# Willkommen beim IAM-Circle!

SWISS MADE IAM

abraxas

Delinea
Defining the boundaries of access

ti&m
big ideas. creative technology.

ARCTIC WOLF

TREND MICRO

netzmedien

white rabbit Communications

#4

# Tücken und Herausforderungen eines übergeordneten Rollenmodells (RBAC)

# Ziele von RBAC

Role-Based-Access-Control (RBAC) verfolgt das Ziel, die Sicherheit, Effizienz und Compliance der Zugriffsverwaltung in Organisationen zu verbessern, indem es eine strukturierte, übersichtliche und kontrollierte Methode zur Verwaltung von Berechtigungen bereitstellt.

- **Zentrale Zugriffsverwaltung** - RBAC zielt darauf ab, die Verwaltung von Zugriffsrechten zu vereinfachen, indem es eine **zentrale Methode** zur Definition, Verwaltung und Zuweisung von Berechtigungen bereitstellt.
- **Granulare Zugriffskontrolle** - Das Ziel von RBAC ist es, eine fein abgestimmte Zugriffskontrolle zu ermöglichen, indem Berechtigungen auf der Ebene von Business-Rollen definiert und zugewiesen werden.
- **Mehr Sicherheit -** RBAC zielt darauf ab, die Sicherheit sensibler Systeme und Daten zu erhöhen, indem es sicherstellt, dass die Nutzer **zu jedem Zeitpunkt** nur auf die Ressourcen zugreifen können, die für ihre jeweilige Funktion/Aufgabe erforderlich sind («Least-Privilege-Prinzip»).
- **Einhaltung von Compliance-Anforderungen** - RBAC hilft, Compliance-Anforderungen einzuhalten, indem es eine transparente Zugriffsverwaltung und -überwachung ermöglicht und sicherstellt, dass Zugriffsrechte gemäss den Richtlinien der Organisation vergeben werden.
- **Skalierbarkeit -** RBAC ist darauf ausgelegt, mit dem Wachstum und den Veränderungen einer Organisation mitzuwachsen, indem es eine skalierbare Methode zur Verwaltung von Zugriffsrechten bereitstellt.

ITSENSE

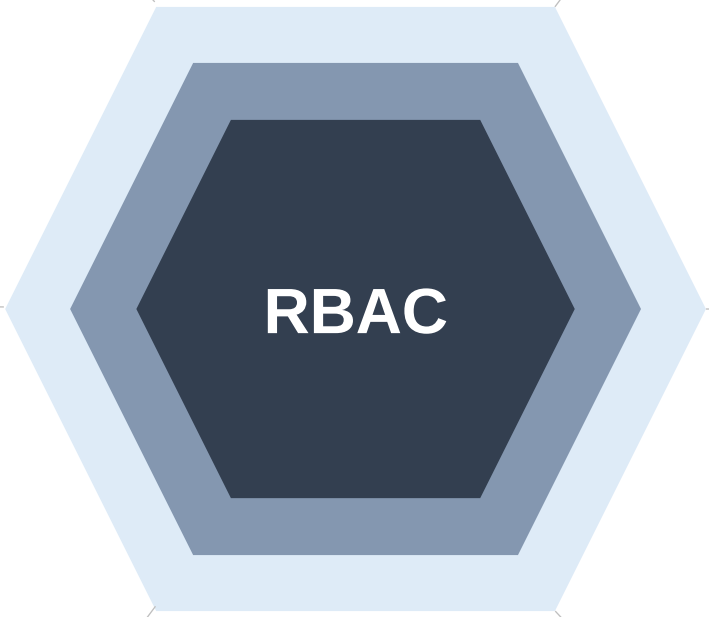
# Einflussfaktoren

## Geschäftsprozesse

Die spezifischen Geschäftsprozesse und -anforderungen einer Organisation bestimmen die benötigten Rollen und Berechtigungen

## Skalierbarkeit / Flexibilität

Die Fähigkeit von RBAC, mit dem Wachstum und den Veränderungen einer Organisation mitzuhalten, ist ein wichtiger Einflussfaktor.




## Organisationsstruktur

Die Struktur und Hierarchie einer Organisation beeinflussen die Rollenmodellierung und -zuweisung

## Technologie

Die vorhandenen Applikationen, Schnittstellen, Systeme sowie die eingesetzten Technologien beeinflussen die Umsetzbarkeit von RBAC

## Bisherige Berechtigungsphilosophie

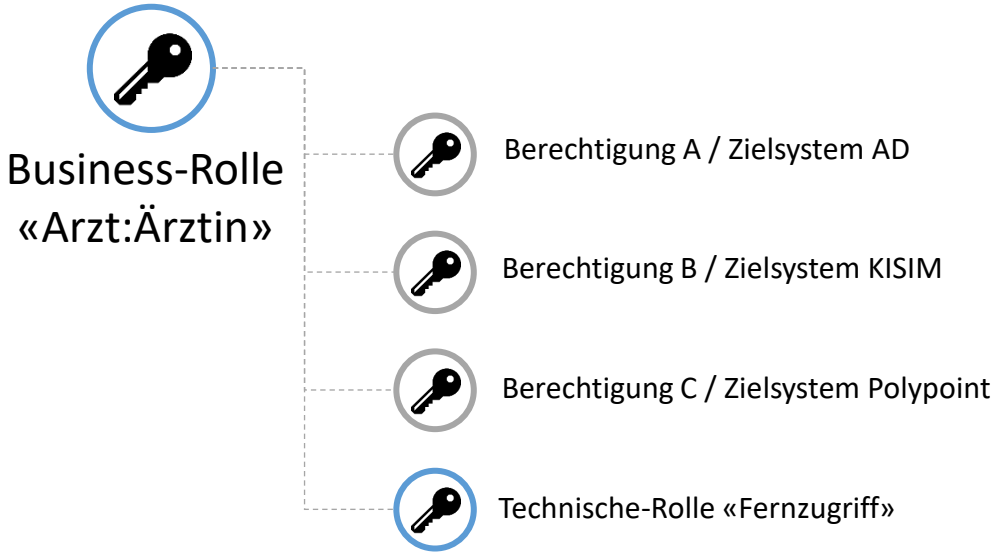
Die Unternehmenskultur und -politik können die Implementierung von RBAC beeinflussen.

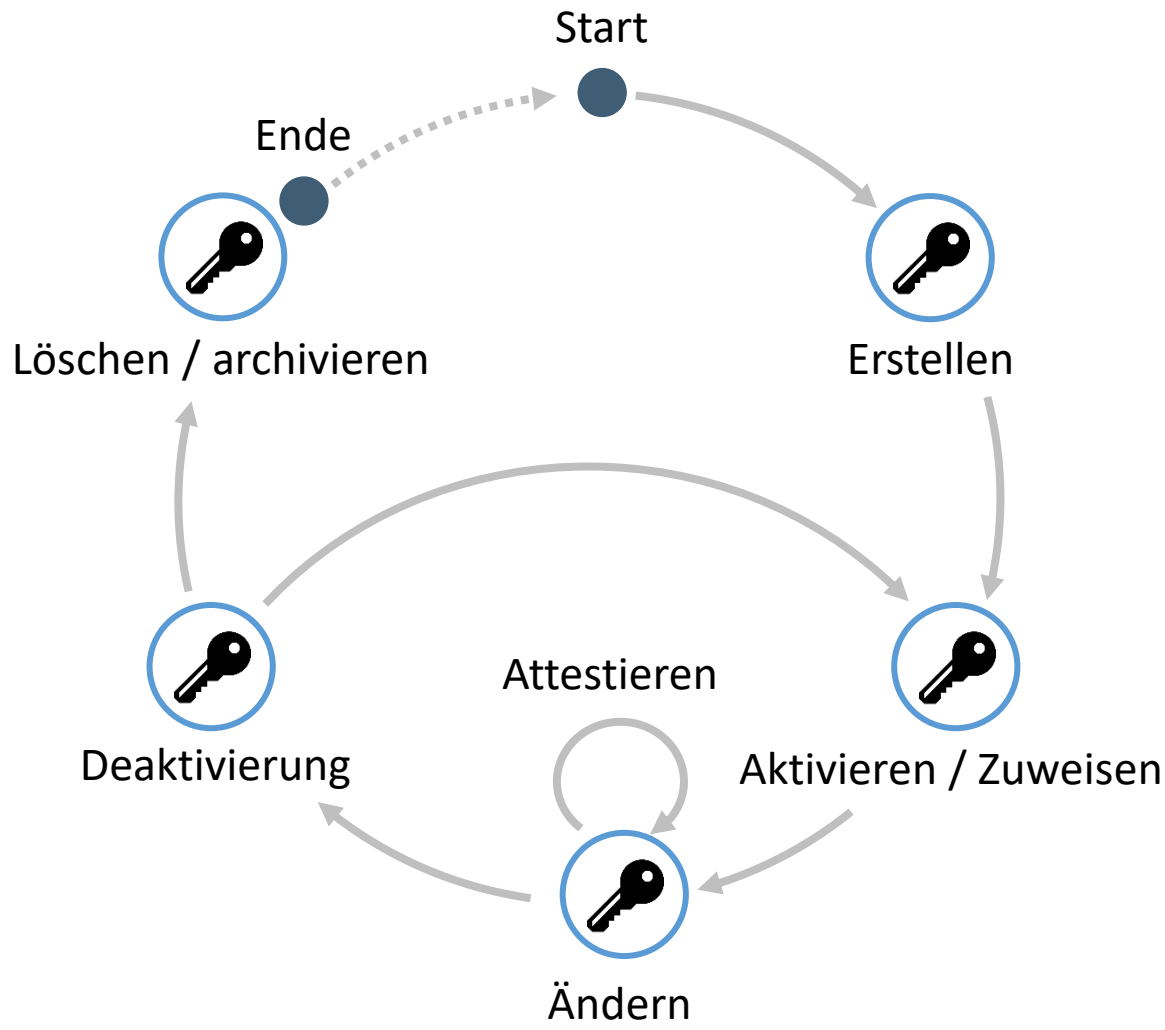
## Compliance Anforderungen

Branchenspezifische Vorschriften und Compliance-Standards wie GDPR, HIPAA oder PCI-DSS können die Rollenmodellierung und -zuweisung beeinflussen.

ITSENSE

# Struktur und Lebenszyklus einer Business-Rolle




ITSENSE

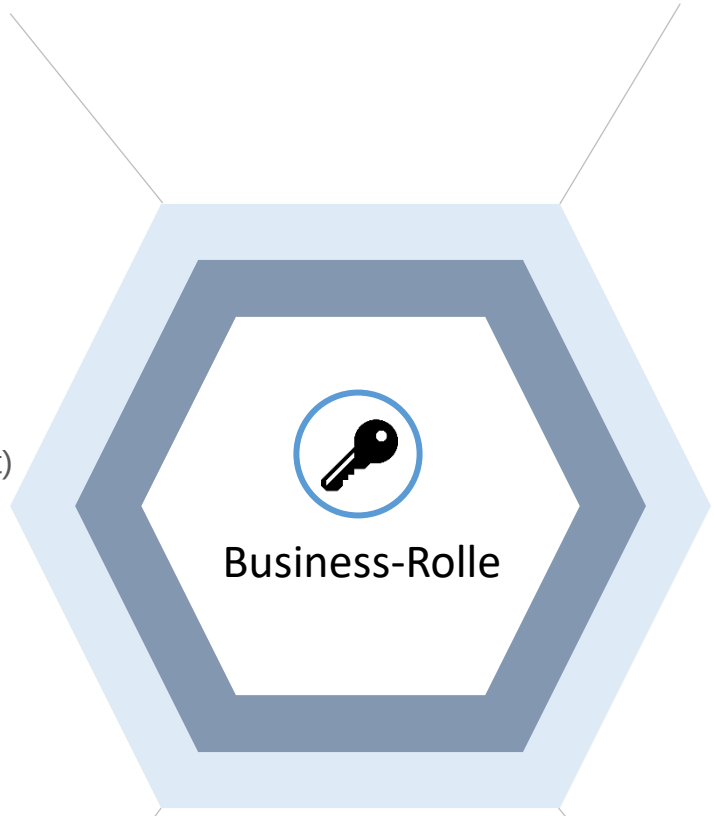
# Stakeholder einer Business-Rolle

## Business-Sicht

**Antragsteller**
Wünscht eine Zuweisung
Wünscht eine neue Business-Rolle (Objekt)

**Genehmiger (1-n)**
Stimmt zu oder lehnt ab

**Nutzer**
Erhält die Business-Rolle




## GRC-Sicht

**Berater**
Compliance
Risk Management
CISO
Datenschutz

## IAM-Management-Sicht

**IAM-Verantwortlicher**
Verwaltet die Business-Rollen (Rollenmanagement)
Kompetenz über Anwendung / Verfahren

**Service-Owner / Applikationsverantwortliche**
Freigabe von Business-Rollen
Beratung beim Rollenbau

**Rollen-Owner**
Pflegt, verwaltet und genehmigt die Business-Rolle als Objekt und deren Inhalt

**Rollen-Attestor**
IAG: Attestiert die Business-Rolle (Objekt)

**Assignment-Attestor**
IAG: Attestiert die Zuweisungen einer Business-Rolle

ITSENSE

Die Stakeholder können im realen Umfeld auch durch wenige Personen besetzt sein, die mehrere Funktionen wahrnehmen.

# Rollenattribute

## Business-Sicht

### Bestellung / Sichtbarkeit
- Bestellfähigkeit
- Shop-Name (Friendly-Name)
- Sichtbarkeit
- Empfangbarkeit
- Zugehörigkeit Rollenkataloge

### Access Governance (Rezertifizierung)
- Rollen-Objekt Attestor
- Rollen-Zuweisung Attestor

### Ownership
- Rollen-Owner

### Genehmigung
- Genehmiger (Zuweisung)
- Genehmigungsworkflow


## GRC-Sicht

### Segregation of Duty (SoD)
- Rollen-Konflikte
- Rollen-Konflikt Ausnahmen

### Klassifikation
- Risiko-Index
- Scope
- Datenschutz

## IAM-Management-Sicht

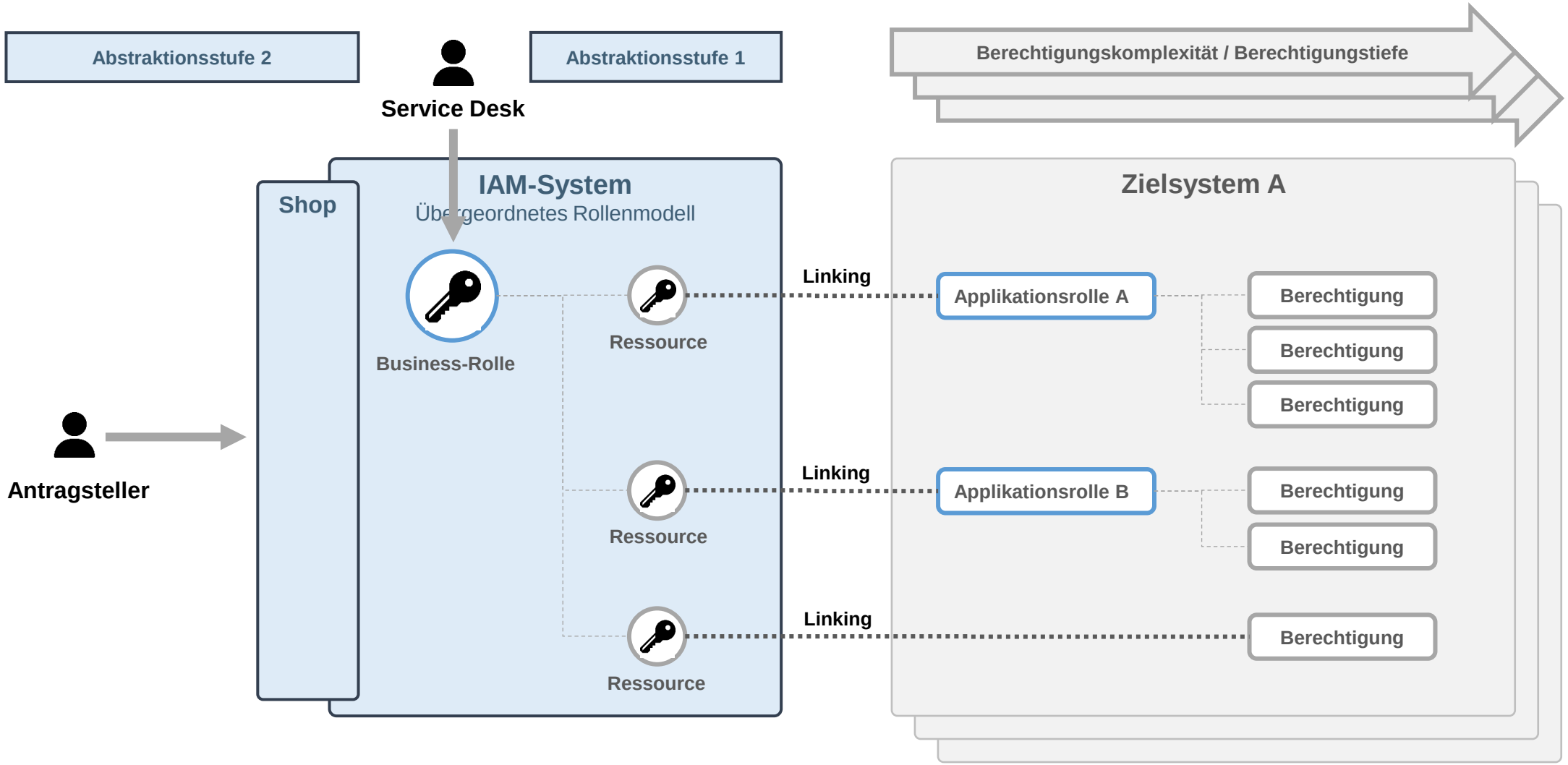
### Allgemein
- Technischer Rollen-Name
- Gültigkeit
- Version
- Status

### Stammdaten Zuweisungen (Mappings)
- Autom. Zuweisungen OrgUnits
- Autom. Zuweisungen Funktionen
- Autom. Zuweisungen Personentypen
- Autom. Zuweisungen Anstellungstypen
- Autom. Zuweisungen Identitätstypen

### Zuweisungen (Assignments)
- Explizite Zuweisung zu Personen
- Gültigkeitszeitraum
- Begründung (Nachvollziehbarkeit)
- Zuweisungsgrund

ITSENSE

# Abhängigkeiten zwischen Business- und Applikationsberechtigungen

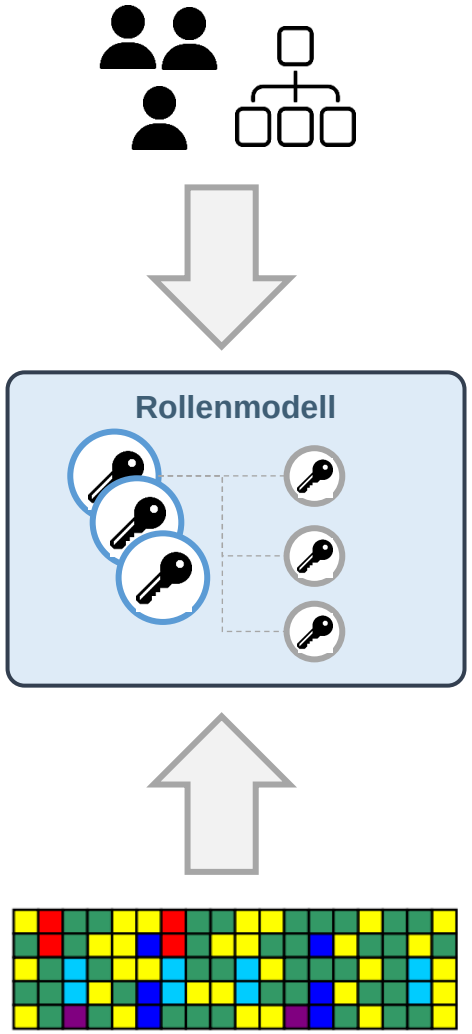



ITSENSE

# Logische Rollenkategorien


ITSENSE

# Rollenfindung (Role-Mining)




Analyse der Organisationsstruktur und von Ähnlichkeiten bei Funktionen, Aufgaben, Organisationszugehörigkeit, Identitätstypen, Anstellungstypen und Personenkreisen

Eine **Business-Rolle** wird so bereitgestellt, dass sie die Bedürfnisse des zu unterstützenden Business-Prozesses erfüllt und alle dafür benötigten Berechtigungen enthält.

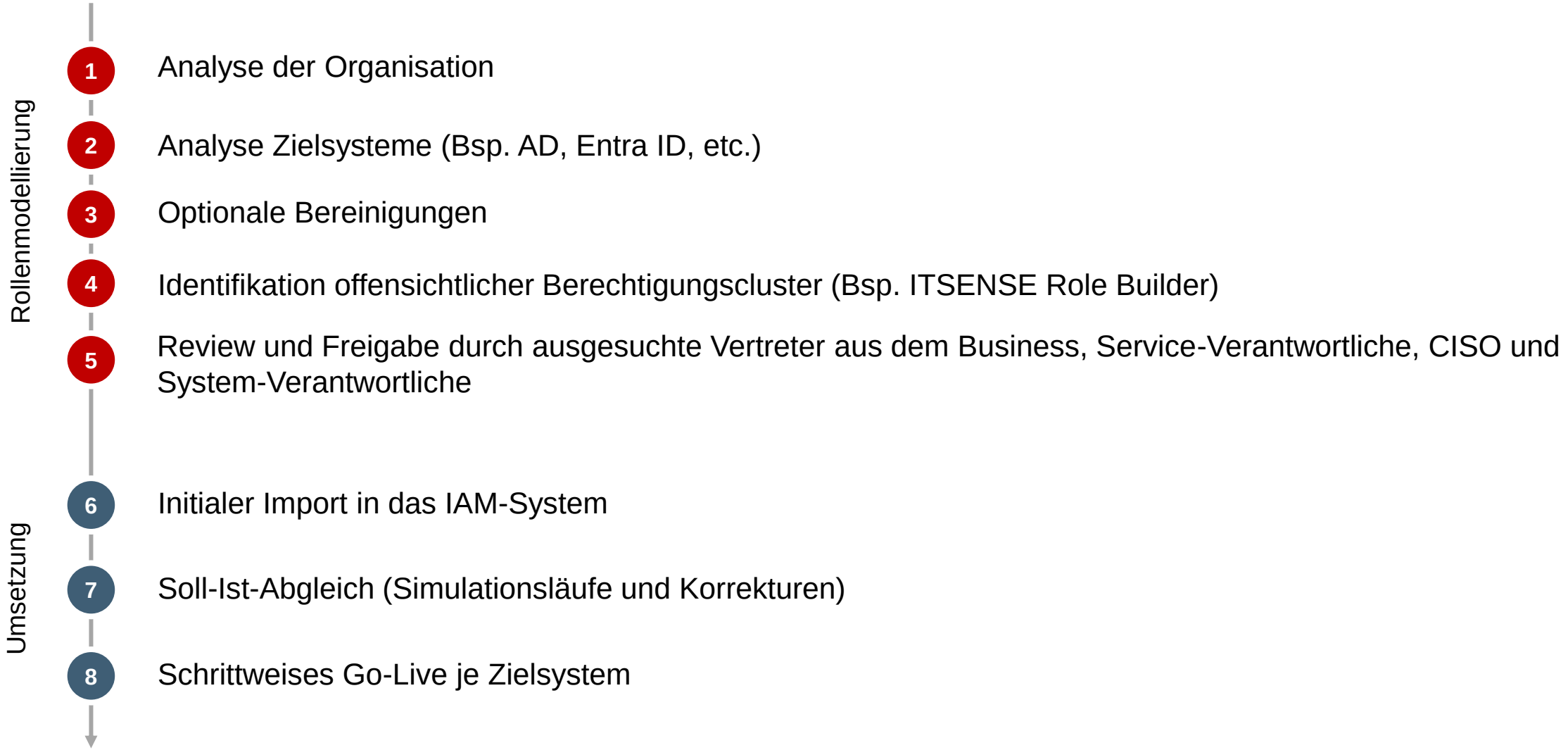
Eine **Technische-Rolle** enthält alle benötigten Berechtigungen, um eine bestimmte Tätigkeit / Aufgabe innerhalb einer Applikation oder eines Systems ausführen zu können.

Eine **Ressource** repräsentiert eine Einzelberechtigung oder eine Applikationsrollen innerhalb des Zielsystems

Suche nach Berechtigungsclustern in den Zielsystemen

ITSENSE

# Bewährtes Vorgehen bei der Einführung eines Rollenmodells




ITSENSE

# Tücken und Herausforderungen aus Sicht Business (Top-down)

- Die Organisation will Role-Based-Access-Control (Fokus Aufgaben- / Funktionsorientiert) einführen, lebt aber seit Jahren hierarchisch orientierte Strukturen und Denkmuster.
- Die Funktionsbezeichnung im HRM-System ist ein Freitextfeld
- Keine harmonisierten Funktionsbezeichnungen, sprich die gleiche Aufgabe/Funktion hat verschiedene Bezeichnungen, Bsp. «Sales», «Verkaufsberater», «Aussendienstmitarbeiter»
- Die Funktionsbezeichnungen im HRM-System sind zu grob für eine möglichst automatisierte und granulare Rollenzuweisung, Bsp. «Kaufmännischer Angestellter» oder «Produktionsmitarbeiter»
- Die Organisationsstruktur existiert nur auf PowerPoint und wird nicht in einem HRM-System geführt
- Das HR setzt organisatorische Veränderung (Reorganisation) um, ohne Rücksprache mit der ICT
- Die Namen der bestellbaren Business-Rollen sind zu technisch und für die Mitarbeiter der Fachbereiche nicht sprechend.
- **Ein Rollenmodell sollte kontinuierlich gepflegt und flexibel an organisatorische Veränderungen angepasst werden.**

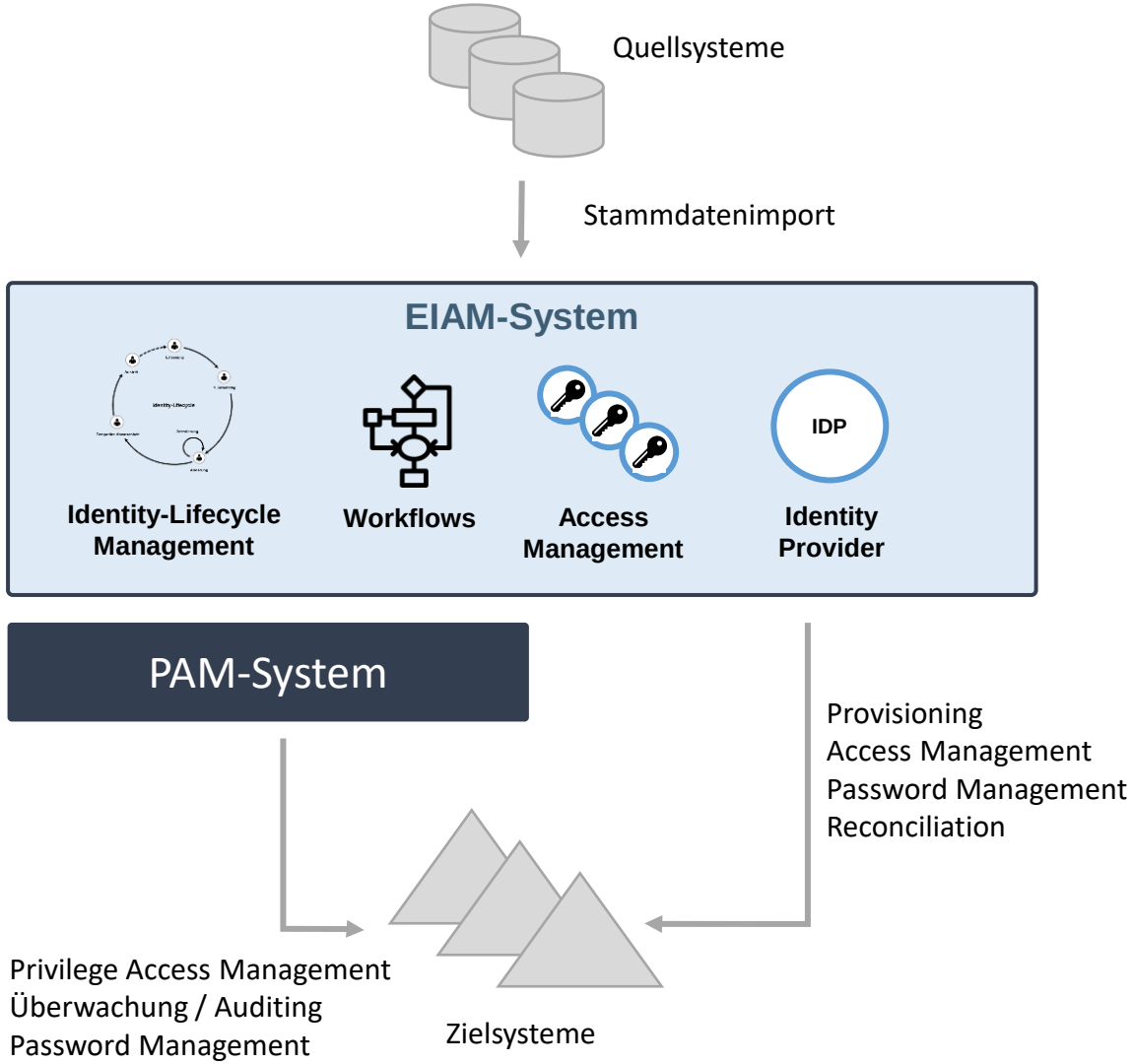
ITSENSE

# Tücken und Herausforderungen aus Sicht IT (Bottom-up)

- Role-Mining, rein auf Basis vorhandener Berechtigungen, tendiert zu technischen Rollen und vernachlässigt den fachlichen und organisatorischen Aspekt.
- **Hohe Datenqualität** ist der Schlüssel für ein erfolgreiches Role-Mining
  - Obsolete Berechtigungsobjekte löschen
  - Obsolete Benutzerkonten löschen
  - Verschachtelte Berechtigungsobjekten auflösen
  - Die Namen von Berechtigungsobjekten aktualisieren und der Namenskonvention anpassen
- In jedem historisch gewachsenen Berechtigungs-Chaos steckt auch ein Stück Wahrheit. Diese Wahrheit zu extrahieren ist nicht einfach.
- Temporäre Berechtigungszuweisungen werden beim Role-Mining oft nicht erkannt oder falsch interpretiert.
- **Ein Rollenmodell sollte kontinuierlich gepflegt und flexibel an technische Veränderungen angepasst werden.**

ITSENSE

# Enterprise IAM und PAM




- **Erhöhte Sicherheit für privilegierte Konten -** Ein PAM-System konzentriert sich darauf, den Zugriff auf privilegierte Konten, wie Administrator- und Systemkonten, zu schützen. Es bietet zusätzliche Sicherheitskontrollen und Überwachungs-funktionen für diese Konten, um Missbrauch oder unbefugten Zugriff zu verhindern.
- **Granulare Zugriffskontrolle**: PAM-Systeme ermöglichen eine granulare Kontrolle darüber, wer auf welche privilegierten Ressourcen zugreifen kann. Durch die Implementierung von Rollen, Richtlinien und Genehmigungsworkflows können Administratoren den Zugriff auf sensible Systeme und Daten steuern.
- **Überwachung und Auditierung**: PAM-Systeme bieten detaillierte Überwachungs- und Auditierungsfunktionen, um Aktivitäten privilegierter Benutzer zu verfolgen.
- **Integration mit IAM-Systemen**: Ein PAM-System kann nahtlos mit einem EIAM-System integriert werden, um eine ganzheitliche Zugriffsverwaltungslösung zu schaffen. Administratoren können privilegierte Zugriffe im Kontext des gesamten Identitätslebenszyklus verwalten.

ITSENSE

# Stay tuned, stay secure!

SWISS MADE IAM

abraxas

Delinea
Defining the boundaries of access

ti&m
big ideas. creative technology.

ARCTIC WOLF

TREND MICRO

netzmedien

white rabbit Communications

#5