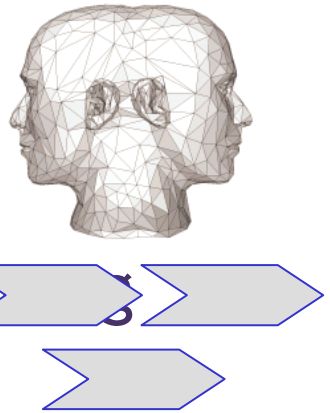
Checkliste für die erfolgreiche IM-Umset[illegible]



Dr. Horst Walther,
Leiter des Expertenforums Identity Management der
Nationalen Initiative für Informations- und Internet-Sicherheit (NIFIS), Deutschland

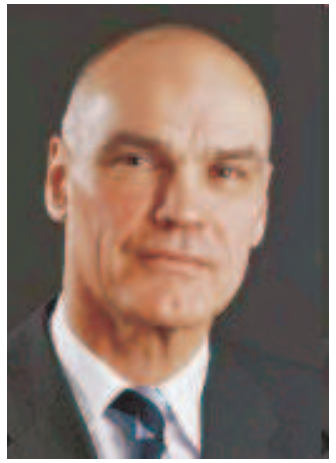
Landesinitiative »secure-it.nrw« und Nationale Initiative für Informations- und Internet-Sicherheit (NIFIS e.V.),
Haus der Technik e.V., Hollestr. 1, 45127 Essen

Version 0.97

Synopse

16:25 - 16:55

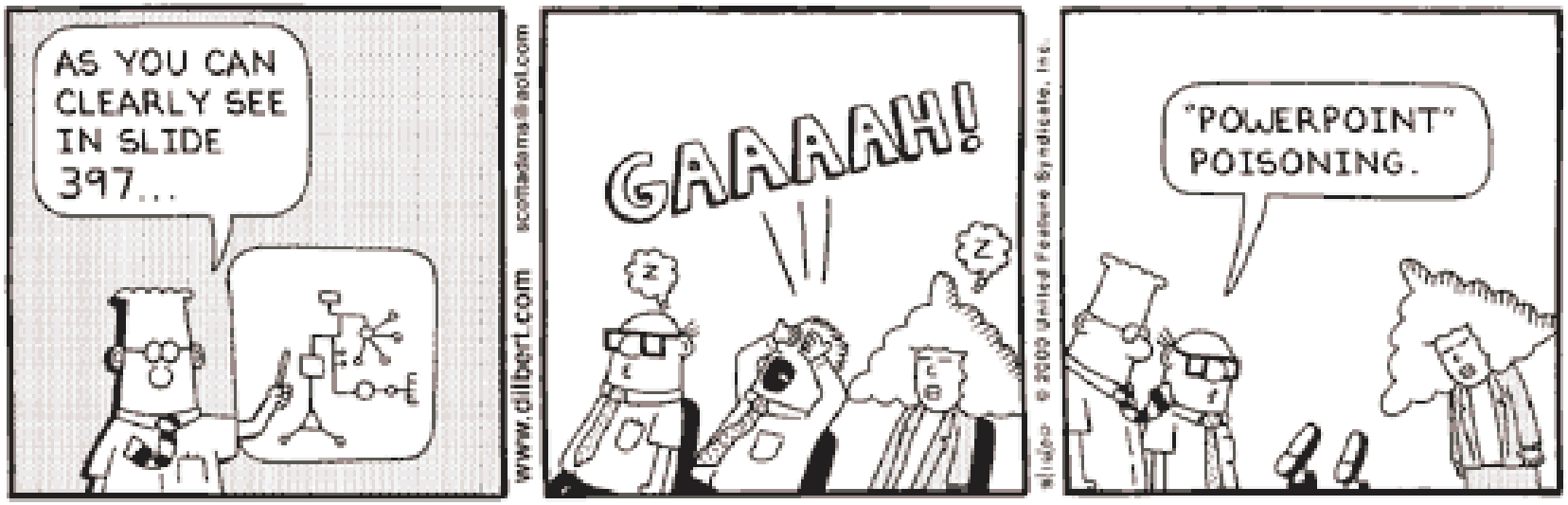
Checkliste für die erfolgreiche IDM-Umsetzung



Dr. Horst Walther

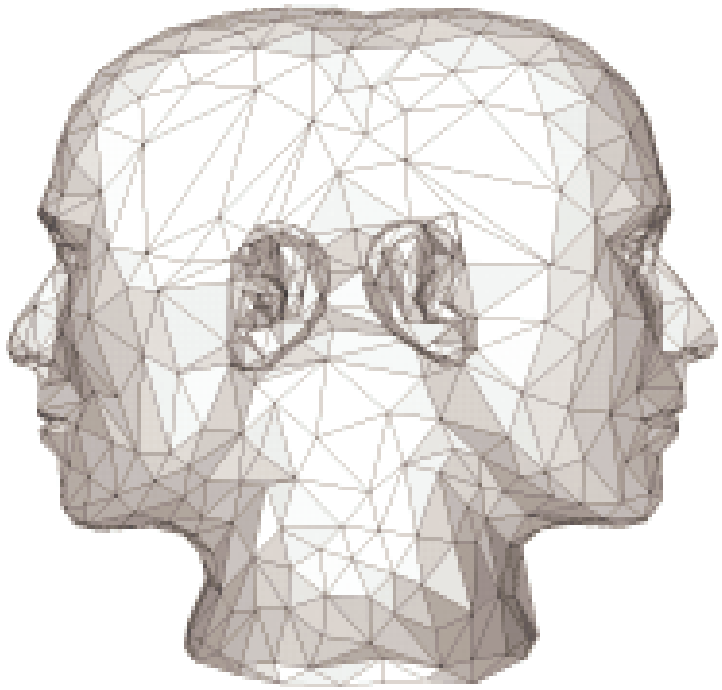
- Oft hilft schon Fehlervermeidung
  Warum IAM-Projekte scheitern & Massnahmen dagegen.
- Expertenrat
  Was wir aus bisherigen Projekten gelernt haben

Ernste Warnung
Stoppen Sie mich – bevor es zu spät ist.



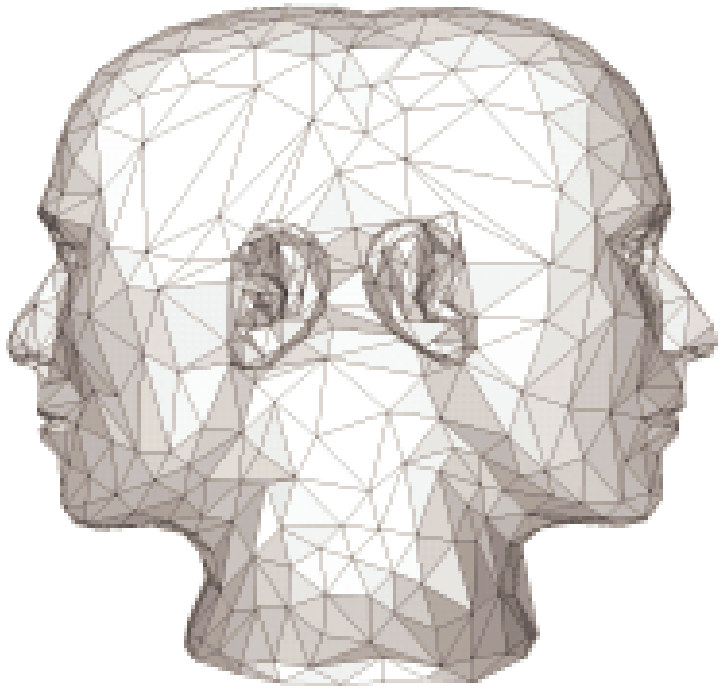
- Akute Powerpoint-Vergiftung ist eine weit verbreitete aber weithin unbekannte Zivilisationskrankheit.
- Sie tritt besonders bei ehrgeizigen Führungskräften und den durch sie Geführten auf.
- Sie ist durch eine Therapie aus frischer Luft, Sonne, absoluter Ruhe und einem Gläschen Wein leicht heilbar.

Definition
Identity- & Access Management – Was ist das?



- **Identity Management** (IdM) ist die ganzheitliche Behundlung digitaler Identitäten.
- **Identity & Access Management** (IAM) schließt auch die Verwaltung von Zugriffsrechten ein.
- Die Aufgaben des IAM sind **nicht neu** – sie sind seit Anbeginn mit den betrieblichen Abläufen fest verbunden.
- Neu ist die **übergreifende** Betrachtung …
  - Der einzelnen Disziplinen und
  - Über das gesamte Unternehmen hinweg
- IAM ist eine **Infrastrukturaufgabe** mit …
  - Einer **fachlich** organisatorischen Komponente
  - Einer **technischen** Komponente und
- Dafür gibt es im klassischen Unternehmens-aufbau keine definierte **„Ownership“**

Identity Management
hat ein fachliches und ein technisches Gesicht.



- **Identity Management** (IdM) ist die ganzheitliche Behundlung digitaler Identitäten.
- **Identity & Access Management** (IAM) schließt auch die Verwaltung von Zugriffsrechten ein.
- Die Aufgaben des IAM sind **nicht neu** – sie sind seit Anbeginn mit den betrieblichen Abläufen fest verbunden.
- Neu ist die **übergreifende** Betrachtung …
  - Der einzelnen Disziplinen und
  - Über das gesamte Unternehmen hinweg

- IAM ist eine **Infrastrukturaufgabe** mit …
  - einer **fachlich** organisatorischen Komponente
  - einer **technischen** Komponente und

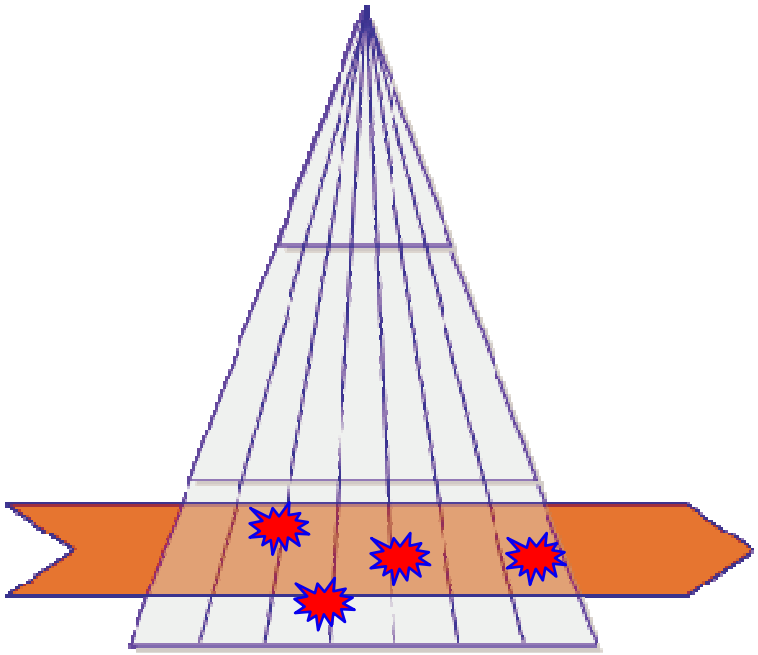
Oft hilft schon Fehlervermeidung

Warum IAM-Projekte scheitern & Massnahmen dagegen.

- **Querschnittscharakter**
  IAM-Projekte berühren eine Vielzahl von Unternehmensfunktionen
- **Ungleiche Prozessreife**
  keine Inseln der Ordnung in einem Meer an Chaos
- **Falscher Projektzuschnitt**
  Im Implementierungsprojekt nicht das Unternehmen organisieren.
- **Folgen der Marktkonsolidierung**
  zusammengekaufte Suiten passen nicht immer zusammen
- **Nicht-Verfügbarkeit von Fachspezialisten**
  Personen mit business domain Wissen sind rare Wesen
- **Zu hohe Fertigungstiefe**
  Nicht immer das Rad neu erfinden
- **Immer noch technische Risiken**
  Technik ist oft mehr Marketing als Realität

Querschnittscharakter

IAM-Projekte berühren eine Vielzahl von Unternehmensfunktionen



Komplexitätsfaktoren

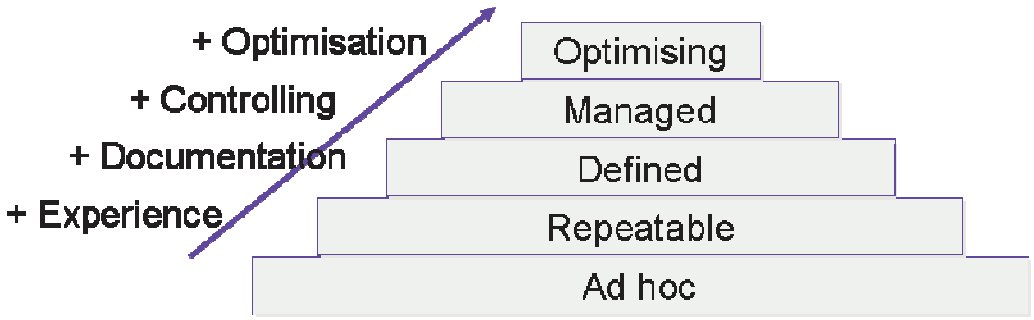
- Identity-Management Prozesse sind typischerweise **bereichsübergreifend**.
- Es sind **viele** gleichberechtigte **Stakeholder** in ein Projekt involviert.
- 3 bis 5 mal höhere **Kommunikationskomplexität** zu „normalen“ IT-Projekten.
- Typischer **Change** Management Prozess

Maßnahmen

- Projektmanagement stärken!
- Kommunikationszuschlag einplanen!
- Auf Macht-Sponsor bestehen!

Ungleiche Prozessreife

keine Inseln der Ordnung in einem Meer an Chaos



Komplexitätsfaktoren

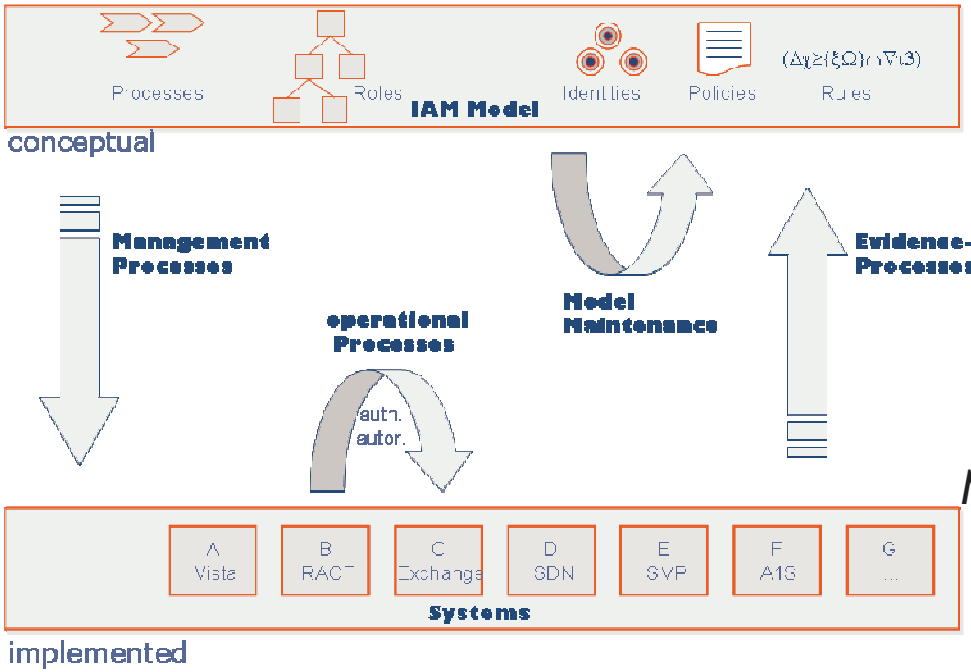
- Je höher die **Reife** der Management-Prozesse (z.B. nach CMMi) umso leichter fällt die Einführung von IAM- Prozessen, -Regeln, -Rollen, -Policies.
- in einem **unreifen Prozess-Umfeld** sind keine reifen IAM-Prozesse implementierbar.
- Die top-down-Definition von Rollen benötigt Prozessdefinitionen.

Maßnahmen

- Nur IAM-Vorhaben umsetzen, die der Prozessreife der Umgebung angepasst sind.
- Auch einmal „nein“ sagen!

Falscher Projektzuschnitt

Im Implementierungsprojekt nicht das Unternehmen organisieren.



Komplexitätsfaktoren

- Implementierungsprojekte sind **überfordert**, wenn sie die organisatorischen Voraussetzungen erst schaffen müssen
- Prozess- und Rollen-Definitionen erfordern eigene **Definitionsprojekte** vor der oder parallel zur Implementierung.

Maßnahmen

- Für die Prozess- und Rollen-Definition eigene Projekte vor der oder parallel zur Implementierung aufsetzen.

Folgen der Marktkonsolidierung
zusammengekaufte Suiten passen nicht immer zusammen

Komplexitätsfaktoren

- Mergers & Acquisitions führen oft zu wenig kompatiblen **Produktsammlungen**.
- Die Software übernommener Unternehmen wird häufig nicht mehr optimal **unterstützt**.
- Es **dauert lange**, bis zusammen gewachsen ist, was zusammen passen sollte.

Maßnahmen

- Erst eine Pilotinstallation unter realen Bedingungen über eine Softwareauswahl entscheiden lassen.

Nicht-Verfügbarkeit von Fachspezialisten

Personen mit business domain Wissen sind rare Wesen

Komplexitätsfaktoren

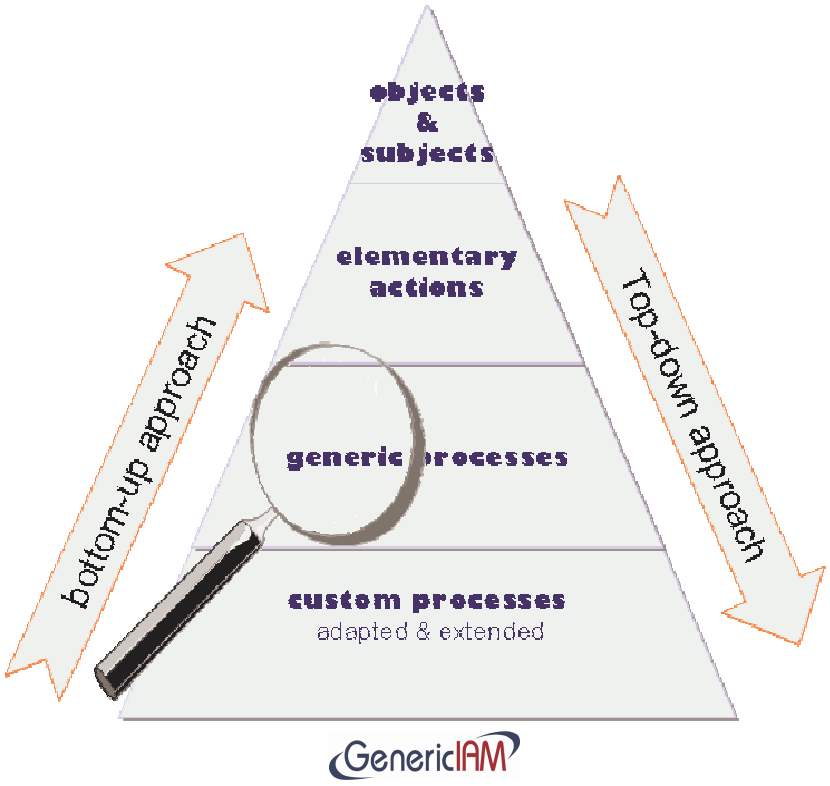
- Verfügbarkeit von Fachpersonen mit **Domänen-Wissen** ist oft der Engpass-Faktor bei Rollen- und Prozess-Definitionen.
- Sie werden in der **Anforderungsdefinition** und der **QS** benötigt.
- Wartezeiten (auf Spezialisten) sind Aufwandstreiber.
- In Projekten neigen sie zum Verschwinden.

Maßnahmen

- Die Projektverantwortung in die Fachabteilung legen.
- Projekte ggf. in fachliche und Implementierungsprojekte teilen.

Zu hohe Fertigungstiefe

Nicht immer das Rad neu erfinden



Komplexitätsfaktoren

- Nur ein Teil der IAM-Prozesse ist wirklich unternehmens-spezifisch.
- Die **Übernahme** von Prozessen und / oder Rollen aus generischen Modellen kann Projekte beschleunigen.
- Immer wieder mit einem weißen Blatt Papier zu beginnen überfordert die Projekte.

Maßnahmen

- Integratoren und Berater nach konsolidierten Erfahrungs-modellen fragen.
- An Standardisierungsinitiativen teilnehmen.

Immer noch technische Risiken
Technik ist oft mehr Marketing als Realität

Komplexitätsfaktoren

- IAM-SW-Suiten sind **komplex** und schwer zu handhaben.
- Ohne **Implementierungserfahrung** in exakt der geforderten Umgebung sind Projektrisiken nicht kalkulierbar.
- Hinter „harmlosen“ Versions-sprüngen stecken oft komplette **Neuentwicklungen**.
- Die Matrix der vom Hersteller unterstützten **Komponenten** vs. Version ist oft dünn besetzt.
- Ersatz von Infrastruktur-Komponenten führt oft zu hohem **Aufwand**.

Maßnahmen

- Ausgewählte Software immer erst im Pilotbetrieb testen.
- Integratoren mit echter Produkterfahrung wählen.

Expertenrat

Was wir aus bisherigen Projekten gelernt haben

Verantwortung
Wer sollte im Unternehmen für Identity Management zuständig sein?

Einführung Tiefe vs. Breite
Welches Vorgehen verspricht den höchsten Nutzen?

Zentral vs. Lokal
IDs & Rollen haben zentralen, Berechtigungen lokalen Charakter.

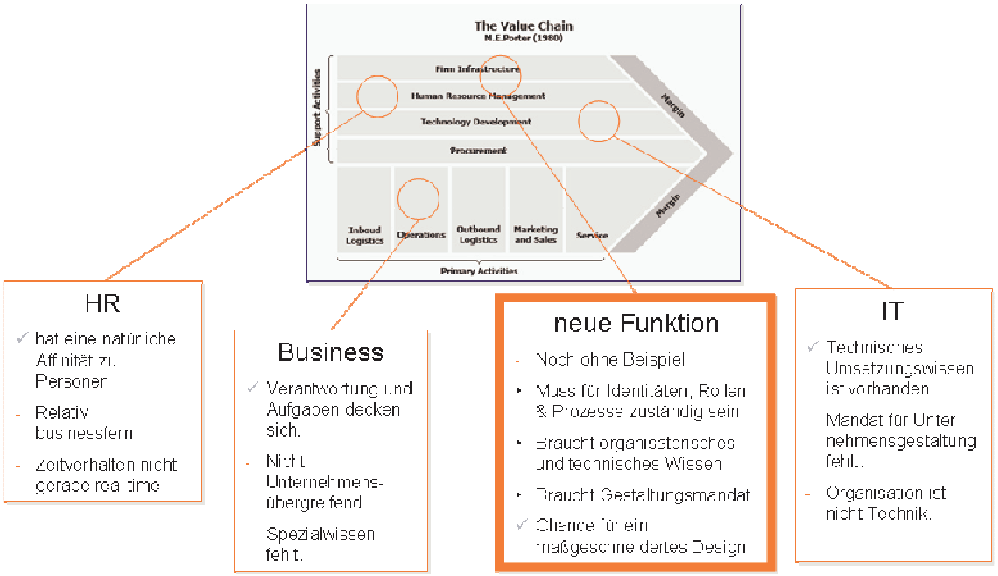
Wo sich der Einsatz von Rollen lohnt
Optimale Ergebnisse bei einer hohen Zahl von Jobs niedriger Komplexität

Rollen oder Rechte?
Was soll provisioniert werden?

Principle of least Berechtigung (PoLP)
risikobasierte Entscheidungen sind erforderlich

Vision: Auslagerung der Autorisierung
Bei Neuentwicklungen authorisation as a Service definieren.

Falsche Zuständigkeiten
Unternehmensorganisation braucht Business Owner



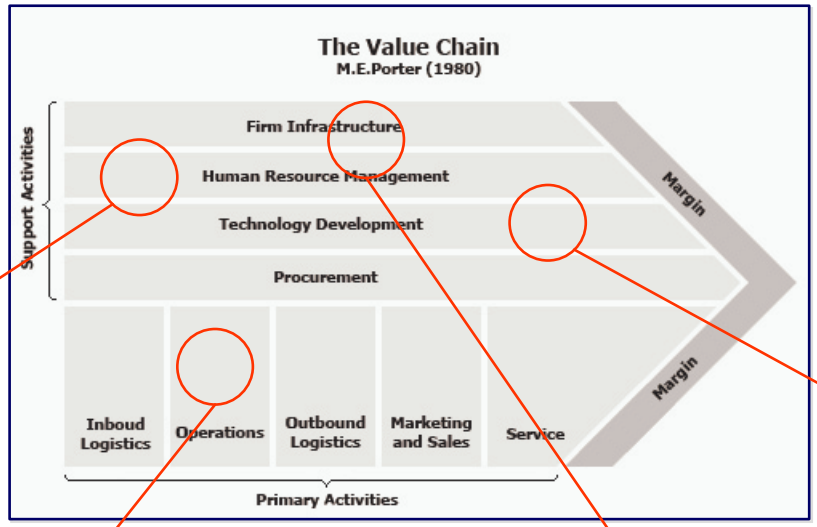
Komplexitätsfaktoren

- Identity Management ist eine fachliche Aufgabe.
- Identity Management ist pure Unternehmensorganisation.
- HR könnte sich dem annehmen – will es aber meistens nicht.
- Die IT kann es umsetzen hat aber nicht das Organisationsmandat.
- Dem Fachbereich fehlen methodisches und technisches Wissen.

Maßnahmen

- Die Verantwortung unternehmensuebergreifend definieren.
- Eine interdisziplinär arbeitende neue Funktion schaffen.

Verantwortung
Wer sollte im Unternehmen für Identity Management zuständig sein?



HR

- ✓ hat eine natürliche Affinität zu Personen
- \- Relativ businessfern
- \- Zeitverhalten nicht gerade real time.

Business

- ✓ Verantwortung und Aufgaben decken sich.
- \- Nicht Unternehmens-übergreifend
- \- Spezialwissen fehlt.

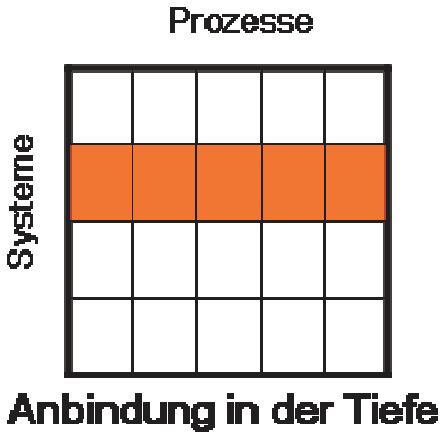
neue Funktion

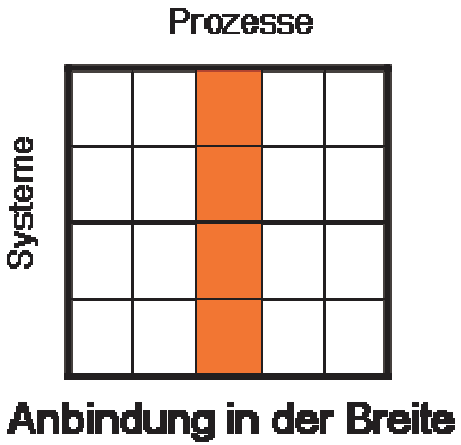
- \- Noch ohne Beispiel
- • Muss für Identitäten, Rollen & Prozesse zuständig sein
- • Braucht organisatorisches und technisches Wissen
- • Braucht Gestaltungsmandat
- ✓ Chance für ein maßgeschneidertes Design

IT

- ✓ Technisches Umsetzungswissen ist vorhanden
- \- Mandat für Unter-nehmensgestaltung fehlt.
- \- Organisation ist nicht Technik.

Einführung Tiefe vs. Breite
Welches Vorgehen verspricht den höchsten Nutzen?



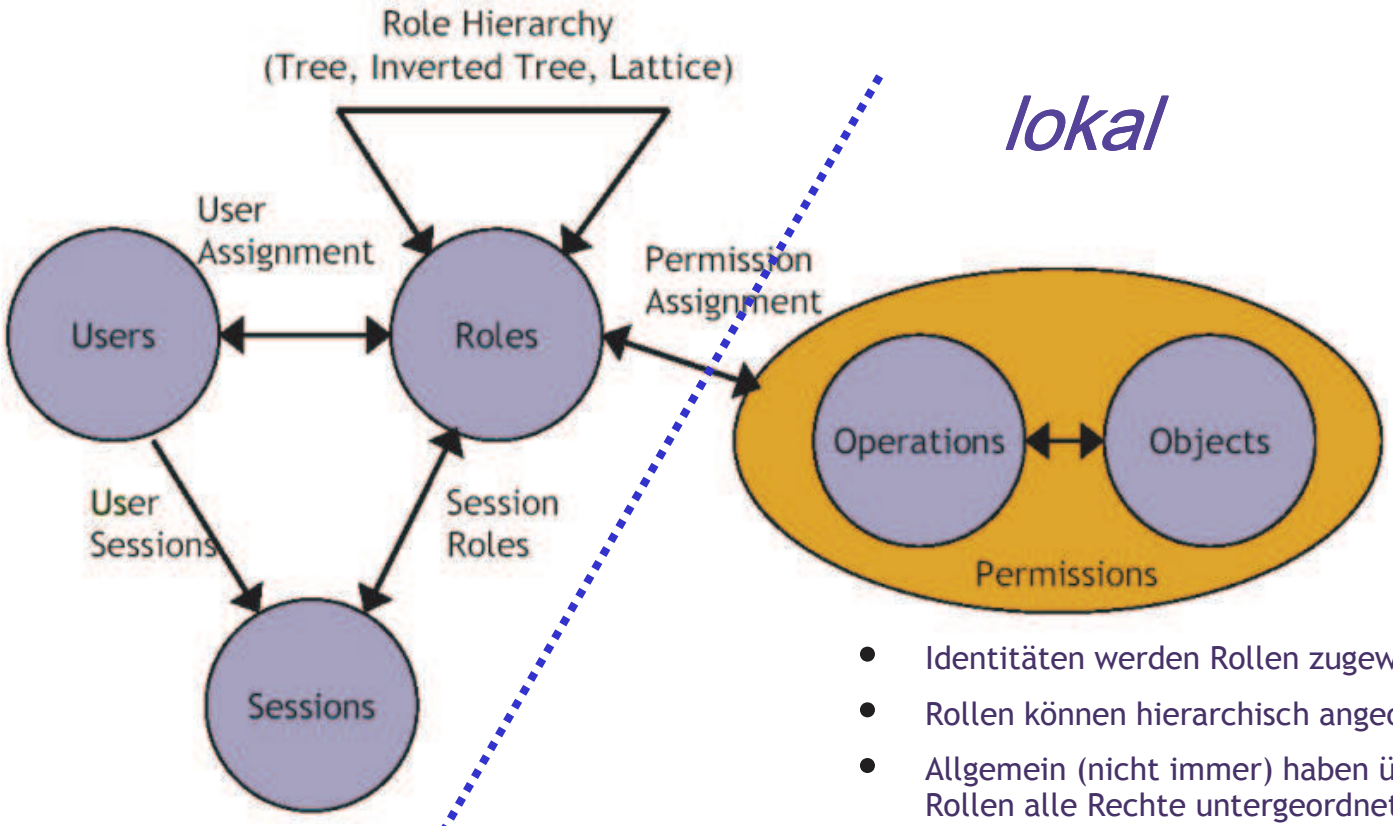


- Durchstich in der Tiefe wenn ...
  - Einige wenige Systeme gut angebunden
  - Rechtesituation gut bekannt
  - bidirektionale Anbindung technisch vorhanden
  - Wichtige Massensysteme:
    - Windows
    - Exchange
    - Lotus NOTES
  - Systemneueinführung
- Evidenzbildung in der Breite wenn ...
  - Eine zentrale Benutzerverwaltung aufgebaut werden soll
  - Sicherheits- und Compliance-Erwägungen im Vordergrund stehen.
  - Viele wichtige und wenig bekannte Altsysteme angebunden werden sollen.

➔ Bei gewachsenen Systemlandschaften lassen sich nicht alle Systeme in einem Schritt einbinden.

Zentral vs. Lokal

IDs & Rollen haben zentralen, Berechtigungen lokalen Charakter.



lokal

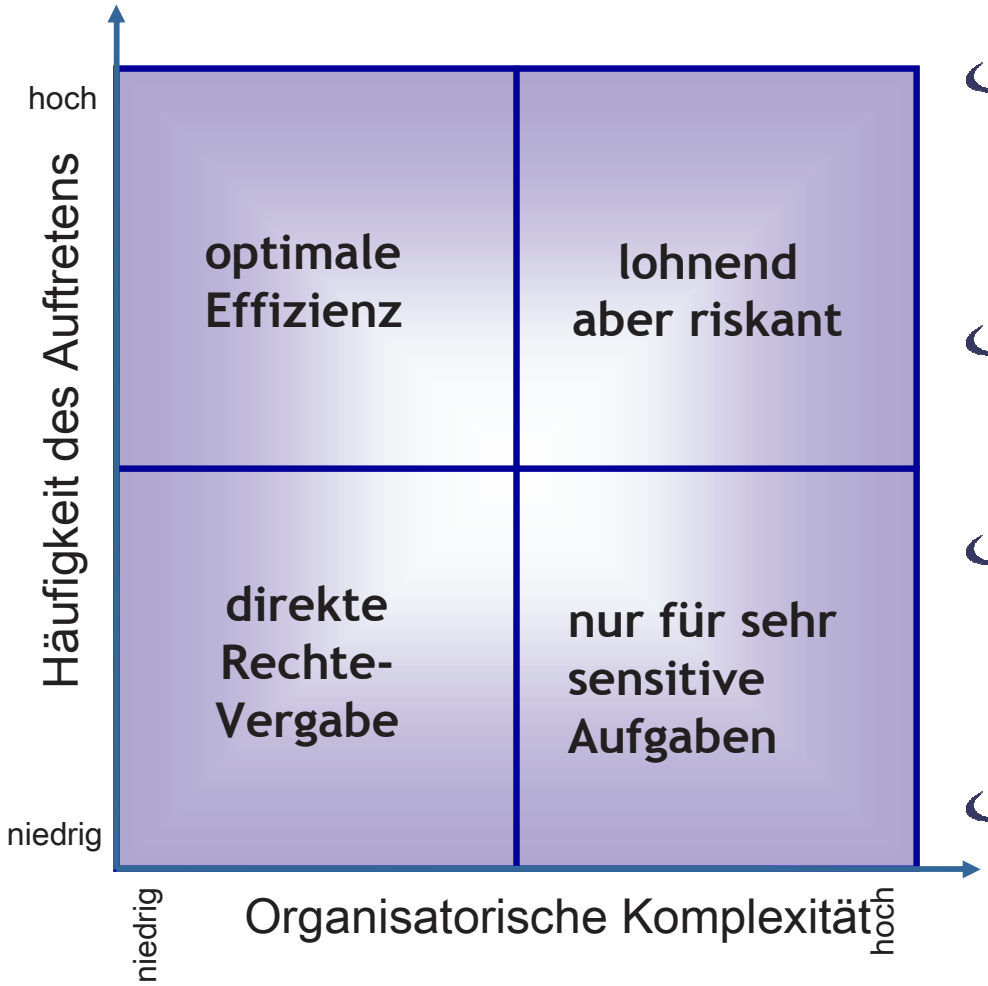
zentral

- Identitäten werden Rollen zugewiesen
- Rollen können hierarchisch angeordnet sein.
- Allgemein (nicht immer) haben übergeordnete Rollen alle Rechte untergeordneter Rollen
- Berechtigungen sind Operationen auf Objekte.
- Berechtigungen können additiv oder subtraktiv zugewiesen werden.
- Rollen können temporär pro Session gelten.

Source: Ferraiolo, Sandhu, Gavrila: A Proposed Standard for Role-Based Access Control, 2000.

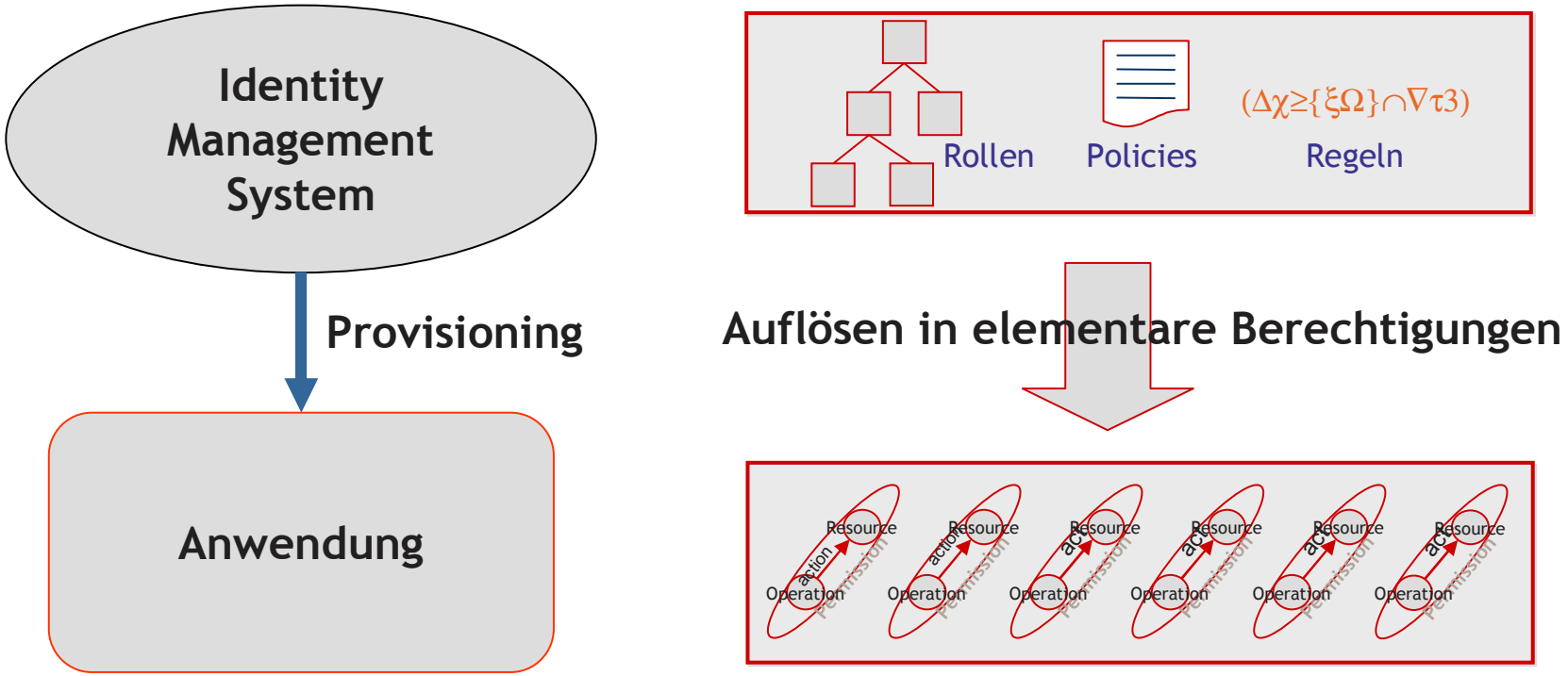
Wo sich der Einsatz von Rollen lohnt

Optimale Ergebnisse bei einer hohen Zahl von Jobs niedriger Komplexität



- häufig – einfach
  - Optimale Effizienz
  - Dafür wurden Rollen erfunden.
  - Hier starten!
- häufig – komplex
  - Lohnend aber riskant
  - Bei Erfolg hier fort fahren.
- selten – komplex
  - Nur für hoch sensitive Jobs
  - Nur bei guten Gründen für ein Rollenengineering.
- selten – einfach
  - Direkte Rechtevergabe
  - Für einfache Fälle lohnt sich kein Rollenengineering.

Rollen oder Rechte?
Was soll provisioniert werden?

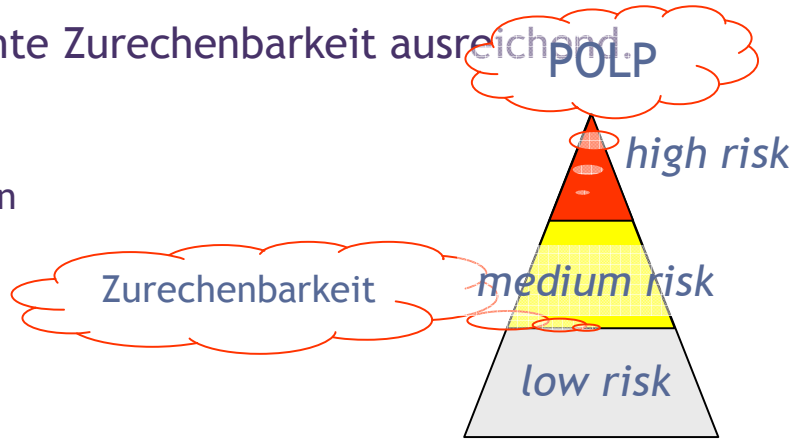


- Da es keinen Standard für das Provisioning von Rollen gibt …
  - Ist es nicht ratsam, die unterschiedlichen nicht-Standard Rollen, Gruppen- und / oder Regel Systeme der Ziel-Anwendungen zu unterstützen.
  - Müssen rollen in elementare Berechtigungen aufgelöst und an die Ziel-Anwendungen provisioniert werden

Principle of least Berechtigung (PoLP)
risikobasierte Entscheidungen sind erforderlich

"Einem Benutzer sollte nicht mehr Ressourcen zugriff gewährt werden, als er zur Erfüllung seiner Aufgaben benötigt."

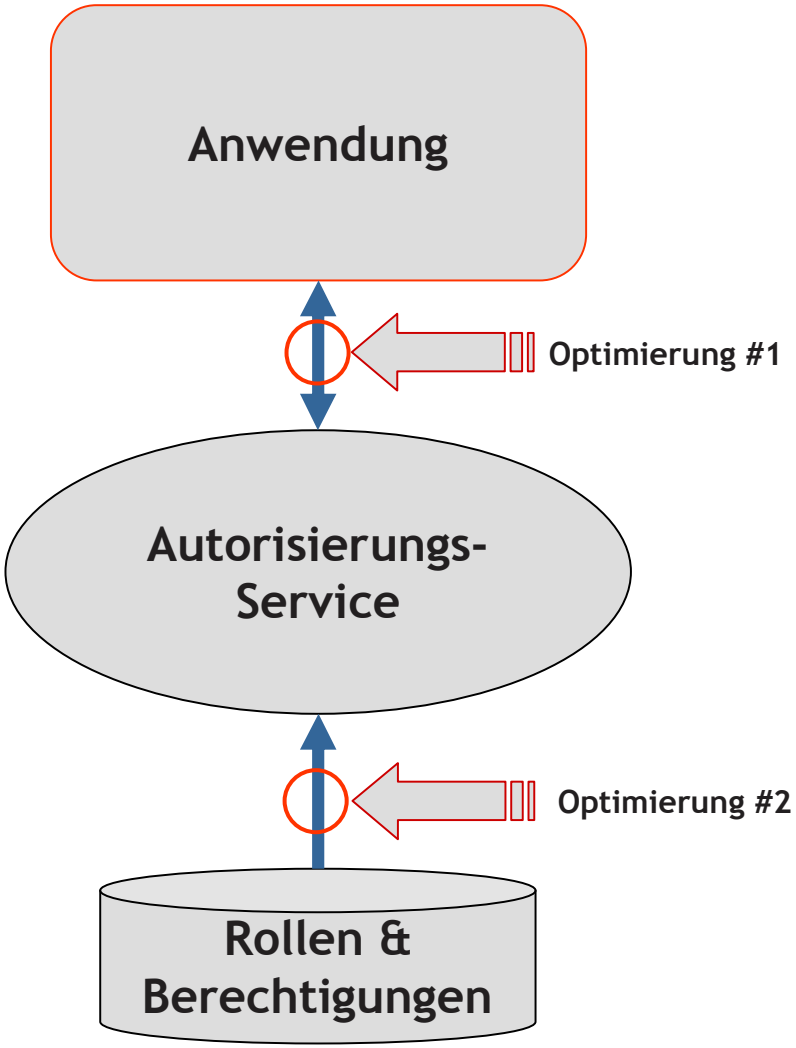
- Die Leitlinie für die Erstellung von Zugriffsrichtlinien
- In der Praxis ist sie jedoch nur schwer zu verwirklichen.
  - Erfordert die Zuteilung sehr feinkörniger Zugriffsrechte.
  - Berechtigungen sind volatil – sie ändern sich im Laufe der Zeit.
  - Die folge ist ein hoher Wartungsaufwand.
  - Die zugrundeliegende Fachlichkeit ist of nicht ausreichend definiert.
- Das „*principle of least Berechtigung*" ist nur für hochrisiko-Zugriffe erforderlich
- Für geringere Risiko Niveaus ist eine transparente Zurechenbarkeit ausreichend.
  - Zugriffsrichtlinie veröffentlichen
  - Alle Ressourcenzugriffe loggen
  - Log-Dateien regelmäßig auf Auffälligkeiten prüfen
  - Bei Auffälligkeiten unmittelbar hundeln.



Prinzip: PoLP für hohe - Zurechenbarkeit für mittlere und geringe Risiken.

Vision: Auslagerung der Autorisierung

Bei Neuentwicklungen authorisation as a Service definieren.



- In einer Service orientierten Umgebung sollte die Autorisierung als unabhängiger Service bereit gestellt werden.
- An jedem Zugriffsent-scheidungspunkt sendet die Anwendung eine Anfrage an den Service.
- Der Service entscheidet nach Rollen und Regeln, ob der Zugriff gewährt werden soll oder nicht.
- 2 Performance Optimierungen sind möglich:
  - Puffern der aufgelösten Berechtigungen in einem Cache.
  - Den lose gekoppelten Service als a fest gekoppeltes Modul in die Anwendung re-integrieren.

Questions - comments – suggestions?

Caution

Appendix

Here the notorious back-up-slides follow ...

Vorab : Der Kontext
Die Industrialisierung der Dienstleistung

Compliance

- Compliance erzwingt die Verwendung von Infrastruktur Standards.
- ITIL ist erst der Anfang – CoBIT, ValIT und andere werden folgen.
- SOA bietet ein technisches Framework für die Implementierung.
- ITIL, SOA, Compliance Frameworks sind Details eines größeren Bildes

2 globale Kräfte wirken ein.

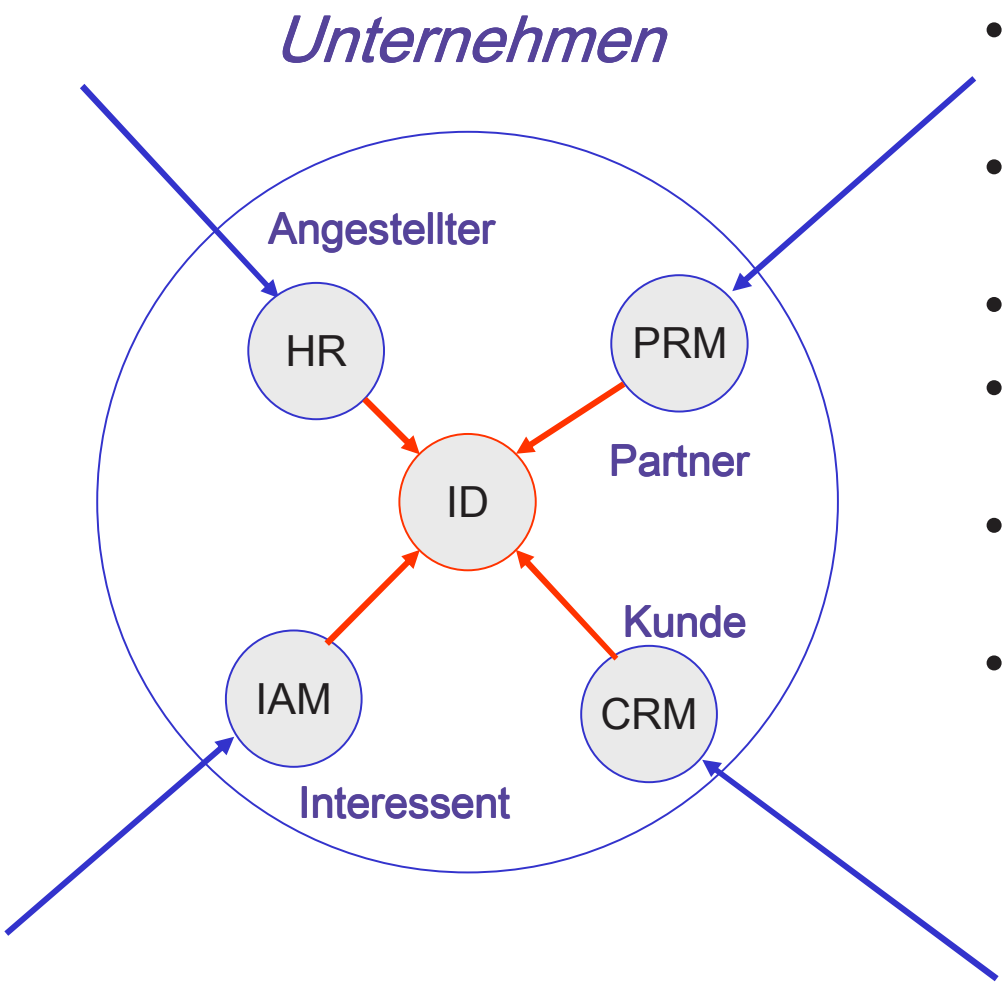
Unternehmen

Standardisierung
Automatisierung
Modularisierung
Kontinuierliche Verbesserung
Kernkompetenzen

Globalisierung

- Marktkräfte erzwingen Konzentration auf Kernkompetenzen.
- Nicht-wettbewerbs-relevante Aktivitäten werden standardisiert.
- Sie werden zu niedrigen preisen weltweit beschafft,
- ausgelagert / von Drittanbietern bezogen
- … oder anhand von *best practice* Referenzmodellen abgearbeitet..

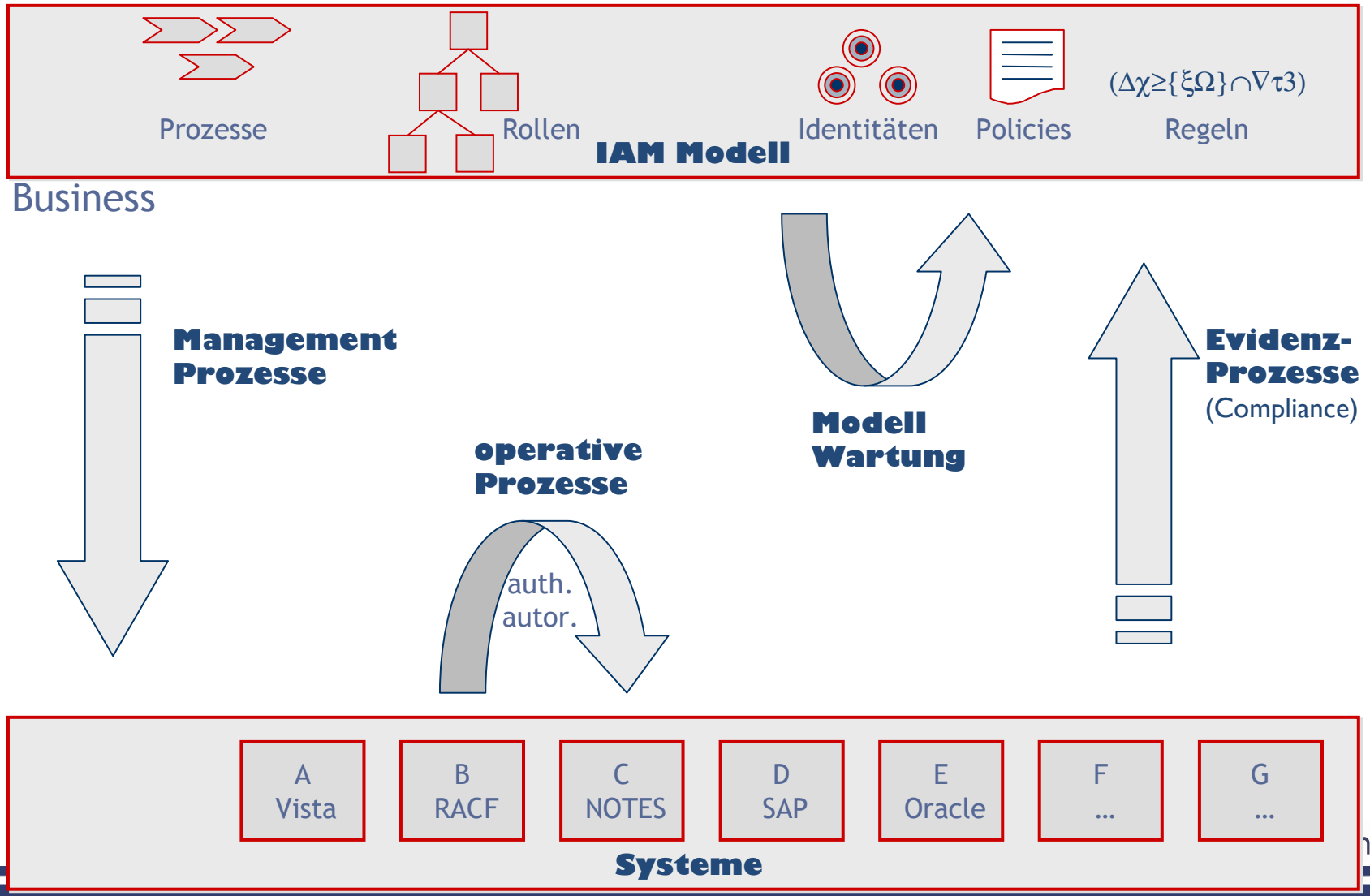
Die zentrale digitale Identität
Wann immer ein Individuum die Unternehmensgrenze passiert …



- Wird seine digitale Identität erzeugt
- Unabhängig ob es als *User* wirkt oder nicht.
- User bedeutet bereits eine Rolle.
- Die digitale Identität ist sein digitales Abbild
- Seine Lebenszeit bestimmt auch die seiner digitalen Identität.
- Seine digitalen Identität ist global und eindeutig.
  - Bereits die Wirkung der Biometrie bedenken!

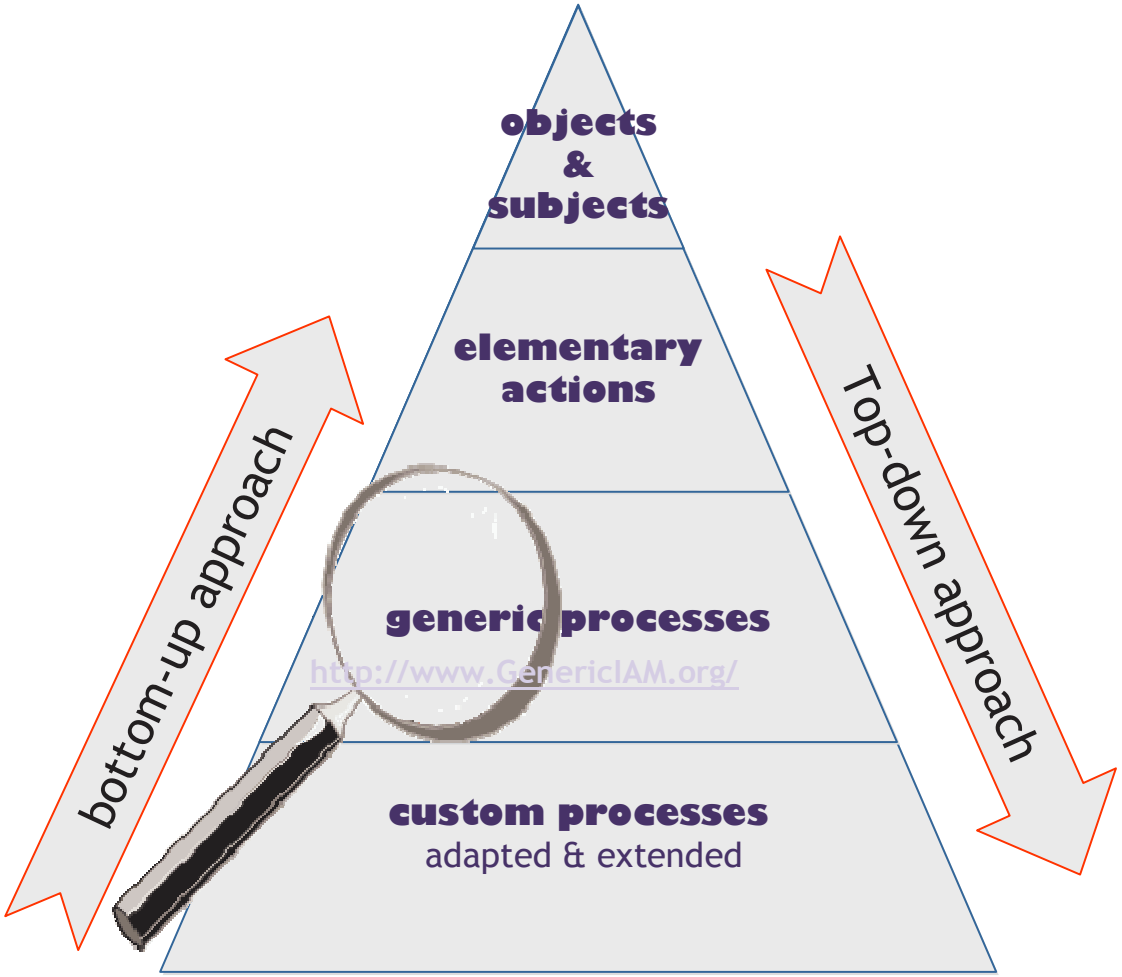
Businessmodell und technische Implementierung

Identity Management hat seinen Schwerpunkt im Business

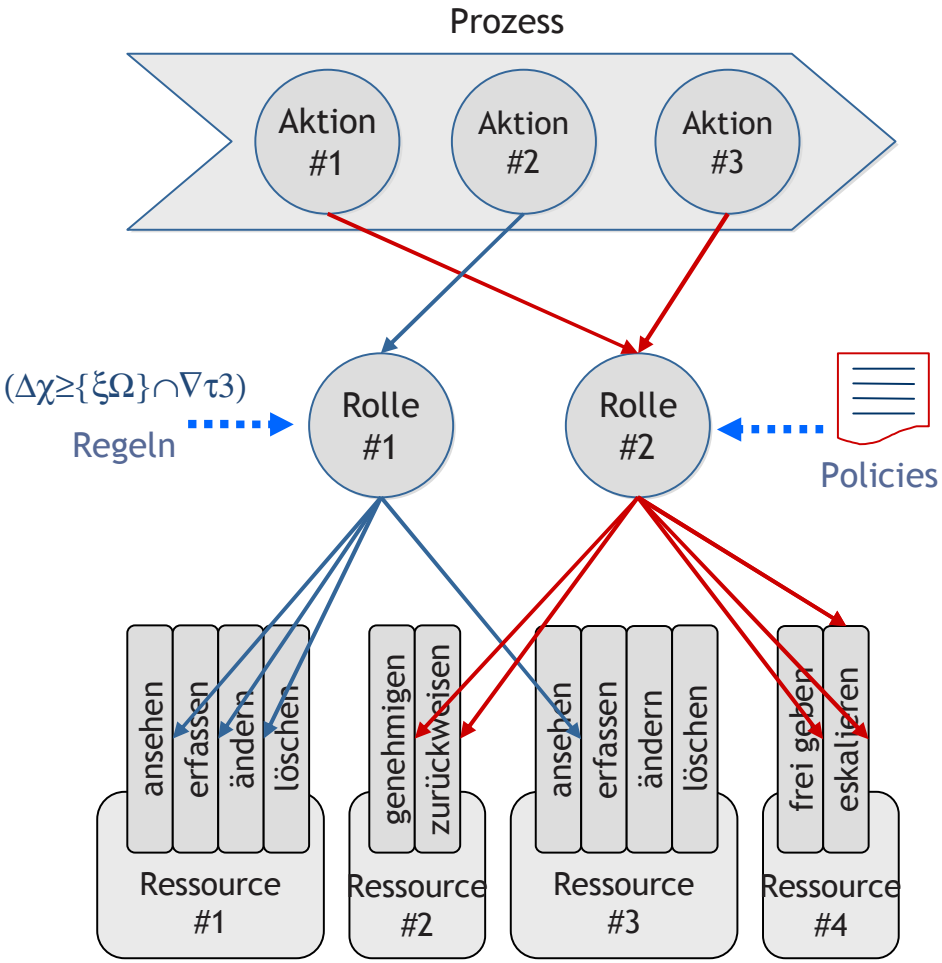


Der NIFIS GenericIAM Modellierungsansatz

bottom-up- und top-down-Ansatz führen zu einem generischen Modell



Prozesse – Rollen – Regeln
Sie bilden die Organisation ab



Top-down Modellierung

- Die Arbeitsweise von Organisationen wird durch ihre Geschäftsprozesse beschrieben.
- Prozesse bestehen aus elementaren Aktionen: eine Person zu einer Zeit an einem Ort
- Aktionen werden von Rollen ausgeführt.
- Dazu benötigen sie definierte Zugriffsrechte auf Ressourcen.
- Prozesse und Rollen lassen sich nicht unabhängig modellieren.

Ratschlag der Weisen

- **Rollen** und **Regeln** kombinieren – für ein einfaches Modell.
- Nicht alle Unternehmensbereiche sind **gleich gut** für ein Rollenengineering geeignet.
- Rollen lohnen sich bei **häufig** auf-tretenden Funktionen geringer Komplexität.
- Sie finden sich am **unteren Ende** der traditionellen Unternehmenspyramide.
- **Operative Funktionen** sind ein guter Ausgangspunkt für Rollenengineering.
- Je näher zu den **Headquarters** und je **höher** in der Unternehmenshierarchie um so schwieriger wird es.
- Rollenengineering ist **Unternehmensorganisation**.
- Rollenengineering kann sich als **gefährlicher Engpass** erweisen.

➔ Rollenengineering, ein Teil der Unternehmensmodellierung, ist nicht einfach und bietet eine Reihe von Stolpersteinen und Fallgruben.

Identity theft

"I found out who stole my identity. It's the same guy who's responsible for all of my missing socks!"