Gesetzliche Vorgaben, Standards und Richtlinien in IdM- und Compliance-Projekten

Agenda

- Kurze Firmenvorstellung Omada
- Allgemeine Herausforderungen des Identity Managements
- Gesetzliche Vorgaben, Standards und Richtlinien
- Beispiele für die Umsetzung

Vorstellung von Omada

Vorstellung Omada A/S

- **Omada ist einer der führenden europäischen Hersteller im Bereich Identity Management, Governance und Compliance**
- Wir bieten eine integrierte unternehmensweite IAM und IAG-Lösung für Mainframe, Unix/Linux, Microsoft-, SAP- und andere Plattformen
- Gegründet 1999 in Kopenhagen, Dänemark
- Die Gründer kommen aus dem SAP Umfeld, SAP Implementierungen ist zweites Standbein der Omada
- 150+ Kunden, viele große und globale Kunden
- Weltweiter Microsoft Partner of the Year for "Security Solutions, Identity and Secure Access" 2008, 2009 und 2011
- Internationale Präsenz mit Omada Büros in den USA und Europa und ein weit ausgebautes Partnernetzwerk
- Mit Kundenprojekten viele Identity Management-Preise gewonnen – u.a. 2009 Ecco (Kuppinger&Cole), 2010 BMW (Kuppinger&Cole), 2011 Vattenfall (IT-Verlag), 2013 HVB/Unicredit (Kuppinger&Cole)

Das macht Omada aus

- Unternehmen
  - Privates Unternehmen aus Dänemark, kein Shareholder Value Denken, persönliches Commitment der Eigentümer
  - Mit kontinuierlichem Wachstum seit 1999, stabilen Umsätzen und >150 Kunden dennoch ein stabiler Player im Markt
  - Klarer Fokus durch Konzentration auf IAM & IAG und SAP-Einführungen
- Technik
  - Produktentwicklung in Kopenhagen – keine Entwicklung in Indien, China, USA
  - IAM & IAG Lösung aus einem Guss (daher z.B. stets Konsistenz aufgrund einheitl. Datenbasis)
  - Nähe zu Microsoft (Einsatz in quasi jedem Unternehmen)
- Referenzen
  - Mittelständler wie Comdirect, HUF & Hülsbeck Schließsysteme, ... bis zu Konzernen wie Bayer AG, BMW
  - Zahlreiche Auszeichnungen, hoher Respekt von Gartner, Microsoft und Kuppinger
- Kosten
  - Faire Preisgestaltung für Lizenzen & Wartung
  - Geringe Einführungskosten (moderne Architektur, z.B. für Report-Erstellung, Templates, ...)
- Sicherung eines geringen Projektrisikos
  - Kurzer Draht unserer Kunden zur Geschäftsführung, CEO/CTO
  - Erzielt überdurchschnittlich hohe Akzeptanz bei den Usern, durch unsere Spezialisten für „Ergonomie der Benutzeroberfläche"

Ausgewählte Kundenreferenzen

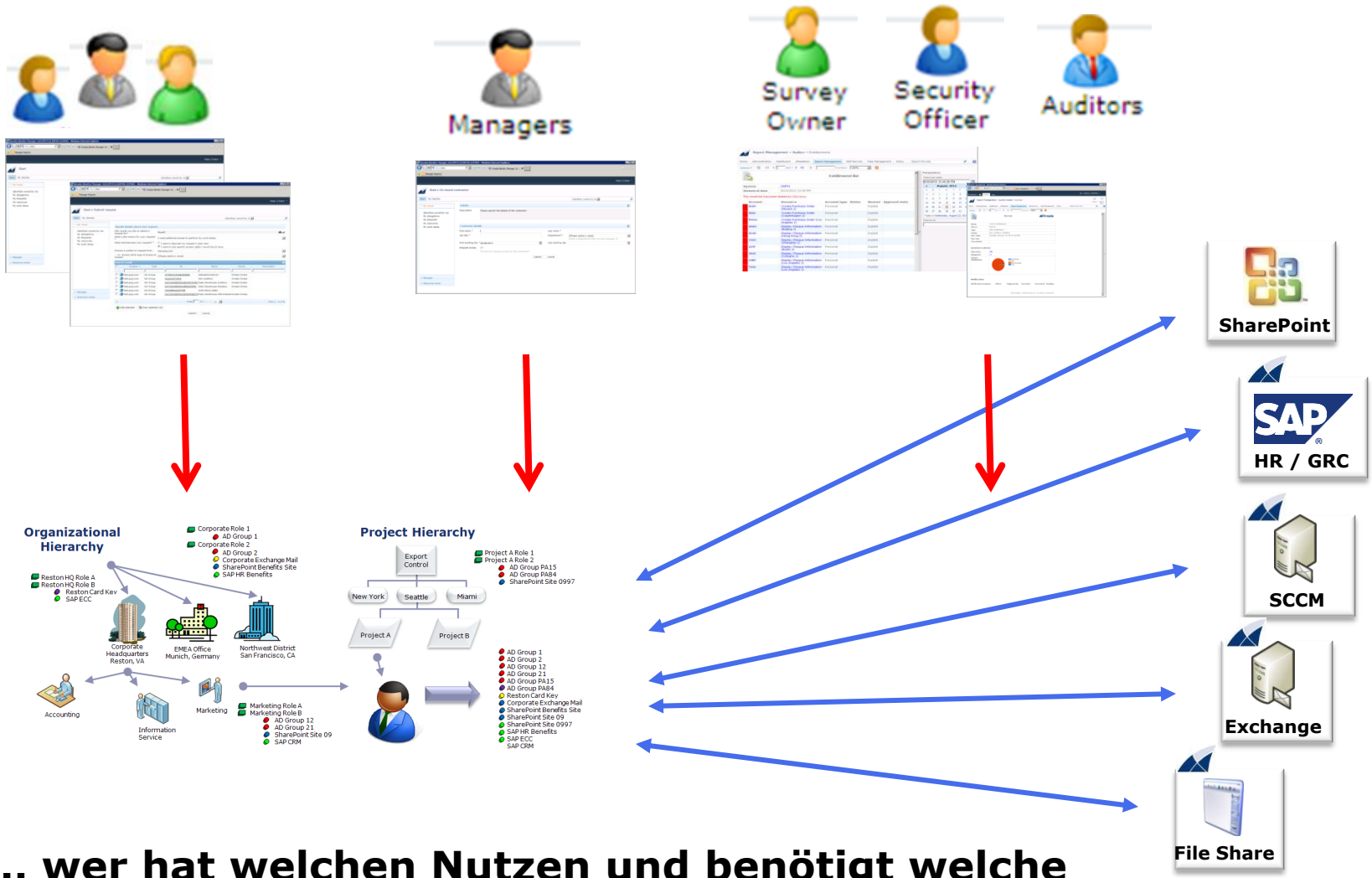
Omada

Allgemeine Herausforderungen des Identity Managements

Schlagworte

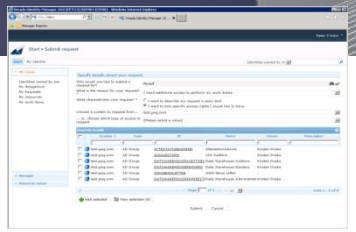
- Automatisierung
- Identity Management
- Entitlement Management
- Role Based Access Control
- Attribute Based Access Control
- User Provisioning
- Identity Life Cycle
- Roles & Rules
- SoD/ Toxic Combinations
- Soll-/Ist-Abgleich
- Violation Management
- Delegated Administration
- Eskalationsmechanismen
- Ein-/Mehrstufige Genehmigungen
- Historisierung
- Nachvollziehbarkeit von Rechtevergaben
- Compliance
- Reporting
- Rezertifizierungen
- Webshop
- …

Thema ist immer …



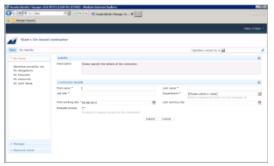
… wer hat welchen Nutzen und benötigt welche Informationen.

… oder anders dargestellt – der "User Life Cycle"

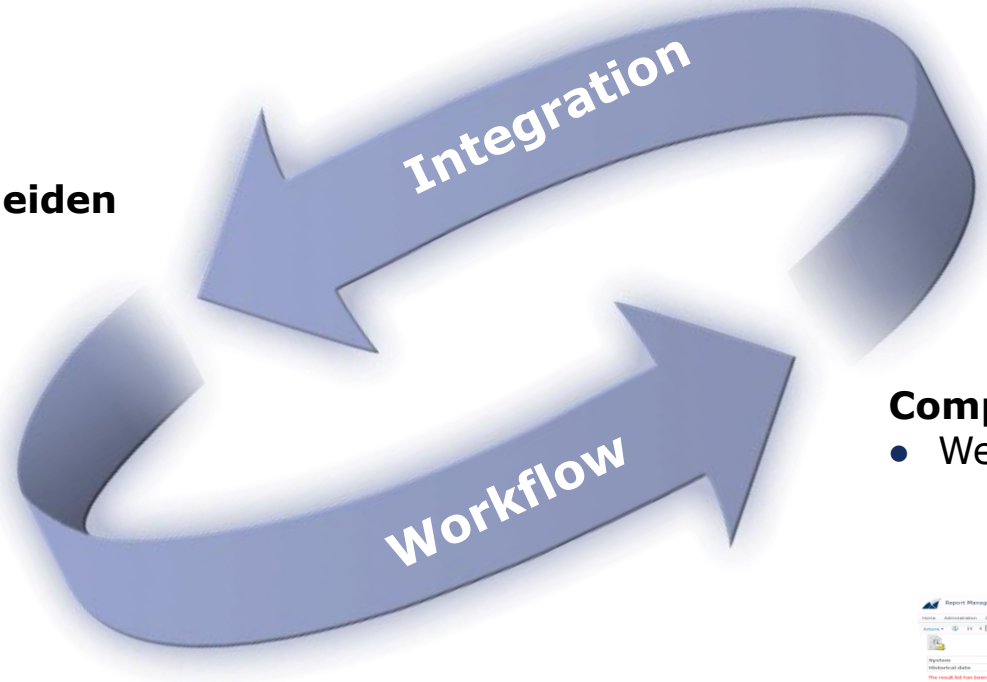


Self Service portal
- Anträge
- Überblick

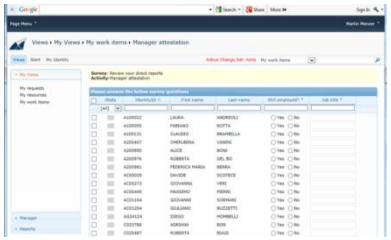
Manager Genehmigung
- Anträge
- Überblick

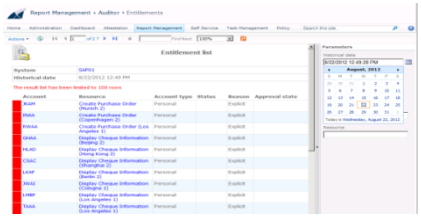


Einstellung/Aus-scheiden von Usern
- Erzeugung von User IDs
- Rollen-basierte Zugriffsrechte



Compliance Reporting
- Wer hat Zugriff und warum





Compliance Rezertifizierung
- Sind die Mitarbeiter noch im Team
- Passen die Rechte noch

Gesetzliche Vorgaben, Standards und Richtlinien

Gesetzliche Anforderungen & Prüfungsfragen

- Gesetzliche Anforderungen
  - HGB - Handelsgesetzbuch
  - AktG - Aktiengesetz
  - GoBS - Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
  - KonTraG - Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (Früherkennung von Risiken)
  - MaRisk - Mindestanforderungen an das Risikomanagement
  - FDA – Regulatorien in der Pharma und Lebensmittel-Industrie
  - HIPAA – Regulatorien im Bereich Healthcare
  - … (ISO, etc.)
- Prüfungsfragen in der wichtigsten Bereichen

  (*Betriebssysteme, Internet/E-Commerce, Anwendungsprogramme)*
  - Berechtigungsstruktur, -analyse
  - Was macht der Administrator ? ...
- Prüfungsfragen bzgl. Daten/Datenträger/Datenbanken/DateWareHouse
  - Datenschutz (Identifizierung, Wer-hat-Zugriff) ...
- Prüfungsfragen bzgl. Rechenzentrumsbetrieb
  - Zutrittskontrolle zum RZ ...
- Methodisch Schwerpunkte der DV-/IT- Revision
  - Berechtigungskonzept, z.B.: Funktionstrennung, Wechsel von kritischen Berechtigungen

Typische Pain Points & Ursachen

- Pain Points
  - Intransparenz auf vergebene Berechtigungen
  - Intransparenz auf „Legalisierungen“ (Anträge/Freigaben nicht nachvollziehbar)
  - Überberechtigungen
  - Verstöße gegen aufsichtsrechtliche (MaRisk bei Finanzinstituten) oder interne Funktionstrennungsvorgaben
  - Berechtigungsprobleme bei einzelnen Systemen, v.a. SAP, Windows-AD, Filesystem, Sharepoints, aber auch Anwendungen u.a.
  - Keine periodische Qualitätssicherung („Rezertifizierung“)

- Ursachen hierfür
  - Zu viele privilegierte Accounts
  - Einzelne nachweisbare Überberechtigungen
  - Vergaben nicht mehr nachvollziehbar
  - Rechte im Unternehmen „mitgenommen“ aus anderen Abteilungen („Azubi-Effekt“)
  - Rechte von „Referenzusern“ unangemessen übernommen
  - Vorhandene Rechte insgesamt intransparent
  - Rechte nicht nach Business-Funktionen organisiert

Beispielhafte Fragen von Auditoren (Verwaltung von Benutzerrechten)

Prüfungsfeststellungen

- Unzureichende bzw. lückenhafte Antrags- bzw. Genehmigungsverfahren
- Keine Prüfung auf Funktionstrennung bei Genehmigungen
- Verwendung bestehender User als Referenzbenutzer („Berechtigung wie Müller“)
- Unzureichende bzw. lückenhafte Prozesse bei Mitarbeiterwechsel
- Kein Entzug von Berechtigungen aus ehemaliger Funktion bei Mitarbeiterwechseln
- Unzureichende Transparenz über Personen und deren Accounts bzw. deren Zugehörigkeit zu Org-Einheiten
- Keine Prozesse zum Benutzerreview
- Fehlende Transparenz über administrative bzw. technische User
- Keine bzw. unzureichende Funktionstrennung bei administrativen Tätigkeiten

Quelle: MaRisk konformes Berechtigungsmanagement / KPMG Advisory / Alfred Koch, Senior Manager / 2011

Beispielhafte Fragen von Auditoren (Verwaltung von Authorisierung)

Prüfungsfeststellungen

- Unzureichende bzw. lückenhafte Richtlinie, Verfahrensdokumentationen, Prozesse und Kontrollen
- Fehlende, veraltete bzw. unzureichende Berechtigungskonzepte, kein Prozess zum Review von Berechtigungen
- Fehlende Einbindung der Fachbereiche bei der Definition von Funktionstrennungen
- Fehlende Einbindung der Fachbereiche bei der Definition von Rollen, Berechtigungsgruppen bzw. Sammelprofilen
- Keine bzw. unzureichende Überprüfung auf Funktionstrennung bei der Definition von Rollen, Berechtigungsgruppen bzw. Sammelprofilen
- Keine bzw. unzureichende systemübergreifende bzw. prozessuale Sicht bei der Definition von Funktionstrennungen
- Unzureichende Berücksichtigung von rechtlichen und regulatorischen Anforderungen (z.B. Funktionstrennung MaRisk)
- Nutzung von Sammel- bzw. Gruppenkonten für administrative Aufgaben

Quelle: MaRisk konformes Berechtigungsmanagement / KPMG Advisory / Alfred Koch, Senior Manager / 2011

Beispiele von Angriffsmöglichkeiten in Unternehmen (Studie von AT Kearney)

Vorstandsbüro
Oft unzureichend vor physischem Zugriff etwa durch Reinigungspersonal oder Handwerker geschützt.

F&E
Meist größter Schutzbedarf in den Unternehmen, aber oft nicht besser geschützt als andere Bereiche.

Rechenzentrum
Zuverlässiger Ort für die private Cloud. Herausforderung: Der sichere Betrieb unzähliger Server inklusive der darauf laufenden Applikationen.

Lieferanten-Netzwerk
Immer engere Vernetzung mit Lieferanten als Risiko, denn kleinere Lieferanten sind meist schlechter geschützt.

Cloudcomputing
Eine externe Cloud ist grundsätzlich sicher. Probleme: Datenschutz außerhalb der EU, Geheimdienstzugriffe.

Produktion
Viele alte Spezialsysteme. Vermehrt vernetzt, aber schwer kontrollierbar. Bei Angriffen droht Produktionsausfall bis hin zur Zerstörung.

Datenbanken
Hier liegen wichtige Daten gut gesichert. Schwachstelle: als Angreifer instrumentalisierte Administratoren.

Endprodukt mit IT
Zunehmend vernetzte Endprodukte ermöglichen IT-Angriffe. Erpressungspotential durch von Hackern ferngesteuerte Produkte, die Unfälle provozieren. Reputationsverluste und Ansprüche der Opfer drohen.

Büro-Netzwerk
Zunehmend digitale Anbindung an fast alle Systeme. Wer einmal drin ist, hat viele Mög keiten.

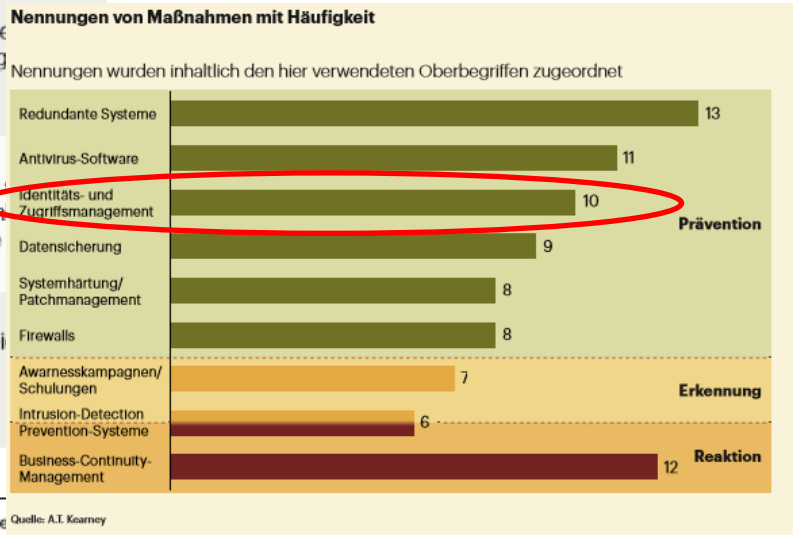
Vertrieb
Marketingpläne, Preise und Kundenkontaktdaten sind hochsensibel. Ihr Verlust zieht große Reputationsschäden nach sich und kann einen Vorsprung am Markt zerstören.

Mobile Endgeräte
Handelsübliche Smartphones: Oft voll mit Daten, immer leicht zu hacken und zu ste BYOD stellt bewährte Sicherheitskonzepte

Onlineshop
Kreditkarten- und Kundendaten werden für Betrugsdelikte, gestohlene Identitäten für IT-Angriffe genutzt.

Telefonate
Dank menschlicher Hilfsbereitschaft ein lei Einfallstor zur Informationsbeschaffung.

Quelle: A.T. Kearney



- Sämtliche Bereiche von Unternehmen sind betroffen
- Gefahren kommen von innen & aussen
- Identitäts- & Zugriffs-Management ist eine der etablierten Präventions-maßnahmen

Informationssiche

http://www.atkearney.de/content/veroeffentlichungen/whitepaper_detail.php/id/51908/practice/sitp

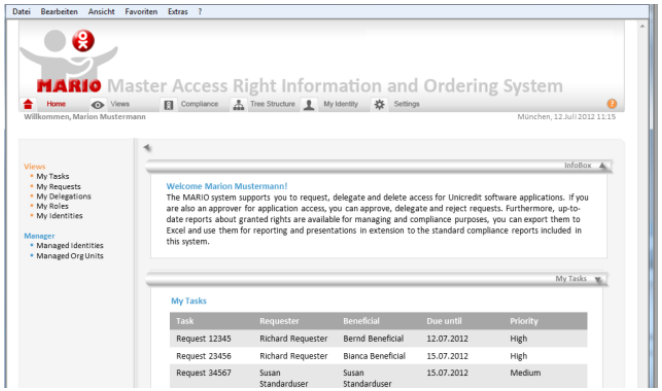
Resultierende Maßnahmen in der Benutzerverwaltung & Auditierung

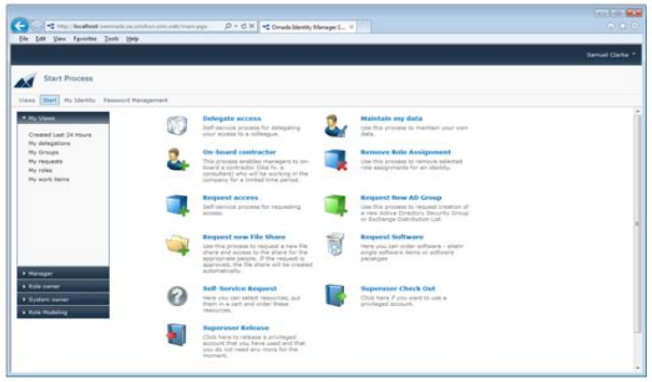
- **Automation** der Benutzerverwaltung über alle Kernapplikationen & Shares und damit geringere Gesamtkosten der Prozesse
- Steigerung der **Transparenz** von Genehmigungsprozessen & der Nachvollziehbarkeit von Änderungen (Auditfähigkeit)
- Regelmäßige Re-Zertifizierung von Rollen & Berechtigungen – abhängig von der Kritikalität – damit eine „**Access Governance**" als nächste Reifestufe zum klassischen Identity- und Access Management
- Reduzierung der **IT-Risiken** bzgl. Datenschutz, Data Loss und potentiellen Produktionsstörungen durch Rollenmanagement, SoD-Kontrollen und Privileged Account Management
- Vereinfachung von User-Interfaces zur Steigerung der **Self-Service** Rate
- Steigerung der **Benutzer-Zufriedenheit** durch schnellere Genehmigungen & Self Service Pflegemöglichkeiten

Beispiele für die Umsetzung

Einheitliches Self Service Portal für die Fachseite

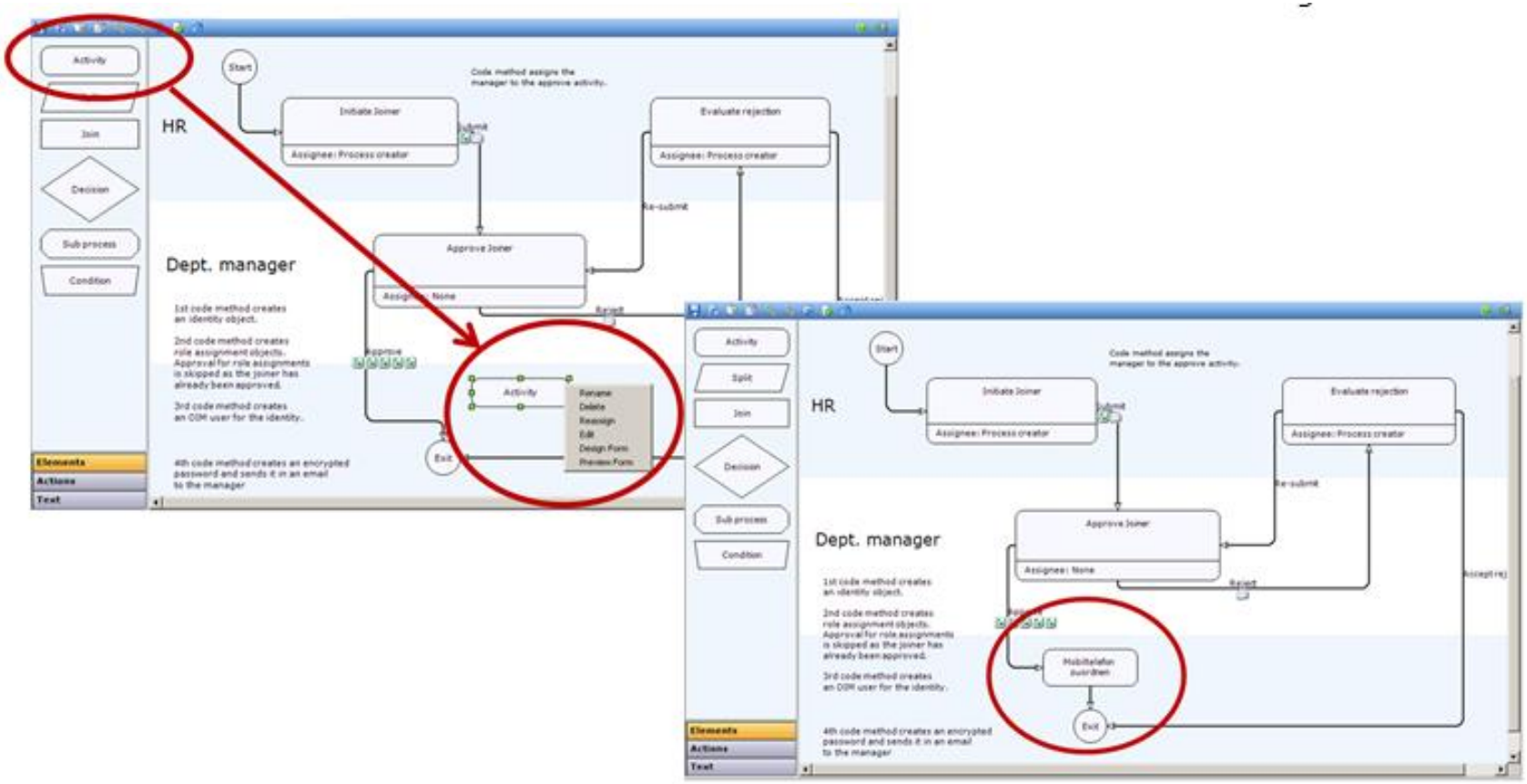
- Personalisierter Startpunkt der meisten Aktionen
- Angezeigte Optionen hängen von den Rechten des Benutzers ab
- Werden Rechte delegiert (Stellvertreterregelung), kommen temporär Optionen auf der Oberfläche hinzu und verschwinden wieder, nach Ablauf der Delegation





Automation über Prozesse

- Die Konfiguration erfolgt über Drag & Drop
- Aktivitäten und Masken werden ebenfalls über die Browser-Oberfläche konfiguriert

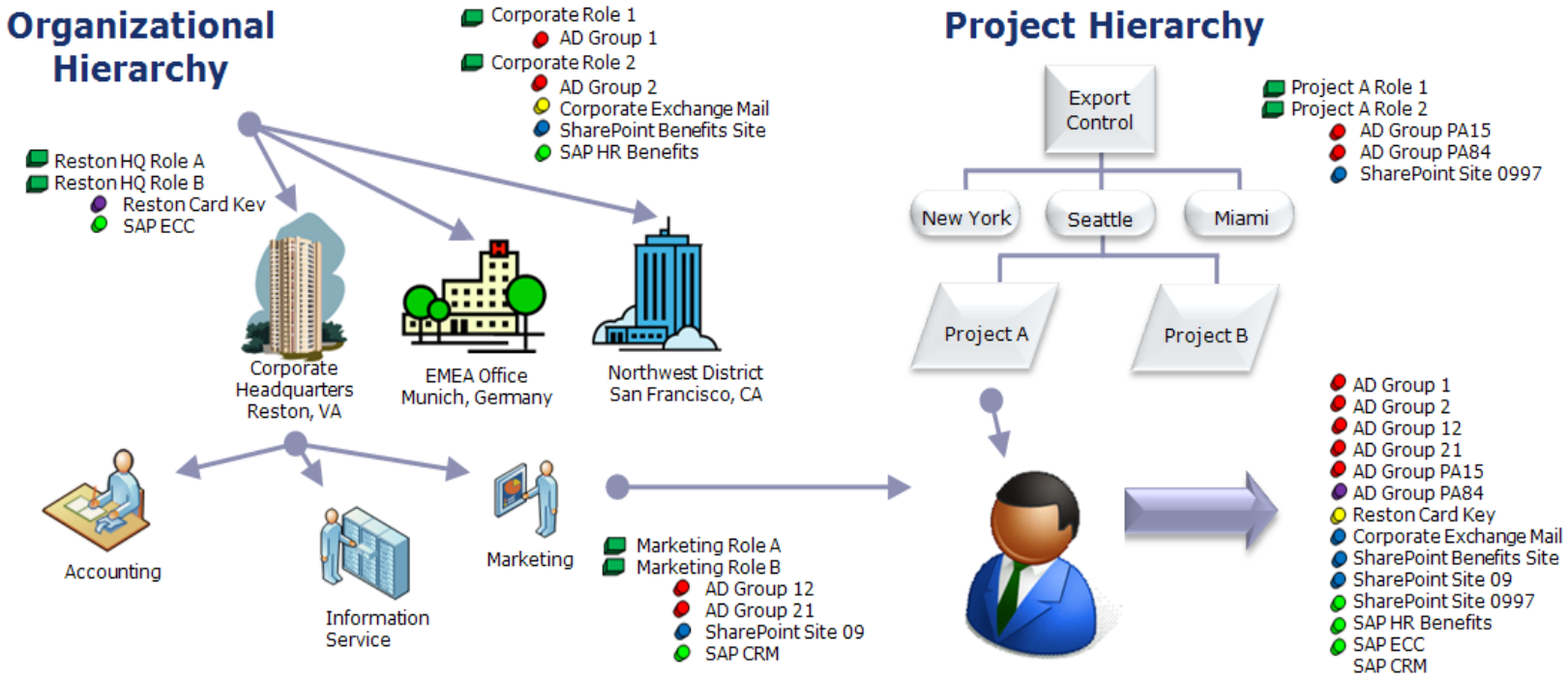


Automation über Prozesse (cont'd)

- Die vorkonfigurierten Workflows decken die üblichen Basisworkflows in Identity Management Projekten ab
- Dies Workflows können mit der vollen Leistungsfähigkeit des Workflow Designer angepasst und verändert werden

Rollen für Automation und Bündelung von Unternehmenswissen und -regeln

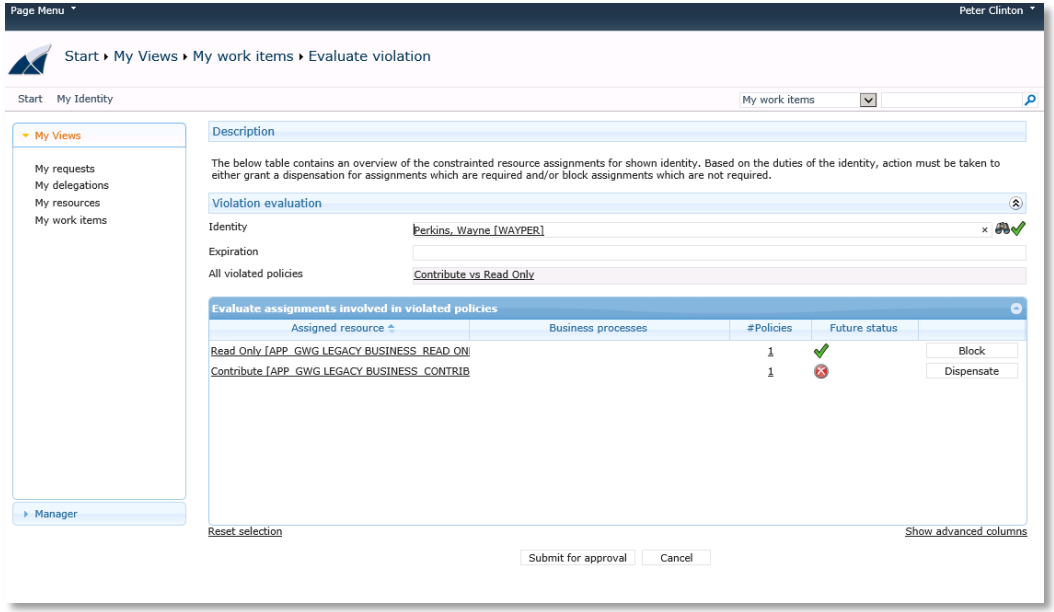
- Intensive Nutzung der Rollen und Strukturen zur Abbildung des Unternehmenswissens
- Rollendefinition auf mehreren Ebenen, intelligente Role Engine
- Ausschlussregeln und Trennung von Funktionen (SoD)

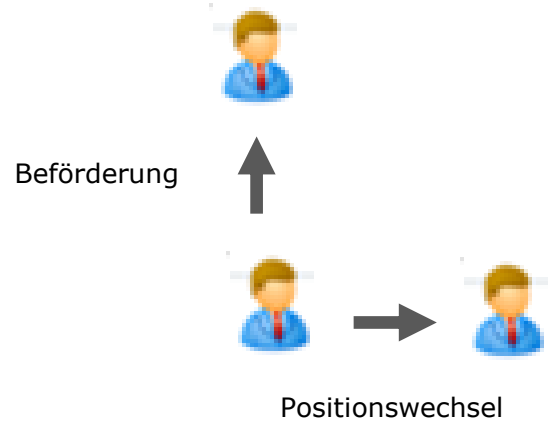


Erkennung von kritischen Kombinationen von Berechtigungen (SoD Verletzungen)

Beispiele von SoD Situationen

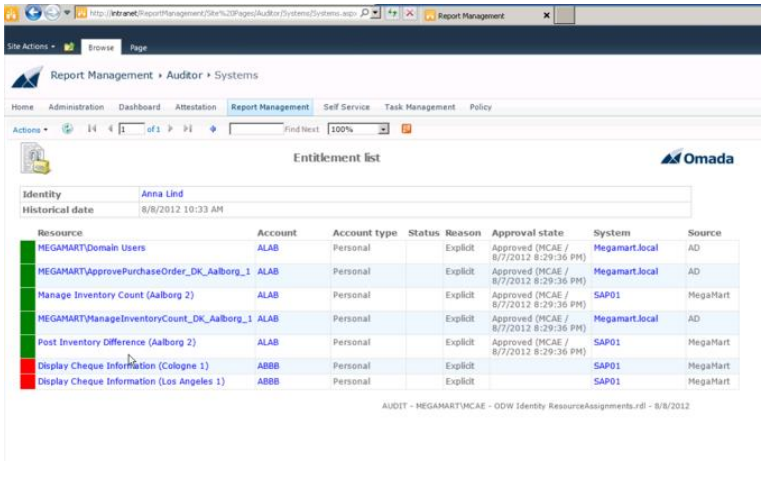
- Keine Funktionstrennung der Risikocontrolling-Funktion
- Beförderung (gleichzeitige Beantrager- & Genehmiger Rechte)
- Wechsel vom Handel ins Controlling
- Wechsel vom Front Office ins Back Office
- Wechsel vom Kreditorenbuchhalter nach Debitorenbuchhalter
- ...

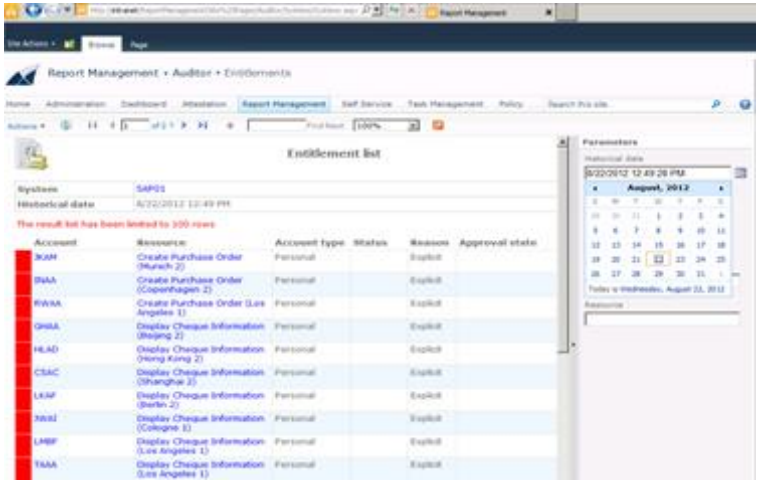


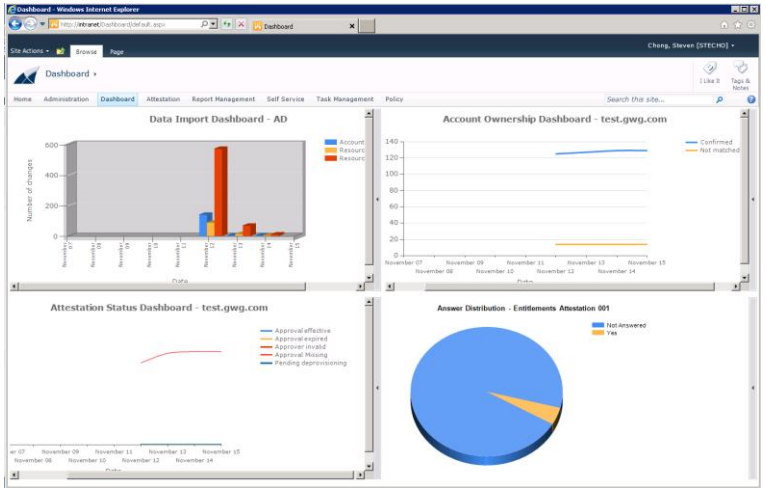


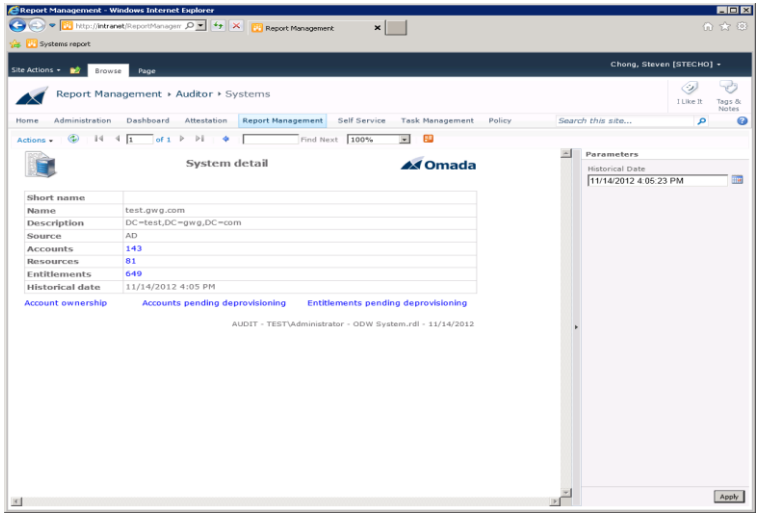
Screenshot der Omada Lösung:
Eingabe von SoD-Regeln

Transparenz - Intuitiver Überblick über die kompletten Berechtigungen





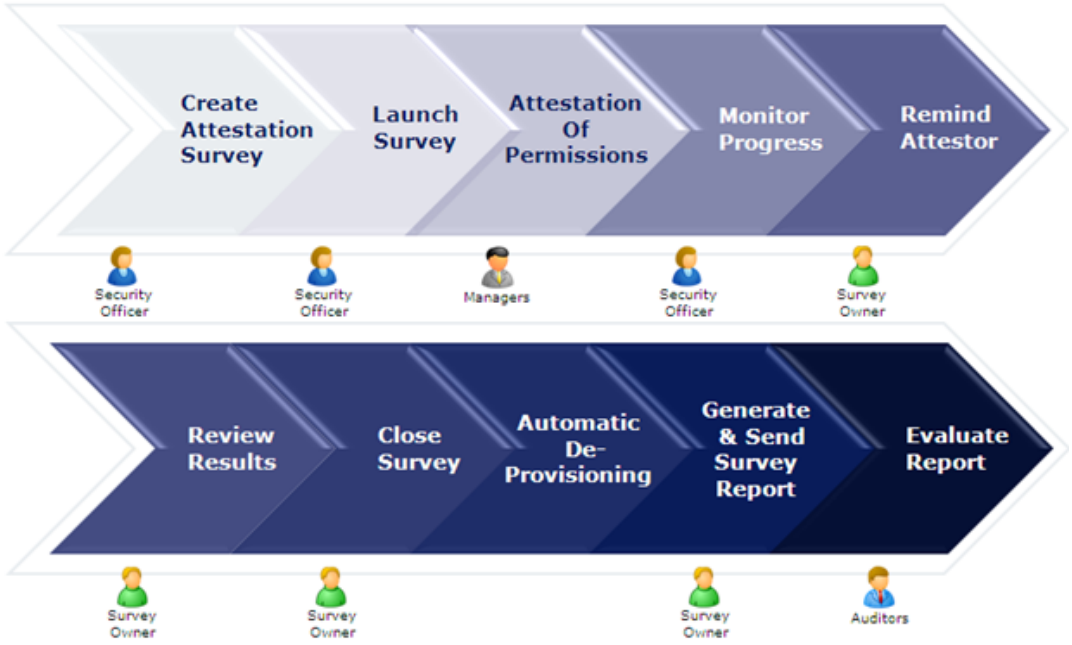




Überprüfung von Rechten – Re-Zertifizierung /Attestierung

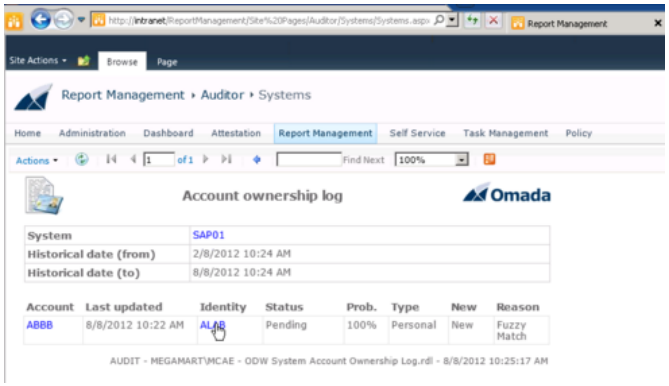
- Oft müssen Rechte und der Zugang zu Assets in Abständen überprüft werden – z.B. für AD und SAP
- Omada Identity Suite automatisiert den kompletten Prozess von der Definition des Surveys bis hin zur Erzeugung der Compliance Reports
- **Eine signifikante Reduktion von Fehlern, Kosten und Zeit** im Vergleich zur Attestierung auf Basis von manuellen Aktionen, Listen und Spreadsheets ist möglich.

- Delegation of attestation to system owners
- Escalation and notification options
- Attestation by line of business managers
- Dashboard for Survey Progress monitoring
- Scheduled, recurring or ad-hoc attestations
- Attest on financially significant permissions
- Attest on Segregation of Duties
- Attest on user permissions

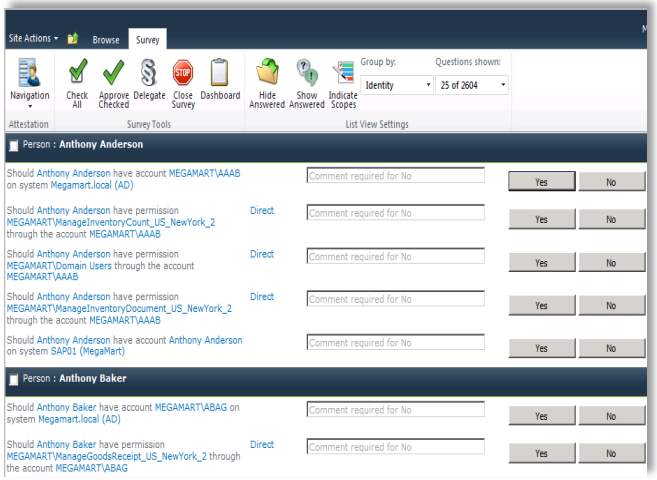


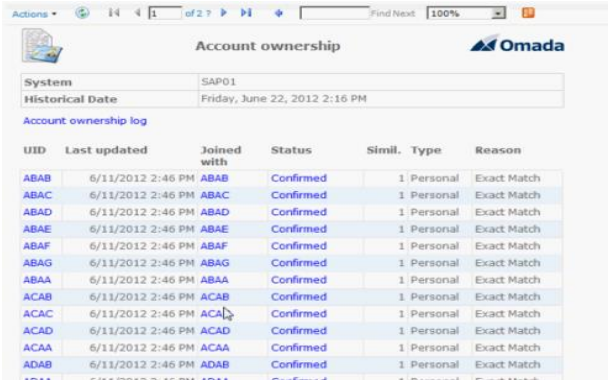
Ausprägung 1:
Zuordnung der Accounts und Bestätigung

- Unterstützung verschiedener Zuordnungsregeln für die Zuordnung von Accounts zu Identitäten
  - Exact Match
  - Custom Match
  - Fuzzy Match



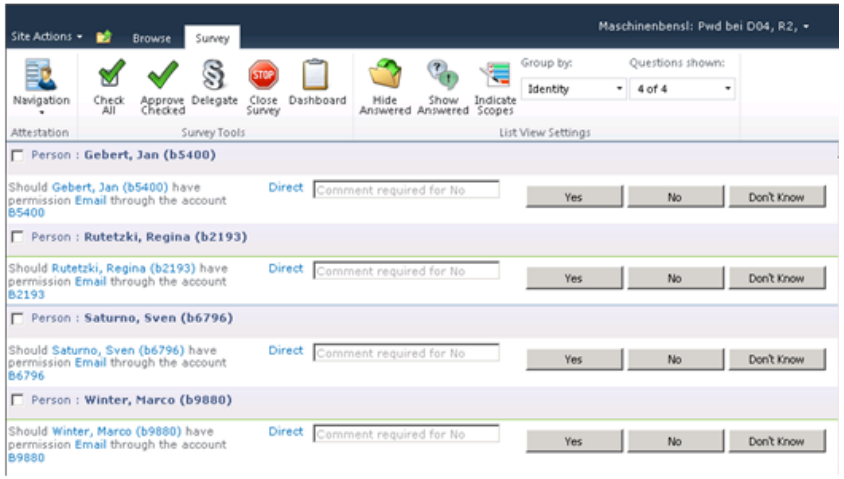
- Account Ownership Survey
  - Bestätigung der vorgeschlagenen Zuordnung





Ausprägung 2:
Rezertifizierung von Account, Entitlements, Rollen

- Surveys zur Überprüfung von
  - User Entitlements
  - Accounts
  - Permission Entitlements
  - Permissions



- Überprüfung der Qualität der Surveys
  - Dashboard mit Antwortverteilung
  - Zulassen der Antwort “Ich weiß nicht”
    -> Business Description Survey

Kontakt

Jutta Cymanek
Country Manager DACH & BENELUX

email: jcy@omada.net
Telefon: 06151 97197 58
Mobil: 0176 6125 8851

