

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



Teil 2 Vorgehensweise in IAM Projekten

Michael Petri
Head Technical Consulting OneIdentity

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

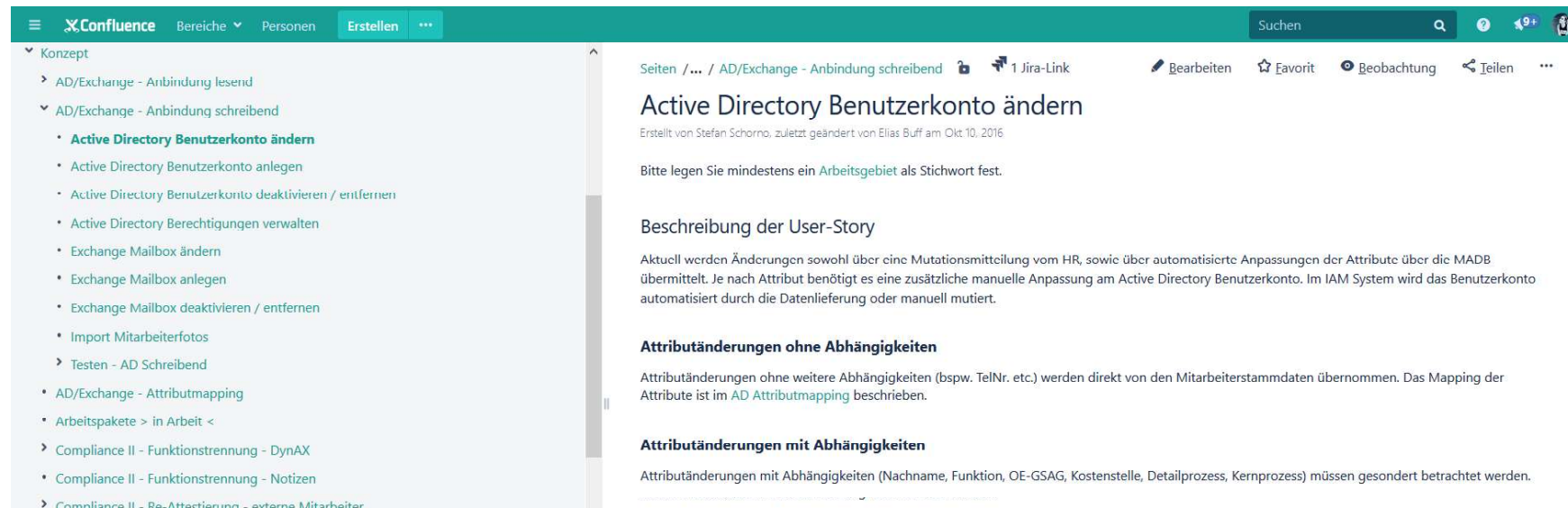
- Welche Systeme sollen an IAM angebunden werden?
- Welche Prozesse werden neu im IAM abgebildet?
- Kennen wir diese?
- Sind die Projektmitarbeiter mit all diesen Prozessen vertraut, braucht es noch Inputs aus dem Fachbereich selbst?
- Eine stabile Organisation und klare Verantwortlichkeiten sind wichtig

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 tree under 'Konzept' with items like 'AD/Exchange - Anbindung lesend', 'AD/Exchange - Anbindung schreibend', and 'Active Directory Benutzerkonto ändern'. The main content area has a breadcrumb 'Seiten / ... / AD/Exchange - Anbindung schreibend' and a title 'Active Directory Benutzerkonto ändern'. Below the title, it says 'Erstellt von Stefan Schorno, zuletzt geändert von Elias Buff am Okt.10. 2016'. The main text includes a note: 'Bitte legen Sie mindestens ein Arbeitsgebiet als Stichwort fest.' and a section 'Beschreibung der User-Story' which states: '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.' There are also sections for 'Attributänderungen ohne Abhängigkeiten' and 'Attributänderungen mit Abhängigkeiten'.



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



Teil 2 – Vorgehensweise in IAM Projekten

Michael Petri, IPG AG



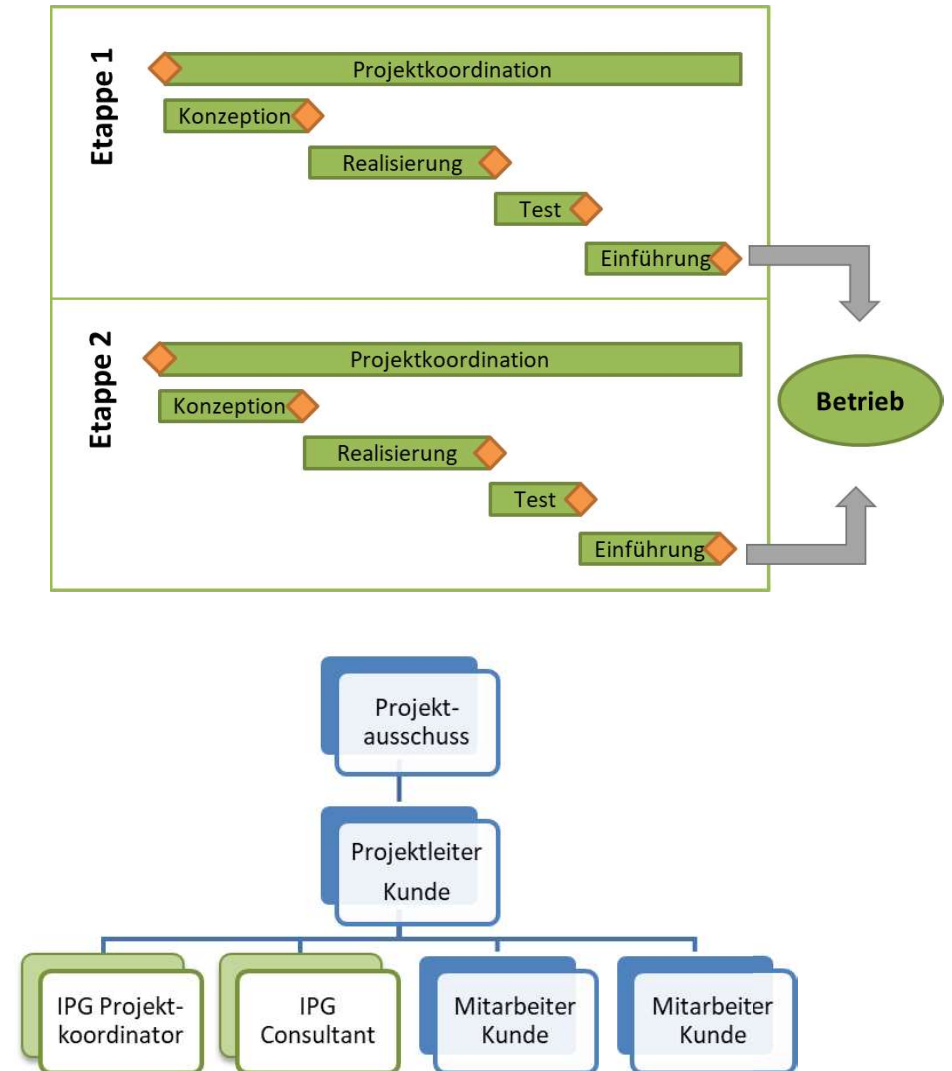
Inhalte

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

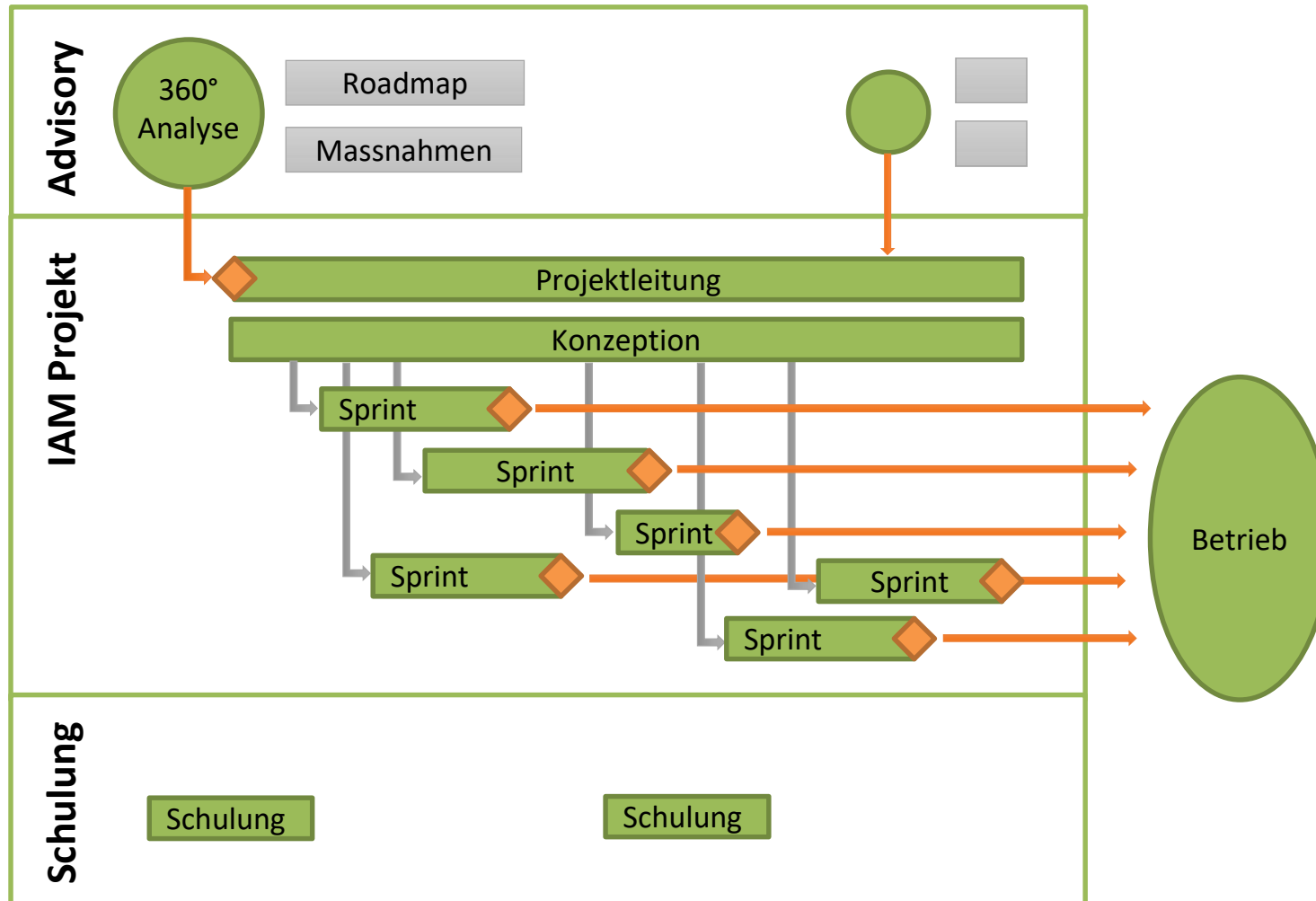


Vorgehensweise von IPG

- 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



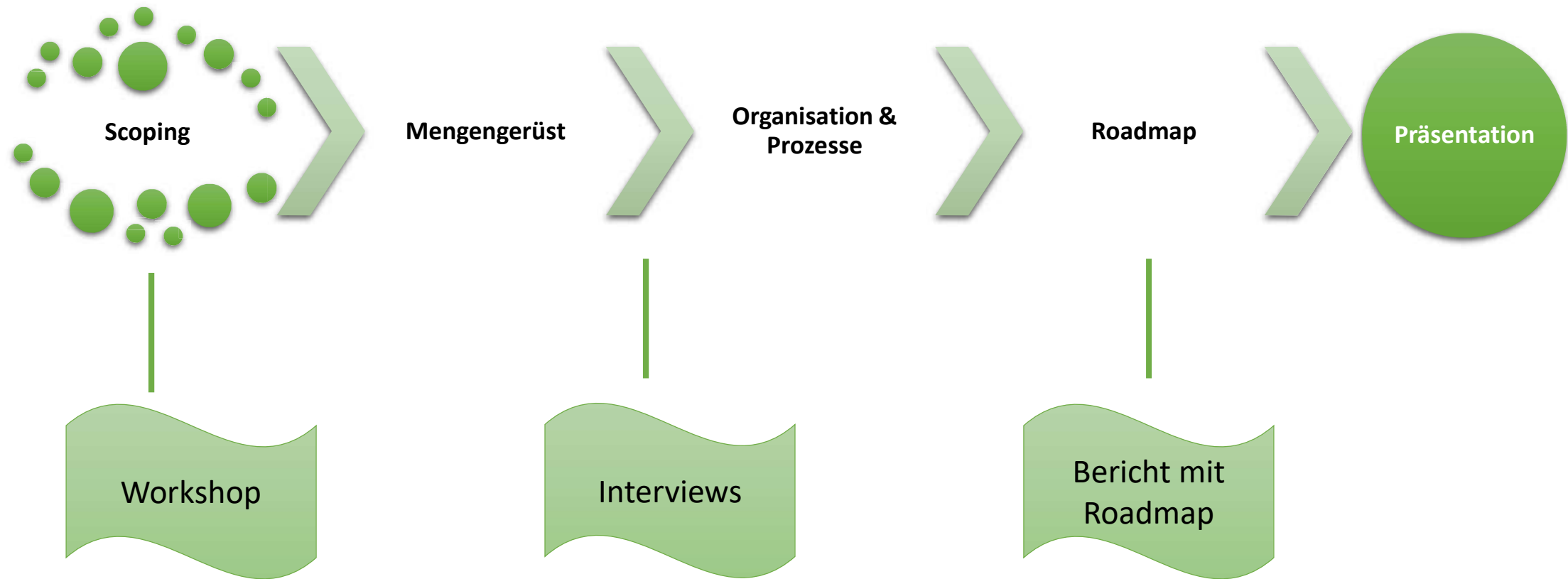
Vorgehensweise bei SWICA



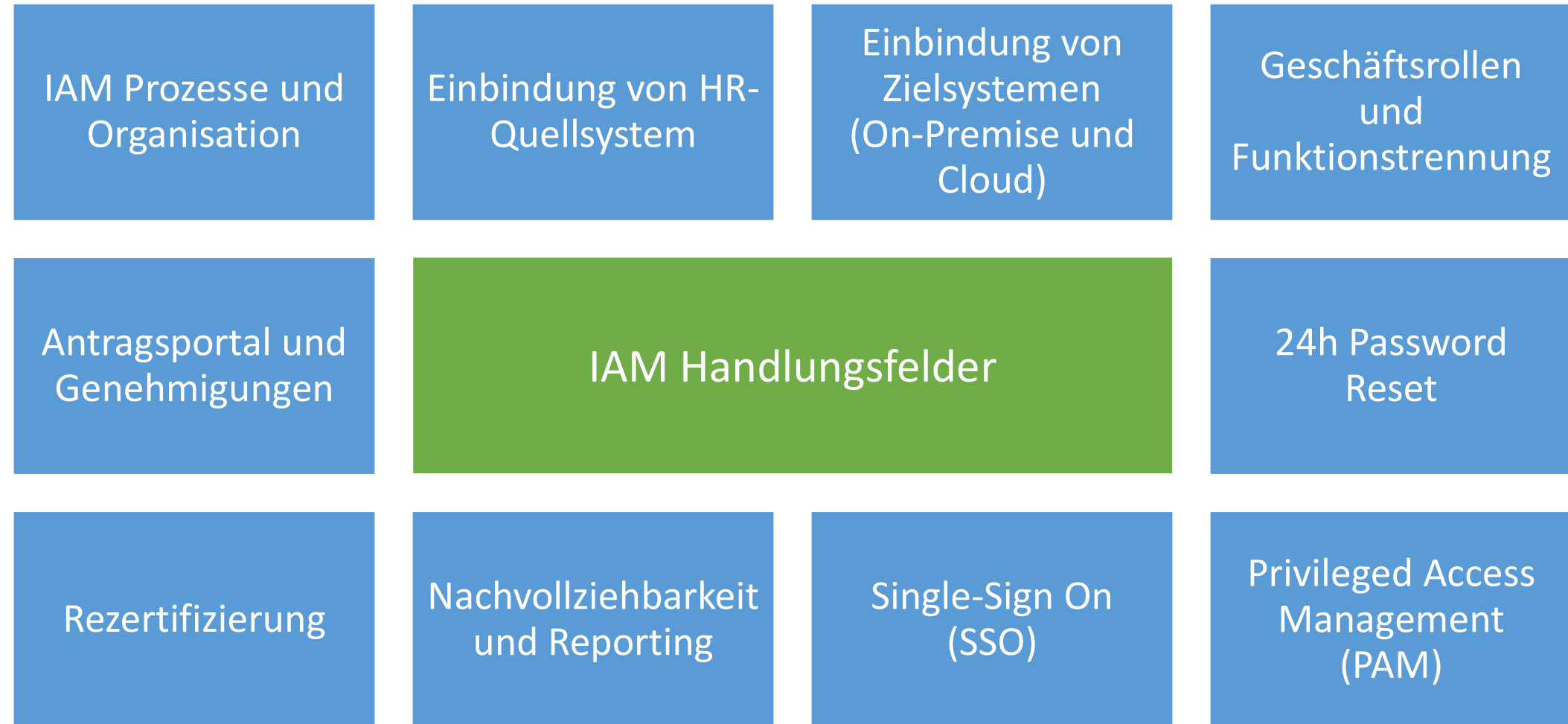
- Bedarf wegen einer Revisionspendenz
- Rascher erster Schritt notwendig
- Ansätze einer agilen Umsetzung mit «Sprints»
- Begriff «Sprint» hat sich eingebürgert und ist nicht gleichbedeutend mit dem Verständnis aus Scrum



Inhalt einer 360° Analyse



Typische Handlungsfelder



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

ONE IDENTITY One Identity Manager Suchen

[Bestellung](#)
[Attestierung](#)
[Compliance](#)
[Verantwortlichkeiten](#)
[Einstellungen](#)

[←](#) Offene Bestellungen i

Ansichtseinstellungen

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](#)

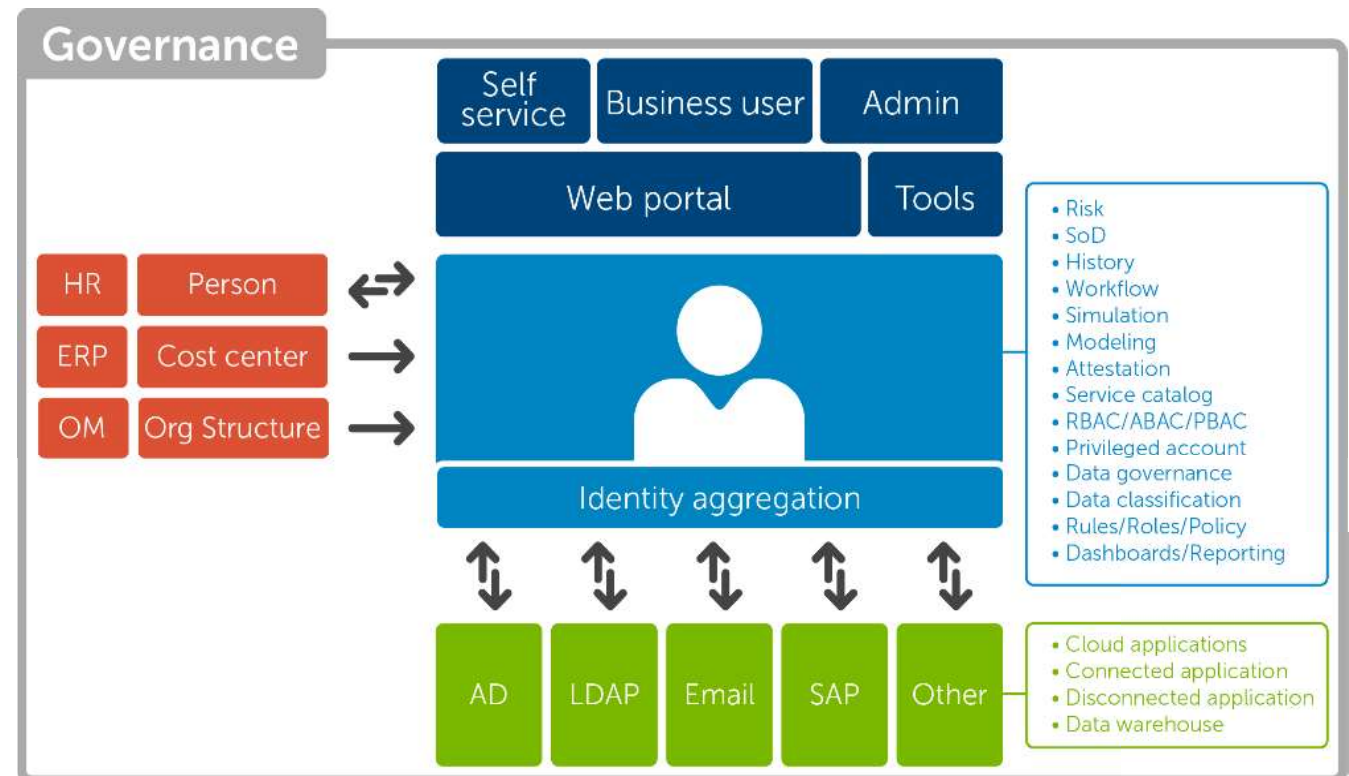
Meine Mitarbeiter (9) Mehr

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

Vorstellung OneIdentity Manager



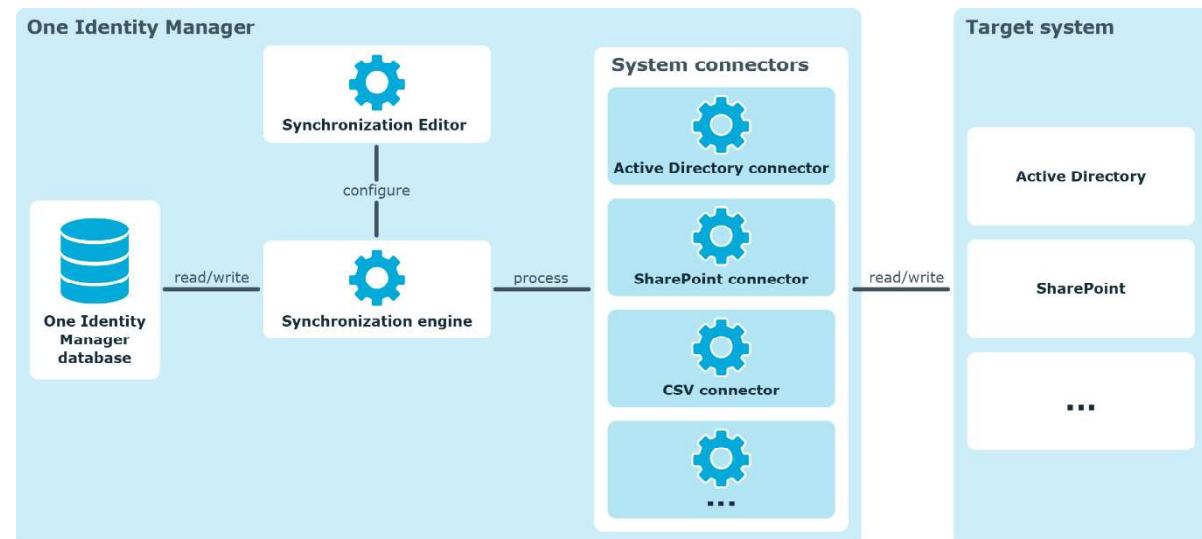
- Personen Lifecycle
- Berechtigungsverwaltung
- Self-Service Portal
- Genehmigungsprozesse
- Rezertifizierungsprozesse
- Geschäftsrollen
- Audit und Compliance
- Funktionstrennung (SoD)
- Reporting und Dashboards



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

