- **Access-Management**
  Das Access-Management regelt den Vergabeprozess von Zugriffsrechten auf IT-Systeme.
- **Atomares Recht**
  Ein „atomares Recht" ist ein in sich geschlossenes, nicht mehr weiter unterteilbares Recht in einem physischen Zielsystem.
- **Authentifizierung**
  Bei der Authentifizierung wird überprüft, ob eine Person oder ein Objekt tatsächlich der oder dasjenige ist, was er oder es zu sein vorgibt. Ein Vorgang, bei dem der Anwender seine Herkunft belegt.
- **Authentifizierungsdienst**
  Der Authentifizierungsdienst ist das System, das den Vorgang der Authentifizierung durchführt.
- **Benutzer**
  Ein Benutzer ist eine natürliche Person oder ein IT-System. Einer natürlichen Person oder einem IT-System können mehrere Benutzer zugeordnet sein, um auf andere IT-Systeme zuzugreifen.
- **Benutzerkennung**
  Die Benutzerkennung ist der eindeutige Name, meist eine Zeichenfolge, die eindeutig einem Benutzer zugeordnet ist. Die Benutzerkennung wird oft zur Anmeldung an einem Benutzerkonto genutzt.
- **Benutzerkonto**
  Bei einem Benutzerkonto handelt es sich um eine technische Repräsentation eines Benutzers in einem konkreten rechteführenden System. Zugriffe auf IT-Systeme werden mit Hilfe des Benutzerkontos gesteuert.
- **Berechtigungskonzept**
  Das Berechtigungskonzept beschreibt je IT-Service Details zu den einzelnen Rechten und Rollen dieses IT-Services. Es wird der Soll-Zustand der Berechtigungen dokumentiert. Die Konzipierung kann in der IAM-Lösung erfolgen, sofern die Entscheidung getroffen wird. Das Wort „Konzept“ beschreibt den Prozess, nicht ein Dokument.
- **Business Rolle**
  Eine Business Rolle ist eine Serviceübergreifende Bündelung von Rollen. Diese

© 2026 Punktgenau Beratung GmbH.
Alle Rechte vorbehalten. Vervielfältigung nur mit schriftlicher Genehmigung.

besteht ausschließlich aus technischen Funktionsrollen. Ein- und dieselbe technische Funktionsrolle kann in mehreren Business Rollen verwendet werden.

- **Dateneigner**
  Der Dateneigner ist der Verantwortliche für eine Rolle. Er ist zuständig für Genehmigungen in Bestellungen und Rezertifizierungen vergebener Berechtigungen seiner Rolle(n).
- **Digitale Identität**
  Die digitale Identität repräsentiert eine natürliche Person in der digitalen Welt.
- **Funktion**
  Eine Funktion ist ein klar definierter Aufgaben-, Verantwortungsbereiche, der in Stellenbeschreibungen beschrieben ist. Einzelne Funktionen können so in Stellenbeschreibungen in einer Stelle zusammengefasst werden. Die Stellen werden schließlich Personen zugeordnet, sodass am Ende jede Funktion inklusive ihrer Aufgaben auch einer oder mehreren Personen (z. B. Vertreter) zugeordnet ist.
- **IAM**
  Identity- und Accessmanagement, ist ein System zur Verwaltung von Identitäten und der Steuerung zugehöriger Berechtigungen (Benutzerberechtigungsmanagement).
- **IAM-Lösung**
  Die IAM-Lösung beschreibt sämtliche Komponenten zur Umsetzung der Benutzerberechtigungsverwaltung. Diese erfolgt sowohl toolbasiert als auch vereinzelt über manuelle Prüf-/Umsetzungsmechanismen.
- **IAM-Tool**
  Das IAM-Tool ist das tatsächlich verwendete Tool.
- **Identität**
  Eine Identität repräsentiert eine natürliche Person. Die führende Datenhaltung erfolgt in der IAM-Lösung. Eindeutiges Kennzeichen ist die Personalnummer. Jede digitale Identität ist eineindeutig einer natürlichen Person zugeordnet. Jede natürliche Person hat nur eine digitale Repräsentation. Jedoch kann eine Identität mehrere Benutzer haben.

© 2026 Punktgenau Beratung GmbH.
Alle Rechte vorbehalten. Vervielfältigung nur mit schriftlicher Genehmigung.

- **Identity-Management**
  Unter dem Identity-Management versteht man die Verwaltung von einer Vielzahl von Identitäten, welche aus dem führenden HR-System an das IAM übermittelt werden.
- **Informationseigentümer**
  Der Informationseigentümer ist für den gewährten Zugriff auf seine Informationen verantwortlich und muss ihre Zugänglichkeit sowie den Umfang und die Art der Autorisierung des Zugriffes definieren.
- **Informationstreuhänder**
  Der Informationstreuhänder ist ein Rechtssubjekt, das aufgrund eines Treuhandvertrages oder gesetzlich dazu verpflichtet ist, die Interessen eines anderen Rechtssubjekts wahrzunehmen, in diesem Fall kann ein Provider per Vertrag zum Informationstreuhänder eines Unternehmens ernannt werden.
- **IT-Service**
  Ein IT-Service ist eine Zeile in der Master-Service-Liste. Auf dieser Ebene müssen die gültigen IAM-Prozesse (speziell Berechtigungskonzipierungen) gelebt werden.
- **IT-System**
  IT-Systeme speichern und verarbeiten Informationen. Information werden in Form von Daten und Datenobjekten repräsentiert.
- **Kennwort**
  Geheimnis, das zur Authentifizierung genutzt werden kann.
- **Non Personal Account (NPA)**
  Ein Non Personal Account ist ein Benutzerkonto, das keiner natürlichen Person fest zugeordnet werden kann
- **Notfall-User**
  Notfall-User sind privilegierte Benutzer für spezielle Einsatzfälle außerhalb des Regelbetrieb. Die Nutzung der Accounts unterliegt besonderen Bedingungen und wird speziell überwacht (z. B. 4-Augen-Prinzip, Protokollierung).
- **Privilegierte Benutzer**
  Im Sprachgebrauch kurz für Benutzerkennungen privilegierter Benutzerkonten. Ebenfalls systemseitig vorgegeben, wie bspw. root, admin, sys, usw. Dem

© 2026 Punktgenau Beratung GmbH.
Alle Rechte vorbehalten. Vervielfältigung nur mit schriftlicher Genehmigung.

Benutzerkonto sind weitreichende, in der Regel administrative Berechtigungen zugeordnet.

- **Rechteführendes System**
  Ein IT-System, bei dem Zugang und Zugriff durch Authentifizierung und Autorisierung geschützt sind. Beides kann am IT-System erfolgen oder an ein anderes IT-System ausgelagert sein, z. B. einen Authentifizierungsdienst.
- **Rechtegruppe**
  Rechtegruppen fassen atomare Rechte zusammen und sind eindeutig einem IT-Service zuzuordnen. Die Einrichtung der Rechtegruppen liegt nicht in der Verantwortung von IAM, sondern des Services, der die Rechtegruppe einrichtet.
- **Ressource Owner**
  Der Ressource Owner ist der Verantwortliche für eine Rolle oder einzelne Berechtigung. Er ist zuständig für Genehmigungen in Bestellungen und Rezertifizierungen vergebener Berechtigungen seiner Rolle(n) oder Berechtigungen.
- **Rolle**
  In IT-Anwendungen werden die zur Wahrnehmung einer Funktion notwendigen Berechtigungen gewöhnlich in sogenannten Rollen zusammengefasst. Die Rolle ist also die Abbildung einer Funktion in einer IT-Anwendung, die dann den in der Anwendung eingerichteten Benutzern zugeordnet werden kann.
- **Rollen-Lifecycle**
  Der Rollen-Lifecycle beschreibt den Lebenszyklus einer Rolle. Von der Entstehung, über Änderung bis hin zur Löschung.
- **Segregation of Duties (SoD)**
  Unter SoD ist die Funktionstrennung zu verstehen, welche gewährleisten soll, dass nicht vereinbare Tätigkeiten auf Ebene der Identität getrennt werden.
- **Funktionsrolle**
  Eine Funktionsrolle besteht aus oder mehreren Rechtegruppen.
- **Vergabe**
  Eine Vergabe beschreibt die Zuweisung einer Rolle an einen Benutzer
- **Zugriff**
  Digitaler Zugriff auf Daten eines IT-Systems gemäß Autorisierung.

© 2026 Punktgenau Beratung GmbH.
Alle Rechte vorbehalten. Vervielfältigung nur mit schriftlicher Genehmigung.