

# **IAM im Betrieb – Eine Herausforderung**

**Tanya Ramstöck, SWICA**

**Michael Petri, IPG AG**



# Inhalt

## Teil 1

### **Erfahrungen aus dem IAM Einsatz**

Tanya Ramstöck

Technische IAM Verantwortliche

[tanya.ramstoeck@swica.ch](mailto:tanya.ramstoeck@swica.ch)



## Teil 2

### **Vorgehensweise in IAM Projekten**

Michael Petri

Head Technical Consulting OneIdentity

[michael.petri@ipg-group.com](mailto:michael.petri@ipg-group.com)



# Teil 1 – Erfahrungen aus dem IAM Einsatz

Tanya Ramstöck, SWICA



- Inhalte
- Prozesse und Beteiligte Fachpersonen
- IT Shop
- Geschäftsrollenmodellierung
- Systemanforderungen langfristig
- Betriebliche Anforderungen
- Datenqualität



# IAM System bei SWICA

- Revisionspendenz als Auslöser für das IAM Projekt
  - Als IAM System nutzt SWICA ein Onedensity Manager
  - Projekt und Betrieb erfolgt gemeinsam mit IPG
  - Quick Win zur Erfüllung der Revisionspendenz
- Heute ist im System enthalten:
    - IT Shop für Bestellung und Genehmigung
    - HR Anbindung
    - Abbildung von Workflows
    - Active Directory mit Dynamics AX, CRM, ELO, Telefonie
    - Versicherungskernsystem SHP mit Syrius, Archiv, etc.
    - Kaba Schliesssystem
    - Rollenmodell für SHP
    - Funktionstrennung
    - Rezertifizierung
    - Reports



## Beteiligte Fachabteilungen und Ihre Prozesse

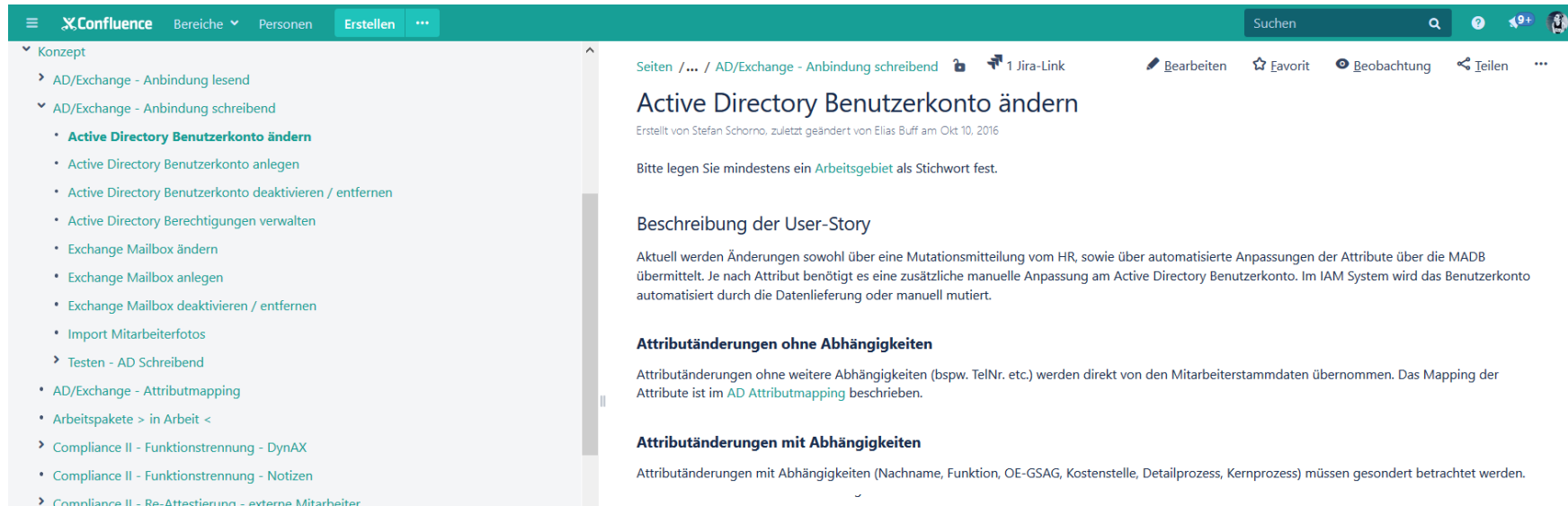
- Welche Systeme sollen an IAM angebunden werden?
- Welche Prozesse werden neu im IAM abgebildet?
- Kennen wir diese?
- Sind die Projektmitarbeiter mit all diesen Prozessen vertraut, braucht es noch Inputs aus dem Fachbereich selbst?
- Eine stabile Organisation und klare Verantwortlichkeiten sind wichtig

HR	Informatik	Applikations- management	Versicherungs- technik	Vorgesetzte
CISO	Datenschutz- beauftragter	IPG als Externer Dienstleister	Support	IAM Verantwortliche



# Bestehende Prozesse hinterfragen

- Warum sind die Prozesse so, liegt es an den Gegebenheiten die sich jetzt ändern lassen?
- Macht es Sinn die vorhandenen Prozesse weiterhin so abzubilden?
- Gibt es Verbesserungsmöglichkeiten mit der Einführung von IAM?



The screenshot shows a Confluence page with a teal header. The left sidebar contains a navigation menu with categories like 'Konzept', 'AD/Exchange - Anbindung lesend', and 'AD/Exchange - Anbindung schreibend'. The main content area is titled 'Active Directory Benutzerkonto ändern' and includes a breadcrumb 'Seiten / ... / AD/Exchange - Anbindung schreibend'. Below the title, there is a note: 'Bitte legen Sie mindestens ein Arbeitsgebiet als Stichwort fest.' The page also features sections for 'Beschreibung der User-Story' and 'Attributänderungen ohne Abhängigkeiten'.

Konzept

- AD/Exchange - Anbindung lesend
- AD/Exchange - Anbindung schreibend
  - Active Directory Benutzerkonto ändern**
  - Active Directory Benutzerkonto anlegen
  - Active Directory Benutzerkonto deaktivieren / entfernen
  - Active Directory Berechtigungen verwalten
  - Exchange Mailbox ändern
  - Exchange Mailbox anlegen
  - Exchange Mailbox deaktivieren / entfernen
  - Import Mitarbeiterfotos
- Testen - AD Schreibend
- AD/Exchange - Attributmapping
- Arbeitspakete > in Arbeit <
- Compliance II - Funktionstrennung - DynAX
- Compliance II - Funktionstrennung - Notizen
- Compliance II - Re-Attestierung - externe Mitarbeiter

Seiten / ... / AD/Exchange - Anbindung schreibend

## Active Directory Benutzerkonto ändern

Erstellt von Stefan Schorno, zuletzt geändert von Elias Buff am Okt. 10, 2016

Bitte legen Sie mindestens ein Arbeitsgebiet als Stichwort fest.

### Beschreibung der User-Story

Aktuell werden Änderungen sowohl über eine Mutationsmitteilung vom HR, sowie über automatisierte Anpassungen der Attribute über die MADB übermittelt. Je nach Attribut benötigt es eine zusätzliche manuelle Anpassung am Active Directory Benutzerkonto. Im IAM System wird das Benutzerkonto automatisiert durch die Datenlieferung oder manuell mutiert.

### Attributänderungen ohne Abhängigkeiten

Attributänderungen ohne weitere Abhängigkeiten (bspw. TelNr. etc.) werden direkt von den Mitarbeiterstammdaten übernommen. Das Mapping der Attribute ist im [AD Attributmapping](#) beschrieben.

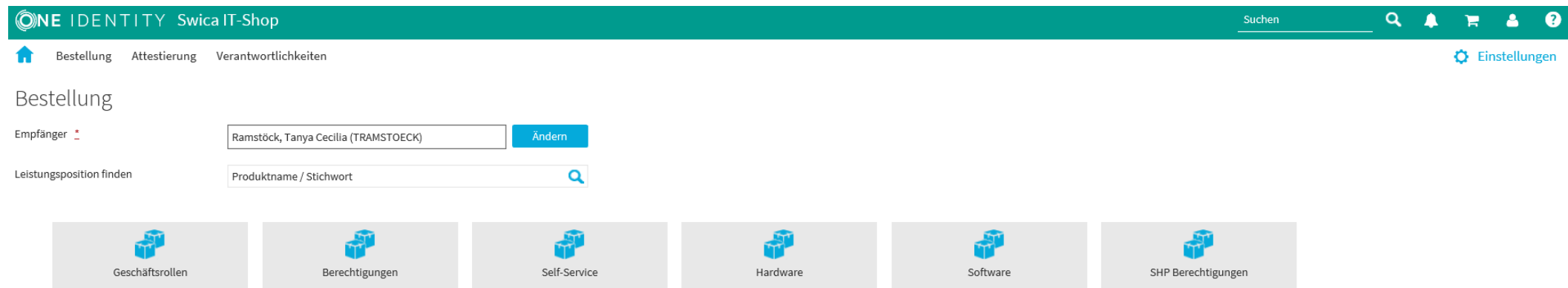
### Attributänderungen mit Abhängigkeiten

Attributänderungen mit Abhängigkeiten (Nachname, Funktion, OE-GSAG, Kostenstelle, Detailprozess, Kernprozess) müssen gesondert betrachtet werden.



# IT Shop nutzen

- Der IT Shop bietet viele Möglichkeiten
- Der Betrieb kann mit Hilfe des IT Shops vereinfacht werden
- Welche Rechte, Rollen, Produkte sollen bestellbar gemacht werden
- Berechtigungsworkflows definieren
- Struktur für Endbenutzer verständlich aufbauen



The screenshot shows the ONE IDENTITY Swica IT-Shop interface. The header is teal with the logo and text 'ONE IDENTITY Swica IT-Shop' on the left, and a search bar with 'Suchen' and navigation icons on the right. Below the header, there are navigation links: 'Bestellung', 'Attestierung', and 'Verantwortlichkeiten'. A home icon is on the left, and 'Einstellungen' is on the right. The main content area is titled 'Bestellung'. It features a form with 'Empfänger' (Receiver) set to 'Ramstöck, Tanya Cecilia (TRAMSTOECK)' and an 'Ändern' button. Below that is a search bar for 'Leistungposition finden' (Find service position) with the placeholder 'Produktname / Stichwort' and a search icon. At the bottom, there is a row of six grey buttons, each with a blue cube icon and a label: 'Geschäftsrollen', 'Berechtigungen', 'Self-Service', 'Hardware', 'Software', and 'SHP Berechtigungen'.





## Vorbereitungen zu Rollen treffen

- Geschäftsrollenkonzepktion sowie die Modellierung dieser benötigt Zeit, diese muss zwingend eingeplant werden
- Die Mitarbeiter im Team sollten Firmenkenntnisse sowie die Eigenheiten kennen, da die ganze Firma als solches davon betroffen ist
- Der Grad der Automatisierung der Berechtigungen ist abhängig von den Geschäftsrollen
- Geschäftsrollenmodel muss ständig gepflegt werden, hier müssen auch Ressourcen für die Zeit nach der Einführung eingeplant werden
- IPG bietet in diesem Bereich Coaching zur Geschäftsrollenmodellierung an



## System soll langfristige Anforderungen unterstützen

- Welche Tools werden in Zukunft noch in die Systemlandschaft implementiert werden
- Grundsatzentscheidung welche Applikationen an IAM angebunden werden müssen
- Bei Softwarebeschaffung die Anforderungen zur IAM-Anbindung vorsehen
- Standardvorgehen bei Einführungen neuer Produkte, Tools festlegen
- Software bzw. die Berechtigung dieser auch parallel in den IT Shop stellen
  
- Auch zukünftige Themen berücksichtigen:
- Rezertifizierung, Revisionsanforderungen, Nachvollziehbarkeit, Funktionstrennung



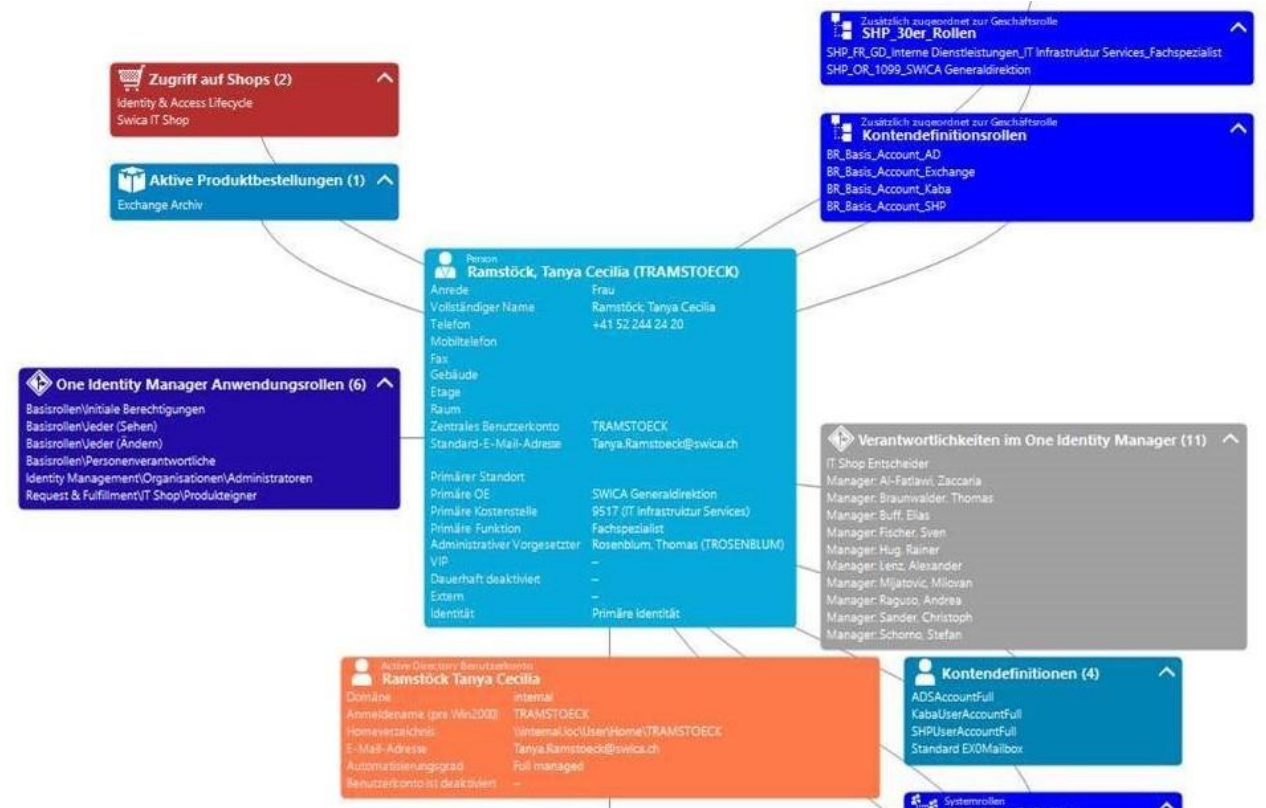
## Betriebliche Anforderungen aufnehmen

- Nach Projektbeendigung wird das IAM System dem Betrieb übergeben
- Wie soll der Support gewährleistet werden?
- Der Betrieb hat eigene Anforderungen. Diese sollten vor der Übergabe in den Betrieb abgeklärt worden sein und wenn möglich auch berücksichtigt werden
- Wissensaufbau intern oder auslagern
- Stellvertretung sicherstellen
- Verantwortlichkeiten für die Zeit nach der Einführung klären und definieren



# Besonders auf die Daten achten

- IAM ist ein Zusammenzug von allen möglichen Daten.
- Datenqualität im Quellsystem!
- HR Daten zu Identitäten und zur Organisation sind grundlegend wichtig
- Datenqualität in den Zielsystemen!
- Altlasten aufräumen, Berechtigungen beschreiben, Owner benennen, Namenskonzepte prüfen
- Vorbereitende Arbeiten auch mit berücksichtigen



# **Teil 2 – Vorgehensweise in IAM Projekten**

**Michael Petri, IPG AG**



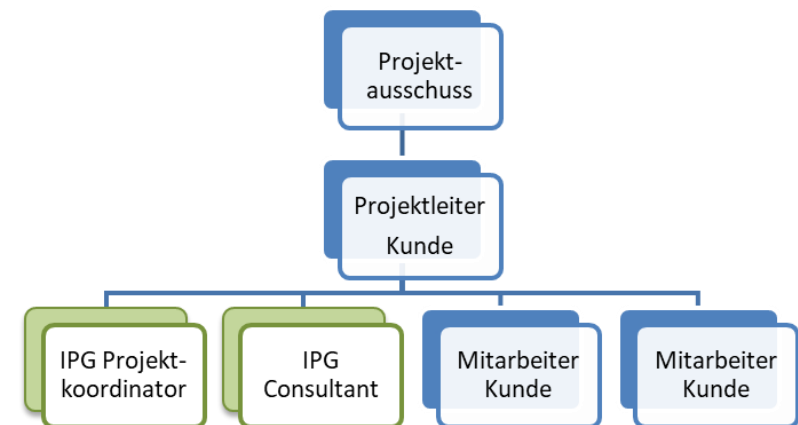
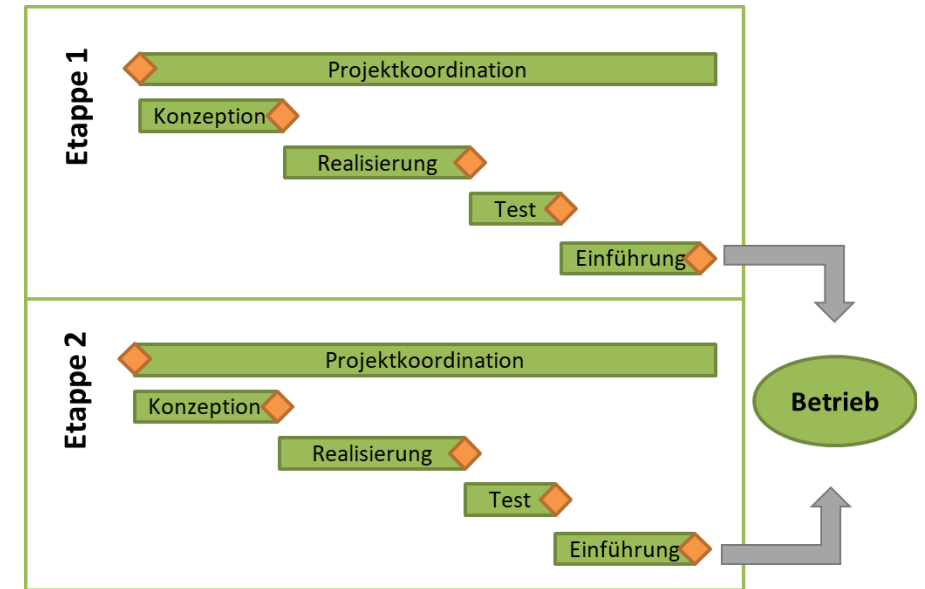
## Inhalte

- Vorgehensweise generell
- Vorgehensweise bei SWICA
- Handlungsfelder für IAM
- Erfolgsfaktoren für IAM
- Vorstellung eines IAM Produktes

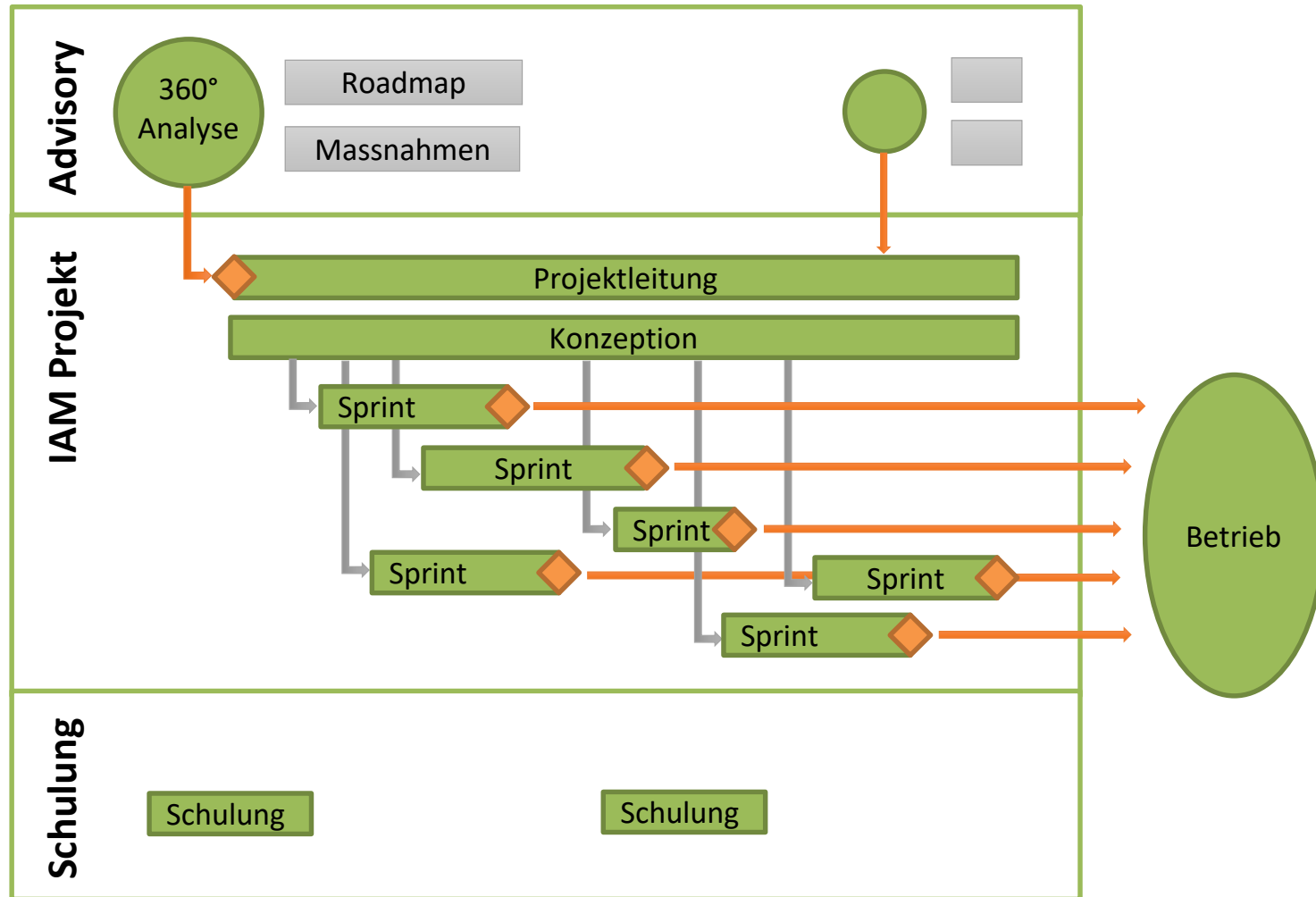


# Vorgehensweise von IPG

- IAM Projekte sind grosse Projekte
  - Technik ist weniger das Problem
  - Aufwändig sind die Themen zur Organisation, Prozesse und Daten
  - Klassische Projektvorgehensmethoden sind üblich
- IAM Projekte sind in Etappen zu unterteilen
  - «Think Big, Start Small»
  - Erreichbare Ziele setzen
  - Abhängigkeiten in den Etappen senken
  - Nutzen schrittweise erhöhen
- Projektorganisation beachten
  - Einen zentralen IAM Verantwortlichen einsetzen
  - Management Support aufbauen
  - Kernteam bilden



# Vorgehensweise bei SWICA

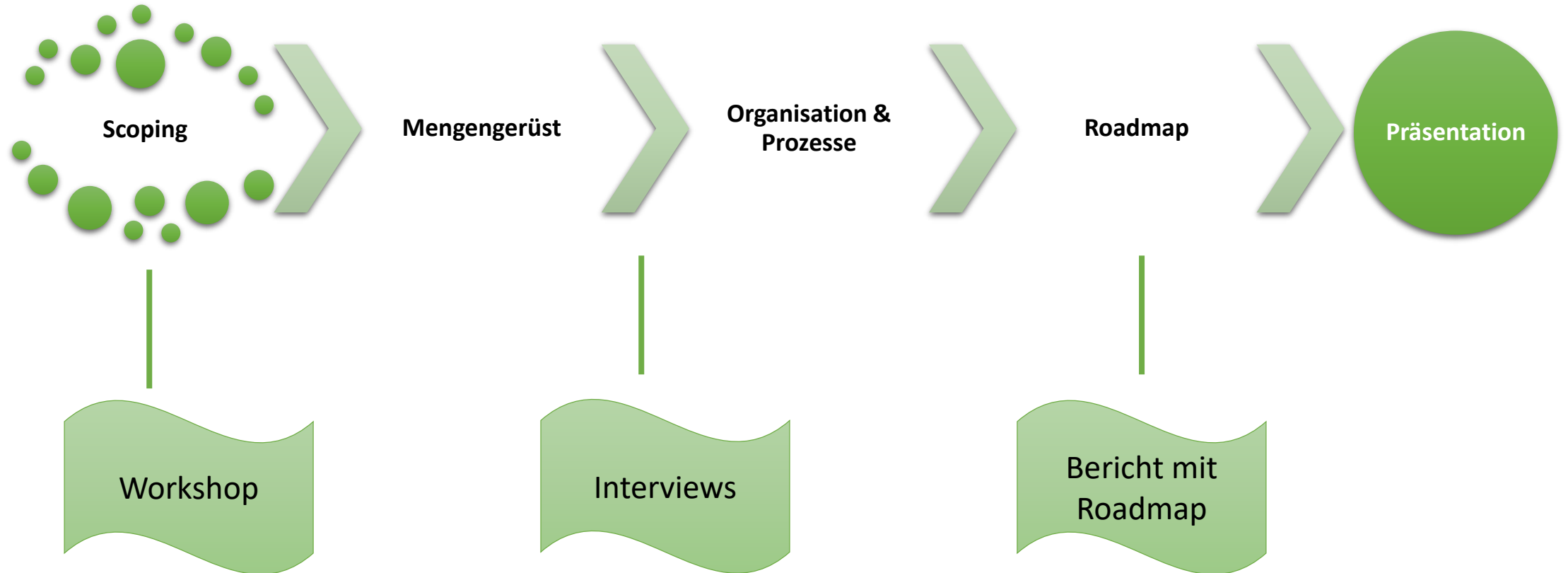


- Bedarf wegen einer Revisionspendenz
- Rascher erster Schritt notwendig
- Ansätze einer agilen Umsetzung mit «Sprints»
- Begriff «Sprint» hat sich eingebürgert und ist nicht gleichbedeutend mit dem Verständnis aus Scrum





# Inhalt einer 360° Analyse



# Typische Handlungsfelder

IAM Prozesse und  
Organisation

Einbindung von HR-  
Quellsystem

Einbindung von  
Zielsystemen  
(On-Premise und  
Cloud)

Geschäftsrollen  
und  
Funktionstrennung

Antragsportal und  
Genehmigungen

IAM Handlungsfelder

24h Password  
Reset

Rezertifizierung

Nachvollziehbarkeit  
und Reporting

Single-Sign On  
(SSO)

Privileged Access  
Management  
(PAM)

# Erfolgsfaktoren für ein IAM Projekt

Einige Tipps für ein erfolgreiches IAM Projekt:

- Frühzeitige grobe Abklärung hilft Risiken, Handlungsnotwendigkeiten, Zeitbedarf und Möglichkeiten einzuordnen
- Wichtige Stakeholder identifizieren und einbeziehen
- Aktive Mitarbeit von vielen Beteiligten ist erforderlich
- Enge und offene Zusammenarbeit zwischen dem Kunden und dem Integrationspartner zwingend
- Datenqualität stets beachten und Massnahmen frühzeitig ergreifen
- Prozessänderungen abstimmen und begleiten
- Betriebsorganisation klären und einsetzen



# Demo eines IAM Systems



ONE IDENTITY One Identity Manager

Suchen

Bestellung Attestierung Compliance Verantwortlichkeiten Einstellungen

Willkommen

Setzen Sie Ihre Kennwortfrage, um Ihr Konto später entsperren zu können.

Offene Attestierungen 35

Neue Bestellung

Offene Bestellungen 7

Meine Mitarbeiter (9) Mehr

- Amoroso, Dr. Diadora Elena Samantha Maria (DIADORAELE)
- Beispiel, Dr. Vreni (VRENIB)
- Bigler, Dr. Samantha (SAMANTHAB)
- Cesario, Dr. Sven-Alexander (SVENALEXANDER)

ONE IDENTITY One Identity Manager

Suchen

Bestellung Attestierung Compliance Verantwortlichkeiten Einstellungen

← Offene Bestellungen

Ansichtseinstellungen Suche

Produkt	Status	Bestelldatum	Empfänger	Priorität	Entscheidung
BR_OR_Employee Delivery Niederdorf Geschäftsrolle: BR_OR_Employee Delivery Niederdorf <-> Person: Dunst, Dr. Marlis (MARLISD)	Bestellung	vor 3 Minuten	Dunst, Dr. Marlis	Standard	<input checked="" type="checkbox"/> <input type="checkbox"/>
BR_OR_Employee Delivery Niederdorf Geschäftsrolle: BR_OR_Employee Delivery Niederdorf <-> Person: Simoni, Dr. Tabea (TABEAS)	Bestellung	vor 3 Minuten	Simoni, Dr. Tabea	Standard	<input type="checkbox"/> <input checked="" type="checkbox"/>

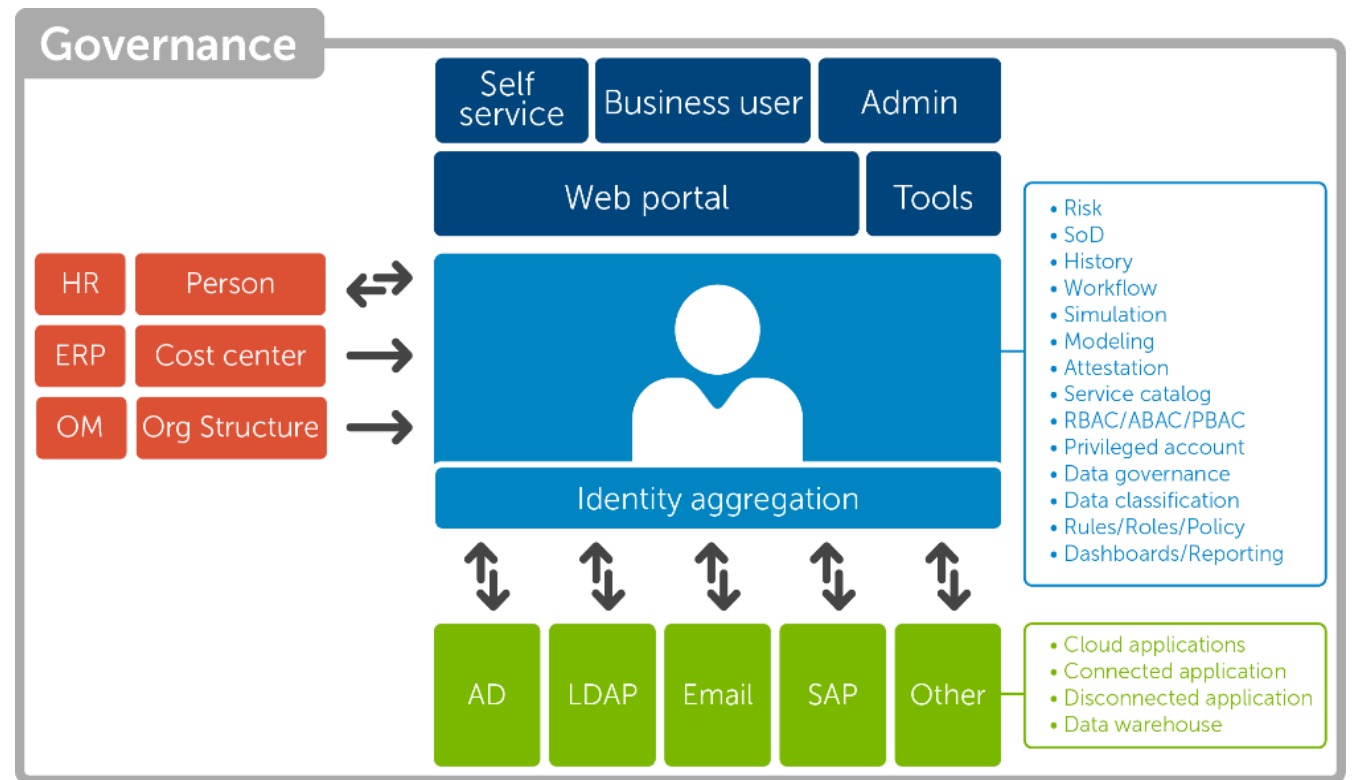
2 Ergebnis(se)

Weiter

# Vorstellung OneIdentity Manager



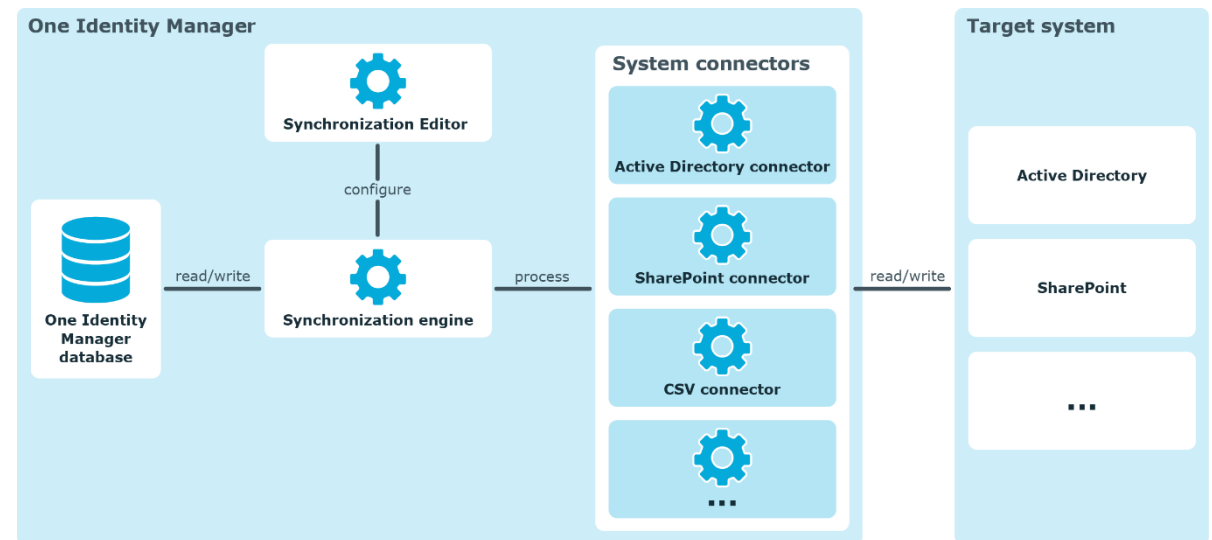
- Personen Lifecycle
- Berechtigungsverwaltung
- Self-Service Portal
- Genehmigungsprozesse
- Rezertifizierungsprozesse
- Geschäftsrollen
- Audit und Compliance
- Funktionstrennung (SoD)
- Reporting und Dashboards



# Vorstellung OneIdentity Manager



- Active Directory und Exchange
- SharePoint-Umgebung
- Windows PowerShell
- LDAP-Umgebung
- SAP R/3-Umgebung und SAP HANA
- IBM Notes-Umgebung
- Unix-basierte Zielsysteme
- Cloud-Anwendungen
  - Azure Active Directory, Exchange und Sharepoint Online
  - G Suite-Umgebung
  - Oracle E-Business Suite
  - SCIM – System for Cross-Domain Identity Management
- kundendefinierte Zielsysteme
  - CSV Konnektor
  - Web Services
- nativer Datenbank Konnektor
  - SQL, MySQL, SQLite, Oracle, DB2, ADO.Net



**Fragen**

**&**

**Antworten**

