ITSENSE

SWISS MADE IAM

Willkommen im IAM-Circle!

abraxas

ti&m

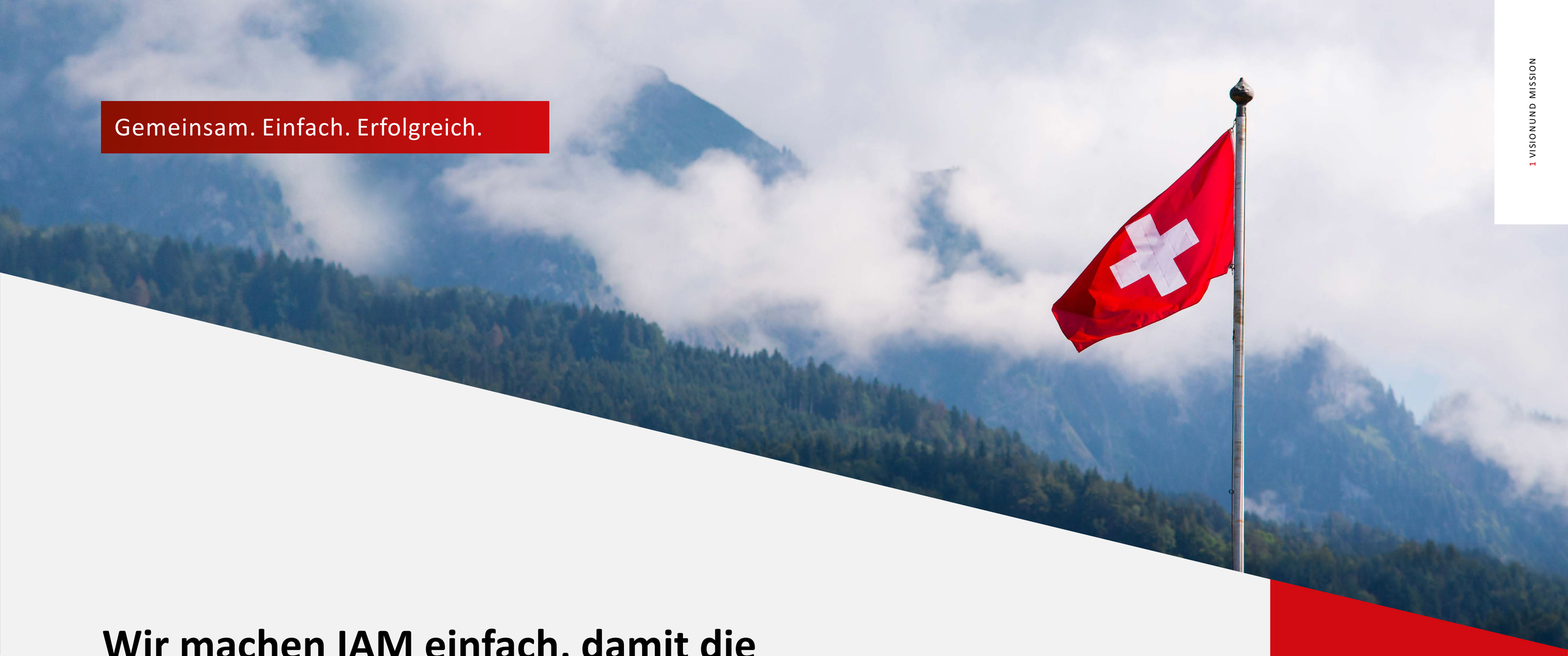
COPEBIT

white rabbit Communications

netzmedien

#9

#Daten- und Persönlichkeitsschutz

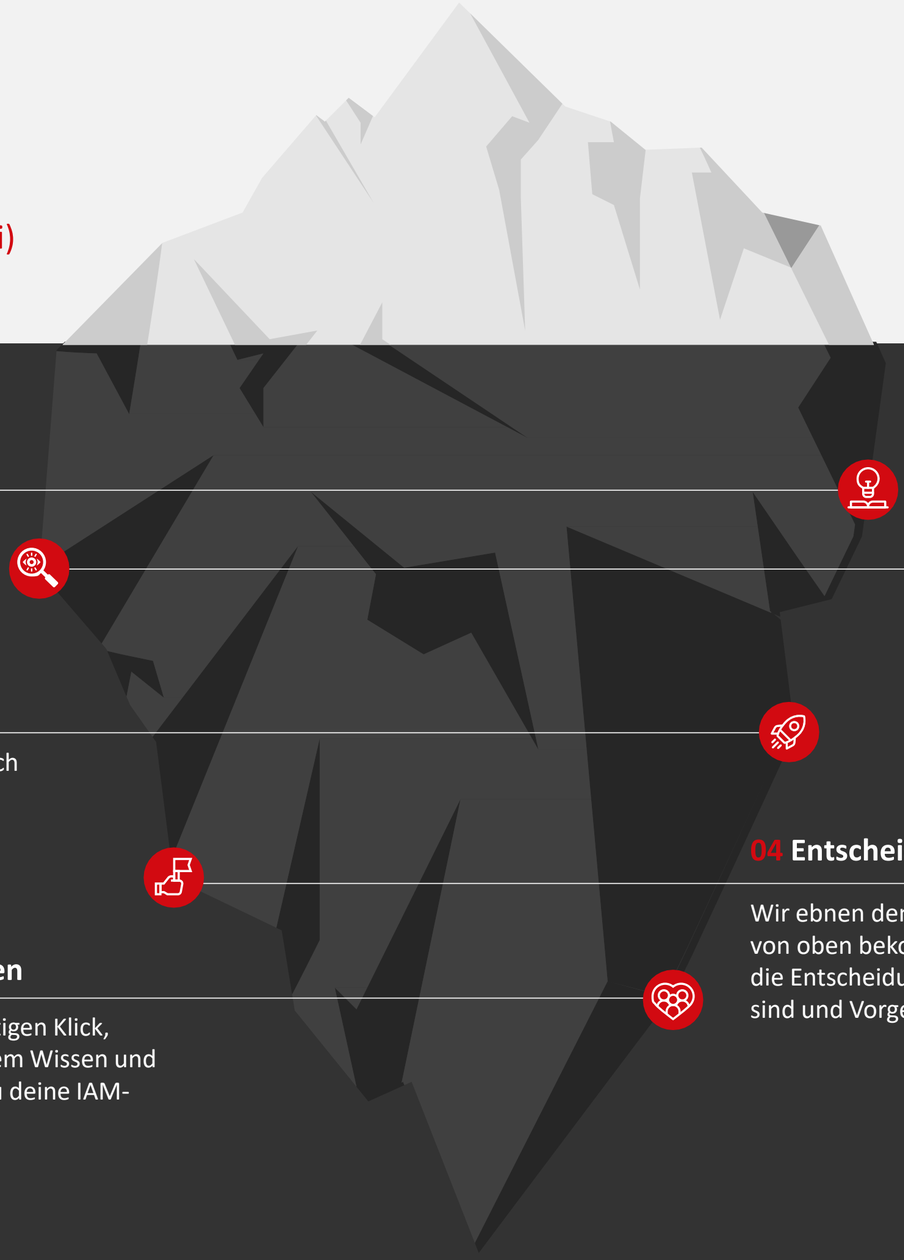


Gemeinsam. Einfach. Erfolgreich.

Wir machen IAM einfach, damit die Schweiz sicher wird: für dich, für uns und für den Rest der Welt!

ITSENSE

5 überzeugende Gründe für eine #Mitgliedschaft (kostenfrei)



01 Fachwissen vertiefen

Im IAM-Circle vertiefen wir gemeinsam mit Gleichgesinnten aktuelles Wissen zu IAM und IT-Security.

02 Projekte erfolgreich realisieren

Mit dem Wissen kannst du IAM-Projekte erfolgreich und wirtschaftlich in Unternehmen initiieren und umsetzen.

03 Community-Support nutzen

Unsere Community schafft den richtigen Klick, wenn du ihn brauchst. Mit relevantem Wissen und passender Kommunikation führst du deine IAM-Projekte zum Erfolg.

04 Entscheidungen erleichtern

Wir ebnen den Weg, damit du Rückendeckung von oben bekommst,
die Entscheidungsprozesse leicht
sind und Vorgesetzte sie verstehen.

05 Sicherheit & Klarheit gewinnen

Als Teil des IAM-Circle gewinnst du Sicherheit. Du erhältst Klarheit über die nächsten Schritte und Zugang zu geballtem Fachwissen.

ITSENSE

#Fokusthema heute

Erfolgsstrategien für Stammdatenverwaltung und Quellsystemanbindung im Kontext des IAM

ITSENSE

Unsere #Speaker

Saša Nikolić
Head of Integration & Operations

ITSENSE

Marc Burkhard
CEO

ITSENSE

#Agenda IAM-Circle

- 🎯 Begrüssung
- 🎯 **Vortragsreihe Teil 1 - «Stammdaten im Griff – Der Schlüssel zu erfolgreichem IAM»** I Marc Burkhard
- 🎯 Workshop
- 🎯 Pause
- 🎯 **Vortragsreihe Teil 2 – «Quellsysteme sauber anbinden – Technische Grundlagen für nachhaltiges IAM»** I Saša Nikolić
- 🎯 Ergebnispräsentation aus Workshop / Panel Discussion / Q&A Session
- 🎯 Ab 17.00 Uhr Apéro

ITSENSE

SWISS MADE IAM

Stammdaten im Griff – Der Schlüssel zu erfolgreichem IAM

abraxas

ti&m

COPEBIT

white rabbit Communications

netzmedien

#9

Was sind relevante Stammdaten für ein IAM-System?

Personendaten
Alle Informationen, die zur Identifizierung einer natürlichen Person dienen oder mit ihr in Verbindung gebracht werden.

- **Vor- und Nachname**
- **Personalnummer**
- **Telefonnummer**
- **E-Mail Adresse**
- **Geburtsdatum**
- **Geschlecht**
- **…**

Organisationsdaten
Strukturierte Informationen, die die Zugehörigkeit, Position und Rolle einer Person innerhalb der organisatorischen Struktur einer Institution oder eines Unternehmens beschreiben.

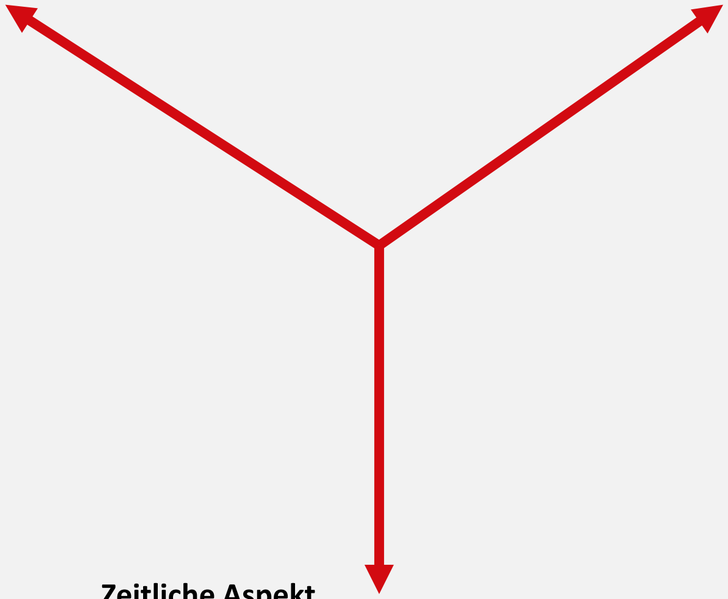
- **Abteilung / Organisationseinheit**
- **Standort**
- **Planstelle (Position)**
- **Kostenstelle**
- **…**

Anstellungsdaten
Personenbezogene Informationen, die sich auf das Beschäftigungsverhältnis einer Person mit einer Organisation beziehen.

- **Funktion**
- **Anstellungszeitraum**
- **Vertragsart (intern, extern, befristet, etc.)**
- **Beschäftigungsstatus (aktiv, inaktiv, etc.)**
- **Beschäftigungsgrad (Pensum)**
- **Arbeitszeitmodell (Vollzeit, Teilzeit, etc.)**
- **Vorgesetzter**
- **Kaderstufe**
- **…**

Was sind wichtige Dimensionen von Stammdaten?

Stammdatenumfang
Bezeichnet die Gesamtheit aller grundlegenden, dauerhaft relevanten und identitätsbezogenen Daten, die für die Verwaltung von Benutzerkonten und Zugriffsrechten im IAM-System erforderlich sind.



Stammdatenqualität
Bezeichnet die Korrektheit, Vollständigkeit, Konsistenz, Aktualität und Eindeutigkeit der geführten Stammdaten im Quellsystem und IAM-System.

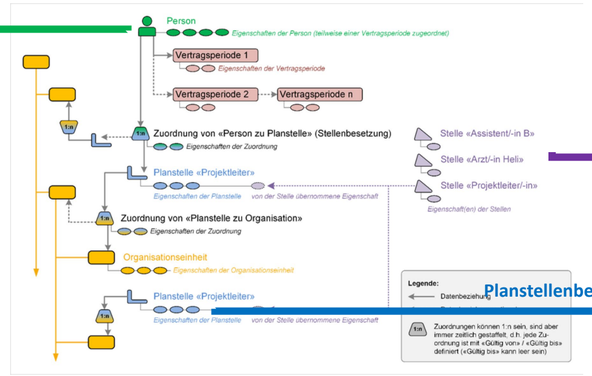
„Eine hohe Stammdatenqualität ist ein zentraler Erfolgsfaktor für die effiziente und sichere Automatisierung von Prozessen“

Zeitliche Aspekt
Beschreibt die Berücksichtigung von Zeitpunkten, Zeiträumen und zeitabhängigen Ereignissen bei der Pflege, Verarbeitung und Nutzung von Stammdaten im Quellsystem und IAM-System.

ITSENSE

Mapping der Datenstrukturen

HRM-System (z.B. SAP HCM)



Stellenbezeichnung

Planstellenbezeichnung

IAM-System

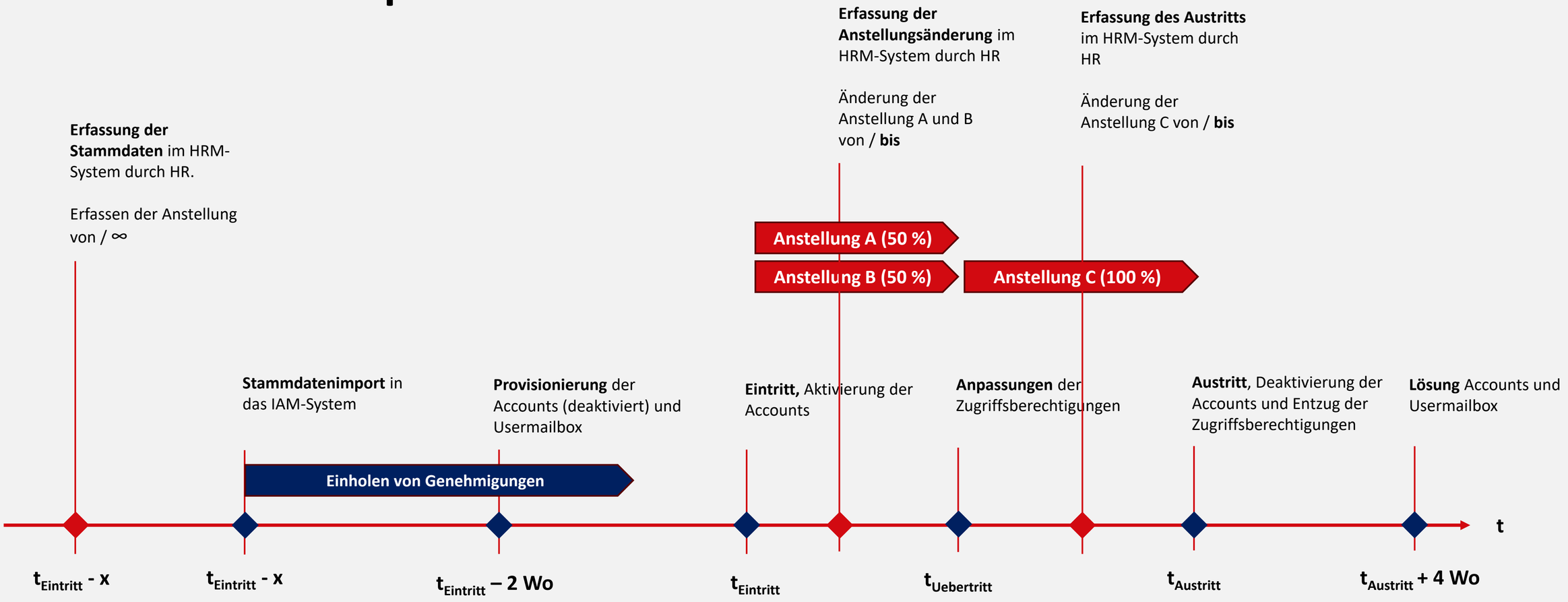
Core Identität (nat. Person)
(Angestellter)

Infotyp	
Vorname	Michael
Nachname	Buser
Titel	
Personalnummer	123456
Telefonnummer	
….	

Anstellung A

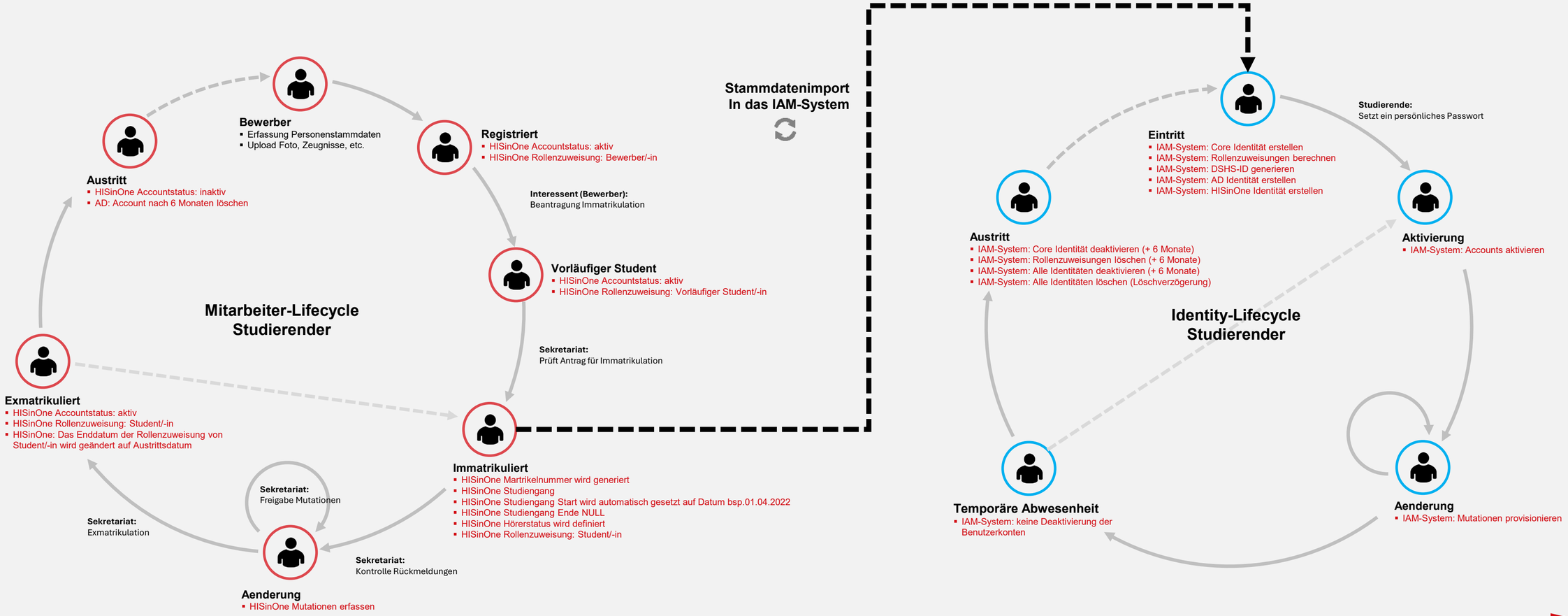
Gültig von	01.09.2013
Gültig bis	unbegrenzt
Beschäftigungsgrad	100 %
Anstellungstyp	Vollzeit
Organisationeinheit	**Bereich A**
Funktion	**Bereichsleiter**

Der zeitliche Aspekt

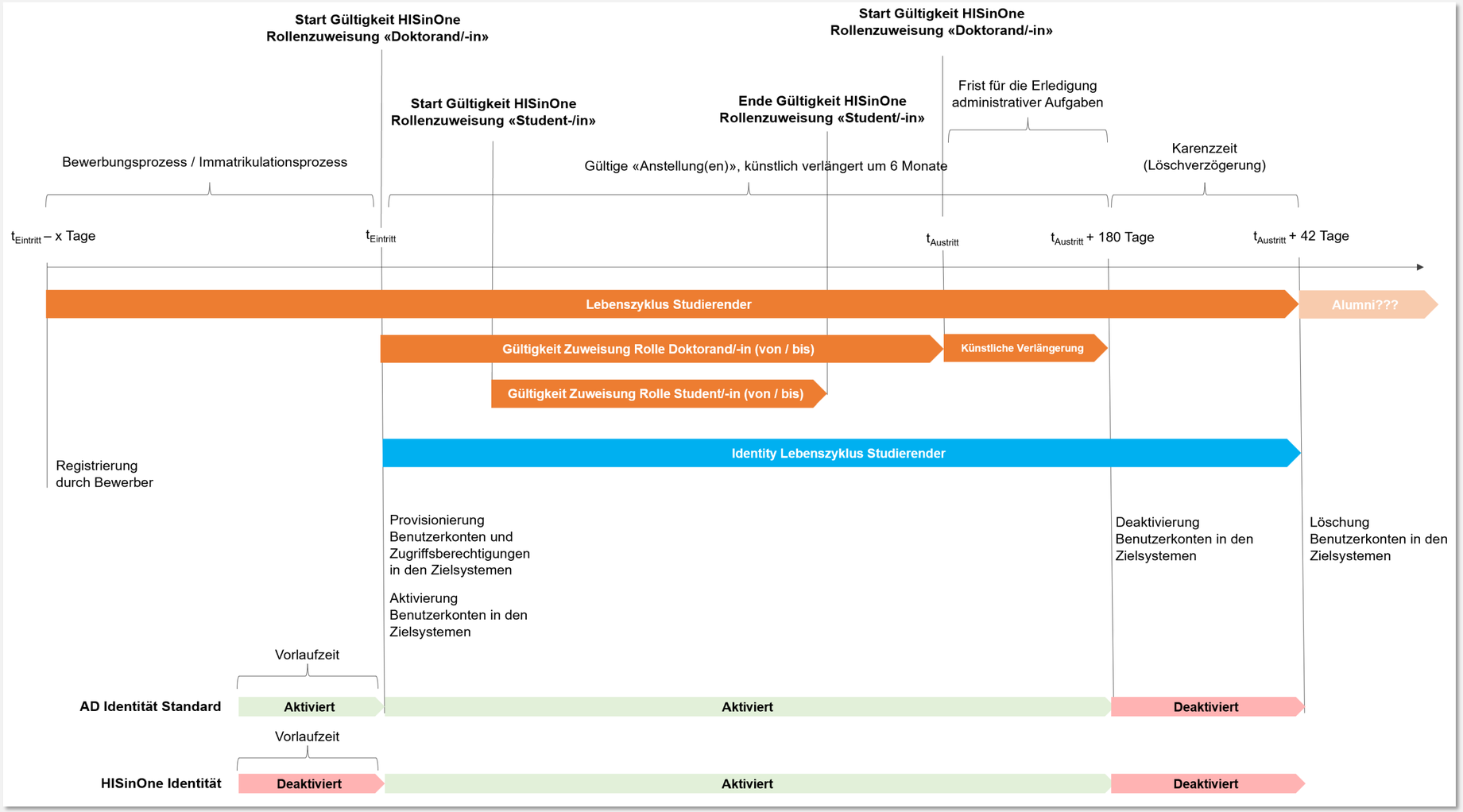


◇ **Vorgang und Triggerpunkt für IAM-System**

Mitarbeiter Lifecycle vs. Identity Lifecycle



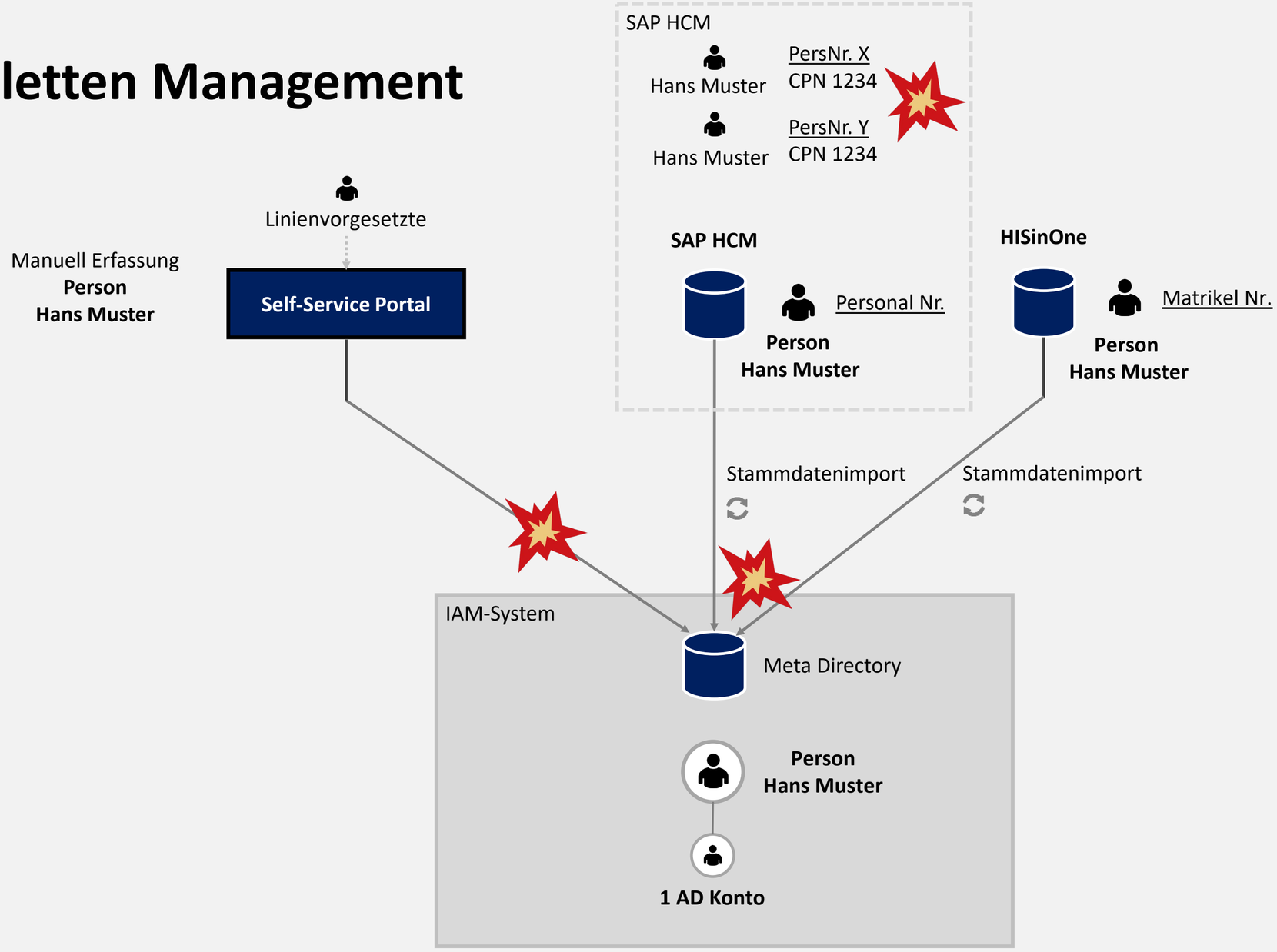
Mitarbeiter Lifecycle vs. Identity Lifecycle



Herausforderungen in der Praxis (Best-Practises)

Umstand	Konsequenz	Mögliche Massnahmen
Im HRM-System wird kein oder unbrauchbarer Funktionskatalog gepflegt	▪ Kein automatisiertes Role based Access Control (RBAC)	▪ HR führt ein Funktionskatalog und damit Stellenbeschreibungen ein ▪ Kompensation auf IAM-Ebene mit bestellbaren Funktions-Rollen
Im HRM-System werden die Funktionen nicht granular genug geführt (z.B. Funktion «Kaufm. Mitarbeiter»)	▪ Kein automatisiertes Role based Access Control (RBAC) ▪ Keine granulare Berechtigungsvergabe nach Least-Privilege-Prinzip	▪ HR passt denn Funktionskatalog und damit Stellenbeschreibungen ein ▪ Kompensation auf IAM-Ebene mit bestellbaren Funktions-Rollen
Erfassung der Stammdaten sehr kurzfristig oder gar nach dem Eintritt	▪ Noch nicht alle Genehmigungen eingeholt ▪ Accounts sind bei Stellenantritt nicht provisioniert	▪ Organisatorische Anpassung im On-Boarding ▪ Selbstverwaltung durch das «Business»
Im HRM-System werden Mehrfachanstellungen nicht erfasst, sondern nur die Hauptanstellung	▪ Kein automatisiertes Role based Access Control (RBAC)	▪ HR führt die wesentlichen Anstellungen (z.B. Bodenpersonal 50% / Fliegendes Personal 50%) ▪ Kompensation auf IAM-Ebene mit bestellbaren Funktions-Rollen
Mehrere HRM-Systeme vorhanden / Holding Struktur / Geschäftszukäufe	▪ Personen sind in mehreren HRM-Systemen bekannt ▪ Erzeugen von Dubletten, z.B. Provisionierung von mehreren Accounts / Usermailboxen ▪ Mühsame und fehlerbehaftete Dubletten-Erkennung	▪ Einführen von übergreifenden Identifikatoren ▪ Aggregierung der HRM-Stammdaten in eine zentrale Datenbank
Im HRM-System werden die amtlichen Vor- und Nachnamen verwaltet, im AD wurde aus Josef der Sepp	▪ Soll-Ist Abweichungen ▪ Ausnahmeregelung nötig	▪ Auflösung oder manuell Erfassung der Ausnahmen
Externe Mitarbeiter werden nicht von HR verwaltet	▪ Ad-hoc Management durch ICT ▪ Chaos bei der Verwaltung der Nachweise und Verträge ▪ Verwaiste, meist hoch privilegierte Accounts	▪ Delegierte Verwaltung durch das «Business» und damit delegierte Verantwortung ▪ Föderation mit Organisationen (IdPs)

Dubletten Management



ITSENSE

Workshop

SWISS MADE IAM

abraxas

ti&m

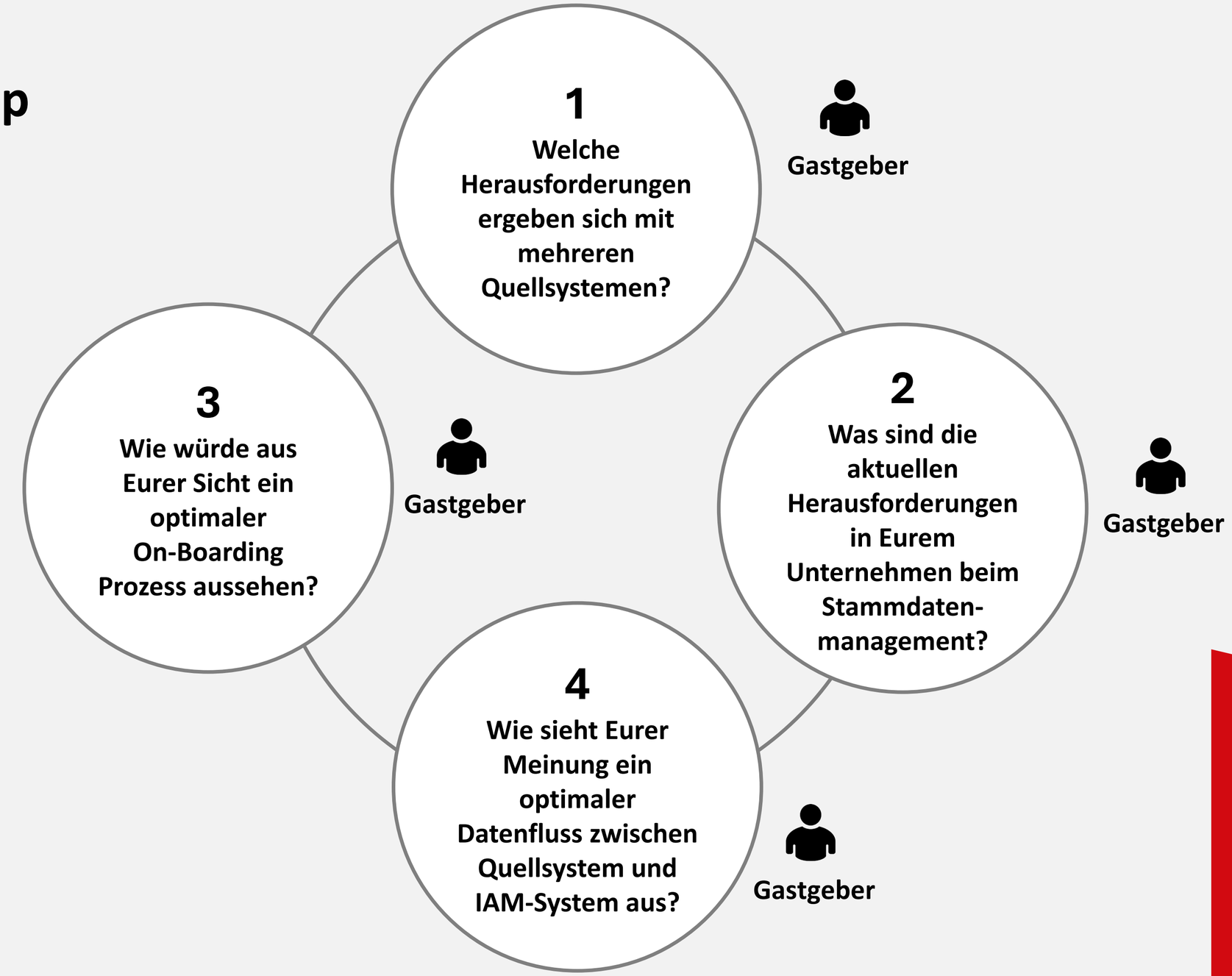
COPEBIT

white rabbit Communications

netzmedien

#9

Workshop



ITSENSE

ITSENSE

Quellsysteme sauber anbinden – Technische Grundlagen für nachhaltiges IAM

SWISS MADE IAM

abraxas

ti&m

COPEBIT

white rabbit Communications

netzmedien

#9

Abhängigkeiten der Stammdaten – Fundament für korrekte Datenflüsse

Personendaten
Alle Informationen, die zur Identifizierung einer natürlichen Person dienen oder mit ihr in Verbindung gebracht werden.

Organisationsdaten
Strukturierte Informationen, die die Zugehörigkeit, Position und Rolle einer Person innerhalb der organisatorischen Struktur einer Institution oder eines Unternehmens beschreiben.

Anstellungsdaten
Personenbezogene Informationen, die sich auf das Beschäftigungsverhältnis einer Person mit einer Organisation beziehen.

ITSENSE

Technische Vorbedingungen – Was muss vor dem Import beachtet werden?

1. Quellsysteme

- Zugriffsmöglichkeiten: API, Dateischnittstellen (CSV, XML), Datenbankzugriffe (ODBC, JDBC)
- Konsistenz und Aktualität: Definierte Intervalle für Datenexporte
- Strukturierte Daten: Einheitliche Attribute, eindeutige Identifikatoren (z.B. Personalnummern)
- Fehlerhandling: Mechanismen für unvollständige oder fehlerhafte Datensätze

2. IAM-Plattform und Infrastruktur

- Anbindungsmöglichkeiten: Unterstützung von gängigen Protokollen (SCIM, LDAP, REST)
- Performance und Skalierbarkeit: Ausreichende Ressourcen für Massendatenverarbeitung
- Schnittstellen-Management: Flexibles Mapping und Transformation der Daten
- Staging-Bereich: Zwischenspeicherung zur Validierung der Daten vor der Verarbeitung

3. Datenmanagement und Sicherheit

- Datenmodell: Eindeutig definierte Strukturen und Attribute im IAM
- Sicherheitsanforderungen: Verschlüsselung, Authentifizierung und Autorisierung der Datenzugriffe
- Audit und Logging: Nachvollziehbare Änderungen und Fehlerprotokolle
- Compliance und Datenschutz: Berücksichtigung von DSGVO, NIS2 und anderen gesetzlichen Anforderungen

ITSENSE

Fremdschlüssel und Hauptanstellungen – Eindeutige Zuordnungen und Datenkonsistenz

🔗 **Kernbotschaften:**

- **Fremdschlüssel als Basis für eindeutige Zuordnung**
  - **Personendaten:** Eindeutige Identifikation der Person (z.B. Personalnummer)
  - **Organisationsdaten:** Struktur und Hierarchie (z.B. Abteilungs-ID)
  - **Anstellungsdaten:** Verknüpfung von Personen und Organisationen (z.B. Anstellungs-ID)

🛠️ **Herausforderungen:**

- Mehrfachanstellungen und deren korrekte Zuordnung
- Konsistente **Vorgesetztenauflösung**
- Berücksichtigung in **Prozessen** und **Trigger-Punkten**

ITSENSE

Schwellwerte – Wie wir fehlerhafte Daten und Massenänderungen erkennen

Warum braucht es Schwellwerte?

- Fehlerhafte HR-Daten frühzeitig erkennen und automatisiert abfangen
- Schutz vor unbeabsichtigten Massenänderungen in Personendaten
- Sicherstellung konsistenter Daten in IAM und Zielsystemen

Unterteilung der Schwellwerte

- Personendaten: Eher tiefe Schwellwerte, um Massenänderungen oder Anomalien zu erkennen
- Anstellungsdaten: Flexible Schwellwerte, je nach Anzahl und Dynamik der Anstellungsverhältnisse
- Organisationsdaten: Höhere Schwellwerte, um versehentliche Reorganisationen oder Strukturänderungen zu prüfen

Vorteile differenzierter Schwellwerte

- Vermeidung von Datenkorruption und fehlerhaften Berechtigungen
- Schnellere Reaktion auf potenziell kritische Datenänderungen
- Präzise Kontrolle und Analyse auf allen Ebenen

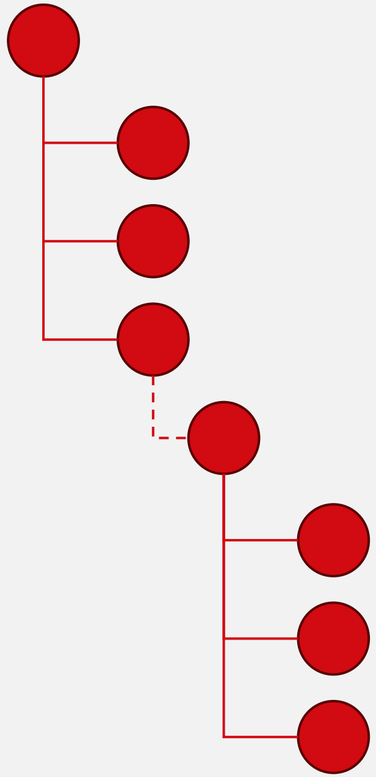
ITSENSE

Attribut-Mapping und Datenqualität – Präzise Übersetzung und Validierung

Frühe Konzeptionsphase – Klare Definition der Nutzergruppen	Attribut-Mapping – Präzision und Konsistenz	Datenvalidierung – Qualität vor Quantität
▪ Alle notwendigen Stammdaten für die Zielapplikationen vorhanden? ▪ Abgleich der Quellsystemdaten mit den Anforderungen des IAM-Systems ▪ Personalabteilung frühzeitig einbeziehen – Qualität der Daten entscheidend für korrekte IAM-Funktionalität	▪ Definition der benötigten Attribute und deren Datentypen ▪ Einsatz von Attribut-Sets zur Strukturierung und Optimierung des Mappings ▪ Klare Zuordnung von Quell- zu Zielattributen (z.B. Abteilung im HR-System zu Organisations-Einheit im IAM)	▪ Mögliche Logiken zur Abwehr fehlerhafter Daten (z.B. Mehrfach-Hauptanstellungen verhindern) ▪ Quellsystem führend bei Eingabe für Datenvalidierung ▪ Überprüfung der Konsistenz und Vollständigkeit der Quellsystemdaten – Prozesse im HR definieren

Fehlerhandling und Edge-Cases – Wie wir Ausnahmen und Fehler abfangen

- Was passiert bei dem Import grundsätzlich?
  - Der Import berechnet zuerst alle Änderungen und den IST-Zustand
  - Versucht die Entitäten zueinander zuzuordnen
  - Sobald eine Abhängigkeit nicht mehr gegeben ist bricht der Import ab
- Warum bricht der Import ab?
  - Abhängigkeit kann nicht mehr korrekt aufgelöst werden
  - Alle nachfolgenden Abhängigkeiten können nicht fix berechnet werden
  - Zum Schutz der Rollen- und Berechtigungsvergabe wird dann nicht importiert



ITSENSE

Vorgesetztenauflösung und Organisationsbaum – Struktur und Hierarchie korrekt abbilden

Verschiedene Quellsystemen führen zu kundenspezifischen und applikationsspezifischen Anforderungen an der Abbildung des Organisationsbaums und der Vorgesetztenauflösung.

Folgende Fragen sind wichtig zu stellen bei der Konzeption und dann bei der Implementation wichtig zu beachten:

1. Wie wird der Vorgesetzte im Stammdatentool geführt?
2. Wie muss der Vorgesetzte aufgelöst werden, falls nicht auf Person geführt? Wichtige Punkte zu beachten?
3. Sind alle Abhängigkeiten in der Organisationsstruktur gegeben? Werden sie konsistent geführt?
4. Führt man Planstellen oder nur Funktionen?

ITSENSE

Prozesse und Triggerpunkte – Wie Änderungen automatisch verarbeitet werden

Lifecycle-Prozesse Teil jedes Unternehmens und eGov-Systems.

1. Welche Prozesse müssen über das IAM abgebildet werden und verwaltet?

2. Werden zu bestimmten Zeitpunkten gewisse Themen abgearbeitet? (z.B. PDFs versendet, E-Mails oder SMS versendet mit Anmeldeinformationen, usw.)

3. Zeitpunkte zu definieren ist essentiell!

IAM bietet verschiedene Einstiegspunkte, um auf gewisse Aktionen reagieren zu können.

Um diese definieren zu können muss beachtet werden, dass alle Prozesse sauber definiert werden müssen und dementsprechend abgebildet.

1. Was passiert, wenn eine Person neu erstellt wird?
2. Was passiert, wenn ein Account ins Zielsystem geschrieben wird?
3. Wenn eine Anpassung an einer Anstellung vorgenommen wird, muss was ausgelöst werden?
4. Was muss passieren bei einer Selbstregistrierung eines Bürgers?
5. Wenn eine Verifikation notwendig war und abgehandelt wurde, was passiert in dem Moment?
6. Und viele weitere Fragen… ☺

Import-Zyklus und Performance – Effiziente Verarbeitung grosser Datenmengen

Letzte Punkte zu beachten wäre wie steuert man einen effizienten Import und welche Mutationen im Stammdatentool erwartet man in welchem Rhythmus und wie relevant sind diese Änderungen für das IAM.

Die Server und Umsysteme müssen dementsprechend performant und hochverfügbar sein, damit ein reibungsloser Import gewährleistet wird.

Die Schnittstelle ist dabei entscheidend für die Performance des Imports, zudem nicht zu unterschätzen wie viele Abfragen und komplexe Abhängigkeiten aufgelöst werden müssen.

Zyklus muss zwingend bestimmt werden. Muss zwingend durch den Tag importiert werden? Muss alle 4 Stunden importiert werden, da möglichst in Echtzeit alle Änderungen abgefangen werden sollen.

ITSENSE

Panel-Diskussion mit #Q&A

ITSENSE

Dein #Gewinn

🚀 **Du bist dir potenzieller Risiken und Stolperfallen bewusst und kannst ihnen gezielt aus dem Weg gehen.**

🚀 **Du hast erkannt, dass IAM nicht ausschliesslich ein technisches Thema ist, sondern auch organisatorische und strategische Aspekte umfasst.**

🚀 **Du hast erkannt, dass qualitativ hochwertige Stammdaten ein essenzieller Erfolgsfaktor für die Prozessautomatisierung sind.**

🚀 **Du hast erkannt, dass die IT-Welt nach wie vor heterogen ist – und dass es robuste „Brücken“ braucht, um Systeme und Prozesse nahtlos zu verbinden.**

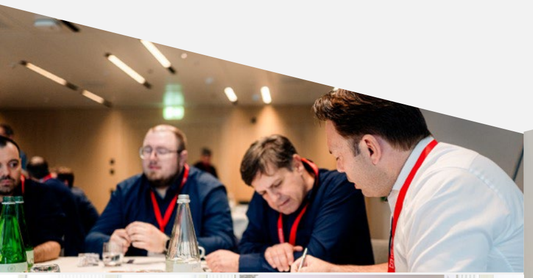
🚀 **Du bist nicht alleine ☺**

Nächste Session IAM-Circle #10

SIEM & IAM: Hand in Hand für eine starke Cybersicherheit!

📅 Donnerstag, 26. Juni 2025

🕐 14:30 bis 17:30 Uhr



ITSENSE

Deine #Meinung ist wichtig – du machst den Unterschied!

Die Umfrage ist anonym. Keine deiner Antworten kann dir zugeordnet werden. Sie umfasst 10 Fragen und dauert gerade einmal 3 Minuten.

👇 **Jetzt scannen und Umfrage ausfüllen.** 👇

ITSENSE

ITSENSE

Stay tuned, stay secure!

SWISS MADE IAM

abraxas

ti&m

COPEBIT

white rabbit Communications

netzmedien

#9