Auf dem Weg zum GRC

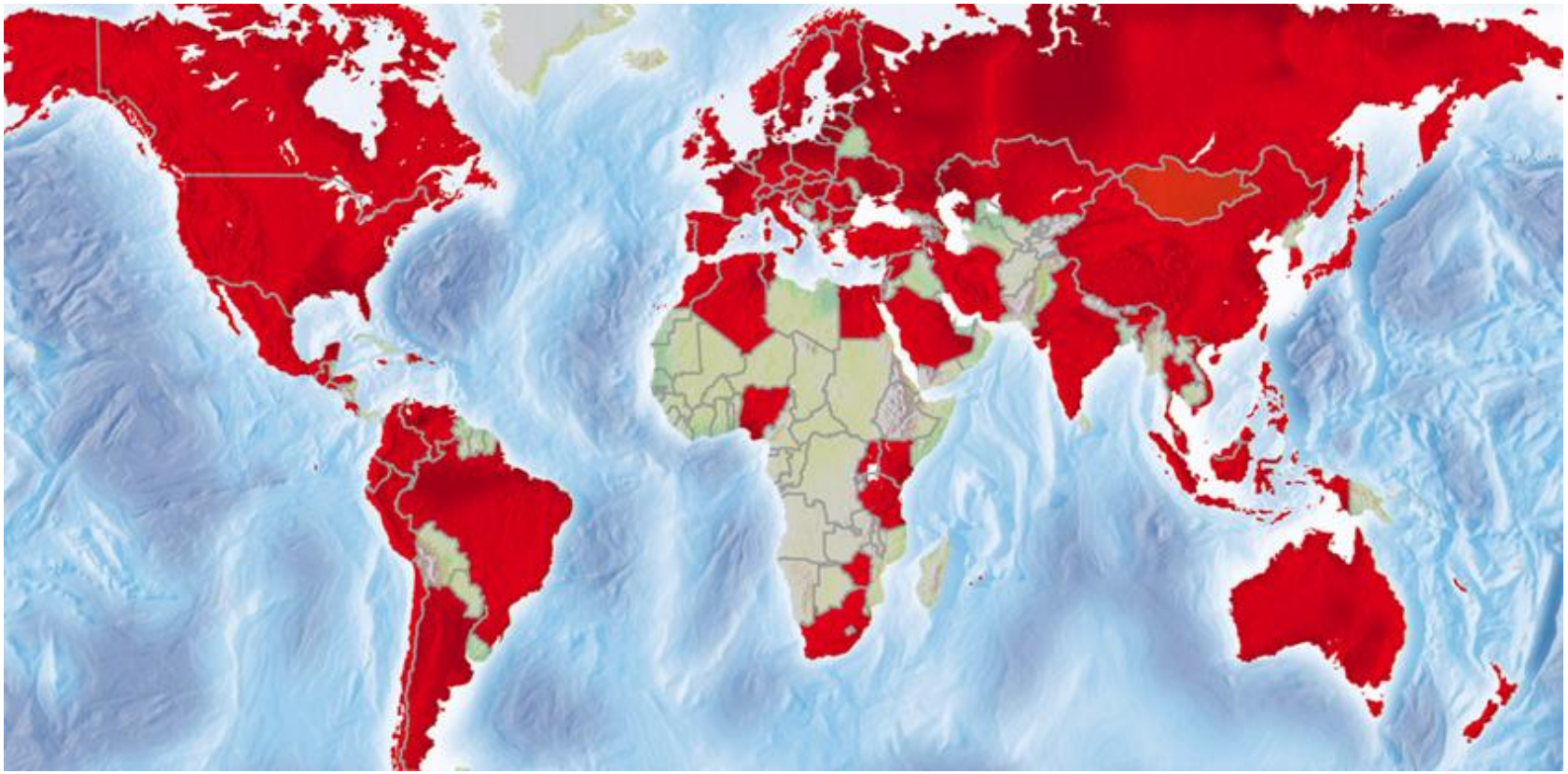
Roland Stahl

Lutz Reinhard

Agenda

- Henkel weltweit
- Start des User-Verwaltung
- Wechsel zum IAM@Henkel
- Ergebnis 2005
- Weiterentwicklung des IAM zum GRC
- Fragen und Diskussion

Henkel weltweit 2008



- **14.131 Mio. Euro Umsatz**
- **55.000 Mitarbeiter**
- **125 Länder**

Der Start bei Henkel

1992	Start USERADMI mit HR-Anbindung	Datenanzeige
1995	Beginn des Ausbaus zu aktiver Verwaltung der Zielsysteme	Provisionierung
1998	Erste Metafunktionen: Erzeugen Dateien für andere Applikationen mit Meta-Daten	IAM?
1999	SAP R/3; Novell NDS, RACF, IMS, MEMO, Lotus Notes, Änderungs-Log Nutzungsüberwachung der wichtigen Systeme (RACF, R/3) Austrittskontrolle Dezentraler Passwort-Reset durch BU	GRC?

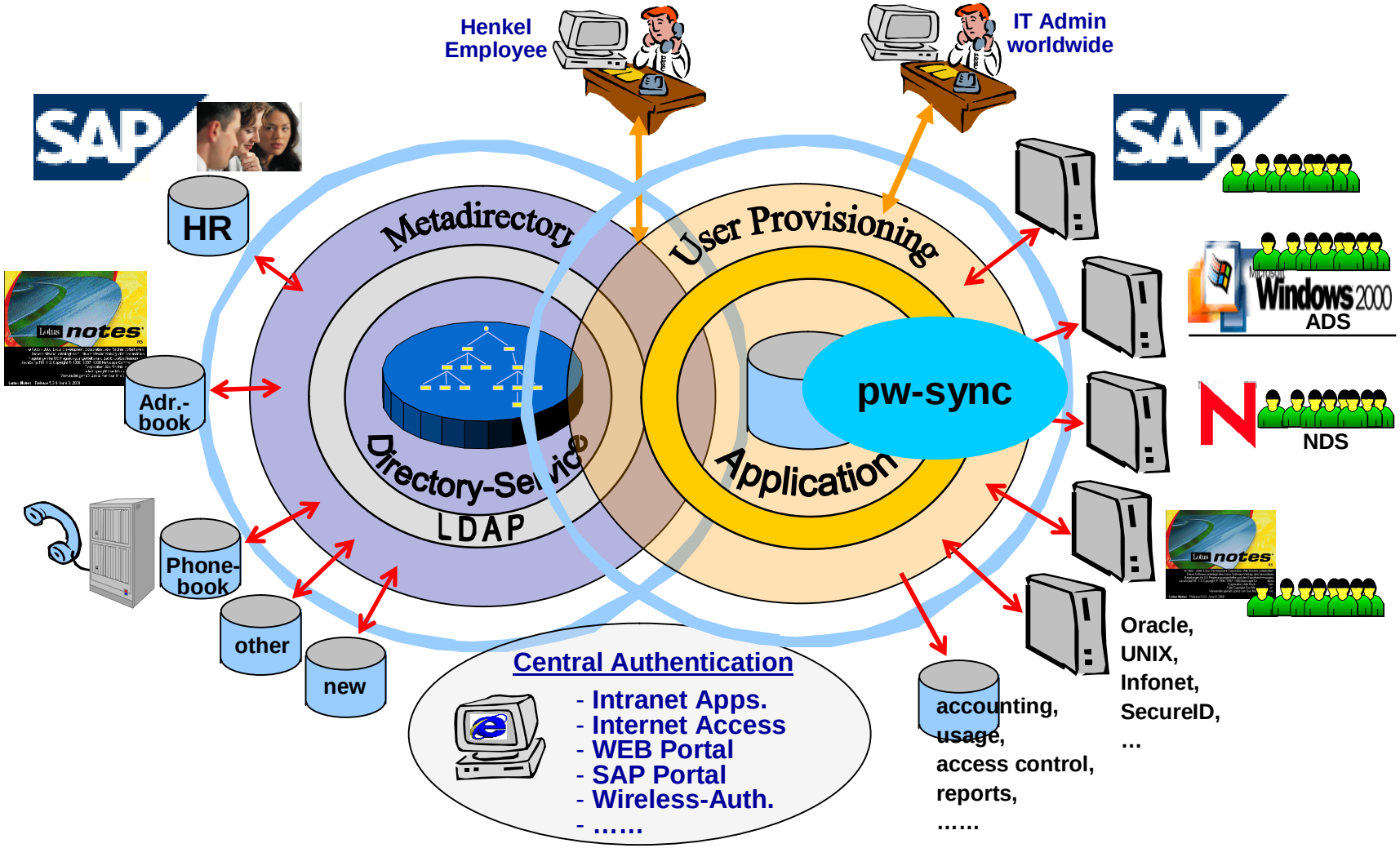
Ist-Analyse USERADMI 2003

- Betrieb ist personenabhängig (Wenn Person nicht anwesend, keine Verarbeitung; ggf. Stillstand der USERADMI)
- Externe Henkel Mitarbeiter werden über USERADMI eingepflegt
- Sperrung der User ID über Merkmale steuerbar
- USERADMI stößt an die Grenzen der Möglichkeiten bezüglich der Metafunktionalität und bedarf einer gründlichen Überarbeitung
- Steuerung dezentraler Funktionen (DVK, Passwort)
- Betrieb auf dem z/OS-Host

Der Wechsel zum IAM

2000	*Erste Suche für Nachfolger der USERADMI. Informationsgewinnung*	
2001	Entwicklung und Einbau eines Verfahrens zur Verwaltung Externer Mitarbeiter	
<2005	Starke Ausweitung der Datenlieferungen Anbindung neuer Systeme (Remote, ADS)	Metafunktionen
2005	Start Metadirectory (HMD) und Nachfolger USERADMI (HAD)	IAM

Ergebnis der Planungen 2004



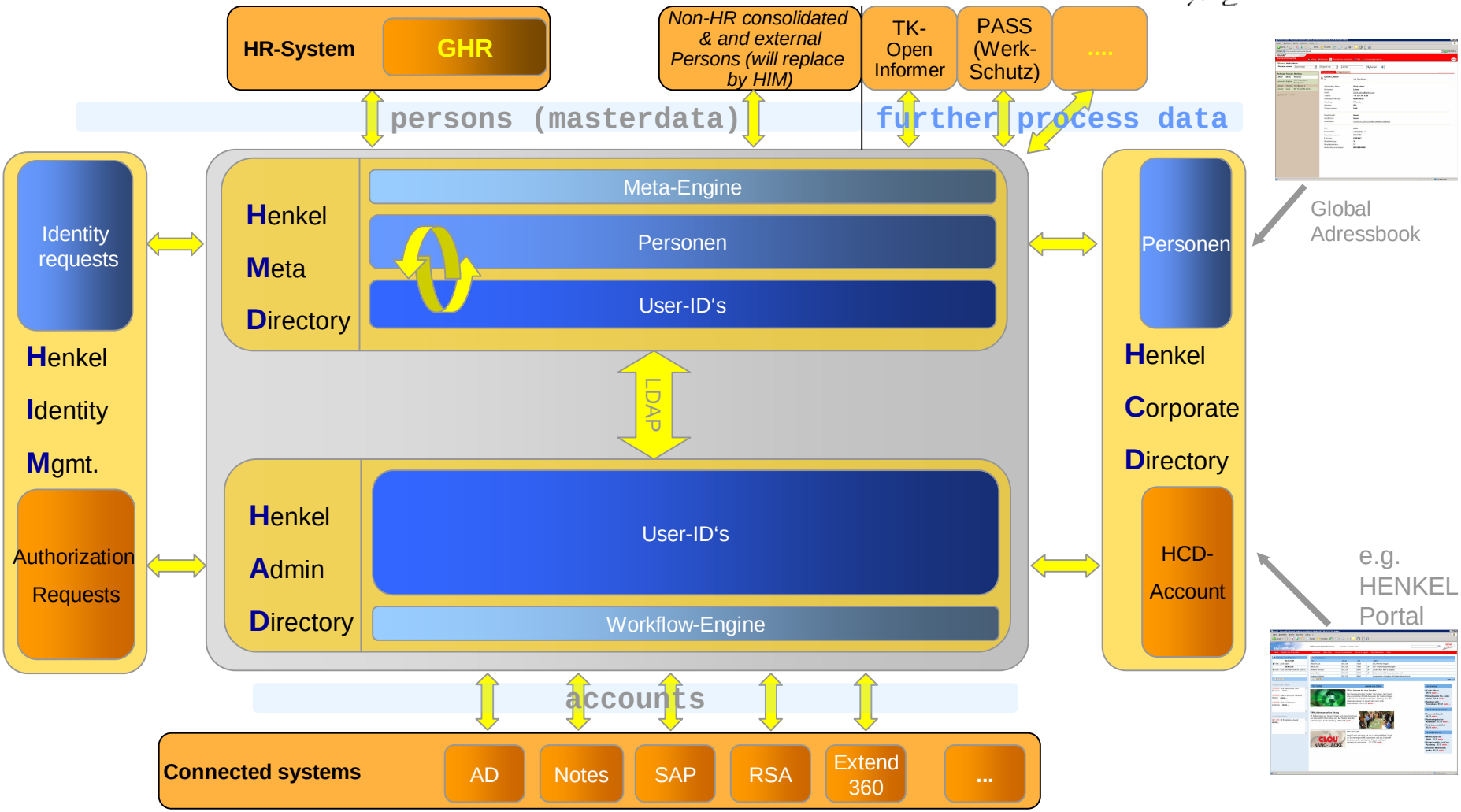
Ergebnis der Installation 2005

Es sind 3 zentrale Dienste implementiert worden:

- HMD: Henkel Meta Directory
  Zentrale Sammelstelle für alle personenbezogenen Daten.
  Geschlossenes System!
- HAD: Henkel Administration Directory
  Zentrales Userprovisioning
- HCD: Henkel Corporate Directory
  1. Öffentliches Adressbuch. Wird vollständig aus dem HMD gespeist, enthält aber nur ein Untermenge der HMD-Daten
  2. Zentrale LDAP-Authentisierung

Identity & Access Management

Architecture – Extension 2008 / 2009



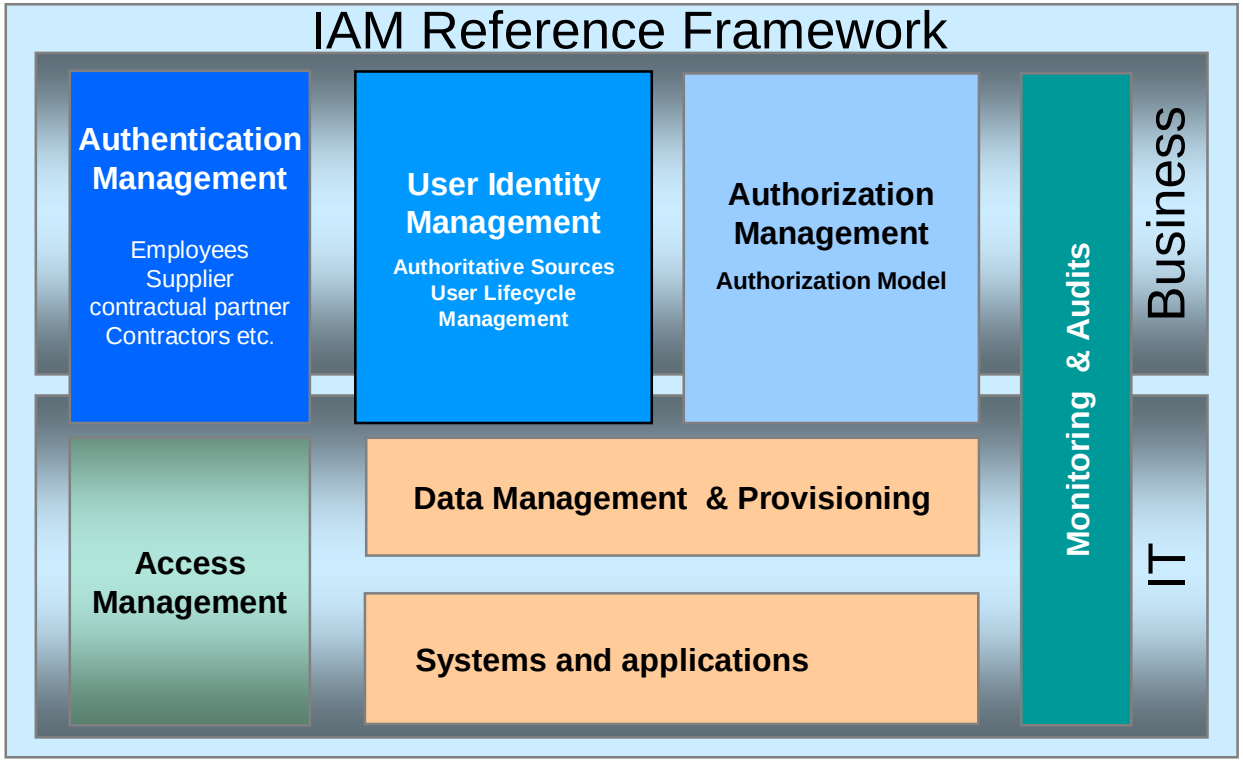
Ein paar aktuelle Zahlen 10/2009

- 78.000 Personen
  - 57.000 Interne aus HR, 4.300 per händischer Eingabe
  - 5.400 Externe
- 43.000 persönliche Userids
  + 9.500 Zweit-Ids (für technische Belange (FTP), Tests, MailIn)
- 107 angebundene Zielsysteme
  59 AD-Domänen
  36 SAP Mandanten
- 288.000 Accounts
- 180 Administratoren, 200 Passwort-Resetter
- Ca. 10.000 administrative Vorgänge im Monat

Erfahrungen Technik HMD/HAD

- Trennung in Metadirectory und Provisioning hat sich als sehr gut erwiesen.
- Dadurch strikte Trennung der Personen- und Account-Prozesse
- Zurzeit der Entscheidung gab es am Markt kein Tool welches beide Aspekte zufriedenstellend beherrschte
- Moderne Technologien für diese komplexen Systeme bieten eine lange Nutzungsdauer
- In der Technik hinterlegte Datenwege ermöglichen einen revisionssicheren Austausch sensibler Daten (z.B. aus dem HR).

IAM Architecture

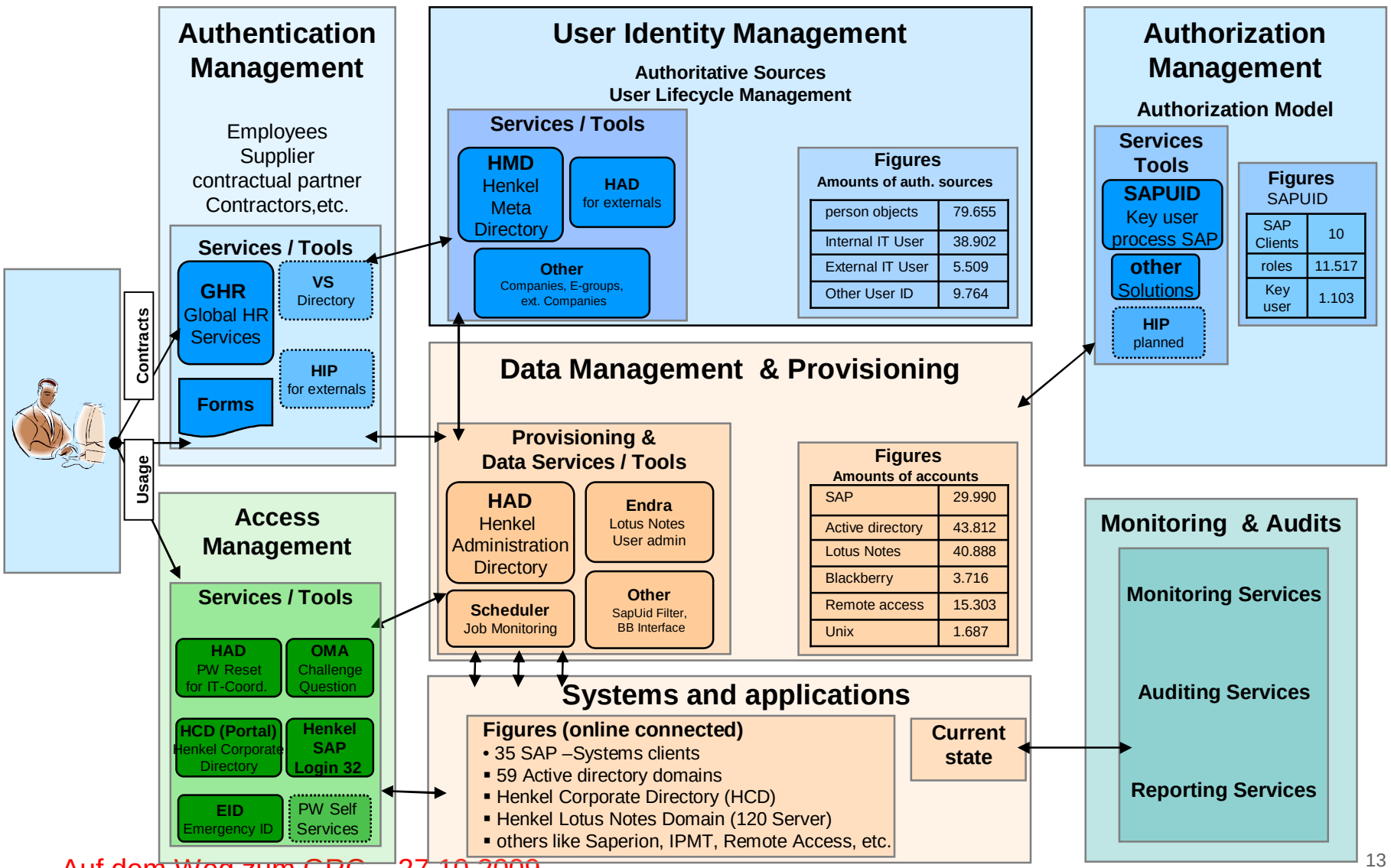


General Template
based on KPMG 2009

- **Authentication Management** Activities for the effective governance and management of the process for determining that an entity is who or what it claims to be.
- **User Identity Management -** Activities for the effective governance and management of the lifecycle of identities.
- **Authorization Management -** Activities for the effective governance and management of the process for determining entitlement rights that decide what resources an entity is permitted to access in accordance with the organization's policies.
- **Access Management -** Enforcement of policies for access control in response to a request from an entity wanting to access an IT resource within the organization.
- **Data Management & Provisioning -** Propagation of identity and data for authorization to IT resources via automated or manual processes.
- **Monitoring & Audit -** Monitoring, auditing and reporting compliance by users regarding access to resources within the organization based on the defined policies.

Identity & Access Management

IAM @ Henkel – current Tool Landscape



Was treibt GRC?

- Externe Audits
- Gesetzliche Anforderungen
- Verschärfung existierender Regeln im Geschäftsverkehr
- Einbindung der Geschäftseinheiten (BU) wird immer wichtiger
- Das Potential für IAM ist weitgehend ausgeschöpft und es bedarf neuer Themen/Aufgaben
- Verlagerung der IT-Verantwortung in die BU

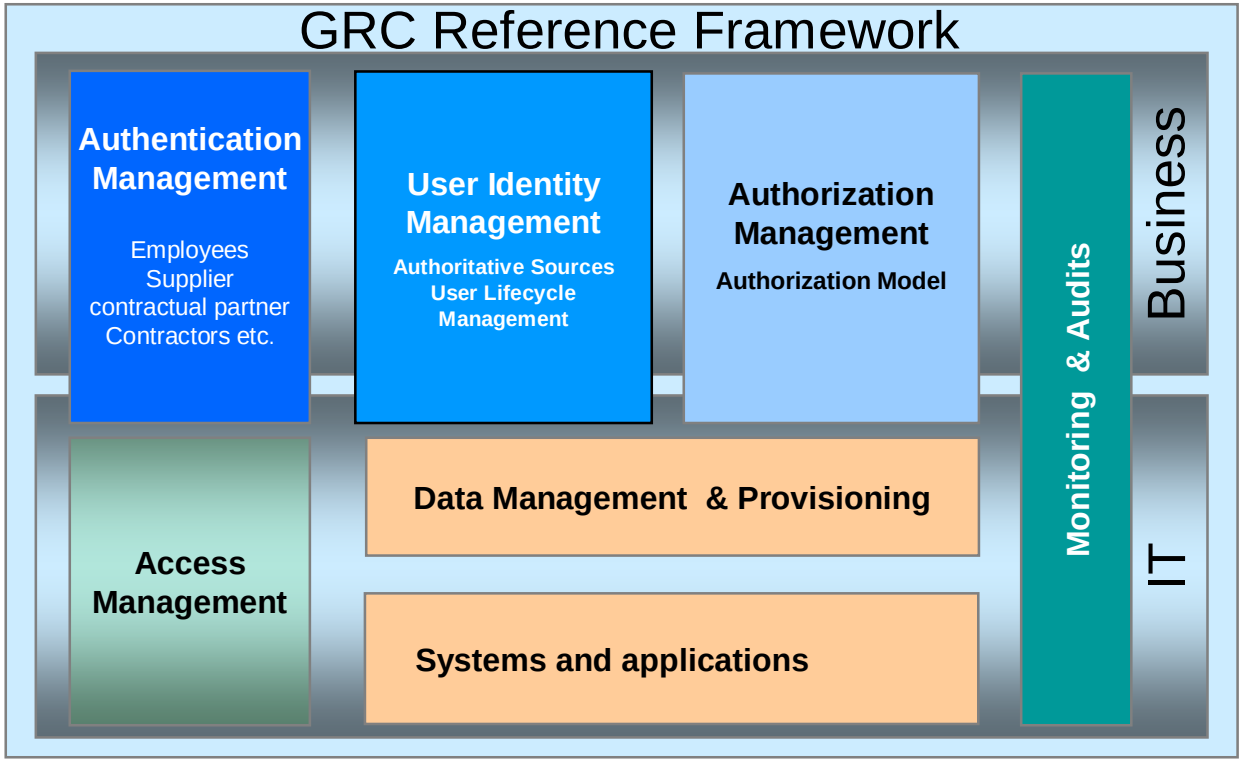
IAM am Ende?
GRC am Anfang?

- Automatisierung = Kosteneinsparung ist in hohem Maße erreicht
- Risiko entsteht an der Schnittstelle Business – IT durch unterschiedliches Verständnis
- Minimierung des Risikos ist nur durch gemeinsames Verständnis lösbar
- Weder durch technische noch organisatorische Maßnahmen allein lösbar
- GRC ist eine neue Wortschöpfung um die divergierenden Sichten auf IT-Sicherheit in der IT und dem Business zusammenzuführen
- GRC ist ein organisatorisches Thema, welches mit IT-Mitteln unterstützt werden kann.
  ➔ **Installation von CD nicht ohne Weiteres möglich!**

Vom IAM zum GRC

2005	Start Metadirectory (HMD) und Nachfolger USERADMI (HAD)	IAM
2007	Erste Selfservices	
2008	Umfassender Ausbau der SAP R/3-Nutzungskontrolle	GRC
2008	Personendaten-Erfassung für Externe durch Fachabteilungen im HMD	
2009	Standardisierung erster GRC-Funktionen	

GRC Architecture



General Template
based on KPMG 2009

- **Authentication Management** Activities for the effective governance and management of the process for determining that an entity is who or what it claims to be.
- **User Identity Management -** Activities for the effective governance and management of the lifecycle of identities.
- **Authorization Management -** Activities for the effective governance and management of the process for determining entitlement rights that decide what resources an entity is permitted to access in accordance with the organization's policies.
- **Access Management -** Enforcement of policies for access control in response to a request from an entity wanting to access an IT resource within the organization.
- **Data Management & Provisioning -** Propagation of identity and data for authorization to IT resources via automated or manual processes.
- **Monitoring & Audit -** Monitoring, auditing and reporting compliance by users regarding access to resources within the organization based on the defined policies.

Danke

für Ihre Aufmerksamkeit

Weitere Folien

USERADMI: Kennzahlen (12/04)

- 48.000 Personen, davon 27.000 Personalstamm geführt, 38.700 mit Userid(s)
- 44.800 Userids mit 130.000 Accounts in verschiedenen Systemen
- 315 dezentralen Administratoren (DV-Koordinatoren und Passwort-Reset)
- 23 SAP mit 13.600 Usern (insgesamt 29.000 Accounts)
- 20 ADS-Domänen mit 12.600 Accounts (davon zz. 7.100 aktiv verwaltet)
- Novell-NDS mit 9.500 Accounts
- LDAP-Authentication-Server mit 8.300 Accounts
- 3 Remote-Zugänge mit 3.100 Accounts
- RSA-ACE-Server mit 5.800 Accounts und 8.000 Token
- RACF mit 1.100 Accounts (entfiel)
- 2 Lotus Notes-Domänen mit 8.400 Accounts
- UNIX-NIS mit 2.800 Accounts
- 6 weitere kleine Systeme teilweise nur als Anzeige

Ist-Analyse USERADMI 2003

- Werkzeug ist eine Eigenentwicklung und ist eher historisch als strategisch gewachsen
- Betrieb, Wartung und Weiterentwicklung durch eine Person
- Hohe Integration der Henkel-Anforderungen
- Konnektoren in vielen Zielanwendungen sind vorhanden, aber über unterschiedliche Schnittstellen und Methoden
- Betrieb der USERADMI-Konnektoren heute nicht unter einheitlicher Hardware und Software.
- Automatismen sind mit Einschränkungen vorhanden (Bsp.: Automatatischer Import aus SAP HR aber nur teilautomatisierte Weiterverarbeitung in Accounts)