



Seminar „Identity Management“

# „ Provisioning-Prozesse - Regelkreis des Access Rights Management“

Version 1.0

Nicole Kleff  
1. Tag, 11:15 – 12:15



24.06.2003 - 25.06.2003 Frankfurt/Main

# Nicole Kleff Beraterprofil



**Nicole Kleff**

Nicole.Kleff@Si-G.com

- freiberufliche Beraterin der *SiG Software Integration GmbH*
- seit 1995 im Bereich Informationssicherheit tätig
- Branchen: Kreditinstitute, Versicherungen, Transport/Logistik
  
- Spezielle Kenntnisse auf den Gebieten ...
  - ▶ Design und Optimierung von Prozessen im Bereich Access Rights Management,
  - ▶ Auswahl und Einführung von User-Provisioning-Systemen,
  - ▶ Role-Based-Access-Control,
  - ▶ Standards und Richtlinien zur Informationssicherheit (ISO/IEC 17799, BSI-Grundschriftbuch, ISO/TR 13335, Common Criteria, ISO/TR 13569 ...) und
  - ▶ Mainframe-Sicherheit (MVS, OS/390, RACF).



# Übersicht

- Access Rights Management – typische Praxissituation
- Modell – Regelkreis des Access Rights Management
  - ▶ Instanzen und Komponenten des Regelkreises
  - ▶ Schnittstellen des Regelkreises
  - ▶ Beispiel: Übersicht Anforderungsdefinition
  - ▶ Beispiel: Übersicht Prozesse/Workflow
- Erfahrungsbericht aus Projekten
  - ▶ Kosten-/Nutzerüberlegungen
  - ▶ Organisatorisch- und technische Voraussetzungen
  - ▶ Projektumfang/Einführung
- Praktische Übung
  - ▶ Ermittlung der unternehmensspezifischen IST-Situation
  - ▶ **<Mittagspause>**
  - ▶ Vorstellung der Kernpunkte und Auswertung
  - ▶ Erarbeitung von Handlungsempfehlungen

# Access Rights Management – typische Praxissituation

- Typische Kennzeichen in der Praxis
  - ▶ hohe IT-Durchdringung im Unternehmen
  - ▶ große Anzahl an IT-Systemen mit unterschiedlichen Benutzerzahlen und heterogenem Berechtigungsmanagement
    - ▶▶ gewachsenen Strukturen und Verantwortlichkeiten
    - ▶▶ unterschiedliche Antragsverfahren und Genehmigungsprozesse
    - ▶▶ unterschiedliche Rechtestrukturen (Gruppen, Rollen ...)
    - ▶▶ unterschiedliche Namenkonventionen (Benutzerkennung, Rechte ...)
    - ▶▶ unterschiedliche Administrationsverfahren
    - ▶▶ unterschiedliche Auswertungs- und Kontrollmöglichkeiten
- Ziel (?)
  - ▶ Steuerung, Administration und Kontrolle der Zugriffsrechte von allen IT-Benutzern für alle IT-Ressourcen auf allen IT-Systemen (des Unternehmens)

# Modell – Regelkreis des Access Rights Management

## Legende

Antragsfluss



Datenfluss



Datenabgleich



## 1. Antragsteller



- beantragt Berechtigungen

## 2. Freigabeinstanzen

- Vorgesetzte genehmigt
- bei Bedarf zusätzliche Qualitätssicherung (ggf. mehrstufig)



## 3. Administratoren

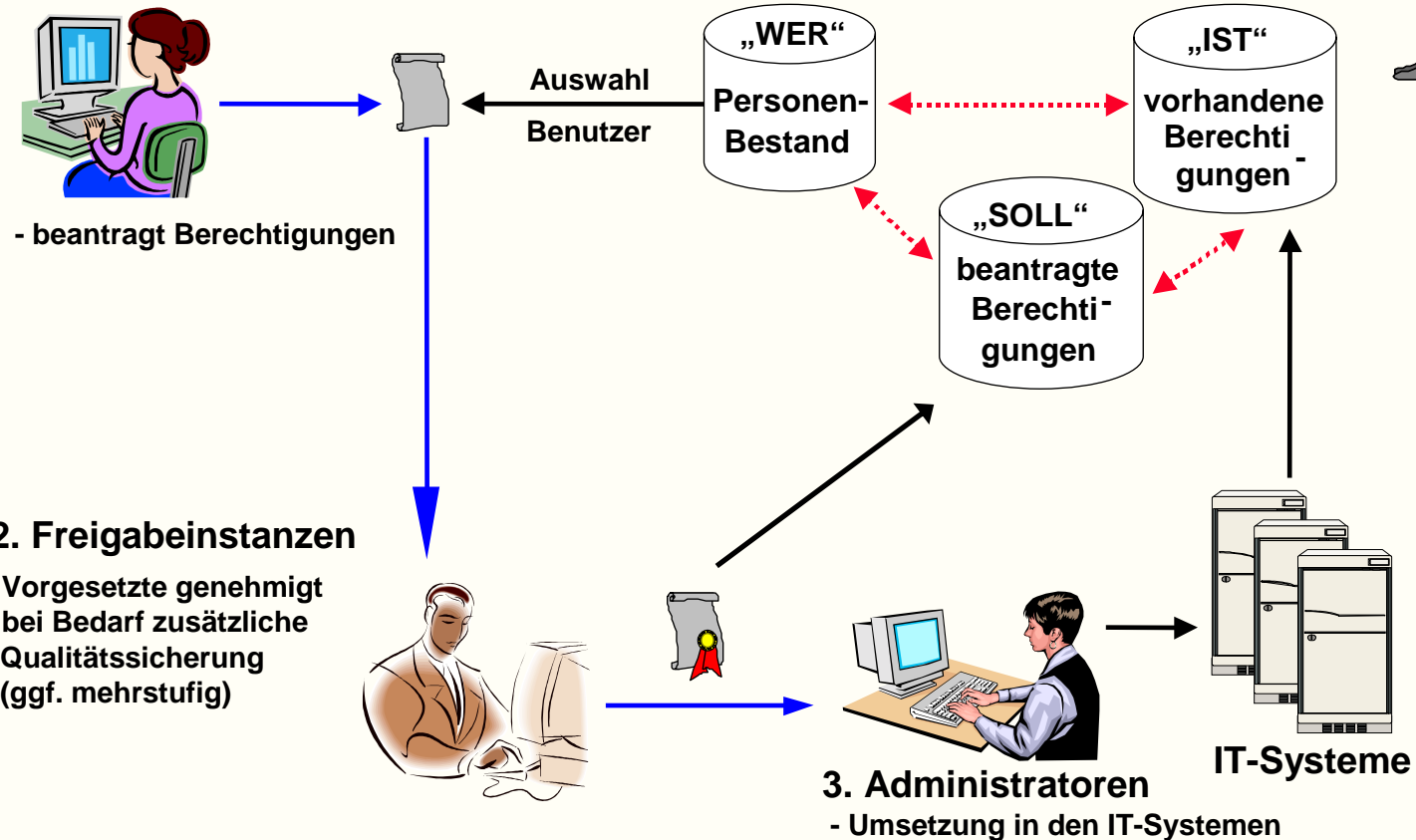
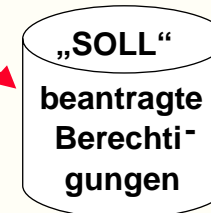
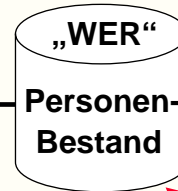
- Umsetzung in den IT-Systemen



IT-Systeme

## 4. Prüfinstanzen

- unterschiedliche Sichten: Abteilung, System, Historie, Abweichungen



# Instanzen und Komponenten des Regelkreises (1)

## 1 Antragsverfahren

- ▶ Elektronisch unterstütztes Antragsverfahren
- ▶ Auswahl des Antragsbetroffenen aus Mitarbeiterstamm
- ▶ Systemspezifische Antragstemplates (möglichst standardisiert)
  - ▶▶ Einrichtung, Änderung und Löschung von Benutzern und Rechten
- ▶ Möglichkeit zur Antragsverfolgung
  - ▶▶ Validierung der Input-Daten
- ▶ Elektronische Archivierung

## 2 Genehmigungsprozess

- ▶ Systemspezifischer Genehmigungsworkflow (Änderung Regelwerk)
- ▶ Möglichst flächendeckenden Standardworkflow festlegen
  - ▶▶ Fachlich Vorgesetzter als erste Prüfinstanz (personelle Verantwortung)
  - ▶▶ Systemverantwortlicher als weitere Prüfinstanz (Systemverantwortung)
- ▶ Ggf. weitere Prüfinstanzen für Sonderfälle (z.B. Revision, Datenschutz ...)
- ▶ Nur autorisierte Personen dürfen als Genehmiger zugelassen sein

# Instanzen und Komponenten des Regelkreises (2)

## 3 Administration

- ▶ Möglichkeit zur Automatisierung mittels Agenten
- ▶ Schnittstelle für manuelle Administration
- ▶ Berechtigungsprüfung erfolgt weiterhin durch die Zugriffssteuerungssysteme der IT-Systeme

## 4 Berechtigungsevidenz

- ▶ Globale Evidenz über Benutzer und Rechte
  - ▶ IST: durch regelmäßigen Input aus den IT-Systemen
  - ▶ SOLL: die komplett genehmigten Anträge stellen das Soll dar
- ▶ Kontroll- und Auswertungsmöglichkeiten
  - ▶ IST <-> SOLL: Administrationsfehler, Hacker
  - ▶ Mitarbeiterstamm <-> IST: Ausscheiden, Abteilungswechsel (WF-Trigger)
- ▶ Unterschiedliche Sichten und Anforderungen
  - ▶ Abteilungssicht (fachlich Vorgesetzter)
  - ▶ Systemsicht (Systemverantwortlicher)
  - ▶ Abweichungen, kritische Rechte, Historie (Revision, Datenschutz)
- ▶ Kann als Grundlage zur Bildung von Geschäftsrollen dienen

# Schnittstellen des Regelkreises

## ■ Mitarbeiter-/Organisationsdaten

- ▶ Anbindung an die Personalverwaltung zur eindeutigen Verknüpfung zwischen dem Unternehmensmitarbeiter und dem IT-Benutzer
- ▶ Redundanzkontrolle der Mitarbeiterstammdaten in den Berechtigungsdaten
- ▶ Anträge nur für aktive Unternehmensmitarbeiter (intern und extern) möglich
- ▶ Organisatorische Änderungen als automatischer WF-Trigger
  - ▶ Ausscheiden MA -> Sperrung bzw. Löschung Accounts
  - ▶ Neuer MA -> Einrichtung Standardrechte
  - ▶ Abteilungswechsel -> Entzug von Abteilungsrechten
- ▶ Beziehung MA <-> fachlich Vorgesetzter
  - ▶ Sicherheit im Genehmigungsverfahren
  - ▶ Abteilungssicht in Auswertungen

## ■ IT-Systeme

- ▶ Manuelle oder automatisierte Administrationsschnittstelle
- ▶ Regelmäßiger Abgleich der IST-Daten (Accounts, Rechte, Rollen)

# Beispiel: Übersicht Anforderungsdefinition (1)

## ■ Informationsobjekte

- ▶ Datenmodell – Berechtigungskonzept
- ▶ Berechtigungsdaten (Rolle, Berechtigung, Account, ...)
- ▶ Antragsdaten
- ▶ Mitarbeiter – und Organisationsdaten

## ■ Berechtigungskonzept

- ▶ Beschreibung der Funktionen/Dialoge
- ▶ Beschreibung der Rollen (inkl. Regeln)
- ▶ Zuordnung von Funktionen und Rechten zu Rollen
- ▶ Provisionieren/Deprovisionieren

## ■ Verwaltung von Mitarbeiter- und Organisationsdaten

- ▶ Unternehmen, Abteilungen (laden, abgleichen, anlegen, ändern, löschen)
- ▶ Mitarbeiter (laden, abgleichen, anlegen, ändern, sperren, löschen)
- ▶ Zuordnung (Unternehmen <-> Abteilung, Abteilung <-> Mitarbeiter, ...)

## ■ Verwaltung von Berechtigungsdaten

- ▶ Rollen, Berechtigungen, Zielsysteme, Accounts, Regeln (anlegen, ändern, löschen)

# Beispiel: Übersicht Anforderungsdefinition (2)

- Prozesse/Workflow
  - ▶ Manuell <-> automatisch initiierte Prozesse
- Information der Prozessbeteiligten
  - ▶ Neue Aktivität zur Bearbeitung
  - ▶ Antrag – Statusinformationen
  - ▶ Eskalation
  - ▶ Änderung von Mitarbeiter- und Organisationsdaten
- GUI-Konventionen
  - ▶ Design-Vorgaben, Ergonomie, Maskenaufbau pro Funktion/Dialog
- Anbindung der IT-Systeme (inkl. des Systems selbst)
  - ▶ Art der Anbindung (manuell, automatisiert)
  - ▶ Prozessdaten (Account, Rechte, Rollen, Antragsdaten, ...)
  - ▶ Initialer Datenimport
  - ▶ Antragsverfahren
  - ▶ Provisionierung
  - ▶ Abgleiche/Auswertungen

# Beispiel: Übersicht Anforderungsdefinition (3)

- Anbindung von Agenten
  - ▶ Generelle Voraussetzungen
  - ▶ Spezifikation des Agenten je Zielsystem (Eigenschaften, Funktionalität, technische Angaben)
- Auswertungen/Reports/Historie
  - ▶ Aktuelle Accounts und Rechte (eigenen, fachl. Vorgesetzter, Systemverantwortlicher ...)
  - ▶ Antragsstatus (Antragssteller, Antragsbetroffener, Genehmiger)
  - ▶ Abgleiche (Soll <-> IST, Mitarbeiter <-> IST, ...)
  - ▶ Nicht zugeordnete Accounts
  - ▶ Sicherheitskritische Ereignisse
- Logging/Audit
  - ▶ Systemmeldungen, Fehlermeldungen, Transaktionen, Tracing, Audit
- Sicherheitsanforderungen
  - ▶ Account-Konventionen, Passwort, Zustellung, Neuanforderung, Verschlüsselung ...
- Performance

# Beispiel: Übersicht Prozesse/Workflow (1)

- Auslöser: manuell, automatisch (zeitlich, Ereignis)
- Antragsprozesse
  - ▶ Antragsdaten (Auswahl, Eingabe, Validierung der Daten)
  - ▶ Information und Einbindung der Prozessbeteiligten
  - ▶ Genehmigungsprozess (Standard, z.B.: Antragsteller -> fachlich Vorgesetzter -> Systemverantwortlicher -> Administrator)
  - ▶ Vier-Augen-Prinzip
- Anbindung IT-Systeme
  - ▶ Initialer Datenimport
  - ▶ Provisionieren/Deprovisionieren
  - ▶ Regelmäßige Abgleiche
- Mitarbeiterprozesse
  - ▶ Neue Mitarbeiter (Laden, Anlegen)
  - ▶ Mitarbeiterstammdaten ändern
  - ▶ Mitarbeiter sperren
  - ▶ Mitarbeiter entsperren
  - ▶ Mitarbeiter löschen

# Beispiel: Übersicht Prozesse/Workflow (2)

- **Berechtigungsprozesse**
  - ▶ Neue Berechtigung
  - ▶ Berechtigung ändern (Gültigkeitszeitraum, Account-Daten, ...)
  - ▶ Berechtigung löschen
- **Accountprozesse**
  - ▶ Account Sperren/Entsperren
  - ▶ Neues Passwort
- **Vertreterregelungen**
  - ▶ Dauerhafte Vertretung, für einen bestimmten Zeitraum
- **Ausnahmen**
  - ▶ Abkürzung des Genehmigungsprozesses
  - ▶ Übertragen von Aktivitäten
- **Eskalation**
  - ▶ Pro Genehmigungsinstanz
  - ▶ Zeitraum konfigurierbar
  - ▶ Vorgelagerte Information per Email

# Nutzenkomponenten (1)

## ■ Quantitativer Nutzen

- ▶ Reduktion von Lizenzkosten durch die Löschung überflüssiger Accounts
- ▶ Reduktion des Archivierungsaufwands für Administratoren
- ▶ Reduktion des Revisionsaufwands bei Systemprüfungen
- ▶ Reduktion des Klärungs- bzw. Kontrollaufwands für Administratoren
- ▶ Reduktion des Administrationsaufwands (Agenten, PW-Self-Service)
- ▶ Reduktion der Wartezeit für Antragsbetroffene
- ▶ Reduktion des Aufwand zur Klärung des Antragsstatus

*< Sollte als Basis der Projektverrechnung dienen !! >*

*< Nicht immer direkt zurechenbar !! >*

*< Beidseitige schriftliche Bestätigung notwendig !! >*

## Nutzenkomponenten (2)

### ■ Qualitativer Nutzen/Sicherheitsgewinn

- ▶ Steigerung der Antragsqualität (Standardisierung und Validierung)
- ▶ Minimierung von Administrationsfehlern
- ▶ Entlastung von Routine-Tätigkeiten
- ▶ Reduzierung der Anzahl ungenutzter Accounts (potentielle Angriffsquelle)
- ▶ Reduzierung der Missbrauchs- bzw. Angriffsmöglichkeiten durch transparente „doppelte Buchführung“ (Soll <-> IST)
- ▶ Eindeutige Verknüpfung zwischen Unternehmensmitarbeiter und IT-Benutzer
- ▶ Auswertungen als Basis zur effizienten Kontrolle und ggf. Korrektur von Berechtigungen (Mitarbeiterstamm, Soll, IST, Historie, Audit)

< *Steigende externe Anforderungen, z.B. Basel II, §25aKWG, KontraG !!* >

< *Steigende interne Anforderungen: Revision, Datenschutz, IT-Security !!* >

# Kostenkomponenten (1)

## ■ Projektkosten

- ▶ Projektmanagement/Kommunikation (15%)
- ▶ Vorstudie (5%)
- ▶ Anforderungsdefinition (10%)
- ▶ Marktanalyse/Produktauswahl (5%)
- ▶ Lizenzkosten/Hardwarekosten (10%)
- ▶ Feinkonzept/IT-Konzept (10%)
- ▶ Entwicklung/Konfiguration/Test (30%)
- ▶ Implementation/Pilot (7,5%)
- ▶ Dokumentation/Schulung (7,5%)

*< Hoher Kommunikationsaufwand !! >*

*< Trotz Standardprodukt hoher Anteil der Entwicklungskosten !! >*

*< Keine Schulung der „normalen“ Benutzer !! >*

# Kostenkomponenten (2)

## ■ Anschlusskosten (Roll-Out)

- ▶ Fachliche Anwendungsbetreuung (30%)
  - ▶ Koordination und Kommunikation
  - ▶ Abschluss Leistungsvereinbarung (inkl. Take-On-Template)
  - ▶ Funktionaler Test
  - ▶ Funktionale Dokumentation
- ▶ Technische Anwendungsbetreuung (30%)
  - ▶ Durchführung der Anbindung
  - ▶ Test der Anbindung
  - ▶ Technische Dokumentation
- ▶ Systemverantwortlicher IT-System (40%)
  - ▶ Abschluss Leistungsvereinbarung
  - ▶ Lieferung Systemdaten
  - ▶ Funktionaler Test, Abnahme

*< Abhängig von Anbindungsart, Komplexität der Rechtestruktur und des Workflows (10-40 PT pro System) !! >*

# Kostenkomponenten (3)

## ■ Laufende Kosten

- ▶ Anwendungsbetreuung funktional (20%)
  - ▶ Funktionale Pflege und Weiterentwicklung
  - ▶ Generelle funktionale Fragen und Probleme
  - ▶ Kontrollfunktion, spezielle Auswertungen
- ▶ Anwendungsbetreuung technisch (20%)
  - ▶ Wartung und Betreuung
  - ▶ Technische Fragen und Probleme
- ▶ Systemadministration (30%)
  - ▶ Interne Systemadministration
  - ▶ Fragen und Probleme Systembenutzer
- ▶ Hardwarekosten (15%)
  - ▶ Entwicklungs-, Test- und Produktionsumgebung
- ▶ Softwarekosten (15%)
  - ▶ Lizenzgebühren, Professional Service

*< Ohne Anschlusskosten, diese wurden bereits separat berücksichtigt !! >*

# Kostenkomponenten (4)

- Refinanzierung
  - ▶ Projektkosten
    - ▶▶ IT-Dienstleister/Anwendungsverantwortlicher per Umlage
    - ▶▶ Hauptnutzerträger per Verrechnung des Nutzens
  - ▶ Anschlusskosten (Roll-Out)
    - ▶▶ Standard: Jede Partei trägt den eigenen Aufwand
    - ▶▶ Non-Standard: Zusatzleistungen müssen separat vereinbart und vom Systemverantwortlichen des IT-Systems getragen werden
  - ▶ Laufende Kosten
    - ▶▶ IT-Dienstleister/Anwendungsverantwortlicher per Umlage

*< Direkt zurechenbarer Nutzen sollte verrechnet werden !! >*

*< Beidseitige Bestätigung als Voraussetzung !! >*

*< Umlageverfahren meist leichter durchzusetzen !! >*

# Weitere Erfahrungen aus Projekten (1)

- Grunderkenntnis: Auswahl des „richtigen“ Werkzeuges ist wichtig, aber allein noch nicht ausreichend
- Organisatorische und technische Voraussetzungen
  - ▶ Transparenz über das jeweilige Berechtigungskonzept der anzuschließenden IT-Systeme
  - ▶ Inhaltlich und organisatorisch standardisierte Antragsworkflows der anzuschließenden IT-Systemen -> Änderung von Prozessen gleichzeitig mit deren „Elektronifizierung“ schafft zusätzliche Risiken
  - ▶ Verfügbarkeit und Aktualität der benötigten Personendaten
  - ▶ Verfügbarkeit und Aktualität der benötigten Organisationsdaten
  - ▶ Verfügbarkeit und Aktualität der benötigten Berechtigungsdaten
  - ▶ Klare und handhabbare Unterschriftenregelung innerhalb des Unternehmens (inkl. Vertreterregelung, virtuelle Organisationseinheiten z.B. Projekte)

# Weitere Erfahrungen aus Projekten (2)

## ■ Organisatorische und technische Voraussetzungen

- ▶ Die verschiedenen IT-System-Accounts einer Person lassen sich z.T. schlecht automatisiert zuordnen (fehlender Schlüssel, unterschiedliche Schreibweise) -> hoher manueller Aufwand
- ▶ Akzeptanz aller Workflow-Beteiligten (Antragsteller, Freigeber, Administrator)
- ▶ Für den Einsatz von Agenten müssen die vorhandenen technischen Anforderungen der IT-Systeme vollständig abbildbar sein (z.T. auf Parameterebene)
- ▶ Hohe Anforderungen an die Stabilität und Korrektheit der Agenten
- ▶ Gutes Einführungskonzept (Marketing, Kommunikation und Schulung)

## ■ Projektumfang/Einführung

- ▶ Pragmatisches Vorgehen bei der Auswahl der zu realisierenden Funktionalität
  - ▶ Stufenweise Einführung (Antragsverfahren, Reports, Konnektoren)
  - ▶ Unterstützung von Standardfälle (Workflow, Antragstemplates, ...)
  - ▶ Sonderfälle (systemseitig und organisatorisch) weiter manuell durchführen
  - ▶ Längere Pilotphase mit „gutwilligen“ Benutzern vor Start des Roll-Outs



# Praktische Übung

- Ermittlung der unternehmensspezifischen IST-Situation (mittels Fragebogen)
- Vorstellung der Kernpunkte
- Auswertung und gemeinsame Diskussion
- Erarbeitung eines Leitfadens -> Handlungsempfehlungen zur Umsetzung in der Praxis (Dr. Horst Walther, letzter Teil der Veranstaltung)

# Fragen, Anregungen, Hinweise?

