Einheitliches Berechtigungsmanagement umsetzen

1. Zweck

Ziel des Regelwerks ist es, einheitliche Vorgaben zum Berechtigungsmanagement zu definieren, die unabhängig von dem zum Einsatz kommenden System[1] gelten. Es stellt somit die Grundlage für weitere spezifische Vorgaben der AUDI BRUSSELS dar. Zusätzliche Feinkonzepte und systemspezifische Berechtigungskonzepte sind weiterhin notwendig und werden nicht durch diese allgemeine Regelung obsolet.
Damit wird bezweckt, Daten und Systeme vor Zugriffen zu schützen, welche eine Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit im Rahmen der Berechtigungsvergabe zur Folge haben.

Dieses Regelwerk trägt dazu bei, das Niveau des Berechtigungsmanagements kontinuierlich zu verbessern. Dieses wird erzielt durch:

- Standardisierte Vorgaben
- Nachvollziehbare, weltweite Umsetzung der Regeln in jeder Organisationseinheit
- Sicherstellung der Wirksamkeit durch ein intern aufzubauendes Kontrollsystem

Die in diesem Regelwerk definierten Vorgaben stellen Mindeststandards für die AUDI BRUSSELS dar und sind über weitere spezifische Richtlinien und Anweisungen zu konkretisieren. Sich daraus ergebene Maßnahmen sind operativ umzusetzen und kontinuierlich auf Wirksamkeit zu überprüfen.
Werden Verbesserungspotenziale auf operativer Ebene identifiziert, so fließen diese in dieses einheitliche Regelwerk zum Berechtigungsmanagement ein (Bottom Up).

[1] Ein System im Sinne dieses Dokumentes deckt alle Ebenen „Applikation“, „Datenbank“, „Betriebssystem“ ab und ist unabhängig von der zum Einsatz kommenden Technologie. Vereinfacht wird im Folgenden - stellvertretend für die einzelnen Ebenen - der Begriff „System“ verwendet.

Einheitliches Berechtigungsmanagement umsetzen

2. Zuständigkeiten

Die nachstehend definierten Vorgaben sind für die AUDI BRUSSELS und ihre Funktionsträger ohne Einschränkung auf bestimmte Geschäftsprozesse verbindlich. Sie ist sofort anzuwenden und umzusetzen.

Unter Berücksichtigung gesetzlicher Vorgaben liegt die Verantwortung für ein funktionierendes internes Steuerungs- und Überwachungssystem (IKS) bei dem Vorstand der AUDI BRUSSELS.

- Verantwortung der Führungskräfte
  Die Führungskräfte sind dafür verantwortlich, dass die Vorgaben in ihrem Bereich kommuniziert, umgesetzt, eingehalten und auf Wirksamkeit kontinuierlich überprüft werden.

- Verantwortung des Dateneigentümer
  Der Dateneigentümer einer Information definiert eigenverantwortlich, welchen Schutzbedarf die Information (Vertraulichkeit, Integrität, Verfügbarkeit) hat. Er orientiert sich hierbei zum Schutzziel Vertraulichkeit - an den in Kapitel 4.2.2 definierten Schutzklassen. (Falls für den Bereich bereits ein Vorgabenkatalog verfügbar ist, dient dieser als Leitbild)
  In diesem Zusammenhang verantwortet ausschließlich der Dateneigentümer die Vergabe von Zugriffsberechtigungen für Informationen der Vertraulichkeitsklasse „geheim“ (siehe Abschnitt 5.2).

- Verantwortung des Datenbesitzers
  Der Datenbesitzer (auch Informationsnutzer durch Erteilung von Leserechten) kann die Weitergabe von Informationen (auch Zugriffsrechteerteilung) unter Berücksichtigung der Empfängerkriterien (Geheimhaltungsvereinbarung vorhanden; Vertragsverhältnis; Need to know) für die Vertraulichkeitsklassen „vertraulich“ und „intern“ verantworten (siehe Abschnitt 5.2).

- Fachlich Verantwortlicher
  Der „fachlich Verantwortliche“ bezieht sich jeweils auf Teilumfänge eines IT-System (Beispiele: Der Fachbereichsvertreter ist „fachlich Verantwortlicher“ für die Anforderung und Definition einer Rechterolle; Der Systembetreiber ist „fachlich Verantwortlicher“ für die Anforderung und Definition einer administrativen Systemrolle)

- Berechtigungsadministration
  Innerhalb der Berechtigungsadministration ist darauf zu achten, die Definition, Pflege und Zuordnung von kritischen Berechtigungen (Bsp. Fachlich, Administration; etc.) nicht nur organisatorisch, sondern auch technisch zu trennen (siehe Kapitel 4.3.3).

Einheitliches Berechtigungsmanagement umsetzen

Die Einhaltung der genannten Funktionstrennung ist hierbei unabhängig von der gewählten Organisationsform des Berechtigungsmanagements (zentral vs. dezentral) zwingend erforderlich.

3. Wechselwirkung des Prozesses

3.1 Steuerungsprozess

Information-Security-Risk-Management

3.2 Detaillierte Erläuterung

Das Berechtigungsassessment ist ein Teil der R10-Regel des Volkswagen-Konzerns und wurde für die AUDI BRUSSELS angepasst. Das Berechtigungsassessment ist für alle in bzw. von der AUDI BRUSSELS betriebenen und /oder verwendeten Anwendungen verpflichtend.

Zum Berechtigungsassessment gehören drei Dokumente:

- Berechtigungs-Checkliste
  Die Checkliste, die die Fragen des Assessments, Erläuterungen und die Auswertungen enthält.
- Template des Berechtigungskonzepts
  Ein Vorschlag für ein Berechtigungskonzept, falls der Anwendungsverantwortliche oder Projektleiter nicht weiß, was alles in ein Berechtigungskonzept einfließen muss.
- Ausgefülltes Berechtigungskonzepts

Das Berechtigungskonzept muss nicht in der Form des bereitgestellten Templates angefertigt werden. Es besteht keine Formvorgabe. Wichtig ist, dass alle erforderlichen Informationen im Konzept vorhanden sind. Aus dem Konzept heraus kann auch auf bestimmte und relevante Kapitel der Handbücher der Anwendung oder andere Dokumente verwiesen werden. Diese Dokumente müssen dann ebenso bereitgestellt werden.

Das Berechtigungsassessment ist ein Teil des Information-Security-Risk-Management Prozess von AUDI BRUSSELS und in diesen eingebettet. Das Assessment findet stets geführt statt, d.h. ein Assessor interviewt den Anwendungsverantwortlichen.

3.3 Chronologischer Ablauf eines Berechtigungs-Assessments

1. Vorbereitung
   a. Der Assessor, der das Assessment durchführt, fordert das Berechtigungskonzept vom Anwendungsverantwortlichen ein.
   b. Existiert kein Berechtigungskonzept, so wird die Anwendung mit „Nicht bestanden“ bewertet.
   c. Der Assessor prüft das Berechtigungskonzept.

Einheitliches Berechtigungsmanagement umsetzen

   d. Der Assessor beraumt einen Termin für das Interview mit dem Anwendungsverantwortlichen an.

2. Assessment
   a. Der Assessor nimmt die Metadaten der Anwendung auf und fügt sie in den Reiter „Auswertung Entscheidungsmatrix“ ein. Außerdem muss die Application Risk Class abgefragt und eingetragen werden, denn diese fließt in die Auswertung mit ein.
   b. Der Assessor geht zusammen mit dem Anwendungsverantwortlichen jede Frage der Berechtigungs-Checkliste (Reiter „Checkliste“) durch, erklärt dem Anwendungsverantwortlichen die jeweiligen Fragen und trägt das Ergebnis ein.
   c. Nach Beendigung der Fragen wechselt der Assessor wieder in den Reiter „Auswertung Entscheidungsmatrix“ und ermittelt das Ergebnis des Assessments (Assessment bestanden oder Assessment nicht bestanden).
   d. Über den Reiter „Risikoeinschätzung“ ermittelt der Assessor anhand der erreichten Punktzahl sowie anhand der Application Risk Class die Risikoeinschätzung (sehr hoch, hoch, mittel oder niedrig).

3. Ergebnis
   a. Lautet das Ergebnis des Assessments „Nicht bestanden“, so kann die Risikoeinschätzung nur „hoch“ oder „sehr hoch“ sein.
   b. Lautet das Ergebnis auch im Nachfolge-Assessment „Nicht bestanden“ bzw. beträgt die Risikoeinschätzung des Assessments die Ausprägungen „hoch“ oder „sehr hoch“, dann muss der Anwendungsverantwortliche ein Umsetzungskonzept innerhalb von 4 Wochen nach dem erfolgten Assessment) vorlegen.
   c. Ist bis zum Livegang der Anwendung das Risiko noch vorhanden, dann muss eine Risikoübernahme unmittelbar eingereicht und genehmigt werden (Risiko muss durch das Management übernommen werden).

4. Risikoübernahmeantrag
   a. Im Risikoübernahmeantrag müssen alle Risiken aufgeführt sein.
   b. Der Assessor initiiert ein Risikoübernahme-Abstimmmeeting. Dabei ist eine Teilnahme von der IT-Sicherheit erforderlich.

5. Zyklische Prüfung
   a. Es wird ein neues Assessment durchgeführt, bei dem die alte Checkliste mit der dann vorhandenen neuen Version der Checkliste abgeglichen wird (sollte in der Assessmentvorbereitung abgeglichen werden).

Einheitliches Berechtigungsmanagement umsetzen

4. Regelung

4.1 Definition

Das Berechtigungsmanagement regelt alle Prozesse, Aufgaben und Verantwortungen zur Verwaltung von Usern und Berechtigungen in allen Systemen mit dem Ziel, auf der einen Seite die gesetzlichen und internen Vorgaben zu erfüllen und auf der anderen Seite materiellen oder immateriellen Schaden für Audi abzuwenden. Es definiert und kontrolliert die System- und Datenzugriffe aller Mitarbeiter und ist somit ein zentraler Baustein der IT-Sicherheit sowie weiterführend des übergeordneten Managements zur Informationssicherheit.

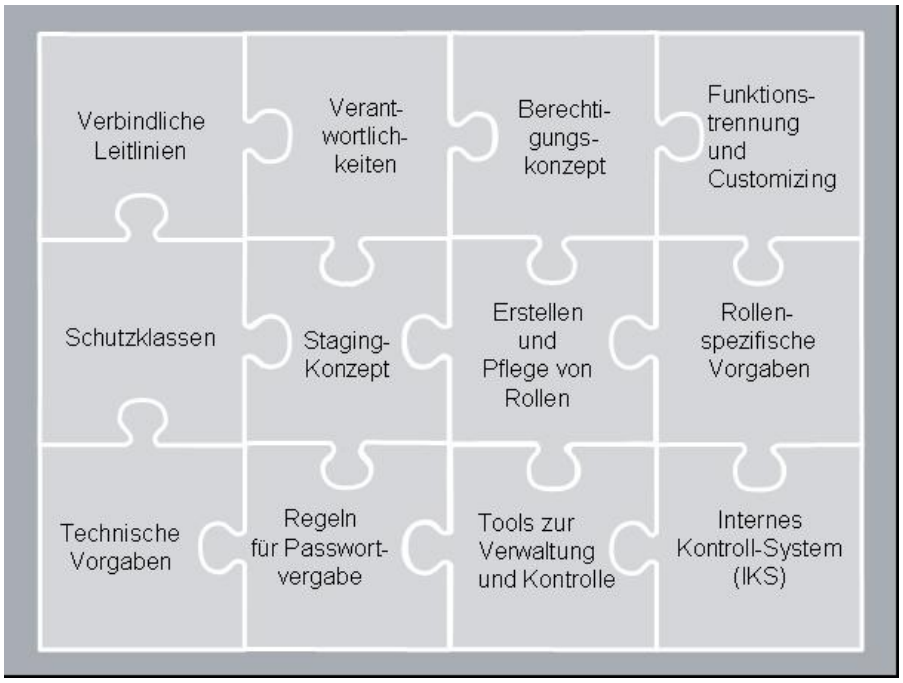


Abbildung 1: Elemente des Berechtigungsmanagements

Die wesentlichen Elemente eines Berechtigungsmanagements sind in der obenstehenden Abbildung 1 dargestellt und in den folgenden Kapiteln als Rahmen für eine gesellschaftsspezifische lokale/dezentrale Umsetzung detaillierter beschrieben.

Inhaltlicher Schwerpunkt nachstehender Kapitel ist das Management von Berechtigungen (Autorisierung). Die User-Authentifizierung sowie damit verbundene Verfahren sind nicht Gegenstand dieses Dokuments. Dennoch werden auch Vorgaben an die Authentifizierungsmechanismen definiert, welche bei der Definition und Implementierung eines angemessenen Authentifizierungskonzepts berücksichtigt werden müssen.

Einheitliches Berechtigungsmanagement umsetzen

4.2 Grundsätzliche Prinzipien

Für die regelkonforme Umsetzung eines ganzheitlichen Berechtigungsmanagements stellen nachfolgende Prinzipien, welche aus den gesetzlichen und regulatorischen Anforderungen abgeleitet sind, die wesentliche Grundlage dar.

4.2.1 Verbindliche Leitlinien

Folgende Prinzipien sind beim Berechtigungsmanagement zu berücksichtigen:

Identitätsprinzip:
Das Identitätsprinzip stellt dabei die logische Grundlage aller Berechtigungskonzepte dar. Dieses Prinzip gewährleistet die eindeutige und jederzeitige Zuordnung einer Identität (Person) zu einem User (IT-ID).

Minimalprinzip:
Die Berechtigungsausprägung orientiert sich an den für die zur Aufgabenerfüllung unbedingt notwendigen, geringstmöglichen Zugang zu Daten / Funktionen.

Stellenprinzip:
Sämtliche Datenzugriffsrechte eines Users müssen sich aus der Prozessfunktion (Aufgabe) des Users in der Organisation oder einer Projektrolle ergeben. Dabei erfolgt die prozessorientierte Bündelung von Aufgaben in Stellen (Aufbauorganisation) oder Prozessrollen.

Eigenverantwortungsprinzip:
Die AUDI BRUSSELS ist eigenverantwortlich für die regelkonforme Etablierung des Berechtigungsmanagements zuständig.

Belegprinzip der Buchhaltung:
Sämtliche zahlungsrelevanten oder bilanzwirksamen Vorgänge müssen belegbar sein (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD).

Belegprinzip der Berechtigungsverwaltung:
Die Zuordnung der User (IT-ID) zu Personen sowie die Zuweisung von System-Berechtigungen zu einem User ist bedarfsgerecht zu dokumentieren.

Funktionstrennungsprinzip:
Damit ein Mitarbeiter nicht allein den gesamten Prozess bearbeiten kann (Gefahr des Kontrollverlustes), besteht die Notwendigkeit zu einer zwingenden Trennung von kritischen Aktivitäten in den Geschäftsprozessen (siehe Kapitel 4.3.3). Die Anforderungen aus bestehenden Regularien wie den GoBD sind unbedingt zu berücksichtigen.

Einheitliches Berechtigungsmanagement umsetzen

Genehmigungsprinzip:

Kritische Systemzugänge und Zugriffe auf Informationen müssen nachvollziehbar genehmigt werden. Es gilt eine bedarfsgerechte Umsetzung des Genehmigungsprinzips.

Standardprinzip:
Die Definition und Einhaltung technischer, prozessualer und rollenbezogener Standards ist bei der Vergabe von Berechtigungen zu fördern und zu etablieren.

Kontrollprinzip:
Die Umsetzung des Berechtigungskonzeptes muss durch Kontrollen innerhalb der Berechtigungsadministration sowie durch neutrale Prüfer überprüft werden können.

Schriftformprinzip:
Ein Berechtigungskonzept muss in einer schriftlichen, genehmigten Fassung vorliegen. Ein sachkundiger Dritter muss in der Lage sein, in angemessener Zeit Auskunft über die Nutzung von Berechtigungen sowie über die Umsetzung normativer Grundlagen und der technischen Realisierung zu erhalten.

Einheitliches Berechtigungsmanagement umsetzen

4.2.2 Schutzklassen

Der Informationseigentümer ist verpflichtet eine Klassifizierung (öffentlich, intern, vertraulich, geheim) der Daten durchzuführen. Weitere Details hierzu in der Anlage 5 der Unternehmensrichtlinie URLB_024 Informationssicherheit
„Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter“

Die Vorgaben dieses Dokumentes gelten prinzipiell für alle Systeme.

Bei der Umsetzung des Regelwerks ist grundsätzlich die Einhaltung des „Gebotes der Verhältnismäßigkeit" zu beachten. Dies besagt, dass der unter Beachtung unternehmerischer Sicherheitsziele sowie der gesetzlichen Auflagen angestrebte Schutzzweck und der hierfür zu erbringende Aufwand in einem vertretbaren Verhältnis zueinander stehen. Eine Beeinträchtigung gesetzlicher und regulatorischer Anforderungen wird jedoch nicht toleriert.

4.3 Vorgaben zur Umsetzung

Die grundsätzlichen Prinzipien *(siehe 4.2)* und die in diesem Kapitel beschriebenen Bestandteile bilden den Rahmen für die Umsetzung auf operativer Ebene. Die Anforderungen an Rechte-Rollen obliegt dem/den Fachbereichen dem die Rolle zugeordnet wird . Dabei hat die Nachvollziehbarkeit oberste Priorität.
Einen wesentlichen Aspekt bildet das Zusammenspiel zwischen Fachbereich und IT, welches in nachstehender Grafik und den folgenden Kapiteln weiter vertieft wird.

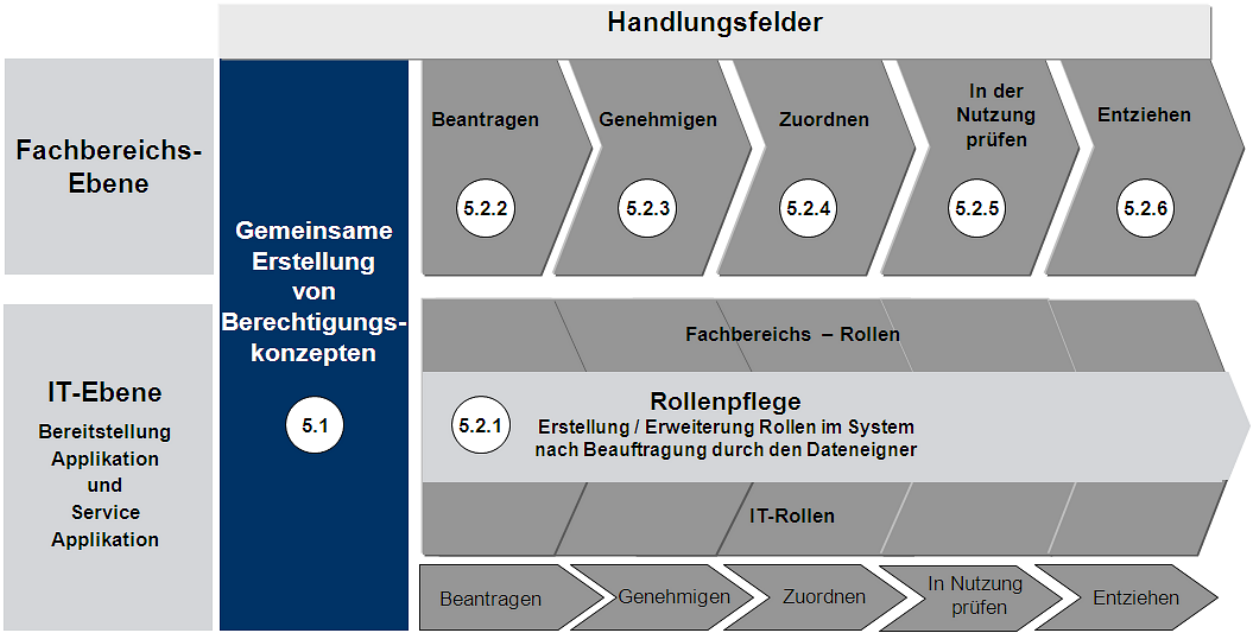


Abbildung 2: Prozessschritte im Rollenmanagement

Einheitliches Berechtigungsmanagement umsetzen

4.3.1 Berechtigungskonzept

Das Berechtigungskonzept eines jeden Systems bildet die zentrale Grundlage für die Beschreibung aller Verantwortlichkeiten sowie aller berechtigungsspezifischen Prozesse. Die Verantwortung für die inhaltliche Ausgestaltung, die Umsetzung und Kontrolle liegt in den Fachbereichen mit Unterstützung durch die IT.
Im Detail ist Folgendes zu berücksichtigen:

- Es definiert Aktivitäten für die Vergabe, die Änderung, die periodische Berechtigungsprüfung, das Entziehen von Berechtigungen sowie zu implementierende Kontrollmechanismen.
- Alle im Produktivsystem vergebenen Berechtigungen (Rollen-Rechte) werden im Berechtigungskonzept dokumentiert.
- Die Definition und Dokumentation von nachvollziehbaren einheitlichen, gesellschaftsspezifischen Namenskonventionen für Rollen, IT-ID und Berechtigungen
- Grundsätzlich sind alle Berechtigungen innerhalb des Produktivsystems sowie deren Zuordnung zu organisatorischen Stellen oder Projektrollen zu dokumentieren. Aus diesem Grund muss sich die Definition und Pflege von Berechtigungen an konkreten organisatorischen Stellen oder Projektrollen orientieren.
- Für das Produktivsystem ist darüber hinaus im Berechtigungskonzept zu verdeutlichen, wie der Umgang mit Administrator-Berechtigungen und mit kritischen Berechtigungen *(siehe Kapitel 4.3.6*) erfolgt.
- Weiterhin sind die Berechtigungen für die Entwicklungs- und Qualitätssicherungsumgebung zu benennen und zu beschreiben.
- In dem Berechtigungskonzept ist die Dokumentation des technischen Customizing (z.B.: Passworteinstellung) mit Bezug zum Berechtigungsmanagement erforderlich.
- Die organisatorischen Verantwortlichkeiten sind im Berechtigungskonzept zu fixieren.
- Das Berechtigungskonzept unterliegt dabei der Pflicht zum regelmäßigen Review. Hieraus resultierende Anpassungen sind unverzüglich vorzunehmen.

4.3.2 Prozess-Schritte im Rollenmanagement

In den Prozess-Schritten des Rollenmanagements sind die unter Kapitel 4.2 formalen Prinzipen zu berücksichtigen. In diesem Zusammenhang sind insbesondere zu beachten:

- Das Minimalprinzip (Need to know; Trennung von Rechten) ist als essentiell hervorzuheben und anzuwenden.
- Die Rollen Beauftrager und Umsetzer sind definiert und dokumentiert
- Die Prozessschritte „Genehmigen“, „Zuordnen“ und „Rollenpflege“ sind jeweils sowohl technisch als auch organisatorisch voneinander zu trennen.
- Die Checkliste zum Berechtigungsmanagement (siehe Anlagen)

Einheitliches Berechtigungsmanagement umsetzen

Ausgestaltung von Rollen (Zuordnung von Rechten oder Systemfunktionen zu einer Systemrolle)
Eine Rollenpflege (Berechtigungspflege) ist erforderlich, wenn die Rollen, die bislang in dem Berechtigungskonzept bzw. der Applikation enthalten sind, angepasst werden müssen oder wenn Rollen neu angelegt werden. Vor der Dokumentation im Berechtigungskonzept und der technischen Umsetzung durch die IT muss eine Freigabe durch zugeordneten Fachbereich (Prozesskettenverantwortlichen) vorliegen. Die Manipulation von Rollen ist im Produktivsystem ohne qualitätssichernden Maßnahmen nicht zulässig. Rechte/Rollen-Änderungen sind im Entwicklungssystem durchzuführen und im Qualitätssicherungssystem zu testen und freizugeben.

Beantragen von Mitgliedschaften in Systemrollen (Rechterollen)
Die Beantragung von Berechtigungen erfolgt durch den Antragssteller bei der fachlich definierten Stelle (Bsp. Systembetreiber, OE-Leiter, Projektleiter) unter Angabe nachstehender Informationen:

- Name, Gesellschaft, Abteilung, Name des Vorgesetzten (inkl. Abteilungsangabe). Je nach Systemaufbau ist zusätzlich der Datenumfang anzugeben (Projektname; Pool; Ordnername etc.)
- Information zum Antrag: Neuanlage, Änderung, Entziehen von Berechtigungen.
- Angabe der benötigten Berechtigungen.
- Angabe, „Wie lange“ die Berechtigung benötigt wird.
- Die Begründung, „Für was“ und „Warum“ die Berechtigung benötigt wird, ist zwingend erforderlich.

Für OE-gesteuerte Systemzugriffe kann als Initiator bei Eintritten von Personen in das Unternehmen dabei der HR-Bereich fungieren. Bei der Beantragung ist sicherzustellen, dass das grundlegende Verfahren sowohl im Fachbereich als auch in der IT einheitlich und nachvollziehbar ist.

Prüfung und Genehmigung von Mitgliedschaften in Systemrollen (Rechterollen)
Im Vorfeld der Zuordnung erfolgt die Prüfung und Freigabe von neuen, geänderten oder von bereits abgestimmten Berechtigungen bedarfsgerecht zweistufig sowohl durch den disziplinarischen Vorgesetzten als auch durch den verantwortlichen Informations-Besitzer oder - Eigentümer. Innerhalb der Prozessschritte Prüfung und Genehmigung müssen die Prinzipien Identitäts-, Minimal- und Stellenprinzip stets Beachtung finden. Das Vier-Augen-Prinzip ist für kritische Systemzugriffe oder Rechterollen auf jeden Fall zu gewährleisten – ansonsten bedarfsgerecht. Die Dokumentation der abschließenden Freigabe / Ablehnung des Antrags ist im Hinblick auf die Nachvollziehbarkeit angemessen festzuhalten.

Zuordnung von IT-ID zu Rechterollen
Die Zuordnung von Usern in genehmigte Systemrollen (Rechterollen) erfolgt durch die verantwortlichen Mitarbeiter des Fachbereichs oder dafür eingerichtete Administrationsstellen. Nach durchgeführter Zuordnung hat eine Rückinformation an den Antragssteller zu erfolgen. In diesem Zusammenhang ist es essentiell, dass sämtliche

Einheitliches Berechtigungsmanagement umsetzen

Zuordnungsaktivitäten nachvollziehbar dokumentiert werden. Es muss ersichtlich sein, wer hat wann, welche Rollen zugeordnet.
Das Identitäts-, Minimal- und Stellenprinzip ist grundsätzlich innerhalb der Rollenzuordnung unabhängig davon zu berücksichtigen, ob interne oder externe User betroffen sind. Insbesondere für Mitarbeiter von Fremdfirmen sind Berechtigungen mit Zeitbeschränkung zu versehen. Diesbezügliche gesellschaftsspezifische Anweisungen sind hierfür zu definieren.

Periodische Berechtigungsprüfung

Ziel einer Berechtigungsprüfung durch den fachlich Verantwortlichen ist es, in den jeweiligen Fachbereichen oder Projekten periodische Personalbewegungen (Abteilungswechsel, Austritt, Rollenänderung etc.) zu identifizieren, Funktionstrennungskonflikte zu erkennen, zu analysieren, zu bewerten sowie die sich daraus ergebenden Kontrollmaßnahmen hinsichtlich ihrer Wirksamkeit zu prüfen. Die Prüfung bezieht sich somit auf die Analysebereiche User und auf deren kritische (z.B. administrative) Berechtigungen.
Der Zyklus dieser Prüfungen orientiert sich dabei an der dem jeweiligen System zugeordneten Schutzklasse: Bei Anwendungen mit geheimen Daten werden Benutzer mit kritischen Rollen / Berechtigungen halbjährlich – in Anwendungen mit vertraulichen, internen Daten jährlich - durch den fachlich Verantwortlichen überprüft. Abweichungen von dem vorgegebenen Prüfungsrhythmus sind mit besonderer Begründung vom Vorstand der AUDI BRUSSELS freizugeben. Die Durchführung erfolgt verantwortlich durch den Fachbereich mit Unterstützung der IT. Nachstehend sind Aktivitäten der periodischen Berechtigungsprüfung dargestellt.

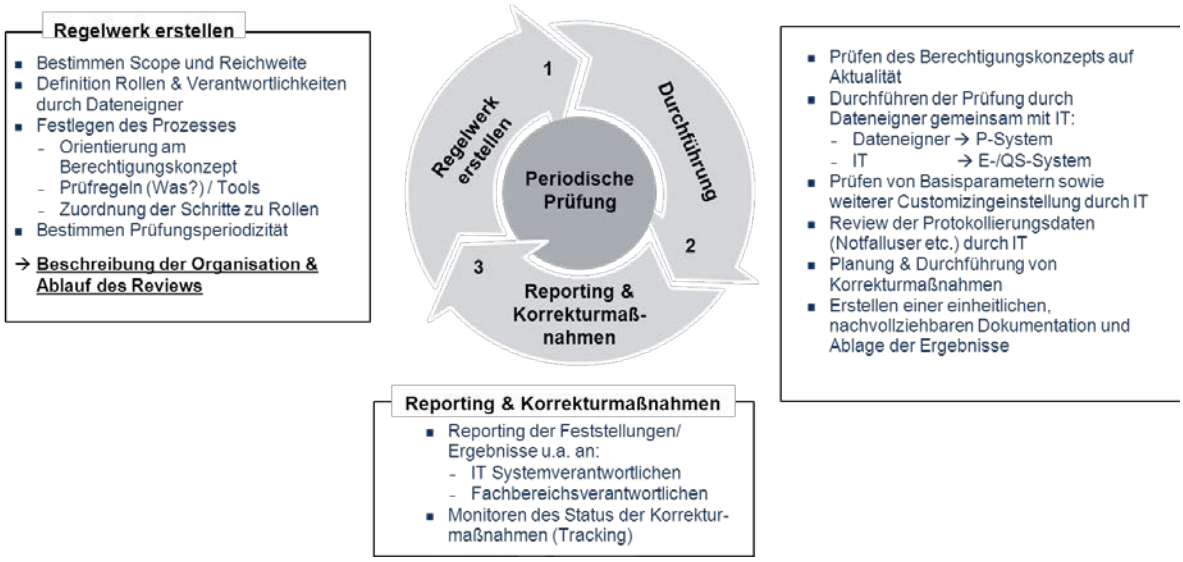


Abbildung 3: Prozessrahmen für „periodische Berechtigungsprüfung“

Während die Phasen 2 „Durchführung“ und 3 „Reporting & Korrekturmaßnahmen“ regelmäßig durchlaufen werden, ist die grundsätzliche Erstellung des konkreten Regelwerks zur periodischen Berechtigungsprüfung innerhalb der Phase 1 einmal zu erstellen und bei jeder Durchführung auf Aktualität zu prüfen und, falls erforderlich, sind Anpassungen

Einheitliches Berechtigungsmanagement umsetzen

vorzunehmen. Eine nachvollziehbare Beschreibung der vollständigen Vorgehensweise (Phase 1-3) ist abschließend im Berechtigungskonzept vorzunehmen.

Entziehen von Mitgliedschaften in Systemrollen (Rechterollen)

Das Entziehen (oder die Beauftragung zum Entziehen) von Berechtigungen erfolgt durch die zuständigen Personen des Fachbereichs. Als Initiator bei Austritten von Personen aus dem Unternehmen kann dabei der HR-Bereich fungieren. Hierbei ist es notwendig, unverzüglich und nachvollziehbar an die verantwortlichen Mitarbeiter zu kommunizieren, um eine zeitnahe Umsetzung zu erwirken. Vorausschauende proaktive Terminierung von Userkonten oder Berechtigungszuweisungen sind obligatorisch. Es bleibt zu beachten, dass sämtliche Tätigkeiten bedarfsgerecht nachvollziehbar dokumentiert werden müssen.
Für IT-Projekte ist sicherzustellen, dass Test- oder sonstige Projektuser sowie die damit verbundenen Projektberechtigungen zum Zeitpunkt des Produktivstarts aus dem System entfernt sind.

4.3.3 Funktionstrennung

Zum Schutz von sensiblen und kritischen Daten sind für die unternehmensspezifischen Prozesse unvereinbare Tätigkeiten aufbau- und ablauforganisatorisch zu trennen. Das damit verbundene Ziel umfasst die Sicherstellung, dass kein Mitarbeiter den vollständigen Prozess (bzw. relevanten Teil-Prozess) alleine bearbeiten kann. Letzteres führt bei Existenz zu einem erheblichen Kontrollverlust und steigert damit das Risiko von Missbräuchen.
Wie in Abbildung 4 dargestellt wird bei der AUDI BRUSSELS die Forderung nach der grundlegendsten „Funktionstrennung“ im Rollenmanagement u.a. durch die organisatorische Trennung „Fachbereich“ und „IT“ umgesetzt:

- Während der Systembetreiber (oder das IT-Projekt) die vom Fachbereich beauftragten Rechterollen erstellt und pflegt, obliegt dem fachlich Verantwortlichen aus dem Fachbereich die Verantwortung zur angemessenen Prüfung, Genehmigung sowie der Zuweisung (oder die Beantragung zur Zuweisung) der beantragten Berechtigungen.
- Darüber hinaus erstreckt sich die Thematik der Funktionstrennung nicht nur auf den Fachbereich (z.B. Finanz- und Rechnungswesen, Beschaffung, Vertrieb etc.) sondern auch auf die IT. Die geforderte organisatorische Trennung der Pflege und Zuordnung ist auch innerhalb des IT-Bereiches selber verpflichtend umzusetzen, falls sich die fachliche Verantwortung innerhalb der IT befindet.

Es ist weiterführend Aufgabe des jeweiligen Fachbereichs, mögliche Funktionstrennungskonflikte innerhalb der Geschäftsprozesse (z.B.: Finanz- und Rechnungswesen, Beschaffung, Vertrieb, IT etc.) zu identifizieren, zu bewerten, zu begegnen sowie nachvollziehbar im Berechtigungskonzept zu dokumentieren. Dabei gibt es keine Einschränkungen auf bestimmte Prozessfamilien. Voraussetzung für die Identifizierung und Klassifizierung von kritischen Berechtigungen und einen sich daraus ergebenden Funktionstrennungskonflikt stellt die risikoorientierte Analyse der Prozesse durch den Fachbereich sowie die Anforderungen aus bestehenden Regularien wie den GoBD dar. Abschließend sind die Analyseergebnisse bei der detaillierten Ausgestaltung von Berechtigungen nachvollziehbar umzusetzen.

Einheitliches Berechtigungsmanagement umsetzen

Im Falle der Nichtumsetzbarkeit von bestimmten Funktionstrennungen muss sowohl auf Ebene der Aufbau- als auch innerhalb der Ablauforganisation der Dateneigener ergänzende (oder kompensierende) Kontrollen definieren und implementieren, welche das Risiko eines Funktionstrennungskonflikts reduzieren bzw. vermeiden. Derartige zusätzliche Kontrollen sind grundsätzlich prüfbar und nachvollziehbar zu konzipieren. Die in diesem Zusammenhang zu erstellende Dokumentation muss dem Grundsatz der Angemessenheit entsprechen.
Die Sicherstellung der Wirksamkeit (Funktionsfähigkeit) der kompensierenden Kontrollen hat dabei höchste Priorität. Die Verantwortung hierfür trägt der fachlich Verantwortliche (siehe Kapitel 4.4.1).

4.3.4 Fachliches Customizing

Die Einhaltung des Funktionstrennungsprinzips bezieht sich nicht nur auf den Zugang zu Daten und Systemen, sondern muss auch bei der Gestaltung des applikationsspezifischen fachlichen Customizing Berücksichtigung finden. In diesem Zusammenhang steht die Umsetzung des Vier-Augen-Prinzips mittels fachlicher Einstellungen in der IT-Applikation im Vordergrund. Nachfolgende Punkte zeigen Beispielhaft Inhalte besonders sensibler Informationsverwaltung, welche vom Fachbereich (ggf. mit Unterstützung der IT) hinsichtlich der Umsetzbarkeit zu prüfen sind:

- Systemseitige Etablierung eines Freigabeworkflows für kritische Stammdatenänderungen.
- Definition von internen Kontrollen bezüglich der Obergrenze von Rabatten, Buchungen, Gutschriften etc. sowie die Zusammenfassung von Mitarbeitern zu speziellen Gruppen.

Die genannten Punkte stellen lediglich eine Orientierung dar und können von den betroffenen Fachbereichen weiter ergänzt werden. Abschließend sind fachliche Customizing-Einstellungen in Verbindung mit der entsprechenden Ausgestaltung der System-und/oder Rollenrechte umzusetzen.
Eine zusammenhängende Dokumentation ist abschließend im Berechtigungskonzept vorzunehmen. Auch hier genießt das Prinzip der Nachvollziehbarkeit Priorität.

4.3.5 Staging-Konzept

Um der Anforderung einer ordnungsmäßigen Entwicklungsdokumentation und Risikominimierung einer IT-Applikation gerecht zu werden, ist die grundlegende logische Aufteilung eines Systems in eine Entwicklungs-, Qualitätssicherungs- und Produktivumgebung erforderlich. Im Falle der Nichtumsetzbarkeit einer 3-stufigen Systemlandschaft ist, sofern technisch realisierbar, mindestens eine Trennung der produktiven Umgebung vom Entwicklungs-/ Qualitätssicherungssystems zu gewährleisten.

Für eine ordnungsgemäße Umsetzung eines angemessenen, wirksamen und ganzheitlichen Berechtigungsmanagements sind nachstehende Punkte nicht nur auf Ebene der Anwendersysteme, sondern auch auf Betriebs- und Datenbankebene zu beachten:

Einheitliches Berechtigungsmanagement umsetzen

- Die Erstellung, Ausgestaltung und Pflege von System- und Rechterollen erfolgt grundsätzlich im Entwicklungssystem. Anschließend ist ein expliziter Test im Qualitätssicherungssystem (QS-System) durch den fachlich Verantwortlichen (dem Anforderer einer Rechterolle bzw. dem Systembetreiber für Administrative-Systemrollen) vorzunehmen und zu dokumentieren. Nach dieser Validierung muss eine Freigabe durch den fachlich Verantwortlichen in dokumentierter Form erfolgen. Diese ist die grundlegende Voraussetzung für eine Produktivsetzung und damit der Nutzung von System- und Rechterollen im Produktivsystem. Abweichungen zu dieser dreistufigen Systemlandschaft sind zu begründen und zu dokumentieren.
- Das Produktiv- und Qualitätssicherungssystem ist grundsätzlich vor direkten Änderungen (Administratorebene) zu schützen. Direkte – administrative - Eingriffe sind grundsätzlich nicht zulässig (Ausnahme: Notfallusereinsatz).
- Ausschließlich in - mit den Fachbereichen zu definierenden - Notfallsituationen sind kritische (administrative) Eingriffe direkt im Qualitätssicherungs- und Produktivsystem möglich. Derartige Eingriffe dürfen ausschließlich von einem kleinen Kreis autorisierter Personen (namentlich gelistet) vorgenommen werden und sind angemessen zu dokumentieren (wer-wann-was). Die Notwendigkeit derartiger Änderungen ist stets unter Berücksichtigung von Auswirkung und Dringlichkeit zu prüfen und zu beurteilen.
- Aktivierung und angemessene Konfiguration der Änderungsprotokollierung: Kritische (administrative) Änderungen im Produktivsystem sind nachvollziehbar und nachträglich unveränderbar zu protokollieren. Dafür sind seitens des fachlich Verantwortlichen in Zusammenarbeit mit der IT die protokollierungsrelevanten Objekte zu benennen.

4.3.6 Vergabe- und Nutzungsvorgaben für spezifische User

Unter Bezugnahme auf das in Kapitel 4.3.2 beschriebene und in Abbildung 4 dargestellte Vorgehen zur Erstellung und Pflege von Rollen sind nachfolgend besondere Vorgaben für spezifische Rollen aufgeführt.
Für IT-Systeme mit besonderen Anforderungen (Bsp. SAP-Systeme zur monetären Verwaltung) sind die einem User zugewiesenen Berechtigungen automatisch (durch das System) vor der Ausführung bestimmter Funktionalitäten auf Zulässigkeit und Gültigkeit zu prüfen (Aktivierung einer automatischen Berechtigungsprüfung).

Fachbereichsrollen

Die Zuweisungen in Rechterollen eines Systems sind ausschließlich an autorisierte Endanwender eines Fachbereichs zu vergeben. Die Beauftragung bezüglich der Zuweisung und Entziehung erfolgt hierbei durch den Fachbereich (Regelgestützte Zuweisungen und Entzüge sind unter Beachtung der in diesem Regelwerk genannten Grundsätze und Regeln statthaft). Die dafür autorisierten Personen setzen die fachlichen Anforderungen um. Sämtliche Aktivitäten innerhalb des Berechtigungswesens sind dabei zu dokumentieren und zu protokollieren.

Einheitliches Berechtigungsmanagement umsetzen

IT-Rollen

Im Vergleich zu dem Kapitel 4.3.2 erfolgt die Erstellung und Pflege von IT-Rollen für Betriebssystem, Datenbank und für das Anwendersystem durch die IT selbst in deren Funktion als fachlich Verantwortlicher. Innerhalb der IT ist zusätzlich sicherzustellen, dass die Berechtigungspflege einerseits und die Zuweisung von Berechtigungen andererseits weder organisatorisch noch technisch durch ein und dieselbe Person möglich sind. Die Protokollierung sowie die Dokumentation aller Tätigkeiten sind sicher zu stellen.

Notfalluser

Der Einsatz des Notfallusers darf ausschließlich in Situationen, in denen eine signifikante Beeinträchtigung des Systembetriebs vorliegt, erfolgen. Derartige Situationen lassen sich in der Regel durch eine hohe Ausprägung der Attribute „Auswirkung und Dringlichkeiten“ beschreiben (siehe Kapitel 4.3.5). Weiterführend sind die nachstehenden organisatorischen / technischen Rahmenbedingungen, ggf. unter Einsatz eines geeigneten Tools, zu beachten:

- Alle Notfalluser sind im täglichen Betrieb grundsätzlich gesperrt. Die Beantragung und Genehmigung hat nach einem standardisierten und einheitlichen Verfahren zu erfolgen.
- Die Freigabe / Administration eines Notfallusers sowie das Management des Zugriffspassworts sind organisatorisch und auf Ebene der Berechtigungen von dem potenziellen Nutzerkreis des Notfallusers zu trennen. Des Weiteren ist das Passwort vor unautorisiertem Zugriff zu schützen und nach einer Nutzung unverzüglich zu ändern (Passwörter sind nach den Handlungsrichtlinien der Vertraulichkeitsklasse „geheim“ zu verwalten).
- Die erforderlichen Zugangspasswörter sind im Vorfeld der Nutzung unter Berücksichtigung der Passwortvorgaben zu ändern und dem Nutzer mittels E-Mailverschlüsselung und digitaler Signatur bereitzustellen. Die Nutzung ist insgesamt auf eine kleine Anzahl von Usern zu beschränken.
- Sämtliche Aktivitäten des Notfallusers werden systemseitig aufgezeichnet und nach Genehmigung durch Datenschutzbeauftragten und ggf. HR mindestens wöchentlich durch fachkundige Mitarbeiter geprüft.
- Die Aufbewahrung der Systemprotokolle liegt außerhalb der „Zugriffsweite“ des potenziellen Nutzerkreises. Die Protokolle müssen vor jeglichen Änderungen / Löschungen geschützt sein.

Die Zustimmung der Nutzung des Notfallusers muss durch den fachlich Verantwortlichen erfolgen. Dabei sind neben der Vollständigkeit und Richtigkeit des Antrags die Angemessenheit und die Notwendigkeit der Nutzung zu beurteilen. Die Grundlage liefert der Antragssteller mit seinen Angaben zu „Was, Wann, Wie getan werden soll?“ und „Welche Auswirkungen generiert werden?“ sowie „Welche Dringlichkeit besteht?“.

Zusammenfassend hat neben der protokollierungspflichtigen Aufzeichnung der Nutzung die Dokumentation der Prüfung und Genehmigung des Antrags an dieser Stelle oberste Priorität.

Einheitliches Berechtigungsmanagement umsetzen

Berechtigungsgruppe Administrator / Support-User

Administratoren bzw. Support-User nehmen aufgrund ihrer sehr weitreichenden Berechtigungen eine besondere Stellung innerhalb des Regelwerks ein. Zum Schutz der Audi-spezifischen Daten und Informationen ist es absolut erforderlich, diese Gruppe von Usern verstärkt in den Fokus sicherheitsrelevanter Vorkehrungen zu stellen. Der Kreis von Administratoren / Super-Usern erstreckt sich hierbei auf die Ebenen Anwendersystem, Betriebssystem und Datenbank. Dabei hat ebenfalls der Grundsatz Gültigkeit, ausschließlich jene IT-Rollen zu vergeben, welche für die tägliche Ausübung der stellenbezogenen Tätigkeiten erforderlich sind (Minimal- / Stellenprinzip).

Weiterführend dürfen derartige User keine anonymisierten Benutzerkonten verwenden. Jedes Benutzerkonto muss dabei eindeutig einem Mitarbeiter zugeordnet (Identifikationsprinzip) sein (für Entwicklungs- und Qualitätssysteme die auf Datenbanken mit Produktivdaten aufsetzen, und für deren Qualitätstests anonymisierte Testuser benötigt werden, sind deren Nutzung revisionssicher zu dokumentieren [wer-wann-was]) . Tätigkeiten außerhalb des täglichen Aufgabenspektrums, welche beispielsweise die Nutzung eines Notfallusers bzw. eines anonymisierten Standardusers (z.B.: auf Unixebene smdadm) erforderlich machen, sind ausgehend von der Genehmigung des Dateneigentümers systemseitig aufzuzeichnen (Änderungsprotokollierung) und periodisch auszuwerten. In diesem Zusammenhang ist weiterführend zu prüfen, inwieweit kritische Aktivitäten als Bestandteil der täglichen Arbeit grundsätzlich zu protokollieren sind (Nachvollziehbarkeitsprinzip).

Änderungen an Protokollierungseinstellungen sind nur nach Freigabe des fachlich Verantwortlichen zulässig. Der autorisierte Personenkreis für die Pflege der Protokollierungseinstellungen muss sich dabei von jenen unterscheiden, welche die Notfalluser nutzen können. Änderungen an den Einstellungen sind grundsätzlich zu protokollieren. Ein entsprechender Review erfolgt periodisch durch den fachlich Verantwortlichen unter Berücksichtigung des Vier-Augen-Prinzips.

Weiterführend sollen IT User unter Berücksichtigung des Stellen- und Minimalprinzips ausschließlich lesend auf das Produktivsystem zugreifen. Sollte allerdings aufgrund Ihrer Stelle die Erfordernis zur Wahrnehmung von Geschäftsprozessfunktionen (z.B.: Bestellungen) bestehen, so sind diese Berechtigungen entsprechend im P-System einzurichten und zu dokumentieren.
Sämtliche hier beschriebenen Vorgaben sowie mögliche Ausnahmen sind im Berechtigungskonzept nachvollziehbar und angemessen zu dokumentieren.

Kritische Berechtigungen

Von den fachlich Verantwortlichen müssen unter Berücksichtigung des Minimal- und Stellenprinzips (siehe Kapitel 4.2.1) grundsätzlich kritische Berechtigungen identifiziert und analysiert werden, welche ausschließlich von einem kleinen, bekannten Userkreis restriktiv bzw. durch keinen User nutzbar sind (z.B.: siehe unten). In diesem Zusammenhang sind kritische Prozesse / Prozessabschnitte von den fachlich Verantwortlichen zu benennen und der Umgang mit ihnen ist darzustellen. Kritische Berechtigungen sowie ein möglicher autorisierter Userkreis sind nachvollziehbar und angemessen im Berechtigungskonzept zu dokumentieren.

Einheitliches Berechtigungsmanagement umsetzen

Weiterführend ist die Nutzung „kritischer Berechtigungen“ systemseitig zu protokollieren und periodisch auszuwerten (Änderungsprotokollierung). [Insbesondere gesetzeskritische Berechtigungen beispielsweise die Pflege von Änderungsbelegen (löschen/ändern) kann in kaufmännischen Systemen zu einem Gesetzesverstoß führen!]

Für IT-System mit besonderen Anforderungen (Buchhaltung; monetäre Verwaltung) sind nachstehende beispielhafte Berechtigungen insbesondere im Hinblick auf die Ordnungsmäßigkeit der Buchführung zu beachten. Daher dürfen im produktiven System folgende Rechte an keinen klassischen Endanwender vergeben werden:

- Vom Systemhersteller bereitgestellte Standardberechtigungen sind keinem User zuzuweisen. Derartige Bündelungen von Berechtigungen sind in der Regel weitreichend ausgeprägt und entsprechen in ihrer Ausgestaltung in den wenigsten Fällen dem organisatorischen Stellenprofil. Die Zusammenstellung von Berechtigungen für Endanwender ist grundsätzlich an den auszuführenden Stellen / Funktionen zu orientieren (siehe Kapitel 4.2.1).
- Des Weiteren dürfen:
    - Entwicklungsrechte,
    - Berechtigungen zur Pflege der Systemänderbarkeit,
    - Berechtigungen zur Daten- / Tabellenpflege / Customizing,
    - Berechtigungen zur Pflege von Änderungsbelegen (löschen / ändern) sowie
    - Berechtigungen zur Parameterpflege für den Systemzugang

  nicht im QS-/Produktivsystem vergeben werden.
- Berechtigungen zur Ausführung systemkritischer Transaktionen sind nicht zulässig. So ist eine direkte Veränderung der Betriebssystem-Parameter oder ein unmittelbarer Zugriff auf Datenbanken unter Umgehung der Applikationsfunktionen nicht erlaubt.

Auslieferungsuser

Auslieferungsuser dürfen aufgrund Ihrer zum Teil weitreichenden Berechtigungen für Endanwender nicht nutzbar sein. Damit verbundene - u.U. triviale - Passwörter sind unverzüglich zu ändern und unter Einsatz angemessener physischer Sicherheitsvorkehrungen zu schützen (siehe Handlungsleitlinien zur Vertraulichkeitsklasse „geheim“). Diese Auslieferungsuser sind im Hinblick auf die Nachvollziehbarkeit zu einer Gruppe mit entsprechender Kennzeichnung zusammenzufassen (z.B.: SUPER). Sofern möglich, ist darüber hinaus eine Sperrung dieser User anzustreben.

Klassische Endanwender

Im Hinblick auf die Nachvollziehbarkeit und Wartung sind klassische Endanwender in entsprechende Usergruppen (Rechterollen) zusammenzufassen. Die Definition und Rechtefreigabe einer Usergruppe (Rechterolle) orientiert sich in der Regel an den typischen Aufgabenbereichen der Endanwender. In diesem Zusammenhang ist eine Unterteilung nach Geschäftsprozessen (Beschaffung, Vertrieb, Rechnungswesen, Personal etc.) denkbar. Sofern eine weitere Konkretisierung möglich ist, ist die Zuordnung der Benutzer zu Teilprozessen (Hauptbuchhaltung, Nebenbuchhaltung etc.) vorzunehmen.

Einheitliches Berechtigungsmanagement umsetzen

4.3.7 Regeln zur Passwortvergabe

Der Zugang zu den IT-Anwendungen ist durch die Implementierung geeigneter Passwortvorgaben zu schützen. Die „*Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter – Kapitel Zugangskontolle*“ sind als Mindestanforderung zu beachten.

4.4 Anforderungen an die Wirksamkeit

Ziel dieses Abschnitts ist es, Rahmenbedingungen zur Sicherstellung einer kontinuierlichen Angemessenheit und Wirksamkeit von Kontrollen innerhalb des Berechtigungsmanagements zu definieren. Mit der konsequenten Umsetzung dieser Vorgaben wird sichergestellt, dass Prüfungen durch „Dritte“ zu keiner wesentlichen Beanstandungen führen.

4.4.1 Das „berechtigungsspezifische“ interne Kontrollsystem

Die Grundlage für die Wirksamkeit bildet ein regelmäßiges Review bzw. die dann gegebenenfalls erforderliche Aktualisierung aller zum Berechtigungsmanagement gehörenden Dokumente (ORL, OA, Berechtigungskonzept etc.), Prozesse, Rollen und Verantwortungen. Es bleibt zu berücksichtigen, dass die berechtigungsspezifischen Prozesse und Kontrollen ausschließlich einen Teil des unternehmensweiten internen Kontrollsystems darstellen. Nachstehende Vorgaben sind zu beachten und umzusetzen:

- Eine eindeutige und aktuelle Definition und Dokumentation sämtlicher Rollen und Verantwortlichkeiten (fachlich Verantwortliche) sowohl für alle berechtigungsspezifischen Prozesse als auch für jede Kontrolle in Abhängigkeit der Datenklassifizierung. Die Dokumentation ist vom Systembetreiber zu verwalten.
- Die Dokumentation sämtlicher Überprüfungen von Kontrollen erfolgt nach Maßgabe der Fragestellung: Wer hat, Was, Wann, Wie, mit Welchem Ergebnis getan/geprüft? Nur unter Beantwortung dieser Fragestellungen wird eine Dokumentation als angemessen betrachtet.
- Abweichungen von den in den vorangegangen Kapiteln beschriebenen Vorgaben sind nachvollziehbar zu begründen und zu dokumentieren. Die damit verbundenen Risiken sowie Risikominimierungsmaßnahmen sind weiterführend nachvollziehbar aufzuzeigen.
- Eine regelmäßige Plausibilitätsprüfung der Änderungsprotokollierung für kritische Datenobjekte (Objekte, Tabellen etc.) durch den fachlich Verantwortlichen, insbesondere jener Protokolle resultierend aus dem Notfalluser-Einsatz.
- Ein „Self-Assessment“ von Kontrollen stellt keine Wirksamkeit sicher. Die Wirksamkeit kann nur von Personen sichergestellt werden, welche den zu prüfenden Sachverhalt nicht selbst durchführen (Vier-Augen-Prinzip); d.h., eine Prüfung ist ggf. durch Dritte vorzunehmen.
- Die Dokumentation muss geschützt sein vor unautorisiertem Zugriff und hat für jede Gesellschaft einheitlich zu erfolgen.

Einheitliches Berechtigungsmanagement umsetzen

Auf Basis des im Kapitel 4.2.1 definierten Eigenverantwortlichkeitsprinzips ist jede Gesellschaft für die Sicherstellung der Angemessenheit und Wirksamkeit des „berechtigungsspezifischen internen Kontrollsystems“ selbst verantwortlich. Die in diesem Zusammenhang erforderlichen Prüfungsaktivitäten für die periodische Verifizierung der Wirksamkeit sind eigenverantwortlich durch die Gesellschaft zu definieren und durchzuführen.

Zur Prüfung der Wirksamkeit stehen verschiedene Vorgehensweisen zur Verfügung:

- Befragung (des Kontrollverantwortlichen bezüglich der Kontrolle)
- Beobachtung (des Kontrollverantwortlichen bei der Kontrolldurchführung)
- Prüfung (Sichtung der vom Kontrollverantwortlichen erstellten Kontrollnachweise)
- Re-Testing (Selbstdurchführung der Kontrolle)

Um ein hohes Maß an Verlässlichkeit und Wirksamkeit der in diesem Regelwerk definierten Vorgaben zu erzielen, sind die beiden zuletzt genannten Vorgehensweisen anzuwenden.

4.4.2 Tools zur Verwaltung/Prüfung von Berechtigungen

Aufgrund der Komplexität des Themas „Berechtigungsmanagement“ ist der Einsatz von Tools zur Unterstützung der Prozesse und Kontrollen für die „Neuanlage/ Änderungen/ periodischer Review“ sowie dem Entziehen von Berechtigungen zweckdienlich. Eine toolgestützte (evtl. regelbasierte) Prozessbearbeitung erleichtert nicht nur die Tätigkeiten der Analyse, Prüfung und Genehmigung, sondern unterstützt maßgeblich die Kontrollwirksamkeit als auch die Anforderungen an die Dokumentation im Hinblick auf die Nachvollziehbarkeit. Der Abdeckungsgrad erstreckt sich dabei nicht nur auf die klassischen Endanwender, sondern schließt die Usergruppe der Administratoren und Notfalluser ein.

4.4.3 Outsourcing

Im Falle ausgelagerter IT-Anwendungen an externe Dienstleister ist sicherzustellen, dass die zugrunde liegenden Verträge (Service-Level Agreements) eindeutig neben den zu erbringenden Services die Aufgaben und Verantwortlichkeiten beschreiben. Als zentraler Schwerpunkt muss in diesem Zusammenhang die Angemessenheit und Wirksamkeit des internen Kontrollsystems vom Dienstleister Berücksichtigung finden. Eine entsprechende Beurteilung und Prüfung des Kontrollsystems ist insgesamt mindestens jährlich vorzunehmen. Als Orientierung dienen die derzeit gültigen Prüfungsstandards IDW PS 951, SAS70 (SSAE 16) etc.

4.5 Prämissenregelung

Aufgrund des Sachverhalts, dass es sowohl Datenbankensysteme (Inhalte werden vor allem durch Datenbankattribute verwaltet) und Dokumentsysteme (Inhalte werden hauptsächlich durch Dokumente und Metadaten verwaltet) gibt, müssen Sachverhalte

Einheitliches Berechtigungsmanagement umsetzen

sinngemäß angepasst werden. Die Handlungsleitlinien der Vertraulichkeitsklassen sind grundsätzlich zu berücksichtigen und haben Vorrang. Die nachfolgenden Prämissenregelungen geben sinngemäße Umsetzungshilfen.

4.5.1 Berechtigungen auf Daten der Organisationseinheit ohne direkten Fachbezug (z.B. Urlaubskalender, Reiseanträge, Verteilerlisten)

Erfolgt die Pflege von Rollen und Berechtigungen durch den Dateneigentümer (i.d.R. der OE-Leiter) selbst oder einer von ihm bestimmten Person [Stellvertreterregelung] (z.B. Loc-Admin Keyuser, Sekretariat) ist hierfür kein gesonderter Antrag notwendig, die Berechtigungsänderungen (Zuweisung, Entfernung, Änderung) sind entsprechend der Vorgaben der Vertraulichkeitsklasse bei Bedarf zu dokumentieren. Folgende Grundsätze sind hierbei anzuwenden:

- Der Dateneigentümer ist in der Verantwortung die Zugriffsrechte stets aktuell und gültig zu halten, d.h. insbesondere:
    - Für Zugriffe auf „geheim“ klassifizierte Dokumente müssen Berechtigungen/Rollen in Systemen halbjährlich durch den Dateneigentümer überprüft werden
    - Für Zugriffe auf „intern“ oder „vertraulich“ klassifizierte Dokumente müssen Berechtigungen/Rollen jährlich durch den Dateneigentümer/Datenbesitzer überprüft werden
    - Externen Mitarbeitern sind nach Abschluss der Beauftragung Zugriffsrechte kurzfristig zu entziehen
    - Internen und externen Mitarbeitern sind nach einem OE-Wechsel Zugriffsrechte auf OE spezifische Daten kurzfristig zu entziehen
    - Internen Mitarbeitern sind nach dem Ausscheiden aus dem Unternehmen sämtliche Zugriffsrechte kurzfristig zu entziehen

Hinweise für die Vergabe von Zugriffsrechten (analog der Datenweitergabe):
- Es ist stets nach dem Need-to-Know Prinzip (Zugriffe sind zur Erfüllung der Aufgabe notwendig) zu handeln.
- Die Datenschutzanforderungen sind zu berücksichtigen.
- Wann immer möglich, können die Berechtigung über Regelwerke zum Einsatz kommen (siehe 4.5.4).

Voraussetzungen: Das zu Grunde liegende Berechtigungssystem ist an die zentralen IAM Prozesse des Unternehmens angeschlossen.

4.5.2 Zugriff auf Daten eines Projektes mit der Vertraulichkeitsklasse Intern

Erfolgt die Pflege von Rollen und Berechtigungen durch den Dateneigentümer (i.d.R. der OE-Leiter) selbst oder einer von ihm bestimmten Person (z.B. Projektleiter) ist hierfür kein gesonderter Antrag notwendig. Folgende Grundsätze sind hierbei anzuwenden:

Einheitliches Berechtigungsmanagement umsetzen

- Der fachlich Verantwortliche muss das Prinzip der Funktionstrennung im Rahmen seiner Möglichkeiten sicherstellen.
- Der fachlich Verantwortliche ist in der Verantwortung die Zugriffe stets aktuell und gültig zu halten, d.h. insbesondere:
    - Alle Berechtigungen externer Anwender müssen durch den fachlich Verantwortlichen jährlich geprüft und wenn nicht mehr benötigt, entfernt werden.
    - In administrativen Bereichen müssen alle kritischen Berechtigungen/Rollen halbjährlich durch den fachlich Verantwortlichen überprüft werden.
    - In allen anderen Bereichen müssen alle Berechtigungen/Rollen jährlich durch den fachlich Verantwortlichen überprüft werden.
- Der fachlich Verantwortliche kann nach einem erweiterten Need-to-Know Prinzip handeln (Bsp. Bibliotheksdaten, etc).
- Jede Berechtigungsänderung (Zuweisung, Entfernung, Änderung) wird dokumentiert und bis zur Löschung der Daten aufbewahrt. D.h. der fachliche Verantwortliche muss über die bestehenden Berechtigungen jederzeit Auskunft geben können.
- Wann immer möglich, sollte die Berechtigung über Regelwerke zum Einsatz kommen (siehe 4.5.4).

Voraussetzungen: Das zu Grunde liegende Berechtigungssystem ist an die zentralen IAM Prozesse des Unternehmens angeschlossen.

4.5.3 Vergabe von Berechtigungen im Bereich Information Publishing (Bereitstellen einer gleichgearteten Information ohne Bearbeitungsmöglichkeit an einen größeren Anwenderkreis)

Der Dateneigentümer kann die Daten für dienstliche Zwecke mit der Vertraulichkeitsklasse Intern klassifizieren.

Es gelten die Regeln zu 4.5.2.

Folgende Regel entfällt:

- Jede Berechtigungsänderung (Zuweisung, Entfernung, Änderung) wird dokumentiert und bis zur Löschung der Daten aufbewahrt. D.h. der fachlich Verantwortliche muss über die bestehenden Berechtigungen jederzeit Auskunft geben können.

Voraussetzungen: Das zu Grunde liegende Berechtigungssystem ist an die zentralen IAM Prozesse des Unternehmens angeschlossen.

4.5.4 Berechtigung über Regelwerke

Erfolgt der Zugriff auf Daten aufgrund eines vom Dateneigentümer fest definierten Regelwerks (z.B. Zugriff für alle Mitarbeiter einer Abteilung; Zugriff für alle Manager) ist

Einheitliches Berechtigungsmanagement umsetzen

hierfür nur ein einmaliger – zur Einrichtung der Regel führender - Antrag notwendig, die Berechtigungsänderungen (Zuweisung, Entfernung, Änderung) müssen nicht dokumentiert werden. Folgende Grundsätze sind hierbei anzuwenden:

- Das Regelwerk muss vom fachlich Verantwortlichen bestimmt und aktuell gehalten werden.
- Der fachlich Verantwortliche muss stets nach dem Need-to-Know Prinzip handeln.
- Regelwerke müssen verbindliche Vorgaben (Bsp. Handlungsleitlinien aus den Vertraulichkeitsklassen) einhalten.

Voraussetzungen: Das zu Grunde liegende Berechtigungssystem ist an die zentralen IAM Prozesse des Unternehmens angeschlossen.

Einheitliches Berechtigungsmanagement umsetzen

5. Weiterführende Erläuterungen

5.1 Begriffsbestimmungen

Die Umsetzung des Regelwerks bedingt eine enge Zusammenarbeit zwischen den fachlich Verantwortlichen aus dem Fachbereich und der IT. Für das Verständnis dieser Zusammenarbeit sind nachstehend wesentliche Begriffe dieses Dokumentes erläutert.

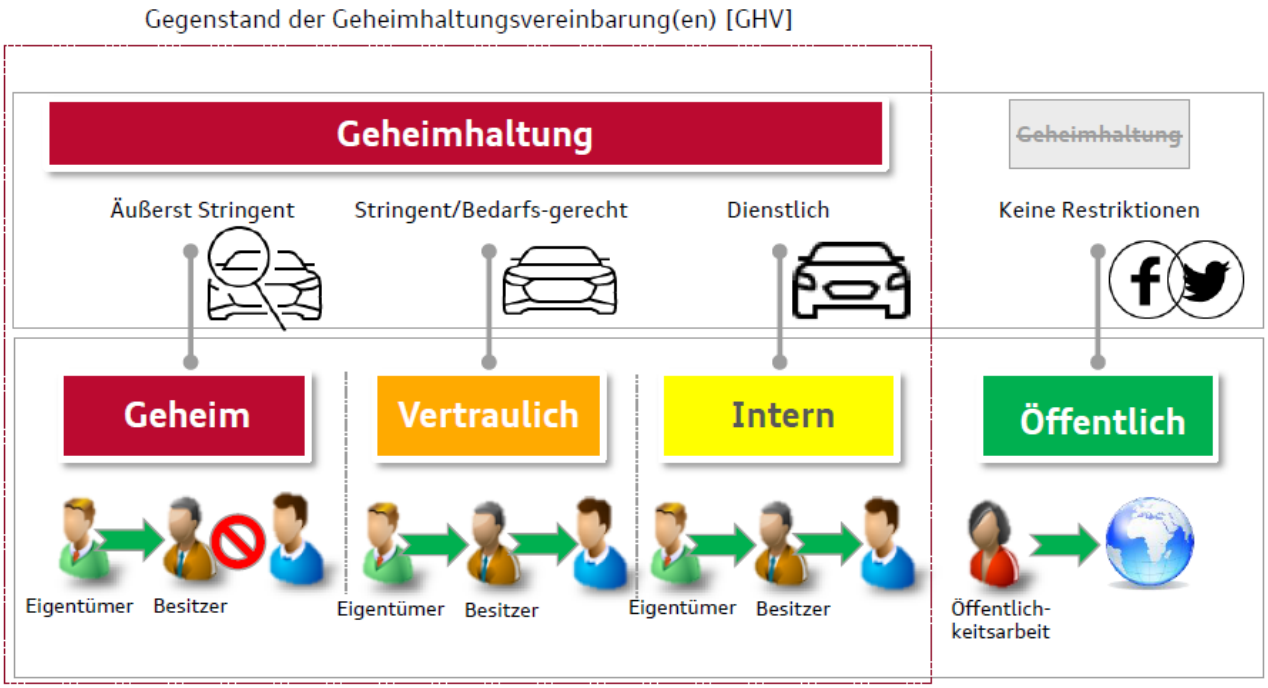
Begriff	**Beschreibung**
AktG	Deutsches Aktiengesetz
Auslieferungs-User	Auslieferungs-User sind vorkonfektionierte Berechtigungsrollen, die mit Implementierung von Standardsoftwarekomponenten automatisch in einem System zur Verfügung stehen.
DSGVO / GDPR	Datenschutzgrundverordnung / General Data Protection Regulation
BilMoG	Bilanzrechtsmodernisierungsgesetz
COSO	Das Committee of Sponsoring Organizations of the Treadway Commission (COSO) hat anerkannte Standards veröffentlicht, um Unternehmen und andere Organisationen dabei zu unterstützen, ihre (insbesondere die Finanz-Perspektive betreffenden) internen Überwachungssysteme zu beurteilen und zu verbessern (COSO-Modell, COSO Enterprise Risk Management Framework, COSO-Leitfaden).
CobiT	CobiT (Control Objectives for Information and Related Technology) ist das international anerkannte Framework zur IT-Governance und gliedert die Aufgaben der IT in Prozesse und Control Objectives.
Dateneigentümer	Im Sinne dieses Dokumentes ist der „Dateneigentümer“ der „Eigentümer von fachlichen Daten“ und damit im Rahmen der Governance und Qualität von Daten für einen bestimmten Teil der Unternehmensdaten zuständig (unabhängig von den zum Einsatz kommenden Systemen). Ausschließlich der Dateneigentümer verantwortet die Vergabe von Zugriffsberechtigungen für Informationen der Vertraulichkeitsklasse „geheim“ (siehe Abschnitt 5.2).
Datenbesitzer	Der Datenbesitzer (auch Informationsnutzer durch Erteilung von Leserechten) kann die Weitergabe von Informationen (auch Zugriffsrechteerteilung) unter Berücksichtigung der Empfängerkriterien (GHV vorhanden; Vertragsverhältnis; Need to know) für die Vertraulichkeitsklassen „vertraulich“ und „intern“ verantworten (siehe Abschnitt 5.2).
Fachbereich	Als „Fachbereich“ werden in diesem Dokument alle Einheiten einer Konzerngesellschaft bezeichnet, für die das Management von Berechtigungen in Systemen notwendig ist. Im Spezialfall, in dem IT-interne Systeme betrachtet werden, ist die IT selbst in der Funktion des Fachbereichs. Diese Sondersituation unterscheidet sich von den Rechten und Pflichten dieses Regelwerkes jedoch in keiner Weise von den anderen Fällen. Es gelten im

Einheitliches Berechtigungsmanagement umsetzen

	exakt gleichen Maße die Maßgaben dieses Regelwerkes. Aus diesem Grund wird unter dem Begriff „Fachbereich“ immer die Sondersituation implizit mit verstanden, dass die IT den Fachbereich darstellt.
GoB	Die Grundsätze ordnungsmäßiger Buchführung (GoB) sind teils geschriebene, teils ungeschriebene Regeln zur Buchführung und Bilanzierung, die sich vor allem aus Wissenschaft und Praxis, der Rechtsprechung sowie Empfehlungen von Wirtschaftsverbänden ergeben
GoBS	Die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) sind von der deutschen Finanzverwaltung aufgestellte Regeln zur Buchführung mittels Datenverarbeitungssystemen.
HGB	Deutsches Handelsgesetzbuch
Klassischer End-User	Unter dem Begriff „klassischer End-User“ ist eine Berechtigungsrolle zu verstehen, die bezogen auf ein System die Rechte für eine übliche Nutzung des Systems abdeckt.
Kritische Berechtigungen	Berechtigungen, die im Sinne der Sicherheit oder aus rechtlicher oder betriebswirtschaftlicher Sicht kritische Operationen erlauben, werden "Kritische Berechtigung" genannt. Betroffen sind z. B. Operationen, die zu Betrug führen können oder über die wichtige Daten und Konfigurationen gelesen oder modifiziert werden können.
KonTraG	Deutsches Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
Rechterolle	Der Begriff Rolle bezeichnet in diesem Dokument durchweg die mit einer Berechtigungsvergabe verbundene Kombination von Berechtigungen bzgl. Daten- und Funktionszugriffen innerhalb eines Systems. Es ist also eine Berechtigungsrolle damit gemeint und nicht die prozessuale oder organisatorische Eingliederung einer Person im Unternehmen.
System	Die Begriffe System, Anwendung und Applikation werden in diesem Dokument synonym verwendet. Darüber hinaus deckt ein System in diesem Dokument alle Ebenen „Applikation“, „Datenbank“, „Betriebssystem“ ab und ist unabhängig von der zum Einsatz kommenden Technologie. Der Begriff „System“ wird in diesem Regelwerk für die einzelnen Ebenen verwendet.
IT	Ist in diesem Dokument von „IT“ die Rede, sind damit IT-Dienstleistungen erbringende Einheiten gemeint, die aufgrund einer Beauftragung eines Dateneigentümers das Berechtigungsmanagement in entsprechenden IT-Systemen umsetzen.

Einheitliches Berechtigungsmanagement umsetzen

5.2 Informations- und Datenklassifizierung – Handlungsleitlinien



Empfängerkriterien:

- ✓ Hat eine gültige GHV
- ✓ Hat einen bestehenden Vertrag
- ✓ Benötigt die Information zur Erfüllung seiner Aufgabe

Einheitliches Berechtigungsmanagement umsetzen

6. Weitere Dokumentation

6.1 Anlagen

Dem Basisdokument zugehörige Dokumente, die verbindlich und zur Umsetzung der Anforderungen notwendig sind.

Dokument	Beschreibung
Roles-and-Rights-Concept-Template_BX	Template Berechtigungsmanagement

6.2 Mitgeltende Dokumente

Nicht mit dem Basisdokument entstandene Dokumente, auf die verwiesen wird. Diese sind verbindlich und zur Umsetzung der Anforderungen notwendig.

Dokument	Beschreibung
RR-Check-Template_BX	Checkliste Berechtigungsmanagement
URLB_024 Ebene 2 (mehrere Dokumente)	URLB_024 - Ebene 2: Informationssicherheitsrichtlinien für - IT-Sicherheitshandlungsleitlinie für Führungskräfte - IT-Sicherheitshandlungsleitlinie für externe Partnerfirmen - IT-Sicherheitshandlungsleitlinie für Systembetreiber und Administratoren - IT-Sicherheitshandlungsleitlinie für Systementwickler

6.3 Weiterführende Dokumente

Nicht mit dem Basis-Dokument entstandene Dokumente, auf die verwiesen wird. Diese dienen zur Information, sind jedoch zur Umsetzung der Anforderungen nicht notwendig.

Dokument	Beschreibung
VW_R10_Regelwerk_zum_Berechtigungsmanagement.pdf	Einheitliches Regelwerk zum Berechtigungsmanagement

7. IT-Systeme

Folgende Standardsysteme sind wenn möglich zu verwenden:

Einheitliches Berechtigungsmanagement umsetzen

IT-System	Langbezeichnung
ZEBRA / VCD	Zentrales Benutzer Ressourcenverzeichnis Audi / Volkswagen Corporate Directory
SPiiDER	Standard Protocol based Internet and Intranet Directory as an Ebusiness Registry
KIRA	Konzern Identitäts- und Rollen Administration
RRV2	Rollen- und Rechteverwaltung 2
TAM SSO	Tivoli Access Manager Single Sign On

Dies gilt nicht für Berechtigungsmanagement im Fahrzeug und für Endkunden.

8. Änderungsdienst, Änderungshistorie, Geltungsbereich

8.1 Änderungsdienst

Nächster Überprüfungstermin: 01.10.2023

8.2 Änderungshistorie:

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	16.09.2019	Veröffentlicht
1.1	Andreas Walter	B/FP	01.10.2020	Anpassung wegen Änderung zu Vorstand

8.3 Geltungsbereich

Diese Regelung gilt für AUDI BRUSSELS und ist mit der Veröffentlichung sofort gültig.