Initial Meeting

„GenericIAM - generische IAM-Prozess als Baukastensystem“

Version 1.0

Dr. Horst Walther

Dienstag, 25.04.2006, Regus An der Welle 4 in Frankfurt

Agenda

- Einführung – Begrüßung - housekeeping
- Kurzvorstellung der Teilnehmer
- Erwartungshaltungen - einfangen und konsolidieren
- Motivation für GenericIAM
- Einige Mitwirkenden präsentieren sich und ihre Erfahrungen
- Sammeln offener Punkte
  - Welche Infrastruktur nutzen wir?
  - Wie arbeiten wir zusammen?
  - Welche Fragen sind offen?
  - Wer macht was bis wann?
  - ...
- Fragen - Anmerkungen – Anregungen?

housekeeping

- Zeiten
- Pausen, Rauchen, Mobiltelephon
- Mittagessen
- Protokoll, gezeigte Präsentationen, Ergebnisse
- Workshop-Charakter
- Kostenumlage
- ...

Ziel der Veranstaltung

Was wollen wir heute erreichen?

- Erwartungen
  - Abstimmen der Erwartungshaltungen der Teilnehmer
- Beiträge
  - Feststellen, welchen Beitrag ein jeder Teilnehmer in die Gruppe einbringen kann.
- Infrastruktur
  - Festlegen einer gemeinsam zu nutzenden Infrastruktur.
  - ggf. müssen wir einen Evaluierungsauftrag an Freiwillige aus unserer Mitte vergeben.
- Zusammenarbeit
  - Organisation der Zusammenarbeit bis zum nächsten Meeting
  - Bestimmen eines Termins für das nächste Meeting.
- Aufgaben
  - Ermitteln der Aufgaben, die wir uns als Gruppe bis zum nächsten Meeting stellen.
- Aufträge
  - Verteilen dieser Aufgaben auf die Teilnehmer

Kurzvorstellung der Teilnehmer

3 – 5 Minuten pro Person

- Wer bin ich?
- Woher komme ich?
- Was hatte ich bisher mit dem Thema zu tun?
- Warum bin ich hier?

Name	Vorname	e-Mail	Unternehmen
Belikan	Oliver	oliver.belikan@doubleSlash.de	doubleSlash Net-Business GmbH
Boenisch	Dr.Kirsten	Kirsten.Boenisch@bmw.de	Bayerische Motoren Werke Aktienges
Boß	Norbert	Norbert.Boss@bov.de	BOV Aktiengesellschaft
Brömme	Arslan	arslan.broemme@it-advisory.com	IT Advisory Group Unternehmensbera
Hohgraefe	Bernd	bernd.hohgraefe@siemens.com	Siemens AG Siemens Region Deutsch
Kuppinger	Martin	mk@KuppingerCole.de	kcp
Lang	Michael	milang@novell.com	Novell GmbH
Netzer	Andreas	netzer@ic-compas.de	iC Compas GmbH & Co KG
Schmidt	Thomas	Thomas.Schmidt@Thoranet.com	THORANET Unternehmensberatung f
Walther	Horst	horst.walther@KuppingerCole.de	Kuppinger, Cole + Partner
Brito	Octavio		

Erwartungshaltungen
einfangen und konsolidieren

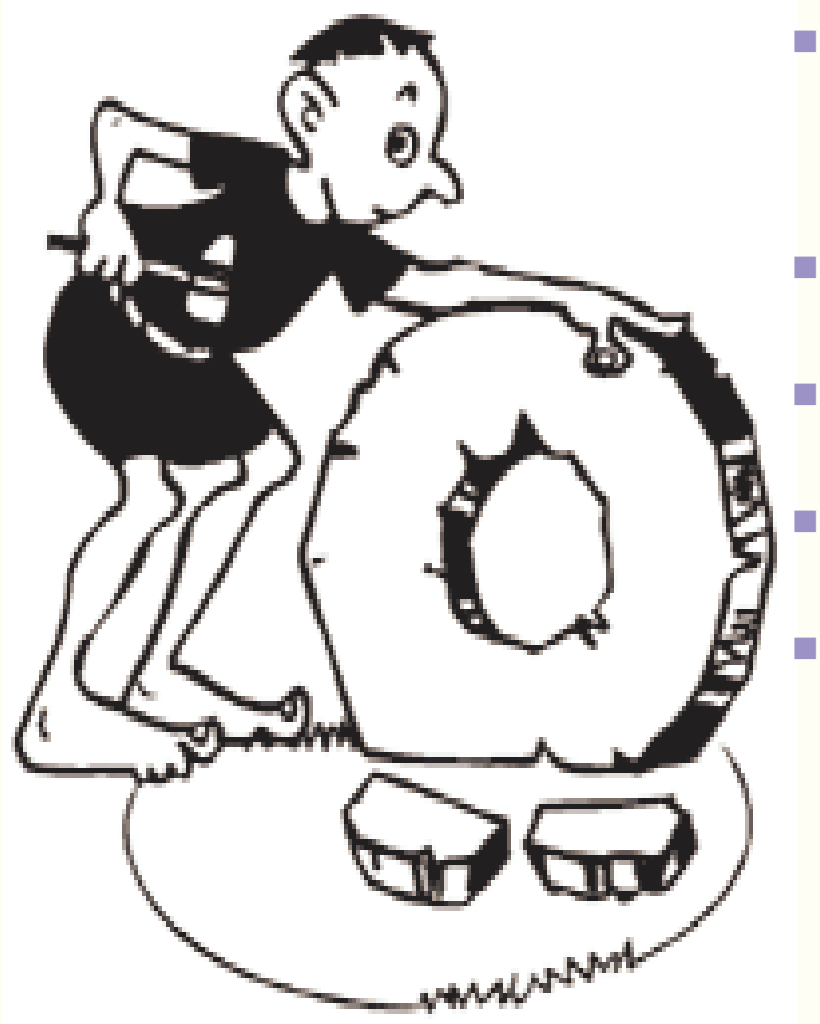
Bitte beantworten Sie **spontan** die folgenden Fragen ...

Anschließend diskutieren wir diese Punkte.

- Warum bin ich hier?
- Welchen Nutzen erwarte ich von der heutigen Veranstaltung?
- Welchen Nutzen erwarte ich von dieser Initiative?
- Was müssen wir dafür leisten?
- Welche Gefahren sehe ich für den Erfolg?
- Glaube ich an ein Gelingen?

Motivation

welche Idee steckt hinter GenericIAM?



- Prozesse verursachen den meisten Aufwand.
  - so gehen bei PKI-Projekten 85% des Aufwandes in die Prozesse.
- Warum mit einem weißen Blatt Papier beginnen?
- Warum, das Rad immer wieder neu erfinden?
- Gibt es nicht auffällige fachliche Ähnlichkeiten?
- Sollten wir uns nicht lieber auf die Unterschiede konzentrieren?

  ... Und das Gemeinsame „von der Stange“ kaufen?

➔ Wo bleibt der Baukasten für Standardprozesse des IdM?

Komplexitätsfaktoren ...

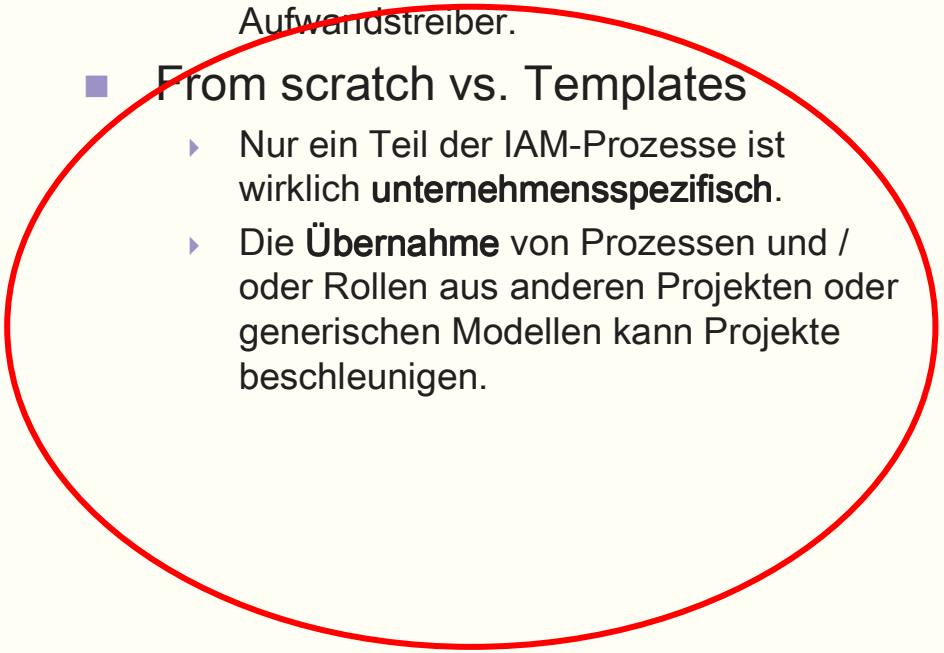
Was macht IAM-Projekte schwierig?

- Bestehende Lösungen
  - Je **mehr bestehende** Lösungen für das Identity Management existieren, umso höher wird der Aufwand, sie zu harmonisieren und zu ersetzen.
  - **Je reifer** die existierenden Lösungen sind, umso schwerer finden neue Ansätze Akzeptanz.
- Querschnittscharakter
  - Identity-Management Prozesse sind typischerweise **bereichsübergreifend**.
  - Es sind **viele** gleichberechtigte **Stakeholder** in ein Projekt involviert.
  - 3 bis 5 mal höhere **Kommunikationskomplexität** zu „normaler“ SW-Entwicklung.
  - Typischer **Change** Management Prozess: Macht-Sponsor erforderlich!
- Prozessreife
  - Je höher die **Reife** der Management-Prozesse (z.B. nach CMMI) umso leichter fällt die Einführung von IAM-Prozessen, -Regeln, -Rollen, -Policies.
  - Reife IAM-Prozesse in einem **unreifen Prozess-Umfeld** finden wenig Akzeptanz (Aufwandstreiber).
- Projektzuschnitt
  - SW-Implementierungsprojekte sind **überfordert**, wenn sie die organisatorischen Voraussetzungen erst schaffen müssen
  - Prozess- und Rollen-Definitionen erfordern eigene **Definitionsprojekte** vor der oder parallel zur Implementierung.
- Marktkonsolidierung
  - Mergers & Acquisitions führen zu wenig kompatiblen **Produktsammlungen**.
  - Die Software übernommener Unternehmen wird häufig nicht mehr optimal **unterstützt**.

... Komplexitätsfaktoren

Was macht IAM-Projekte schwierig?

- Technische Risiken
  - IAM-SW-Suiten sind **komplex** und schwer zu handhaben.
  - Ohne **Implementierungserfahrung** in exakt der geforderten Umgebung sind die Projektrisiken nicht kalkulierbar.
  - Hinter „harmlosen“ Versionssprüngen (z.B.: 5.6 auf 6.0) stecken oft komplette **Neuentwicklungen**.
  - Die Matrix der vom Hersteller unterstützten **Komponenten** vs. Version ist of sehr dünn besetzt.
  - Ersatz von Infrastruktur-Komponenten führt oft zu hohem **Aufwand**.
- Verfügbarkeit von Fachspezialisten
  - Verfügbarkeit von Fachpersonen mit **Domänen-Wissen** ist oft der Engpass-Faktur bei Rollen- und Prozess-Definitionen.
  - Sie werden **Anforderungsdefinition** und der **QS** benötigt.
  - Wartezeiten (auf Spezialisten) sind Aufwandstreiber.
- From scratch vs. Templates
  - Nur ein Teil der IAM-Prozesse ist wirklich **unternehmensspezifisch**.
  - Die **Übernahme** von Prozessen und / oder Rollen aus anderen Projekten oder generischen Modellen kann Projekte beschleunigen.



Gefordert – der Prozessbaukasten

Was ist dafür zu tun?

- Sammeln **implementierter** IAM-Prozesse
- Herausfaktorisieren von **Gemeinsamkeiten**.
  - unternehmensübergreifend
  - redundanzfrei
  - ggf. branchenspezifisch
- **Bereitstellen** für Interessenten
- Pflege und **Aktualisierung**
- Regelmäßige **Releases** (jährlich)
- **Kompatibel** zu gebräuchlichen Prozess-Definitionen (ITIL).
- „Moderat“ **Tool**-unterstützt.

➔ Die Zeit ist reif für einen rationalen Ansatz Prozessmodellierung.

GenericIAM

Welchen Nutzen haben wir davon?

- Anwender
  - Unternehmen mit eingeführten IAM-Prozessen haben überwiegend nur Teile der notwendigen Prozesse definiert und eingeführt.
  - Sie erhalten hier kostengünstig eine Möglichkeit, ihr Prozessmodell zu **optimieren** und zu vervollständigen.
- Integratoren
  - Integratoren und Systemanbieter können bereits umfangreiche und wirklichkeitsnahe Musterprozesse mitliefern.
  - Sie können ihren Kunden ermöglichen, die hohen **Modellierungskosten** vor der Implementierung zu **senken** und die Einführungszeit zu kürzen.
- Berater
  - Freiberufliche Berater können mit vorgefertigten **Baumustern** antreten.
  - Sofern der Systemanbieter sie nicht bereits implementiert mitliefert.
- Die Disziplin
  - wir tragen zur **Professionalisierung** der Disziplin des IAM bei.
  - Damit senken die Schwelle zur Einführung IAM-Systemen
- Mitwirkende
  - Die unmittelbar Mitwirkenden können sich als **Experten** profilieren.

Aufgaben

Was müssen wir dafür tun?

- Sammeln implementierter IAM-Prozesse
  - Sammeln einer möglichst große Anzahl von IAM-Prozessen.
  - Sie sollen im Unternehmen bereits projektiert und implementiert sein.
- Herausarbeiten von Gemeinsamkeiten
  - Daraus werden die sich wiederholenden Sequenzen heraus selektiert.
  - Die sie werden gegebenenfalls branchenspezifisch gruppiert.
- Weitergabe an Interessenten
  - Die Modelle werden gegen eine kostendeckende Gebühr veräußert.
- Pflege und Aktualisierung
  - Die mitwirkenden Unternehmen melden neue oder geänderte Prozesse an den Verantwortlichen für die Modelle – der sie einpflegt.
- Regelmäßige Releases
  - Die Gruppe veröffentlicht jährlich ein konsolidiertes generisches IAM-Prozessmodell (z.B.: GenericIAM2006 oder GenericIAM2007-banking).
- Dokumentation
  - Die Gruppe dokumentiert die Modelle, so dass sie kompatibel zu gebräuchlichen Prozess-Definitionen wie z.B. ITIL sind.
  - Sie gibt dabei frei zugänglichen Formaten den Vorzug.

Orientierung an Standards

Beispiel: Process Notation nach ITIL

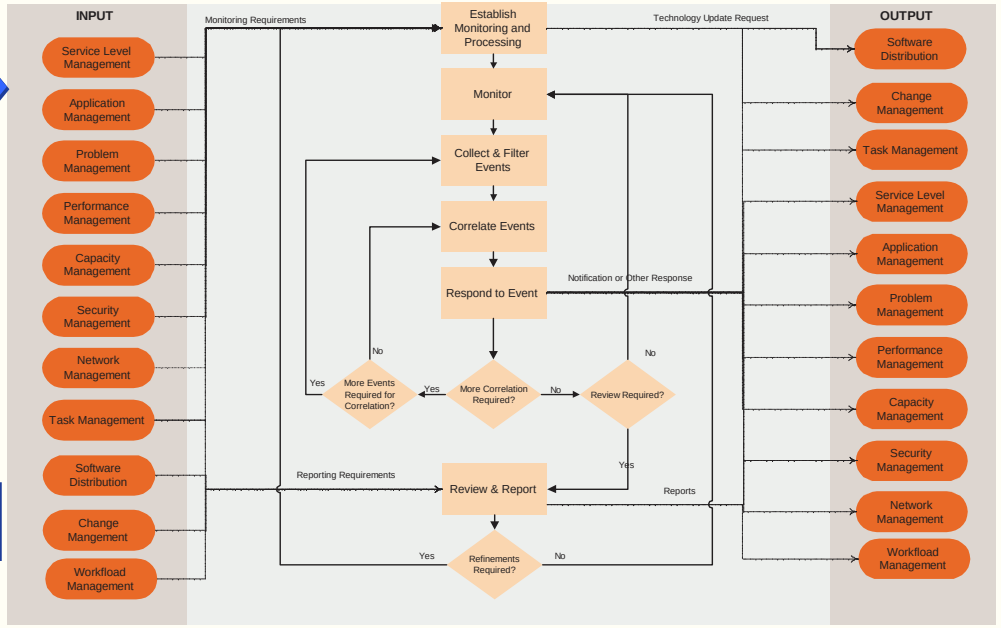
Level A – Process Vision

Incident Management
IM

1

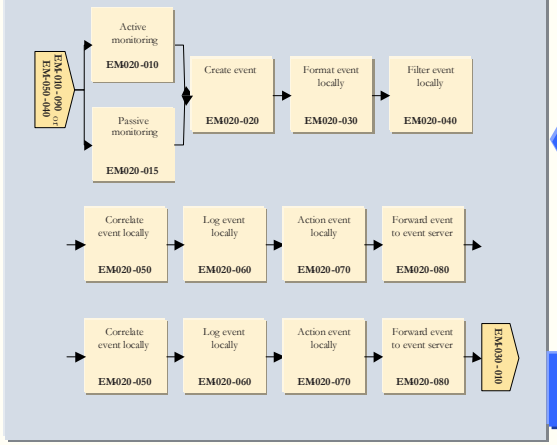
Level B - Process Steps

Event Management - Process and Data Flow Diagram



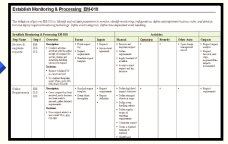
2

Level C - Subprocess Steps



3

Level D – Activities



4

Policies & Procedures

➔ Die ITIL Prozess-Notation wird weithin akzeptiert und verstanden.

Die Mitwirkenden

Welche Erfahrungen haben wir mit diesem Thema?

- Die Mitwirkenden präsentieren ihre Erfahrungen dem Gebiet des Identity Management.
- Dadurch soll klarer werden, was die Teilnehmer möglicherweise beisteuern können.
- Im Idealfall hält jeder von uns einen Teil eines Puzzels Hand.
- Durch Zusammensetzen fügen wir die Teile zu einem großen Bild.

Infrastruktur

Welche technischen Hilfsmittel wollen wir nutzen?

- Festlegen einer gemeinsam zu nutzenden Infrastruktur
  - ggf. müssen wir einen Evaluierungsauftrag an Freiwillige aus unserer Mitte vergeben.
- Ausrüstung, die das Team GenericIAM für seine Arbeit benötigt
  - Diskussionsforum,
  - Gemeinsamer Kalender,
  - Web-Seite,
  - Projektakte
  - Blog,
  - Wiki,
  - Modellierungswerkzeuge,
  - Plattform für audio- oder video-conferencing (Skype, Gizmo, GoogleTalk, ...),
  - ...

Zusammenarbeit

Wie wollen wir zusammen arbeiten?

- Rechtsform
  - BGB-Gesellschaft; Verein oder was?
  - ggf. NIFIS.org
- Organisation der Zusammenarbeit bis zum nächsten Meeting
- Bestimmen eines Termins für das nächste Meeting.

Offene Punkte

Welche Fragen müssen noch geklärt werden?

- Gliederung der IAM-Prozesslandschaft
  - Objektorientiert?
- Verkehrssprache, Dokumentationssprache?
- Qualitätskriterien
- Begriffsdefinitionen

Aufträge

Wer macht was bis wann?

- Ermitteln der Aufgaben, die wir uns als Gruppe bis zum nächsten Meeting stellen.
- Verteilen dieser Aufgaben auf die Teilnehmer

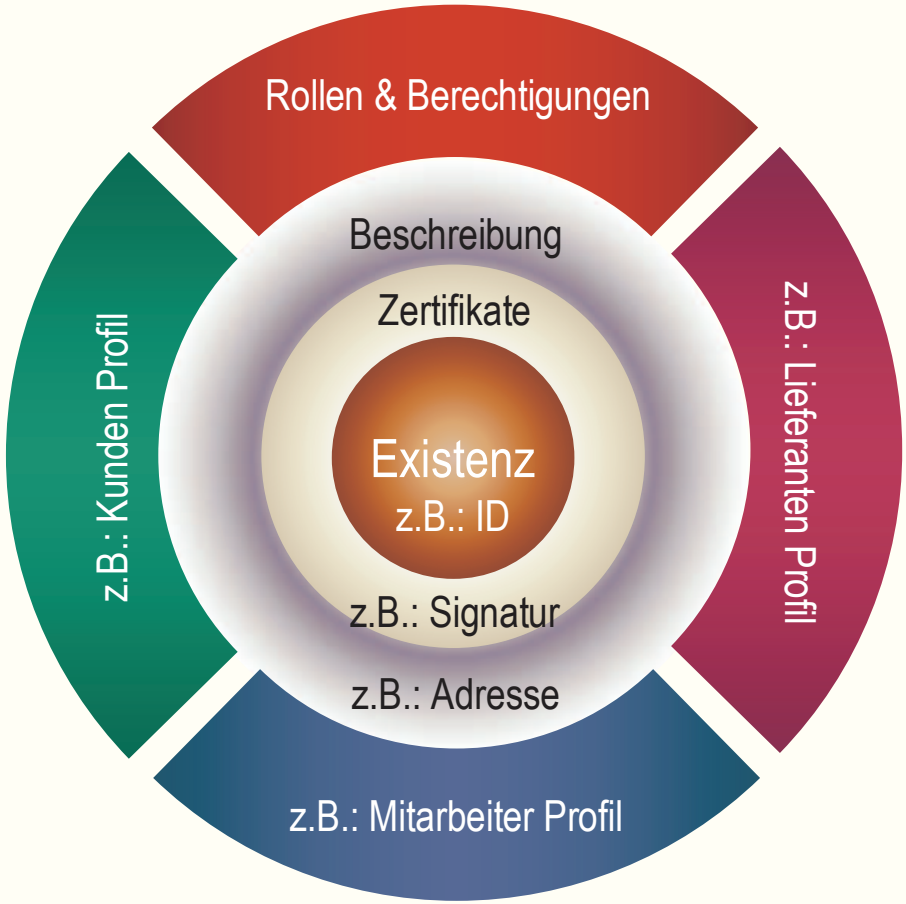
Fragen - Anmerkungen – Anregungen?

Achtung Anhang

Hier kommen die berüchtigten back-up-Folien ...

Grundlagen - die digitale Identität

Die digitale Identität lässt sich gut mit einem Schalenmodell beschreiben.



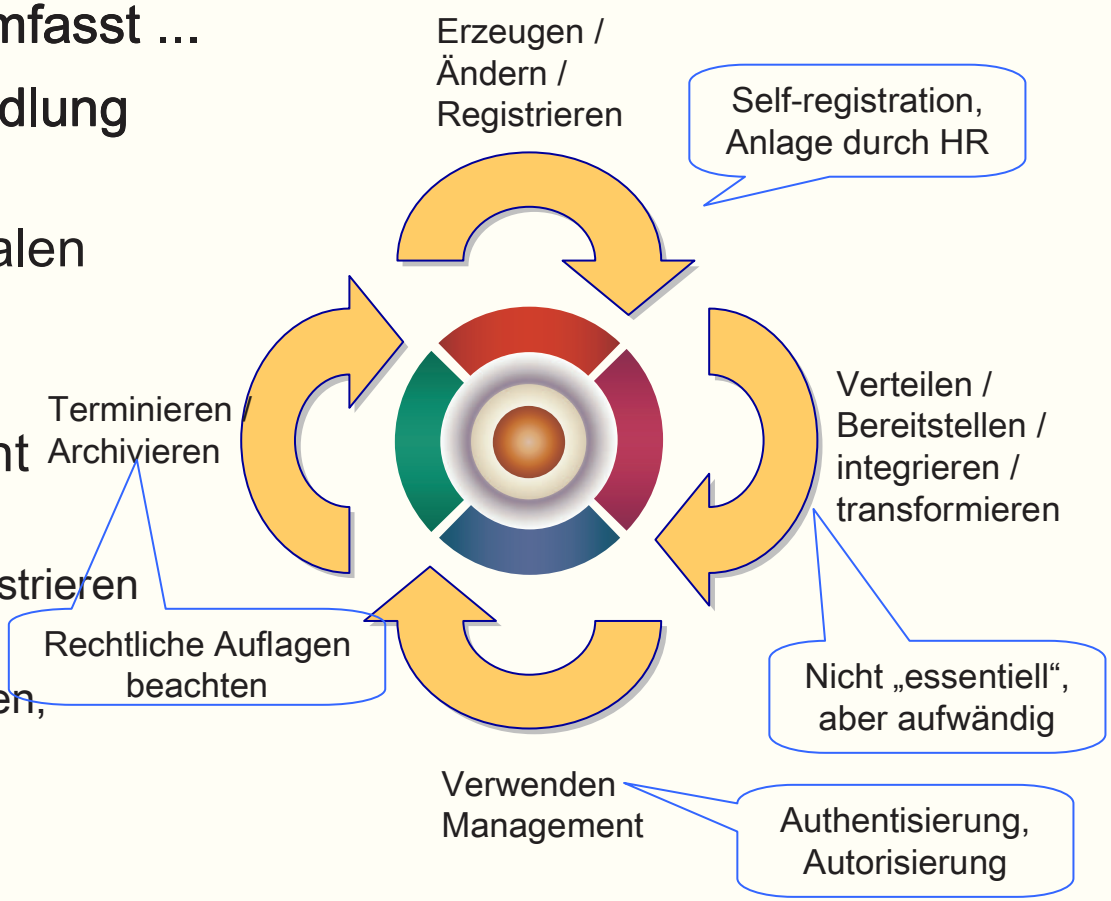
- Der Kern - **Existenz**:
  - eindeutige Identifikation.
  - “ID”, Name, Nummer
  - natürliche oder juristische Person, Anwendung oder Hardware.
  - Gleiche Gültigkeit wie Objekt
- Die erste Schale - **Zertifikate**:
  - Zertifikate,
  - unterschiedlich stark
  - Password bis qualifizierte digitale Signatur
- Die zweite Schale - **Beschreibung**:
  - Rollen-unabhängige gemeinsame Attribute
  - Adressinformationen
  - charakteristische Merkmale.
- Die dritte Schale - **Kontext**:
  - Rolle
  - Berechtigungen

Vergleichbar in analogen Welt mit einem Reisepass mit Visa für den Grenzübertritt

Lebenszyklus einer digitalen Identität

Das Identity Management umfasst ...

- Die ganzheitliche **Behandlung von digitalen Identitäten.**
- Die Prozesse einer digitalen Identität im **Laufe ihres Lebenszyklus.**
- Das Identity Management befasst sich mit dem ...
  1. Erzeugen / Ändern / Registrieren
  2. Verteilen / Bereitstellen / Integrieren / Transformieren,
  3. Verwendung und
  4. Terminieren / Archivieren

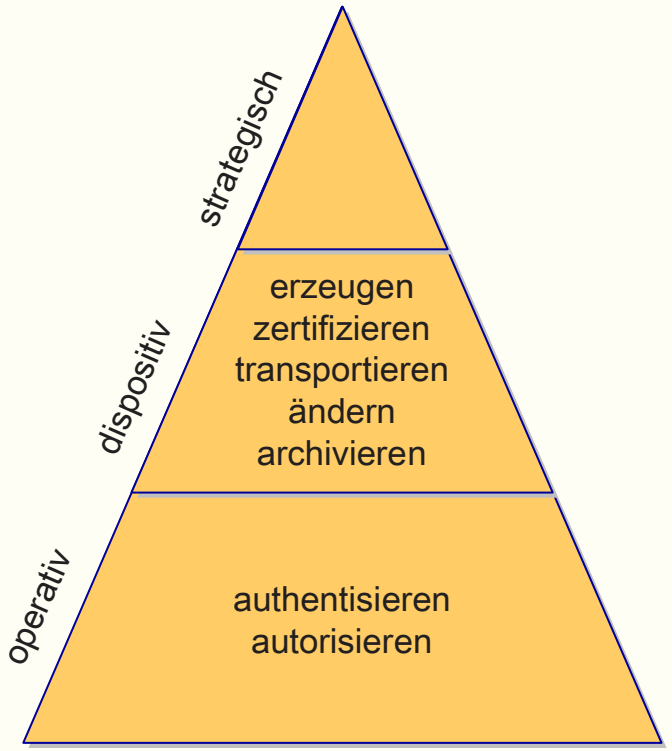


➔ Der Lebenszyklus liefert Anhaltspunkte für eine Klassifizierung.

Prozesse des Identity Management

Die Prozesse des Identity Management lassen sich gruppieren ...

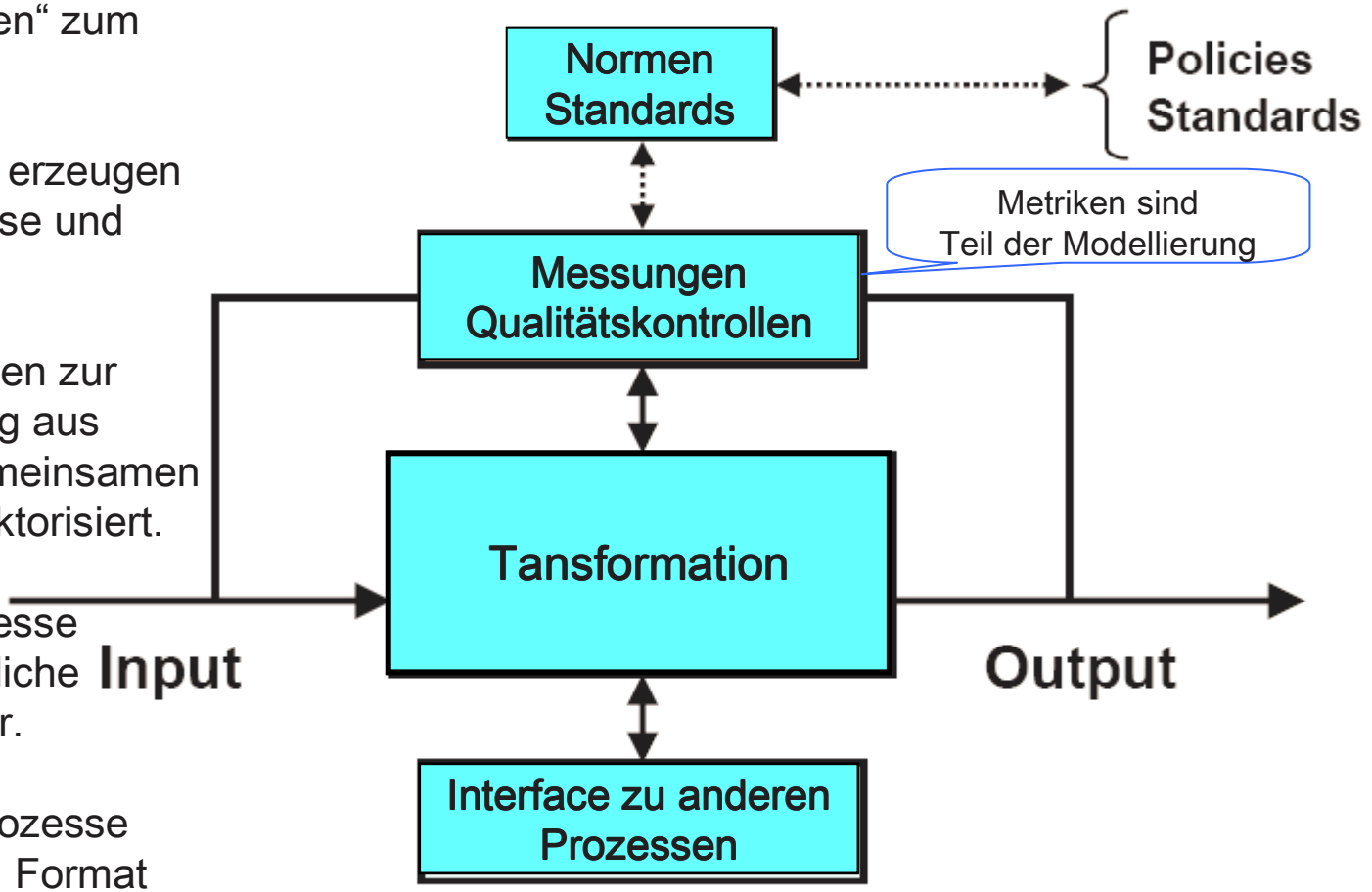
- Nach operativ und dispositiv
  - operativ: authentisieren und autorisieren
  - dispositiv: verwalten digitaler Identitäten
- Nach fachlich und physisch
  - fachlich: verwalten und verwenden
  - physisch: integrieren, transportieren, transformieren und publizieren
- Nach Existenz, Zertifikat und Kontext
  - anlegen, erfassen, ändern, löschen
  - zertifizieren, widerrufen
  - zuweisen, ändern, entfernen von Rollen und Berechtigungen



➔ Jede Klassifizierung hat ihren besonderen Wert.

Was ist ein Prozess?

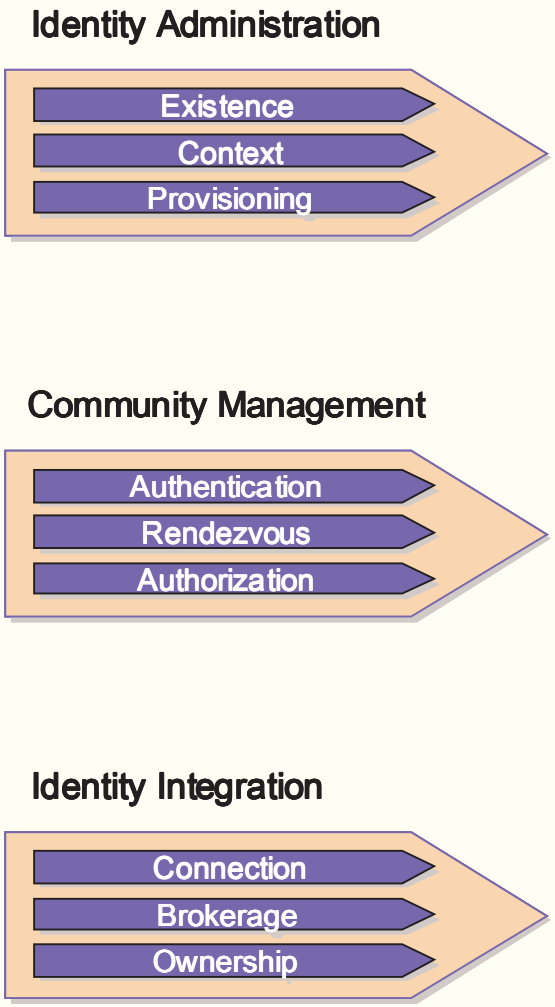
- **Fundamentale** Prozesse laufen vom „Kunden“ zum „Kunden“
- **Support**-Prozesse erzeugen Zwischenergebnisse und speichern sie.
- **Teilprozesse** werden zur Wiederverwendung aus Prozessen mit gemeinsamen anteilen heraus faktorisiert.
- „**Essentielle**“ Prozesse nehmen eine fachliche Transformation vor.
- „**Physikalische**“ Prozesse verändern nur Ort, Format oder Sprache.



➔ Startpunkt der Modellierung sind fundamentale, essentielle Prozesse.

Gruppen von Identity Management Prozessen

Gruppierung obersten Ebene



- Identity Administration – *die dispositive Ebene*
  - Verwalten von digitalen Personenidentitäten, ihren Beziehungen zur Organisationseinheit und die Zuweisung von Ressourcen.
- Community Management – *die operative Ebene*
  - Authentisierung, Bereitstellen / Publizieren und Autorisierung von Personen gemäß ihren digitalen Personenidentitäten.
- Identity Integration – *die übergreifende Aufgabe*
  - Mechanismen für die Aktualisierung und Synchronisation von digitalen Personenidentitäten, die verteilt und teilweise redundant gehalten werden.

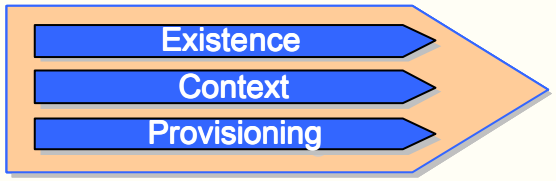
Quelle: Microsoft

➔ Die bisher umfassendste Definition stammt von Microsoft.

Identity Administration

Gruppierung Ebene 2

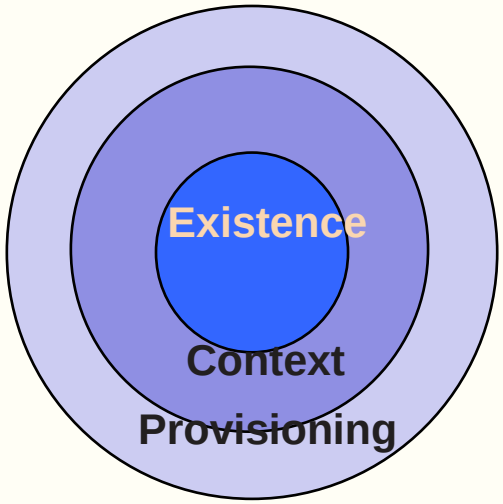
Identity Administration



Verwalten von digitalen Personenidentitäten, ihren Beziehungen zur Organisationseinheit und die Zuweisung von Ressourcen.

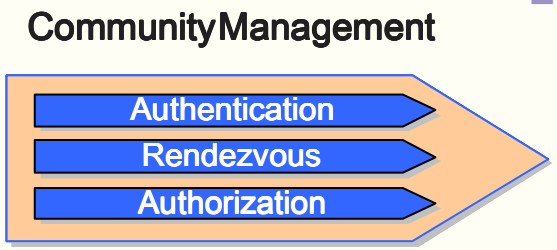
- **Existence**
  - Erzeugen, Verwalten, Synchronisieren von digitalen Personen-Identitäten.
- **Context**
  - Verwalten der Beziehungen von Personen zur Organisation (Rollen) und ihren Ressourcen (Rechte).
- **Provisioning**
  - Versorgen von Personen mit den ihrer Rolle entsprechenden Ressourcen und einbringen der Zugriffsrechte in die Zielsysteme, die die Ressourcenzugriffe steuern.

Identity Administration



Community Management

Gruppierung Ebene 2



Authentisierung, von Personen gemäß ihren digitalen Personenidentitäten und Bereitstellen / Publizieren Autorisierung.

- **Authentication**
  - Authentisierung, ist der Prozess der Verifikation der Identität anhand von Zertifikaten im allgemeinen Sinne.
- **Authorisation**
  - Autorisierung ist der Prozess, Personen gemäß ihrer digitalen Personenidentität (*Existence*) und der über ihre Rolle im Unternehmen definierten Zugriffsrechte (*Context*) den Zugriff auf Ressourcen zu gestatten oder zu verweigern.
- **Rendezvous**
  - Zusammenstellen und **Publizieren** von Adressbüchern, Verzeichnissen, Kalenderfunktionen für Terminvereinbarungen, Online-Meetings und gemeinsamer Ressourcennutzung.

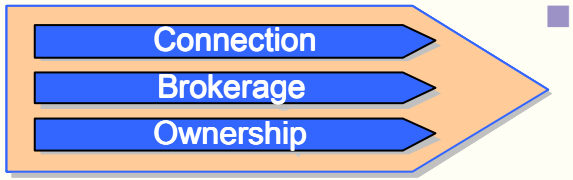
Identity Integration (Evidenz)

Gruppierung Ebene 2

Zusammenführung, Aktualisierung und Synchronisation von digitalen Personenidentitäten und Berechtigungen, die verteilt und teilweise redundant gehalten werden.

- **Connection**
  - Mechanismen, die Eigenschaften von Verteilung und Heterogenität überwinden helfen. Technisch sind das **Konnektoren** zum Zugriff auf Standard Verzeichnisse (z.B. LADP, DAP, ANS-SQL) oder Nicht-Standard-Verzeichnisse.
- **Brokerage**
  - Mechanismen, die es gestatten Attribute unterschiedlicher Informationsobjekte **aufeinander abzubilden**. Technisch realisiert z.B. über Regelmaschinen, die auf einem Satz definierter Abbildungsregeln operieren.
- **Ownership**
  - Mechanismen, die bei redundant gespeicherten Informationsobjekten festlegen (und überwachen), in welcher (autoritativen) Quelle bestimmte Attribute führen geändert werden dürfen.

Identity Integration



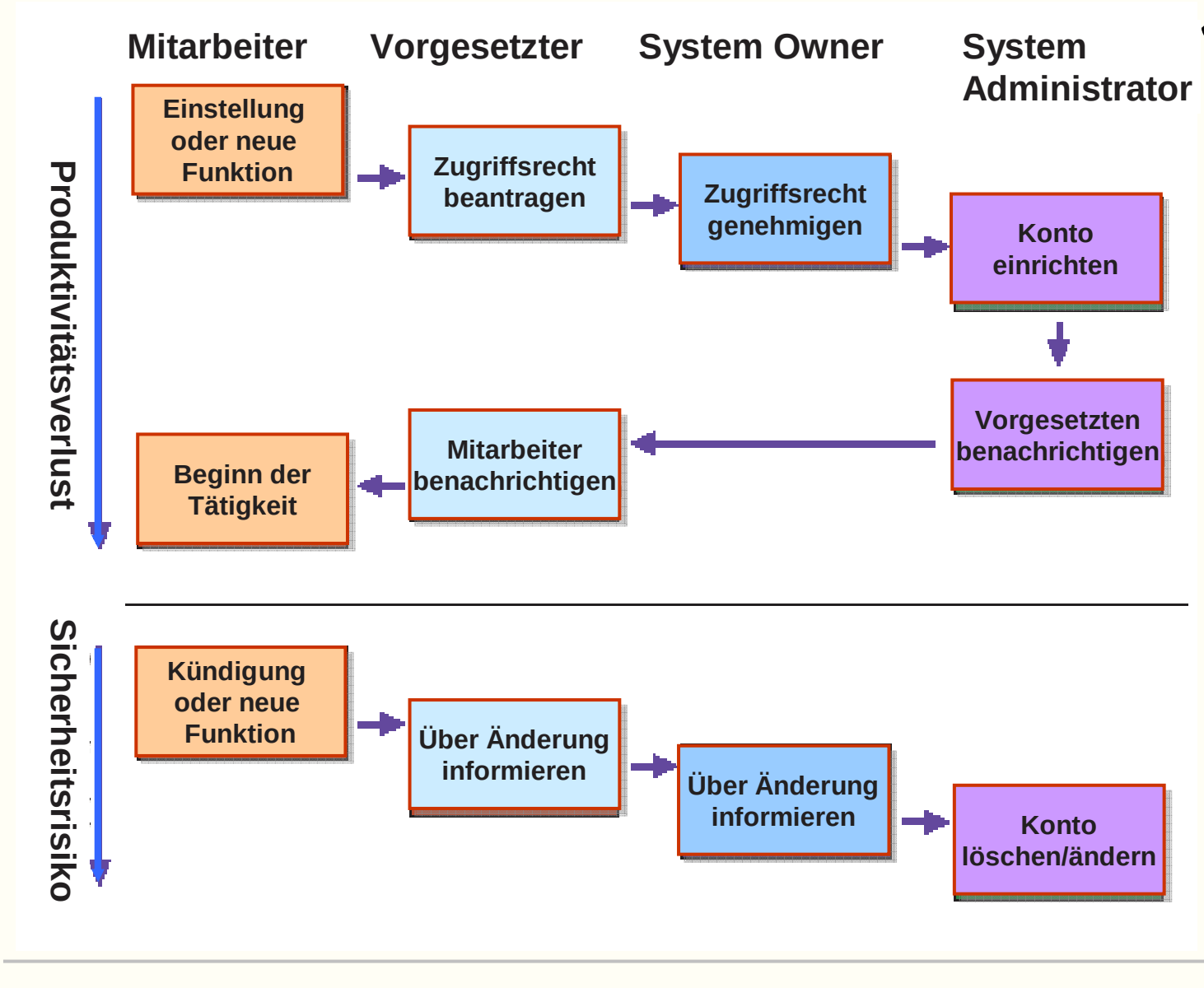
Ressource Provisioning Prozesse

Gruppierung Ebene 3

- Provisioning …
  - **Versorgung** mit Ressourcen
  - die automatisierte **Zuweisung** von Berechtigungen zur Systemnutzung.
  - **Änderung** der Geschäftsrolle (Beförderungen, Abteilungswechsel) und Ausscheiden eines Mitarbeiters.
- De-Provisioning ...
  - Unterstützung der Änderung und des Entziehens von Ressourcen.
  - Aus Sicherheitsgründen wichtiger als das Provisioning.
- Begleitende **Prüfprozesse**:
  - Abgleich der tatsächlichen Zugriffsrechte in den Systemen (Ist) mit den vergebenen Rechten (Soll) überein?
- **Manuelle** Beantragung und Vergabe von Einzelrechten ...
  - Die Rechtestruktur eines Unternehmens lässt sich mit vertretbarem Aufwand nicht vollständig über ein Rollenmodell abbilden.
- Die **semiautomatische Versorgung** von Systemen,
  - für es nicht möglich ist oder sich nicht lohnt, Konnektoren zu erwerben oder zu erstellen.

Liste der Prozesse

Provisioning - Produktivität und Sicherheit



Liste Provisioning-Prozesse

- **Anwender** (Existence)
  - Hinzufügen eines Anwenders
  - Entfernen eines Anwenders
  - Ändern eines Anwenders (Name, Abteilung, Vertragsende)
- **Rolle** (Context)
  - Hinzufügen einer Rolle (und Zuweisen der damit verbundenen Rechte, auch über „Klonen“ oder über Vorlagen / Templates)
  - Entfernen einer Rolle (auf die keine Referenz mehr existiert)
  - Ändern einer Rolle.
  - Prüfen auf Konfliktfreiheit
- **Konto** (Context)
  - Vergeben individueller Rechte,
  - Entziehen individueller Rechte,
  - Zuordnen zu einer Rolle
  - Lösen von einer Rolle
  - Konten unwirksam werden lassen (Ausscheidedatum erreicht)
  - Wiederinkraftsetzen abgelaufener Konten (Ausscheidedatum erreicht) Passwort setzen (Initial-Passwort und Neuvergabe)
- **Regel** (Context)
  - Hinzufügen einer Regel
  - Entfernen einer Regel
  - Ändern einer Regel
- **Genehmigungsstellen** (Provisioning)
  - Hinzufügen einer Freigabeautorität (mit Vertretungsregelung),
  - Entfernen einer Freigabeautorität,
  - Ändern einer Freigabeautorität,
- **Information** (Provisioning)
  - Information des Anwenders über eigene Zugriffsberechtigungen
  - Information des Verantwortlichen über die Zugriffsberechtigungen Dritter
  - Information des Anwenders über den Status eines Antrages auf Rechtevergabe,
- **Abgleich** (Provisioning)
  - Feststellen von Abweichungen der Rechte in den Zielsystemen vom Sollzustand (Hacker, Prozessmängel, Managementfehler, …)
- **Bericht** (Provisioning)
  - Berichten der Rechtestruktur pro System oder Organisationseinheit,

Aktueller Status

- Approve customer
- Bulk Portal Provisioning
- Chain Identities
- Change Password and pass phrase
- Complete and check user data of partner users
- Create organization
- Create user manually
- Customer Self Registration
- Delegated Privileges assignment/removal
- Deliver initial credentials
- Deliver Password HQ Employee Users
- Deliver Password of Partner Master Users
- Delivery Password in bulk initially
- Escalate issue
- Forgotten Password Service
- Initial Login
- Load from Partner Master
- Load User from HR
- Lock Organization manually
- Lock User automatically
- Lock User manually
- Logout
- Mainframe Password Synchr
- Modify Organization
- Modify User ..

- Eigene Erfahrungen ...
  - ~ 180 Prozesse
  - Von 4 Großunternehmen
  - Aus Banking, Transport und Automotive
- Erfahrungsschatz von Kuppinger Cole & Partner.
- Mitwirkungsbereitschaft bei aktuellen und ehemaligen Kunden.
- Organisatorisches Framework ...
  - IAM Process Manifest
  - Mitwirkungsvereinbarung
  - Kommunikationsforum
  - Quartalsweise Peer-Meetings
  - Jährliche Modell-Releases
  - Freier Bezug für mitwirkende Unternehmen

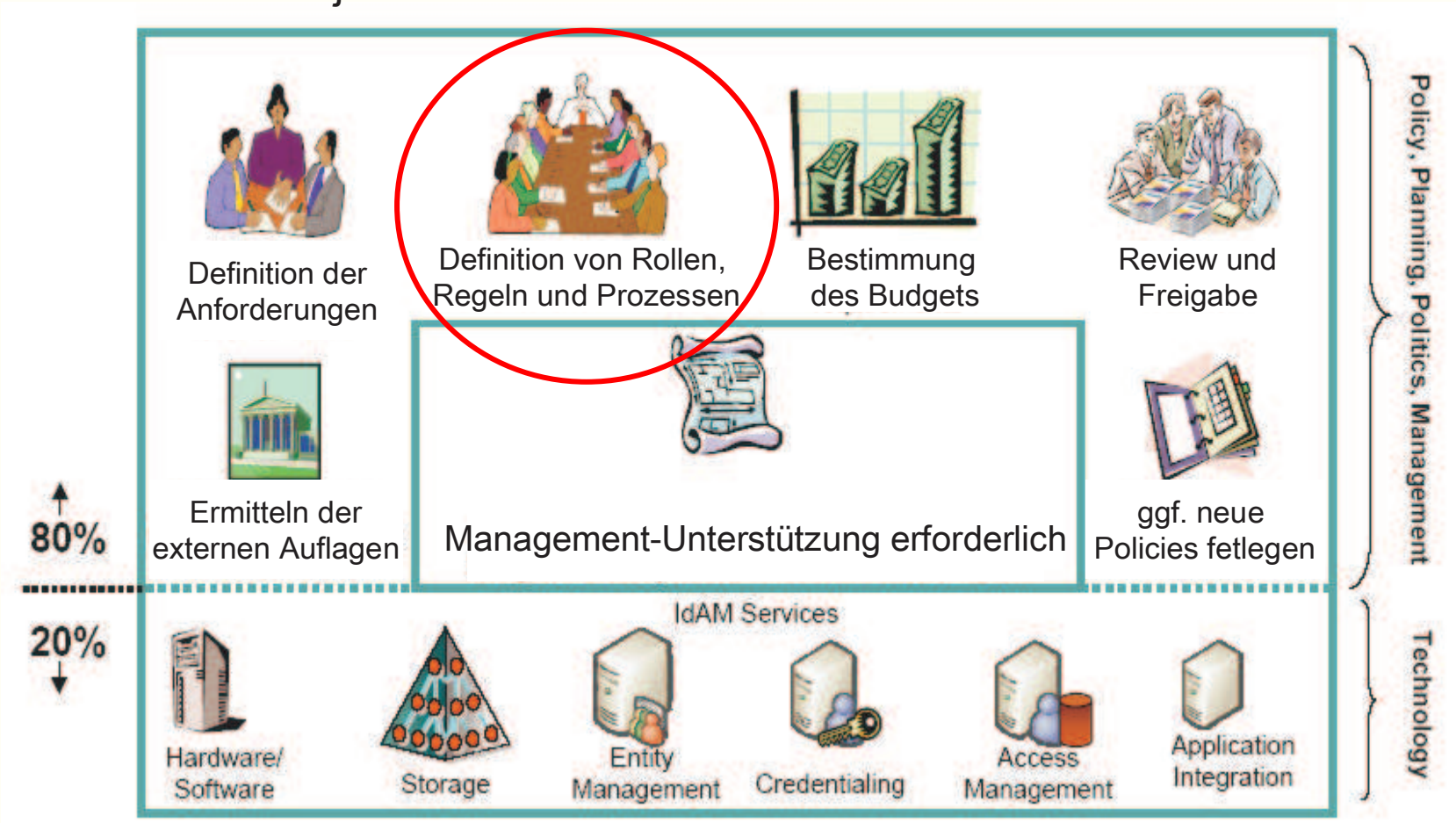
➔ Wir müssen nicht bei „Null“ beginnen.

Kandidaten für Generische Prozesse

- Beantragen von Systemberechtigungen
- Beantragen der Zuweisung von Rollen
- Vergeben von Berechtigungen an neue Mitarbeiter
- Verwalten von Richtlinien (policies)
- Entziehen von Berechtigungen ausscheidender Mitarbeiter
- Sperren von Benutzern (sofort, zum Termin)
- Ändern von Rechten bei Mitarbeiterübergängen
- Wiedereintreten in Konzernstrukturen
- Rollenbasiertes Vergeben von Berechtigungen
- ...

Prozesse sind aufwändig ...

- 80% des Aufwandes gehen in die Definition von Prozessen, Policies, Rollen, Regeln und deren QA.
- 20 % des Projektaufwandes verursacht die Technik.



Quelle: Booz, Allen & Hamilton