IAM-Regelung

Gültig ab	TT/MM/JJJJ
Verantwortlich / Name	Abteilung / Vorname Name
Sprachversion	DE
Sicherheitsklasse	Einstufung nach Unternehmensvorgaben

Inhalt

1. Umfang

Der Anwendungsbereich der Richtlinie Identity and Access Management (IAM) umfasst alle im Unternehmen **(Name des Unternehmens)** verwendeten IT-Dienste sowie alle damit verbundenen Infrastruktur- und Sicherheitsmaßnahmen im Zusammenhang mit den beteiligten IT-Systemen.
Der Anwendungsbereich umfasst alle Standorte mit allen organisatorischen Einheiten, Projekten, Managern und Mitarbeitern von **(Name des Unternehmens)**, d. h. die Richtlinie ist für alle im Kontext von Diensten und -Anwendungen gültig und verbindlich.
Diese Regelung muss von allen Einheiten eingehalten werden, die für die Entwicklung, Bereitstellung und Implementierung von Identitäts- und Zugriffsmanagementsystemen verantwortlich sind, sowie von allen IT-Diensten (IT-Systeme, Plattformen, Anwendungen).
Nutzen Sie dieses Dokument, um Produkt- oder Anbieterstrategien zu bewerten und dabei alle Konzepte und Verfahren auf die Machbarkeit zu berücksichtigen.

2. Gegenstand

Diese Verordnung beschreibt die Umsetzung von Identity- und Access-Management (IAM) im Unternehmen **(Name des Unternehmens)** mit der IAM-Lösung **(Name des Herstellers)**. Alle Prinzipien, Spezifikationen, Verfahren und Prozesse sind in der **(Name des Herstellers)**-Dokumentation technisch und fachlich zu beschreiben.

3. Inhalt

A. Anforderungen

(Name des Unternehmens) muss die Anforderungen von Gesetzen, Verträgen und seinen eigenen Richtlinien einhalten. Der folgende Abschnitt beschreibt ausführlich, welche Anforderungen und welche Prinzipien für **(Name des Unternehmens)** relevant sind. Die Vorschriften des IT-Grundschutzes, insbesondere Kapitel ORP.4 Identitäts- und Berechtigungsmanagement nach Bundesamt für Sicherheit in der Informationstechnik (BSI) und der ISO 27001-Norm gelten. Die folgenden Prinzipien sind für **(Name des Unternehmens)** definiert.

Identitätsprinzip
Benutzer-IDs sind eindeutig mit Einzelpersonen verknüpft, sodass sie nicht neu zugewiesen werden können. Das Identitätsprinzip beschreibt die Zuweisung von Identitäten an Mitarbeiter und IT-Ressourcen.

Least privilege Prinzip
Dieses Prinzip besagt, dass den Nutzern nur die Zugriffsrechte gewährt werden sollten, die für die Ausführung ihrer spezifischen Aufgaben notwendig sind. Rechte, die über das Notwendige

hinausgehen, stellen ein potenzielles Sicherheitsrisiko dar und müssen vermieden werden. Zugriffsrechte sollten so detailliert wie möglich vergeben, regelmäßig überprüft und automatisch angepasst oder widerrufen werden, wenn sich Rollen oder Aufgaben ändern. Dieser Ansatz verringert die Angriffsfläche des gesamten Systems und erhöht die Vertraulichkeit der Daten.

Dokumentationsprinzip

Ein zentrales Element des Dokumentationsprinzips ist die auditsichere Rückverfolgbarkeit aller entscheidungsrelevanten Aktivitäten. Jede Abtretung, Änderung oder Entzug von Rechten sollte systematisch dokumentiert, genehmigt und dauerhaft speicherbar sein. Dazu gehört das Protokollieren von Zugriffsversuchen, die Genehmigung durch den Vorgesetzten (z. B. über Workflows) sowie die Begründung temporärer Ausnahmen oder Sonderrechte. Ziel dieses Prinzips ist es, vollständige Transparenz und Rechenschaftspflicht im Falle von Sicherheitsvorfällen, Prüfungen oder internen Kontrollen sicherzustellen.
Eine qualifizierte Begründung erfordert einen Verweis auf die Tätigkeit, die mit den beantragten oder erteilten Genehmigungen durchgeführt werden soll. Begründungen sind Teil der Kontroll- und Überwachungsdokumente und müssen "systematisch und verständlich für sachkundige Dritte erstellt werden". Um die Rechteanforderungen zu klären, geben Sie sowohl die Rolle des Mitarbeiters als auch die relevante Tätigkeit an.
Eine praktische Vorlage für eine qualifizierte Begründung ist wie folgt:

- In meiner Funktion als <eigene Funktion> benötige ich diese Rolle (oder Genehmigungen?)
- damit die <Aktivität(en)> ausgeführt werden sollen.

Je spezifischer die Platzhalter <eigene Funktion> und <Aktivitäten> sind, desto besser. Im Folgenden finden Sie einige Beispiele für qualifizierte Begründungen, die nach diesem Muster erstellt wurden:

- In meiner Rolle als DB2-Datenbankadministrator brauche ich diese Rolle, um die Datenbankleistung zu überwachen und zu optimieren.
- In meiner Rolle als Sicherheitsadministrator brauche ich diese Rolle, um Workflows im IAM-Tool bereitzustellen.
- In meiner Funktion als Anwendungsadministrator brauche ich diese Rolle, um die Anwendung xyz auf Linux-Servern zu installieren.

Es ist wichtig, dass der angegebene Grund verständlich ist und dass die Rechteanforderung daraus abgeleitet werden kann. Eine unverständliche Begründung ist dabei keine Begründung.

Genehmigungsprinzip

Das Genehmigungsprinzip umfasst die Rückverfolgbarkeit von Genehmigungen, insbesondere bei der Beantragung von Genehmigungen.

Vier-Augen-Prinzip

Dieses Kontrollprinzip besagt, dass besonders sicherheitskritische Maßnahmen, wie das Löschen sensibler Daten oder die Übertragung weitreichender Administratorrechte, nur nach

Genehmigung durch eine zweite autorisierte Person durchgeführt werden dürfen. Ziel ist es, Fehler oder Missbrauch durch Einzelpersonen zu vermeiden und mehr Transparenz in entscheidungskritischen Prozessen zu gewährleisten. Das Vier-Augen-Prinzip wird üblicherweise mittels technischer Hilfsmittel oder Genehmigungsmechanismen umgesetzt – eine technische Implementierung sollte daher, wo möglich, genutzt werden, um Geschäftsrisiken zu reduzieren.

Regelungsprinzip

Das Kontrollprinzip besagt, dass eine unabhängige dritte Kontrollinstanz stets die Einhaltung der Autorisierungsmanagementprinzipien und -prozesse überprüfen kann. Dazu gehört die Eignung des Geschäftsantrags und der damit verbundenen Prozesse bezüglich der regelmäßigen Überprüfung der Genehmigungen durch die jeweiligen Prozessakteure sowie die Überprüfung durch die interne Revisionsabteilung oder externe Prüfer. Das Kontrollprinzip stellt sicher, dass sowohl historische als auch aktuelle Autorisierungszuweisungen überprüft werden können.

Funktionstrennungsprinzip

Das Prinzip der Funktionstrennung muss bei der Gestaltung und Vergabe von Rollen beachtet werden. Die Trennung der Funktionen beschreibt die sich gegenseitig ausschließenden Kombinationen von Aufgaben und Verantwortlichkeiten. Bei der Gestaltung der organisatorischen und operativen Struktur muss darauf geachtet werden, dass unvereinbare Aktivitäten von verschiedenen Mitarbeitern durchgeführt werden und Interessenkonflikte vermieden werden.
Das Prinzip der Trennung der Funktionen wird in allen IT-Dienstleistungen organisatorisch geregelt und umgesetzt. Der Eigentümer der Daten ist für die Regeln und Kontrollen der Implementierung verantwortlich.

Verantwortungsprinzip

Im Kontext des Autorisierungsmanagements beschreibt das Verantwortungsprinzip die Verantwortung der jeweiligen Abteilungen für die Umsetzung und Einrichtung des Genehmigungsmanagements. Das Verantwortungsprinzip definiert auch die Verantwortlichkeiten der Prozessakteure hinsichtlich der Einhaltung der Anforderungen an das Autorisierungsmanagement.

Zero-Trust-Prinzip

Dieses Prinzip setzt voraus, dass kein Nutzer automatisch vertrauenswürdig ist. Es spielt keine Rolle, ob es im internen oder externen Netzwerk ist. Jeder Zugang sollte einzeln überprüft und bei Unsicherheit abgelehnt werden. Zero Trust erfordert daher nicht nur starke Authentifizierungsmechanismen, sondern auch dynamische, feinkorrelierte Autorisierungsrichtlinien, die in Echtzeit angepasst werden können. Vertrauen ist daher keine Voraussetzung, aber jede Systeminteraktion muss kontinuierlich überprüft werden.

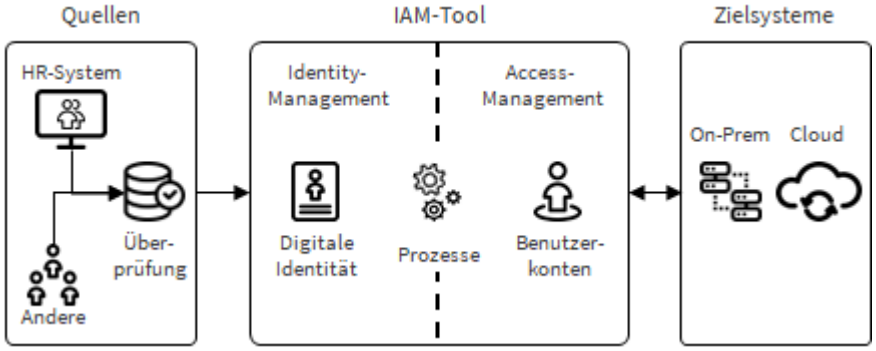
Rollenbeschreibungsprinzip

Rechte und Rollen müssen für alle IT-Dienste entworfen und schriftlich festgehalten werden. Die oben genannten Prinzipien müssen immer angewendet werden. Rechte und Rollen sollten

angemessen für den Empfänger beschrieben werden. Ziel ist es, sicherzustellen, dass eine sachkundige dritte Partei schnell ein Verständnis dafür entwickelt, welcher Zweck mit welcher Rolle erreicht werden kann. Detaillierte Rollenbeschreibungen für jede Rolle müssen im individuellen Autorisierungskonzept eines IT-Dienstes festgehalten werden.

B. Identity- und Access-Management (IAM)

IAM umfasst alle Prozesse, Technologien und Richtlinien, die sicherstellen, dass nur autorisierte Personen oder Systeme zur richtigen Zeit, im richtigen Umfang und unter den richtigen Bedingungen auf IT-Ressourcen zugreifen können. Es handelt sich um ein systemisches Sicherheits- und Organisationskonzept, das alle digitalen Identitäten und deren Zugriffsrechte regelt. IAM wird nicht nur für die technische Kontrolle des Zugangs genutzt, sondern auch für die organisatorische Kontrolle von Verantwortlichkeiten und Sicherheitsrichtlinien.
Das Ziel von IAM ist es, digitale Identitäten einzigartig zu verwalten und den Zugang zu Systemen, Netzwerken, Anwendungen und Daten rückverfolgbar, verifizierbar und kontrollierbar zu machen. Eine digitale Identität kann nicht nur ein menschlicher Nutzer sein, sondern auch eine technische Einheit wie eine Maschine, ein Servicekonto oder eine Anwendung. Die Genauigkeit und Aktualität der erfassten Identitätsinformationen sind entscheidend für die Sicherheit des gesamten Systems.



Wie in der obigen Abbildung gezeigt, integriert das IAM-Tool diese Aspekte nahtlos, um den operativen Overhead zu minimieren und gleichzeitig ein erhöhtes Sicherheitsniveau zu gewährleisten. Basierend auf überprüften Identitäten des HR-Tools oder ähnlichen Tools erstellt das IAM-Tool digitale Identitäten und weist Benutzerkonten für den Zugriff auf Zielsysteme zu. Auf diese Weise beantwortet das IAM-Tool die grundlegenden Fragen: Wer ist ein Nutzer? Was darf dieser Nutzer tun? Und wie wird sichergestellt, dass dies kontrolliert, dokumentiert und, falls nötig, geändert oder zurückgezogen werden kann? Zu diesen Aufgaben gehören die technische Implementierung von Zugriffskontrollen sowie die organisatorische Gestaltung von Prozessen, Vorbildern, Eskalationskanälen und Genehmigungsschritten.

Identity-Management

Identity-Management stellt sicher, dass jede digitale Identität, wie die von Mitarbeitern, Geschäftspartnern, Kunden oder technischen Systemen, klar erfasst, verwaltet und gepflegt wird.

Sie umfasst die gesamten Informationen, die eine Person eindeutig beschreiben. Dazu gehören nicht nur klassische Masterdaten wie Name, E-Mail-Adresse oder Personalnummer, sondern auch kontextuelle Attribute wie die Mitgliedschaft in einer Abteilung, eine Position oder standortbezogene Merkmale.
Eine digitale Identität ist daher ein strukturierter Datensatz, der sowohl identifizierende Merkmale (z. B. Benutzername) als auch beschreibende Eigenschaften (z. B. Abteilung, Position) enthält. Jede Identität durchläuft einen Lebenszyklus, der beginnt, wenn sie einer Organisation beitritt (z. B. eine neue mitarbeitende Person), und endet mit dem vollständigen Entzug aller Rechte sowie der Löschung oder Archivierung (z. B. Beendigung oder Vertragsende). Wichtige Funktionen sind:

- Erfassen und pflegen von Masterdaten, zum Beispiel Name, Abteilung, Position, Standort oder Kontaktinformationen.
- Verbindung zu Attributen sicherstellen, zum Beispiel Sicherheitsniveau, Zertifizierungen oder Vertragsstatus.
- Laufende Synchronisierung mit verbundenen IT-Systemen wie zum Beispiel Verzeichnisdienst, HR-System oder Plattformen, um konsistente Identitätsinformationen bereitzustellen.
- Automatisierte Prozesse bereitstellen, wie zum Beispiel den Joiner-Mover-Leaver-Prozess.
- Vermeidung von Duplikaten durch Identitätskonsolidierung und systematische Pflege von Quell- und Zielsystemen.

Effizientes Identitätsmanagement ist eine Voraussetzung für ein funktionierendes Autorisierungssystem, da es die Grundlage für jede Form der Zugriffskontrolle bildet. Sie stellt sicher, dass alle Zugriffe eindeutig einer verifizierten, aktuellen und vertrauenswürdigen Identität zugeordnet werden können.

Access-Management

Das Access-Management baut auf den durch das Identity-Management bereitgestellten Informationen auf und kontrolliert den tatsächlichen Zugriff auf Ressourcen. Konkret umfasst es die Autorisierung (d. h. die Entscheidung, wer auf welche Daten, Systeme oder Anwendungen zugreifen darf sowie die technische Umsetzung dieser Verordnung innerhalb der IT-Infrastruktur. Die Authentifizierung ist eine notwendige Vorphase, in der die Identität eines Nutzers überprüft wird. Die eigentliche sicherheitskritische Entscheidung erfolgt jedoch im Rahmen der Genehmigung.
Die Authentifizierung stellt sicher, dass die Person oder das System, das den Zugriff anfordert, die beanspruchte Identität besitzt. Dies geschieht über gängige Verfahren wie Passwort, Token, biometrische Verfahren oder Multi-Faktor-Authentifizierung (MFA). Letzteres erhöht die Sicherheit, indem es die Kombination verschiedener Faktoren aus den Kategorien Wissen (z. B. Passwort), Besitz (z. B. Smartphone) und biometrischen Daten (z. B. Fingerabdruck) ermöglicht.

Die Autorisierung regelt, auf welche Ressourcen der authentifizierte Benutzer zugreifen darf, in welchem Umfang (z. B. lesen, schreiben, verwalten) und unter welchen Bedingungen.

C. Benutzerkonten

Benutzerkonten sind technische Merkmale der Nutzer in den jeweiligen IT-Diensten. Wir unterscheiden zwischen zwei Arten von Benutzerkonten: persönlichen und nicht-privaten Konten. Die Identifikation erfolgt über den Anmeldenamen.

Persönliche Konten
Persönliche Konten werden zu jedem Zeitpunkt einer verantwortlichen Person zugewiesen. Dadurch können alle Aktionen innerhalb eines IT-Systems identifiziert und dieser Person zugewiesen werden. Zwei Arten von Konten sind möglich:

- Persönliches Konto
  In **(Name des Herstellers)** darf nur ein Konto des Typs **persönlich** einer Person zugewiesen werden. Dieses Konto wird für Ressourcen verwendet, die nicht als kritisch gekennzeichnet sind.
- Administratives Konto
  In **(Name des Herstellers)** darf nur ein Konto des Typs **administrativ** einer Person zugewiesen werden. Dieses Konto wird für Ressourcen verwendet, die als kritisch gekennzeichnet sind.

Nicht-persönliche Konten
Nicht-persönliche Konten werden von verschiedenen Personen oder Systemen genutzt. Jede Nutzung muss immer auf eine bestimmte Person oder ein bestimmtes System zurückgeführt werden können. Beispiele für nicht-persönliche Benutzerkonten sind:

- Systemkonten (technische Benutzer)
- Notfallkonten
- Trainingskonten
- Testkonten

Grundsätzlich wird in **(Name des Herstellers)** für jede Anwendung eine sogenannte technische Identität erstellt, der die nicht-persönlichen Konten zugewiesen sind.

D. Rollen

Rollen werden für die Konsolidierung von Rechten definiert. Es gibt zwei Arten von Rollen:

- Anwendungsrollen (AR)
- Geschäftsrollen (GR)

Anwendungsrollen sind in **(Name des Herstellers)** erstellte Rollen, die aus einer oder mehreren Berechtigungen einer Anwendung gebildet werden.

Geschäftsrollen sind in **(Name des Herstellers)** erstellte Rollen, die aus Berechtigungen mehrerer Anwendungen zusammengestellt werden und Anwendungsrollen enthalten können.

E. Automatisierte Zuweisungen von Rollen oder Berechtigungen

Automatisierte Zuweisungen von Rollen oder Berechtigungen (sogenannte Birth-rights oder „Geburtsrechte“) werden genutzt, um die Zuweisung von Rollen erheblich zu vereinfachen. Diese Geburtsrechte können direkt bei der Aufnahme ins Tool an definierte Personengruppen vergeben werden, z. B. Mitarbeiter oder Auftragnehmer. Zusätzlich können sie an Personen definierter Gesellschaften im Unternehmen, von Abteilungen / Teams, einzelner Projekte oder mit festgelegten Positionen zugewiesen werden. Im Falle von Versetzungen werden die alten Rollen automatisch entzogen und die neuen Rollen zugewiesen.

Zuweisungen für Mitarbeitende

Die Zuweisungen für Mitarbeitende umfassen grundlegende Rechte für alle Mitarbeitenden, unabhängig von Unternehmen, Abteilung / Team oder Position. Eine verantwortliche Person wird für diese Zuweisungsrichtlinie benannt und im Tool eingetragen.

Zuweisungen für Auftragnehmer

Die Abweisungsrichtlinie für Auftragnehmer wird grundlegende Rechte für alle Mitarbeiter festlegen, unabhängig von Unternehmen, Team oder Position. Eine verantwortliche Person wird als Eigentümer für diese Zuweisungsrichtlinie benannt und im Tool eingetragen.

Zuweisungen für eigenständige Gesellschaften

Jede Person, die einer rechtlich eigenständigen Gesellschaft im Unternehmen zugewiesen ist, erhält automatisch die in der Unternehmensrolle enthaltenen Rechte. Dazu muss die Gesellschaft in **(Name des Herstellers)** angelegt sein und als Referenz ausgewählt werden können. Voraussetzung ist, dass:

- eine verantwortliche Person als Rolleninhaber für die Rolle in **(Name des Herstellers)** eingetragen wird.
- der Rolleninhaber die Zusammensetzung der Rolle vorschlägt und sie mit den Ressourcenbesitzern der für die Rolle vorgesehenen Ressourcen abstimmt.

Zuweisungen für Abteilungen / Teams

Für jede Abteilung oder jedes Team kann eine Rolle festgelegt werden, die jeder Person der Abteilung oder des Teams automatisch zugewiesen wird. Dazu muss die Abteilung oder das Team in **(Name des Herstellers)** angelegt ist und als Referenz ausgewählt werden kann. Voraussetzung ist, dass:

- eine verantwortliche Person als Rolleninhaber für die Rolle in **(Name des Herstellers)** eingetragen wird.
- der Rolleninhaber die Zusammensetzung der Rolle vorschlägt und sie mit den Ressourcenbesitzern der für die Rolle vorgesehenen Ressourcen abstimmt.

Zuweisungspolitik für Positionen

Für jede Position kann eine Rolle festgelegt werden. Jeder Person mit der jeweiligen Position wird diese Rolle automatisch zugewiesen. Dazu muss die Position in **(Name des Herstellers)** angelegt ein und als Referenz ausgewählt werden können. Voraussetzung ist, dass:

- eine verantwortliche Person als Rolleninhaber für die Rolle in **(Name des Herstellers)** eingetragen wird.
- der Rolleninhaber die Zusammensetzung der Rolle vorschlägt und sie mit den Ressourcenbesitzern der für die Rolle vorgesehenen Ressourcen abstimmt.

F. SOLL / IST - Abgleich

Beim SOLL / IST -Abgleich (Reconciliation), werden die Benutzerkonten, Benutzerrechte und die Verbindung zwischen Benutzerrechten und Benutzerkonten aus dem Zielsystem ausgewertet und mit dem gewünschten Zustand in **(Name des Herstellers)** verglichen. Ausnahmen davon sind möglich und müssen entsprechend dokumentiert werden, zum Beispiel im Berechtigungskonzept.
Der Abstimmungszyklus hängt von den Schutzanforderungen der Zielsysteme und der Kritikalität der Berechtigungen ab. Typische Zyklen wie täglich, wöchentlich, monatlich, vierteljährlich, halbjährlich oder jährlich leiten sich daraus ab.
Der angegebene Zyklus muss in einem Kalender für jedes Zielsystem festgelegt werden (Recon-Kalender).
Grundsätzlich kann der Abgleich auf zwei Arten erfolgen:

- Automatisierte Synchronisation von Anwendungen, die nach jedem Datenimport direkt mit **(Name des Herstellers)** verbunden sind.
- Übereinstimmung erfolgt über CSV-Dateien vom Zielsystem, das alle Informationen zu einem bestimmten Zeitpunkt über alle Benutzerkonten, alle Berechtigungen und die Zuweisung von Benutzerkonten zu Berechtigungen in drei verschiedenen Dateien bereitstellt.

Die technische Umsetzung für beide Wege wird im **(Name des Herstellers)** -Betriebshandbuch beschrieben.

G. Rezertifizierung

Um sicherzustellen, dass Menschen zu jedem Zeitpunkt nur die Berechtigungen haben, die sie für ihre tägliche Arbeit benötigen, müssen Daten wie z. B. Identitäten, Konten, Rollen, Berechtigungen und Autorisierungskonzepte regelmäßig überprüft werden. Dies wird durch Rezertifizierungen erreicht. Regelmäßig zertifiziert werden:

- Berechtigungskonzepte – die Rezertifizierung erfolgt außerhalb von **(Name des Herstellers)**
- Identitäten – die Rezertifizierung erfolgt in **(Name des Herstellers)**

- Rollen – die Rezertifizierung erfolgt in **(Name des Herstellers)**
- Zuweisung von Rollen an Konten / Identitäten – die Rezertifizierung erfolgt in **(Name des Herstellers)**

Die Arten und Verfahren für die Rezertifizierung sind im **(Name des Herstellers)** - Betriebshandbuch beschrieben. Die Überprüfungsperioden sind in der **(Name der Richtline, die die Überprüfungszyklen regelt)** beschrieben.
Wenn eine Anwendung nicht mit **(Name des Herstellers)** verbunden ist oder nicht verbunden werden kann, muss ein vergleichbarer Prozess sichergestellt werden.

H. Funktionstrennung (SoD)

Basierend auf einem SoD-Konzept können Ressourcen entsprechend gekennzeichnet werden, um toxische Kombinationen zu identifizieren. Dies gilt für:

- Anwendungsrollen (AR)
- Geschäftsrollen (GR)

I. Berechtigungskonzept (BK)

In Berechtigungskonzepten werden alle Informationen zum Identity- und Access-Management wie z. B. Rechte und Rollen, privilegierte Nutzer, kritische Rechte und Rollen, dokumentiert. Der spezifische Inhalt eines BK wird in einem Template festgelegt.

4. Inkrafttreten

Diese Richtlinie gilt ab dem TT.MM.JJJJ.

Autor	Compliance-Überprüfung	Genehmigung
(Organisationseinheit)	**Compliance (Organisationseinheit)**	**Management (Organisationseinheit)**
TT/MM/JJJJ Vorname, Name	TT/MM/JJJJ Vorname, Name	TT/MM/JJJJ Vorname, Name

Anhang 1: Abkürzungen im Rahmen von IAM

Begriff	Beschreibung	Beispiel
AAD	Azure Active Directory	
AD	Active Directory	
App	Application	
BI	Business Intelligence	
ERP	Enterprise Resource Planning	
GUI	Graphical User Interface	
IAG	Identity and Access Governance	
IAM	Identity and Access Management	
IGA	Identity Governance and Administration	
LDAP	Lightweight Directory Access Protocol	
OU	Organizational Unit	
PAM	Privileged Access Management	
RBAC	Role-Based Access Control	
SLA	Service Level Agreement	
SoD	Segregation of Duties	
SSAS	Microsoft SQL Server Analysis Services	
SSIS	Microsoft SQL Server Integration Services	
SSL/TLS	Secure Sockets Layer/Transport Layer Security	
SSRS	Microsoft SQL Server Reporting Services	

Anhang 2: Glossar

Begriff	Beschreibung	Beispiel
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.	
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.	
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.	
Deprovisioning	Das Entfernen einer zugewiesenen Rolle oder Berechtigung.	
Emergency lockout	Ein Prozess, der alle mit einer Identität verbundenen Konten deaktiviert, wenn ein Sicherheitsverstoß vermutet wird.	
HR system	Das Personalführungssystem, aus dem das IAM-Tool relevante Personaldaten erhält und verarbeitet.	

Identity	Die Abbildung einer physischen Person oder technischen Einheit im IAM-Tool.	
Identity lifecycle management	Der Prozess, der den gesamten Beschäftigungszyklus einer Person im Unternehmen, von der Einstellung bis zum Ausscheiden, abbildet.	
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.	
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.	
Privileged account	Ein privilegiertes Benutzerkonto, das direkt einer Identität zugewiesen ist und einen privilegierten Zugang beinhaltet, zum Beispiel ein Administratorkonto.	
Provisioning	Die Bereitstellung einer automatisierten oder beantragen Zuweisung von Rollen oder Berechtigungen.	
Resource	Eine Ressource kann entweder eine Berechtigung oder eine Rolle sein.	
Resource Owner	Die verantwortliche Person für eine Berechtigung oder Rolle.	
Resource assignment	Die einer Person zugewiesene Berechtigung oder Rolle.	
Segregation of duties (SoD)	Ein Prinzip (Funktionstrennung), das sicherstellt, dass an eine Person keine unvereinbaren Rollen oder Berechtigungen vergeben 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.	

5. Änderungen

Datum	Herausgeber	Abschnitt	Grund
TT/MM/JJJJ	Name, Vorname	alle	Veröffentlichung

6. Referenzdokumente

Name des Dokuments	Wirksam ab
Name der Richtlinie	TT/MM/JJJJ