

- **Access-Management**  
Die Verwaltung von Zugangsrechten.
- **Access request**  
Die Anforderung des Zugriffs auf Ressourcen.
- **Access request process**  
Der gesamte Prozess, um Ressourcen anzufordern, einschließlich Genehmigung und Zuweisung.
- **Account**  
Benutzerkonto
- **Account ownership**  
Die für ein Benutzerkonto verantwortliche Identität.
- **Account type**  
Die Art des Benutzerkontos – persönlich (nicht-privilegiert / privilegiert) oder nicht-persönlich.
- **Actual state**  
Aktuelle Zugriffsrechte, die Nutzer auf IT-Systeme haben.
- **Application**  
Eine Anwendung, deren Berechtigungen vom IAM-Tool als Rollen verwaltet werden.
- **Application owner**  
Die im IAM-Tool hinterlegte verantwortliche Person für eine Anwendung.
- **Application role**  
Zusammenfassung einer oder mehrerer Berechtigungen einer Anwendung in Rollen, die im IAM-Tool verwaltet werden.
- **Assignment policy**  
Eine Zuweisungsrichtlinie, die definiert, dass eine Menge von Identitäten einer Menge von Ressourcen automatisch zugewiesen werden sollen.
- **Attestation**  
Die Überprüfung und Validierung von Zugriffsrechten im IAM-Tool.
- **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 rechtführenden 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.

- **Birthrights**

Birthrights sind „Geburtsrechte“, die Personen automatisch zugewiesen werden, wenn sie beispielsweise über die Zugehörigkeit zu einem Unternehmen, einer Abteilung, einem Team oder einer Position im IAM-Tool zugeordnet werden können.

- **Business Rolle**

Eine Business Rolle ist eine Serviceübergreifende Bündelung von Rollen. Diese besteht ausschließlich aus technischen Funktionsrollen. Ein- und dieselbe technische Funktionsrolle kann in mehreren Business Rollen verwendet werden.

- **Classification tags**  
Eine Methode, um Rollen oder Berechtigungen zu kennzeichnen, damit geeignete Richtlinien angewendet werden können, um die Einhaltung von Vorgaben sicherzustellen.
- **Compliance**  
Die Einhaltung klar definierter Vorgaben.
- **Compliance status**  
Die Bewertung von Zuweisungen von Rollen oder Berechtigungen zu Benutzerkonten anhand eines festgelegten Maßstabs.
- **Connected system**  
Das Quellsystem, das die tatsächlich vorhandenen Konten und Zuweisungen zu Berechtigungen ausweist. Siehe auch: Actual state.
- **Constraint**  
Toxische Kombinationen von Ressourcenzuweisungen, die vorher im IAM-Tool definiert wurden.
- **Constraint policy**  
Eine Richtlinie im IAM-Tool, die die Zuweisung toxischer Kombinationen verhindert.
- **Context**  
Eine Möglichkeit, Nutzer zu gruppieren, damit sie auf die gleiche Weise verwaltet werden können.
- **Dateneigner**  
Der Dateneigner ist der Verantwortliche für eine Rolle. Er ist zuständig für Genehmigungen in Bestellungen und Rezertifizierungen vergebener Berechtigungen seiner Rolle(n).
- **Deprovisioning**  
Das Entfernen einer zugewiesenen Rolle oder Berechtigung.
- **Digitale Identität**  
Die digitale Identität repräsentiert eine natürliche Person in der digitalen Welt.
- **Emergency logout**  
Ein Prozess, der alle mit einer Identität verbundenen Konten deaktiviert, wenn ein Sicherheitsverstoß vermutet wird.

- **Funktion**  
Eine Funktion ist ein klar definierter Aufgaben-, Verantwortungsbereich, 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.
- **Funktionsrolle**  
Eine Funktionsrolle besteht aus oder mehreren Rechtegruppen.
- **HR system**  
Das Personalführungssystem, aus dem das IAM-Tool relevante Personaldaten erhält und verarbeitet.
- **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.
- **Identity-Lifecycle-Management**  
Der Prozess, der den gesamten Beschäftigungszyklus einer Person im Unternehmen, von der Einstellung bis zum Ausscheiden, abbildet.
- **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 Zugriffs 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.

- **Manager**

Der Manager ist die im IAM-Tool eingetragene Führungskraft von Mitarbeitenden.

- **Master data**

Persönliche und andere relevante rechtliche Informationen über Mitarbeitende oder Externe, wie Name, Position oder Manager, die im IAM-Tool verarbeitet werden.

- **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).

- **Offboarding**  
Ein Prozess, der sicherstellt, dass Personen nach dem Ausscheiden aus dem Unternehmen alle im IAM-Tool verwalteten Zugriffe entzogen werden.
- **Onboarding**  
Eine Identität im IAM-Tool zu erstellen.
- **Orphan account**  
Ein Benutzerkonto im IAM-Tool, für das keine verantwortliche Person eingetragen ist.
- **Privilegierte Benutzer**  
Im Sprachgebrauch kurz für Benutzerkennungen privilegierter Benutzerkonten. Ebenfalls systemseitig vorgegeben, wie bspw. root, admin, sys, usw. Dem Benutzerkonto sind weitreichende, in der Regel administrative Berechtigungen zugeordnet.
- **Provisioning**  
Die Bereitstellung einer automatisierten oder beantragen Zuweisung von Rollen oder Berechtigungen.
- **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.
- **Resource**  
Eine Ressource kann entweder eine Berechtigung oder eine Rolle sein.
- **Resource 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.

- **Resource assignment**

Die einer Person zugewiesene Berechtigung oder Rolle.

- **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.

- **System**

Ein physisches IT-System wie ein Verzeichnisdienst, eine Finanzanwendung oder ein HR-System.

- **System owner**

Die verantwortliche Person für ein System.

- **Technical identity**

Eine Identität, der die nicht-persönlichen Benutzerkonten zugeordnet werden, zum Beispiel in einer Applikation.

- **Vergabe**

Eine Vergabe beschreibt die Zuweisung einer Rolle an einen Benutzer

- **Zugriff**

Digitaler Zugriff auf Daten eines IT-Systems gemäß Autorisierung.