertes Software-Änderungs- und Entwicklungs-Verfahren** **Risiko:** Die erforderlichen Funktionstrennungen eines geordneten Entwicklungs-, Tests- und Freigabeverfahrens sind nicht im SAP-System abgebildet. Schwachstellen bei der Implementierung des Software-Transport-Systems ermöglichen ein Umgehen der internen Kontrollen und gefährden System- und Datenintegrität.
1.1.	Wird die Datenbank mit von SAP freigebenden Revisionen regelmäßig auf dem neuesten Stand gehalten?
1.2.	Gibt es eine Entwicklungsrichtlinie für die Entwicklung in HANA sowie den sicheren Transport der Entwicklungsobjekte?
1.3.	Kommt eine Mehrsystemlandschaft für den ordnungsgemäßen Transport von Entwicklungs- und Änderungsobjekten zum Einsatz?
1.4.	Welche Mechanismen und Tools werden für den Transport der Entwicklungsobjekte genutzt? **Hinweis 1:** Grundsätzlich gibt es vier verschiedene Möglichkeiten für den Transport von Entwicklungsobjekten: **1** Transport mit Hilfe des HANA Studios **2** Transport mit Hilfe von CTS+ zum Transport von ABAP- und NON-ABAP-Entwicklungsobjekten **3** Transport mit Hilfe des Solution Managers zum Transport von ABAP-Objekten (Die Transportartefakte oder Delivery Units werden in diesem Fall einem ABAP-Objekt angehängt.) **4** Verwendung des SAP HANA Lifecycle Managers **Hinweis 2:** Zum Zeitpunkt der Erstellung des Leitfadens hat SAP den SAP HANA Application Lifecycle Manager (HALM) für den Transport von Entwicklungsobjekten eingeführt. Mit Hilfe dieses Tools soll der automatische Import der Transportartefakte zwischen zwei HANA-Systemen möglich sein. Dadurch sollten auch die bis dato für die Produktion notwendigen Import (REPO.IMPORT, CREATE SCENARIO) und separaten Aktivierungsrechte (REPO.ACTIVATE_IMPORTED_OBJECTS, REPO.ACTIVATE_NATIVE_OBJECTS) für das Repository obsolet werden, da das HALM implizit in den SYS_REPO-Benutzer wechselt und die Änderungen vornimmt. Ein ändernder Zugriff auf das Repository der produktiven Umgebung sollte somit für den normalen Betrieb nicht notwendig sein, wodurch sich gleichzeitig das Risiko von unautorisierten Änderungen weiter reduziert. Insofern ist zu vermuten, dass der Einsatz des HALMs empfehlenswert ist. Inwiefern das Tool ein sicheres und ordnungsmäßiges Transportwesen unterstützt, konnte jedoch zum Zeitpunkt der Erstellung des Leitfadens nicht geprüft werden.
1.4.	Wie ist sichergestellt, dass die Änderungsobjekte für die Produktion getestet und freigeben sind?
1.5.	Ist eine Versionskontrolle bei dem Import von Entwicklungsobjekten vorgesehen? **Hinweis:** Falls nicht der HALM im Einsatz ist, erfolgt das Einspielen der Delivery Unit, in denen die Entwicklungsobjekte zugewiesen sind, i.d.R. manuell. Dementsprechend ist sicherzustellen, dass die eingespielte Version der freigegebenen entspricht.

NR.	DATENBANKMANAGEMENT
2.	**Kontrollziel: Es ist ein angemessenes und funktionierendes Datenbanksicherungs- und Disaster-Recovery-Konzept definiert.** Risiko: Nicht funktionsfähige Datensicherungskonzept und Disaster-Recovery-Konzepte gefährden die Datenintegrität, Vertraulichkeit und Verfügbarkeit der Daten. Dies könnte unter anderem zum Verlust von Daten führen.
2.1.	Besteht ein Datenbanksicherungskonzept und was ist geregelt?
2.2.	Wie ist sichergestellt, dass keine Daten verloren gehen bzw. unvollständige Datensicherungen erkannt werden?
2.3.	Besteht ein Disaster-Recovery-Konzept und was ist geregelt?
2.4.	Werden die SAP-Mechanismen zur Datenreplikation eingesetzt, um Disaster-Recovery-Funktionalitäten für SAP HANA bereitzustellen? Sind bei der Nutzung der asynchronen Replikation kompensierende Maßnahmen definiert, die die konsistente Datenübertragung sicherstellen? **Hinweis:** SAP HANA unterstützt unterschiedliche Replikationsmechanismen zur Datenübertragung, die insbesondere für den Einsatz von Disaster-Recovery-Funktionalitäten eingesetzt werden. Bei der synchronen Replikation wartet die primäre Datenbank mit der Verarbeitung auf die Verarbeitungsbestätigung der sekundären Datenbank. Im Rahmen der asynchronen Replikation wartet die primäre Datenbank nicht auf die Verarbeitung in der sekundären Datenbank. Insofern steigt das Risiko des Datenverlustes. Dementsprechend sollten kompensierende Maßnahmen zur Überwachung der Replikation definiert und wirksam sein.
2.5.	**Welche Maßnahmen sind implementiert, um die Sicherheit der Datenreplikation zu unterstützen?** **Hinweis:** Es sind unterschiedliche Maßnahmen denkbar, die das Risiko vermindern, dass die Vertraulichkeit, Integrität und/oder Verfügbarkeit der Datenübertragung durch Angreifer verletzt wird. Beispiele solcher Maßnahmen können genereller Art sein, wie eine direkte, sichere Glasfaserkabel-Verbindung der beiden Rechenzentren, oder aber speziell für das SAP-HANA-Disaster-Recovery-Konzept definiert werden wie die Verschlüsselung des Datentransfers.
2.6.	Liegen Nachweise vor, die die Funktionsfähigkeit des Datenbanksicherungskonzeptes belegen? Werden regelmäßig Datensicherungen durchgeführt und diese geprüft? Werden die Datensicherungen geschützt?
2.7.	Liegen Nachweise vor, die die Funktionsfähigkeit des Disaster-Recovery-Konzeptes belegen? **Hinweis:** Es sollte ein periodischer Test des Disaster-Recovery-Konzeptes durchgeführt werden, um den Nachweis der Funktionsfähigkeit zu erbringen.

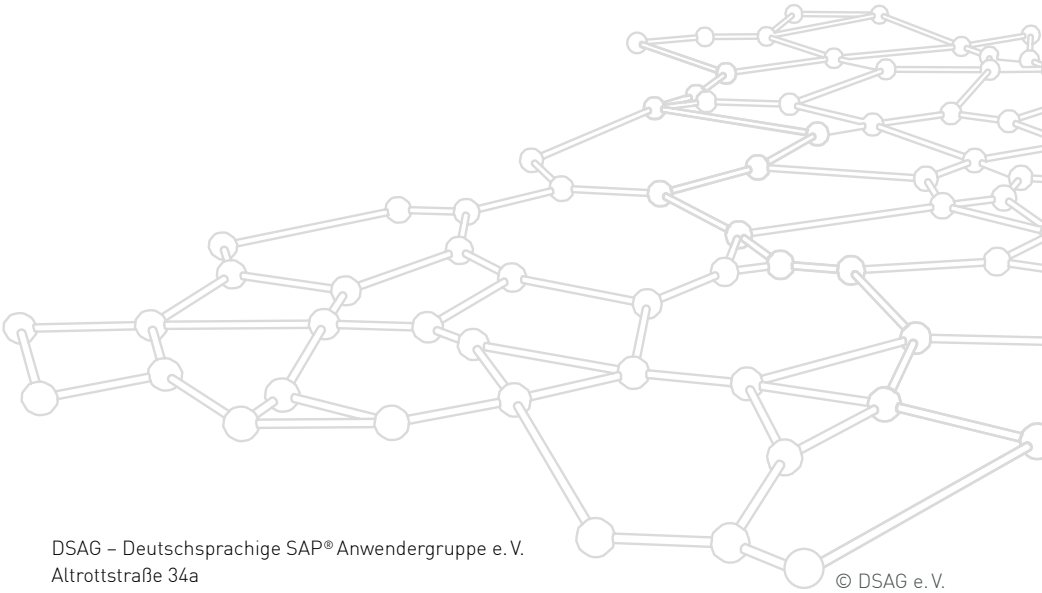
NR.	DATENBANKMANAGEMENT
3.	**Kontrollziel: Es besteht ein angemessener und funktionierender Patch-Management-Prozess.** **Risiko:** Wesentliche sicherheitsrelevante Patches für die Appliance sind nicht installiert, sodass Angreifer bekannte Sicherheitsschwachstellen ausnutzen können.
3.1.	**Wird die Datenbank mit von SAP freigegebenen SAP-HANA-Sicherheits-Patches (im Rahmen der regulären Revisionen) auf dem neuesten Stand gehalten?** **Hinweise:** Sicherheitshinweise von SAP werden auf http://service.sap.com/securitynotes kommuniziert (Filtern auf Komponente HAN*)
3.2.	Gibt es einen geregelten und dokumentierten Prozess zur Freigabe und Installation von Patches?
3.3.	Gibt es einen gemeinsam geregelten und dokumentierten Prozess zur Freigabe und Installation von Patches für das Betriebssystem und Betriebsystem-Diensten/-Programmen zwischen dem Provider der Appliance und dem Unternehmen?

10.7. PRÜFPROGRAMM: ÜBERWACHUNG VON SICHERHEITSVERLETZUNGEN UND REGELMÄSSIGE ÜBERPRÜFUNG POTENZIELLER SICHERHEITSSCHWACHSTELLEN DER SAP-HANA-SERVER

NR.	ÜBERWACHUNG VON SICHERHEITSVERLETZUNGEN UND REGELMÄSSIGE ÜBERPRÜFUNG VON SICHERHEITSSCHWACHSTELLEN
1.	**Kontrollziel: Sicherheitsrelevante Ereignisse werden protokolliert und überwacht. Kritische Sicherheitsverstöße werden nachverfolgt.** **Risiko:** Kritische Sicherheitsverstöße oder der Missbrauch von Benutzern werden gar nicht oder zu spät erkannt, sodass keine Gegenmaßnahmen eingeleitet werden können. Bei dem Verdacht auf Missbrauch kann im Nachhinein nicht mehr auf automatisch erfolgte Systemaufzeichnungen zurückgegriffen werden, die zur Aufklärung des Vorgangs oder Verfolgung der Angreifer dienen können.
1.1.	**Ist die native SAP-HANA-Datenbank-Protokollierung, das sogenannte Auditing, aktiviert?** *SQL> SELECT KEY, VALUE FROM M_INIFILE_CONTENTS WHERE KEY = 'global_auditing_state' AND VALUE !='true';* (Das SQL-Statement zeigt einen Verstoß gegen den Vorschlagswert an.)

NR.	ÜBERWACHUNG VON SICHERHEITSVERLETZUNGEN UND REGELMÄSSIGE ÜBERPRÜFUNG VON SICHERHEITSSCHWACHSTELLEN
1.2.	**Sind SAP-HANA Protokollierungsvorgaben, sogenannte Audit Policies, definiert und aktiviert, die festlegen, welche sicherheitsrelevanten Ereignisse durch die Datenbank protokolliert werden?** *SQL> SELECT * FROM "SYS"."AUDIT_POLICIES" WHERE IS_AUDIT_POLICY_ACTIVE='TRUE';* **Hinweis:** Bei der Prüfung ist insbesondere darauf zu achten, dass die Audit Policies auch aktiviert sind. Bei der Protokollierung des SYSTEM-Benutzers ist zu beachten, dass eine Protokollierung aller Aktivitäten dazu führt, dass auch Datenbank-interne Operationen protokolliert werden, da diese im Kontext des SYSTEM-Benutzers erfolgen. Dies kann zu einer enormen Anzahl an protokollierten Ereignissen führen und die Performance des Systems negativ beeinflussen.
1.3.	**Sind die Protokolle vor dem ändernden Zugriff von Datenbankadministratoren geschützt?** *SQL>SELECT * FROM M_INIFILE_CONTENTS WHERE SECTION='auditing configuration';* **Hinweis:** Um die Protokolle vor dem ändernden Zugriff zu schützen, bietet es sich bspw. an, das SYSLOGPROTOCOL als default_audit_trail_type festzulegen. Wird die HANA-Datenbanktabelle (...) als audit_trail_type definiert, kann der ändernde Zugriff durch Datenbankadministratoren technisch unterbunden werden, indem das Privileg AUDIT_OPERATOR nicht an den Datenbankadministrator vergeben wird.
1.4.	**Sind die Protokolle vor dem ändernden Zugriff von Betriebsadministratoren geschützt?** **Hinweis:** Um die Protokolle vor dem ändernden Zugriff zu schützen, bietet es sich an, den syslog an einen zentralen Server zu streamen, der außerhalb des Zugriffsbereichs der SAP-HANA-Betriebssystemadministratoren liegt (falls das SYSLOGPROTOCOL überhaupt als ein default_audit_trail_type festgelegt ist).
1.5.	Werden die Protokolle regelmäßig und nachvollziehbar überwacht?
1.6.	Ist definiert und dokumentiert, was eine Sicherheitsverletzungen darstellt und wie werden diese identifiziert?
1.7.	Gibt es einen dokumentierten Prozess für die Behandlung von Sicherheitsverletzungen?
2.	**Kontrollziel: Regelmäßige Sicherheitsprüfungen der Datenbank durchführen, Sicherheitsschwachstellen identifizieren und kompensierende Maßnahmen einleiten.** Risiko: Bestehende Sicherheitsschwachstellen in den Systemen werden nicht erkannt und können von Angreifern ausgenutzt werden.
2.1.	**Gibt es Vorgaben für die sichere Konfiguration von SAP-HANA-Servern?** **Hinweis:** Eine Konfigurations-Checkliste kann dem SAP HANA Security Guide entnommen werden. Auf dieser Liste basiert auch der EarlyWatch-Alert für SAP HANA.
2.2.	Gibt es einen Prozess der regelmäßig die Datenbank-Server auf Sicherheits-Schwachstellen und Einhaltung auf Konfigurationsvorgaben prüft?
2.3.	Gibt es einen geregelten Prozess, zur Einleitung von Gegenmaßnahmen bei der Identifikation von Schwachstellen oder Fehlkonfigurationen?

Deutschsprachige
SAP® Anwendergruppe



DSAG – Deutschsprachige SAP® Anwendergruppe e. V.
Altrottstraße 34a
69190 Walldorf
Deutschland
Fon: +49 (0) 6227 – 358 09 58
Fax: +49 (0) 6227 – 358 09 59
www.dsag.de I info@dsag.de