



Omada

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

- ✦ **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)

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



DAYMON
WORLDWIDE

BMW Group



VATTENFALL



Bayer

Deloitte

HypoVereinsbank



MAERSK

AO Foundation



suva

.comdirect

Sydbank



DSM
BRIGHT SCIENCE. BRIGHTER LIVING.

Heraeus info systems



COMMERZ REAL
Commerzbank Gruppe



GRUNDFOS



Services



„DekaBank

DANISCO

DONG
energy



Transport
for London



KING'S
College
LONDON
University of London



NEUROSEARCH

MULTIDATA
FORSKELLEN ER MENNESKENE BAG

Sjællandske Medier

HOGESCHOOL
UTRECHT

MINISTRY OF ECONOMIC AND BUSINESS AFFAIRS
DENMARK

DANISH MINISTRY
OF THE ENVIRONMENT

Dansk Supermarked A/S

ENERGINET/DK



EITZEN GROUP



- Naturgas med varme



københavns E



PFA



UNIVERSITY OF SOUTHERN DENMARK



Danfoss
Universe

UMC St Radboud
met mensen kennis

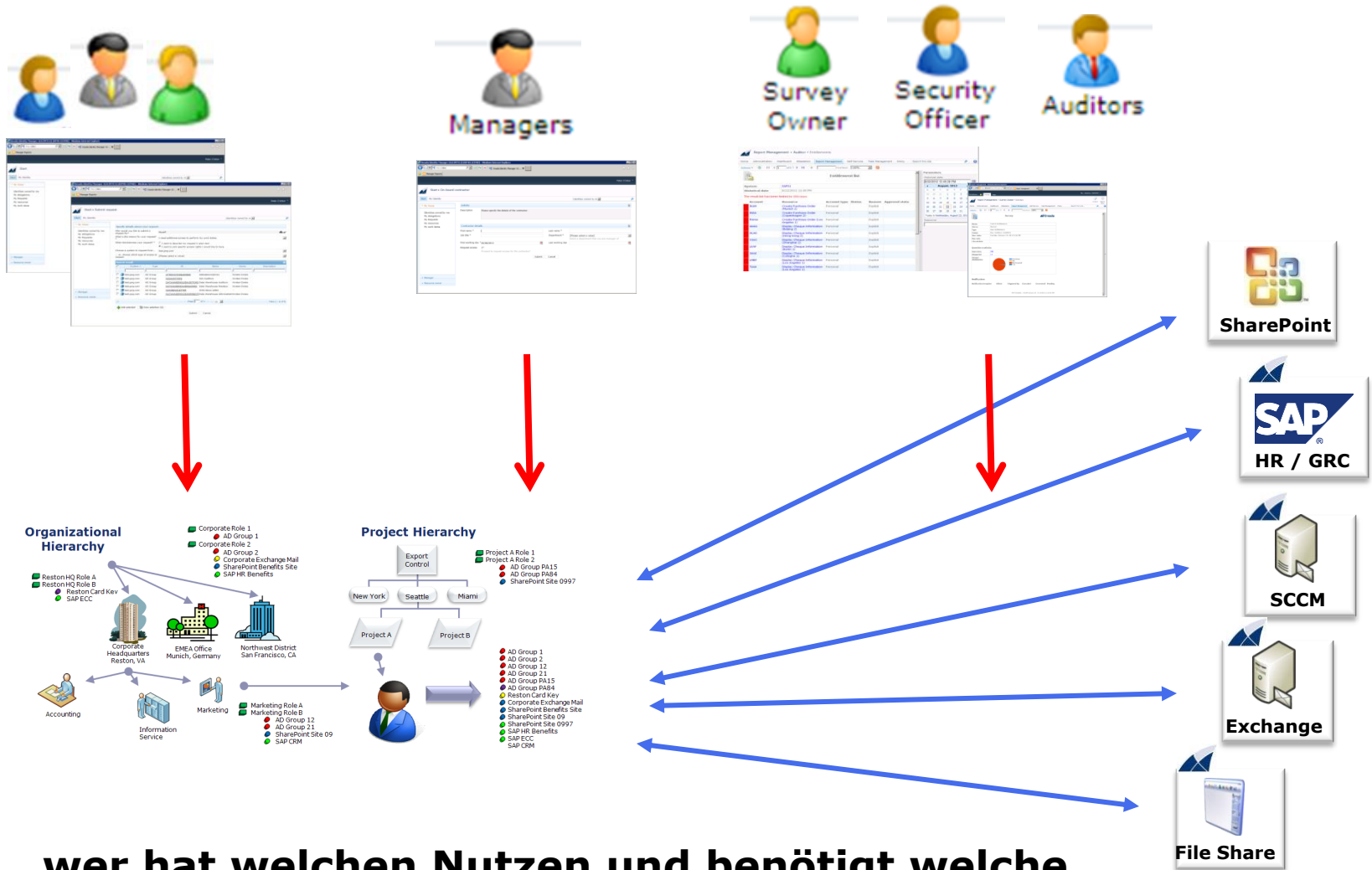
BMD
Bonnier Magazine Data A/S

AMAG
Austria Metall AG

Allgemeine Herausforderungen des Identity Managements

- 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 ...



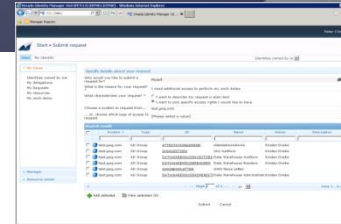
... wer hat welchen Nutzen und benötigt welche Informationen.

... oder anders dargestellt – der “User Life Cycle”



Self Service portal

- Anträge
- Überblick



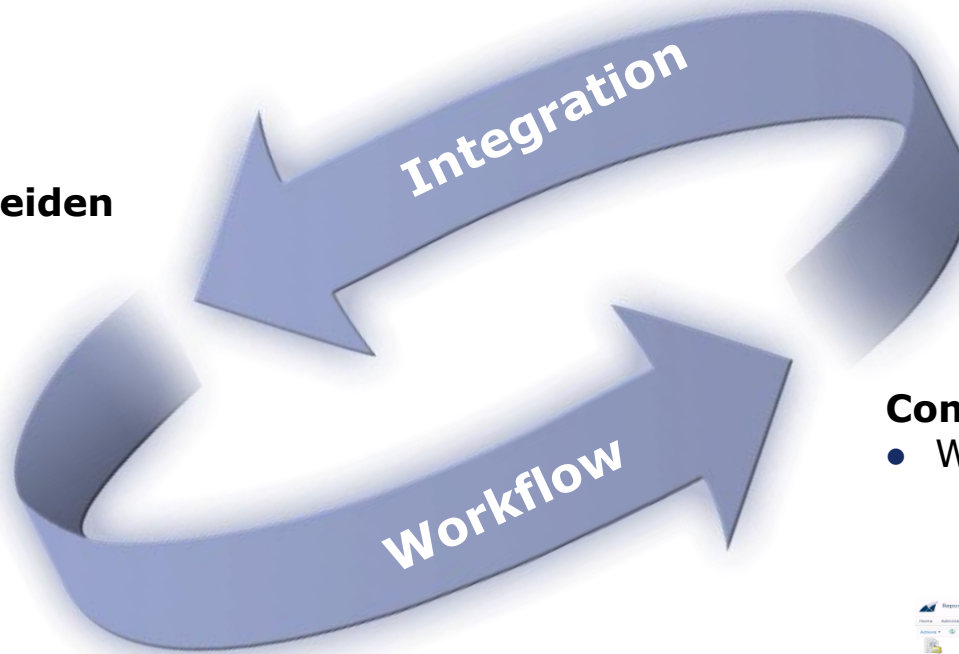
Manager Genemignung

- Anträge
- Überblick



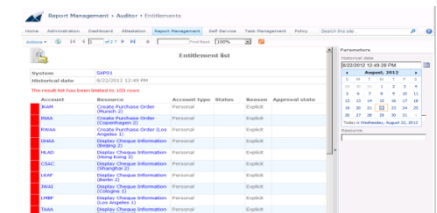
Einstellung/Aus-scheiden von Usern

- 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

- 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

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 Möglichkeiten.

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 Identitäts- und Zugriffsmanagement. BYOD stellt bewährte Sicherheitskonzepte

Onlineshop

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

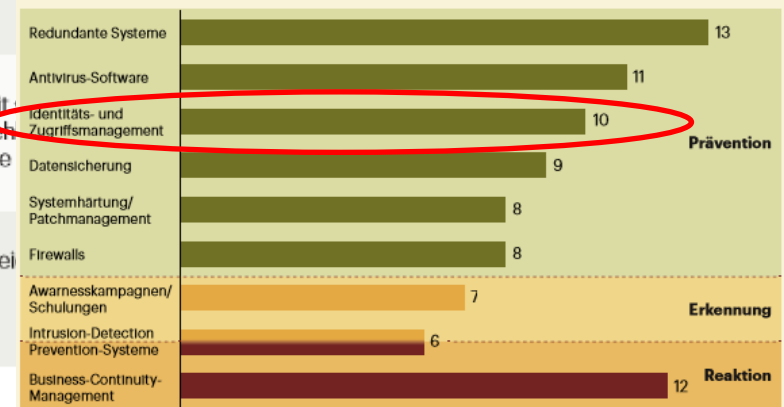
Telefonate

Dank menschlicher Hilfsbereitschaft ein leichtes Einfallstor zur Informationsbeschaffung.

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

Nennungen von Maßnahmen mit Häufigkeit

Nennungen wurden inhaltlich den hier verwendeten Oberbegriffen zugeordnet



Quelle: A.T. Kearney

Informationssicherheit

Quelle: A.T. Kearney

Resultierende Maßnahmen in der Benutzerverwaltung & Auditierung



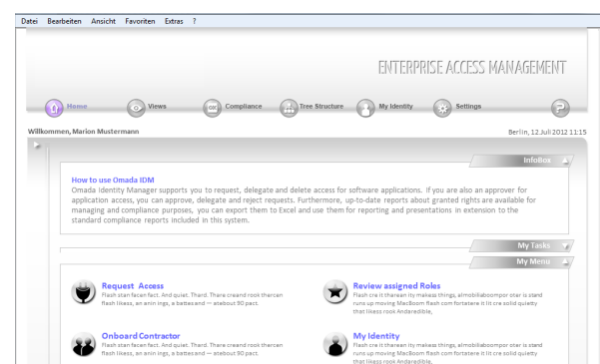
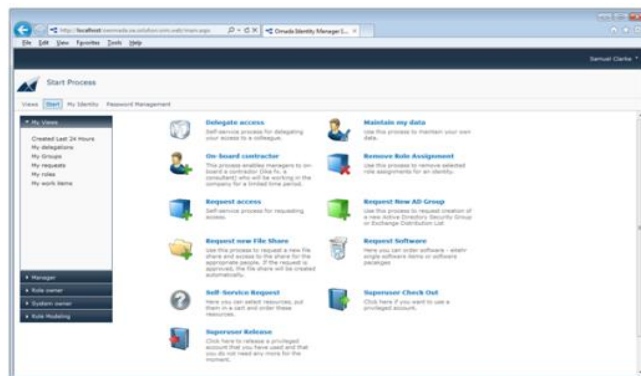
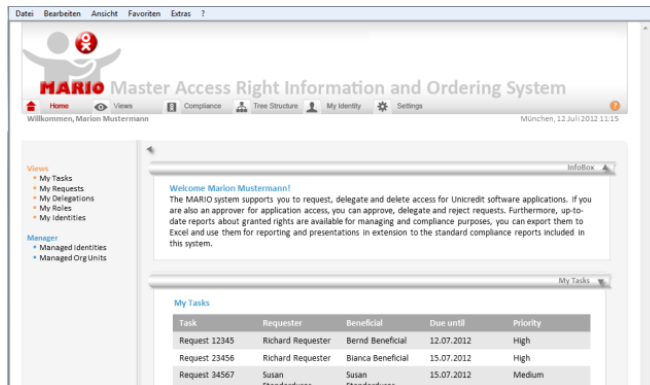
- ✦ **Automation** der Benutzerverwaltung über alle Kernapplikationen & Shares und damit geringere Gesamtkosten der Prozesse
- ✦ Steigerung der **Transparenz** von Genehmigungsprozessen & der Nachvollziehbarkeit von Änderungen (Auditfähigkeit)
- ✦ Regelmäßige Re-Zertifizierung von Rollen & Berechtigungen – 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

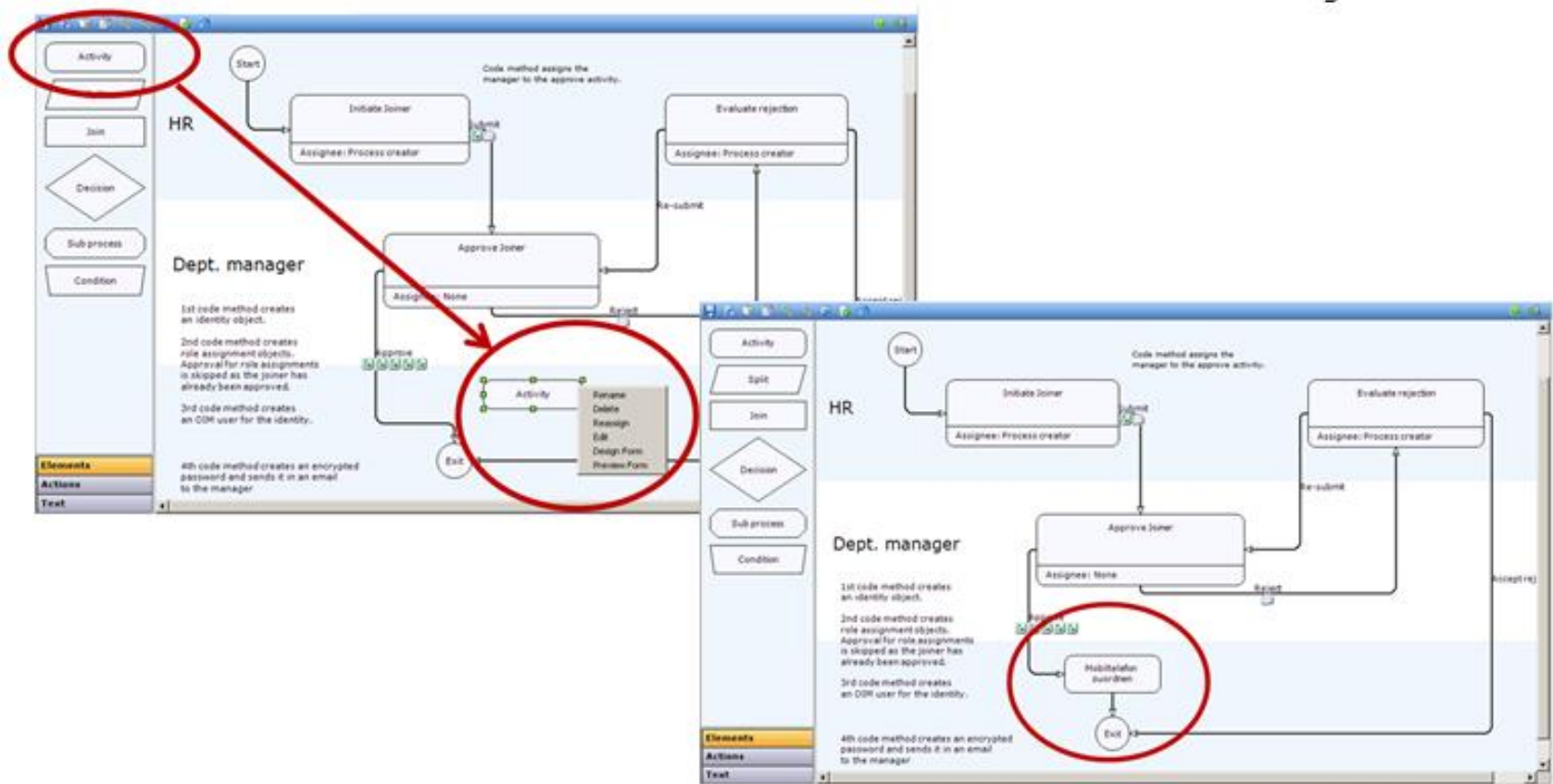


- Personalisierter Startpunkt der meisten Aktionen
- Angezeigte Optionen hängen von den Rechten des Benutzers ab
- Werden Rechte delegiert (Stellvertreterregelung), kommen temporär Optionen auf der Oberfläche hinzu und verschwinden wieder, nach Ablauf der Delegation



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

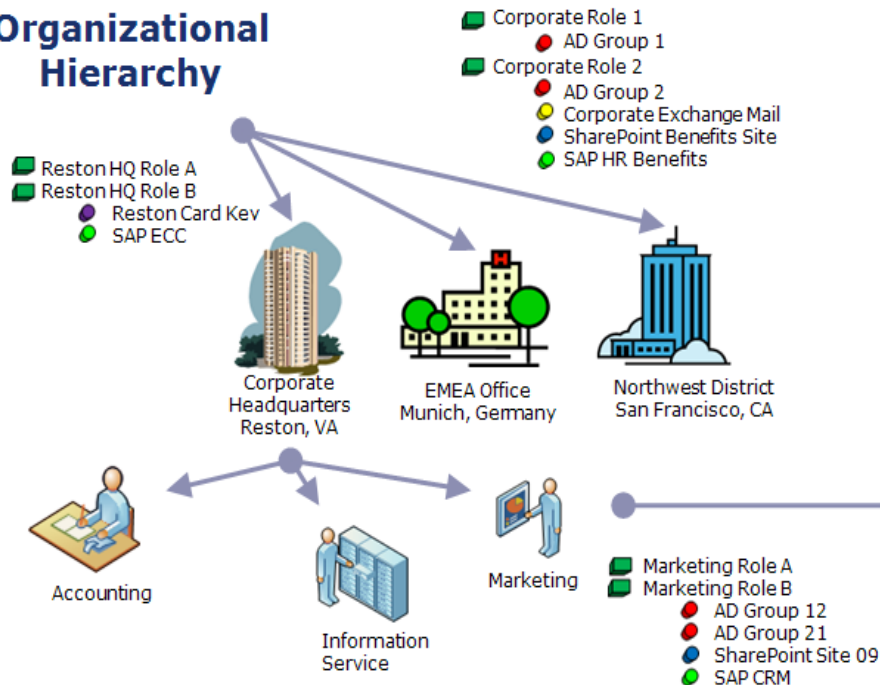
3.6	Process Templates (Scenarios)	13
3.6.1	On-Board Employee.....	14
3.6.2	On-Board Contractor	15
3.6.3	Transfer Identity	17
3.6.4	Request Access.....	19
3.6.5	Approve Role Assignments (One Step)	21
3.6.6	Approve Role Assignments (Two Steps).....	22
3.6.7	Review Assigned Roles.....	24
3.6.8	Delegate Access.....	25
3.6.9	OIS Management.....	27
3.6.10	Manual Provisioning.....	32
3.6.11	Evaluate Violation	36

Rollen für Automation und Bündelung von Unternehmenswissen und -regeln

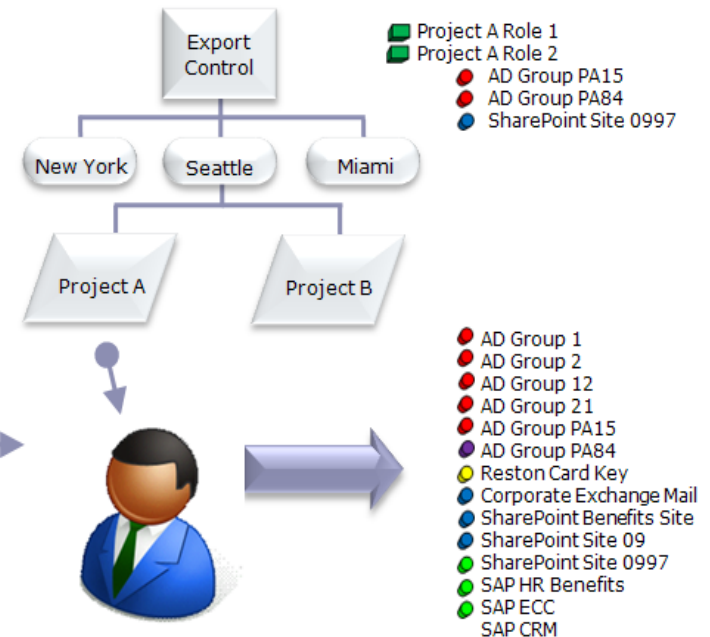


- Intensive Nutzung der Rollen und Strukturen zur Abbildung des Unternehmenswissens
- Rollendefinition auf mehreren Ebenen, intelligente Role Engine
- Ausschlussregeln und Trennung von Funktionen (SoD)

Organizational Hierarchy



Project Hierarchy



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
- ...

Page Menu Peter Clinton

Start > My Views > My work items > Evaluate violation

Start My Identity My work items

My Views

- My requests
- My delegations
- My resources
- My work items

Manager

Description

The below table contains an overview of the constrained resource assignments for shown identity. Based on the duties of the identity, action must be taken to either grant a dispensation for assignments which are required and/or block assignments which are not required.

Violation evaluation

Identity: Perkins, Wayne [WAYPER] x 00 ✓

Expiration:

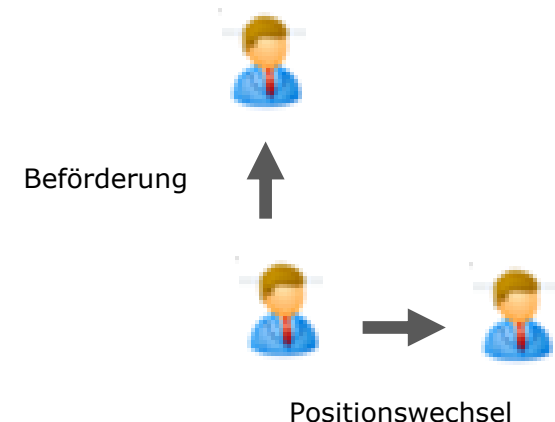
All violated policies: Contribute vs Read Only

Evaluate assignments involved in violated policies

Assigned resource	Business processes	#Policies	Future status	
Read Only [APP_GWG_LEGACY_BUSINESS_READ_ON]		1	✓	Block
Contribute [APP_GWG_LEGACY_BUSINESS_CONTRIB]		1	✗	Dispensate

Reset selection Show advanced columns

Submit for approval Cancel



Screenshot der Omada Lösung:
Eingabe von SoD-Regeln

Transparenz - Intuitiver Überblick über die kompletten Berechtigungen



Report Management - Auditor - Systems

Entitlement list

Identity: Anna Lind
Historical date: 8/8/2012 10:33 AM

Resource	Account	Account type	Status	Reason	Approval state	System	Source
MEGAMART\Domain Users	ALAB	Personal			Approved (MCAE / 8/7/2012 8:29:36 PM)	Megamart.local	AD
MEGAMART\ApprovePurchaseOrder_DK_Aalborg_1	ALAB	Personal	Explicit		Approved (MCAE / 8/7/2012 8:29:36 PM)	Megamart.local	AD
Manage Inventory Count (Aalborg 2)	ALAB	Personal	Explicit		Approved (MCAE / 8/7/2012 8:29:36 PM)	SAP01	MegaMart
MEGAMART\ManageInventoryCount_DK_Aalborg_1	ALAB	Personal	Explicit		Approved (MCAE / 8/7/2012 8:29:36 PM)	Megamart.local	AD
Post Inventory Difference (Aalborg 2)	ALAB	Personal	Explicit		Approved (MCAE / 8/7/2012 8:29:36 PM)	SAP01	MegaMart
Display Cheque Information (Cologne 1)	ABBB	Personal	Explicit		Approved (MCAE / 8/7/2012 8:29:36 PM)	SAP01	MegaMart
Display Cheque Information (Los Angeles 1)	ABBB	Personal	Explicit		Approved (MCAE / 8/7/2012 8:29:36 PM)	SAP01	MegaMart

AUDIT - MEGAMART\MCAE - ODW Identity ResourceAssignments.rdl - 8/8/2012

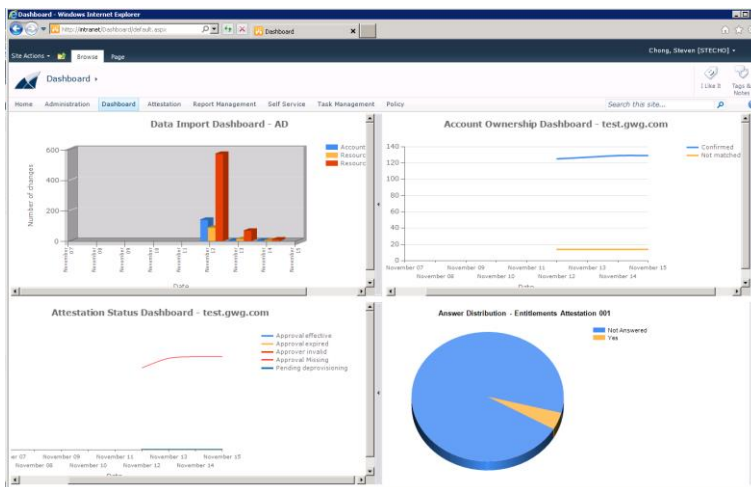
Report Management - Auditor - Entitlements

Entitlement list

System: SAP01
Historical date: 8/22/2012 12:49 PM

The result list has been limited to 300 rows

Account	Resource	Account type	Status	Reason	Approval state
3KAA	Create Purchase Order (Munich 2)	Personal	Explicit		
5NAA	Create Purchase Order (Copenhagen 2)	Personal	Explicit		
6VAA	Create Purchase Order (Los Angeles 1)	Personal	Explicit		
QMAA	Display Cheque Information (Shanghai 2)	Personal	Explicit		
4LAD	Display Cheque Information (Hong Kong 2)	Personal	Explicit		
CSAC	Display Cheque Information (Shanghai 2)	Personal	Explicit		
LSAF	Display Cheque Information (Berlin 2)	Personal	Explicit		
3MSI	Display Cheque Information (Cologne 1)	Personal	Explicit		
LMSE	Display Cheque Information (Los Angeles 1)	Personal	Explicit		
TAAA	Display Cheque Information (Los Angeles 1)	Personal	Explicit		



Report Management - Windows Internet Explorer

System report

Cheng, Steven [STECHE]

Report Management - Auditor - Systems

System detail

Short name: test.gwg.com
Name: test.gwg.com
Description: DC=test,DC=wgw,DC=com
Source: AD
Accounts: 143
Resources: 81
Entitlements: 649
Historical date: 11/14/2012 4:05 PM

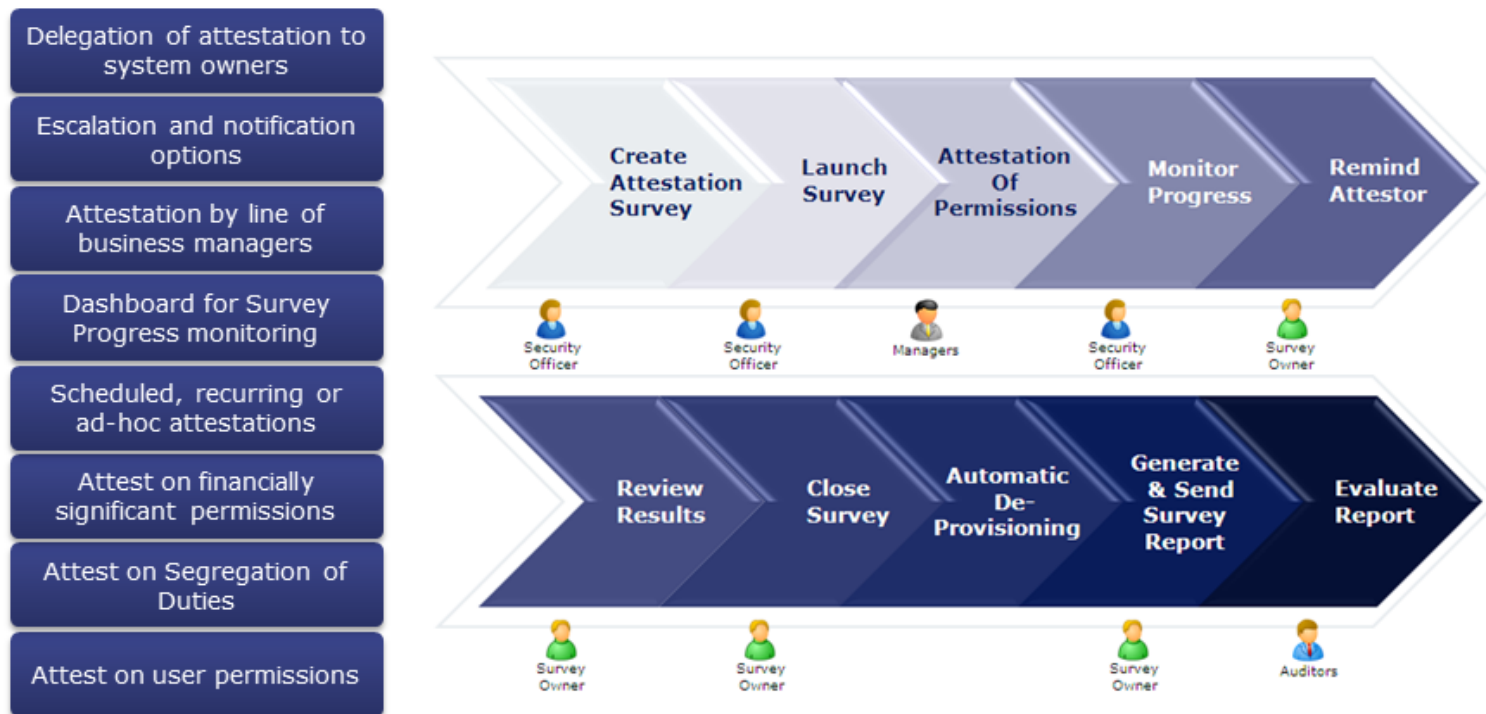
Account ownership: Accounts pending deprovisioning Entitlements pending deprovisioning

AUDIT - TEST\Administrator - ODW System.rdl - 11/14/2012

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.



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

System	Historical date (from)	Historical date (to)	Account	Last updated	Identity	Status	Prob.	Type	New	Reason
SAP01	2/8/2012 10:24 AM	8/8/2012 10:24 AM	ABBB	8/8/2012 10:22 AM	ALB	Pending	100%	Personal	New	Fuzzy Match

AUDIT - MEGAMART\MCAE - ODW System Account Ownership Log.rdl - 8/8/2012 10:25:17 AM

Person: Anthony Anderson

Should Anthony Anderson have account MEGAMART\AAAB on system Megamart.local (AD) Comment required for No

Should Anthony Anderson have permission MEGAMART\ManageInventoryCount_US_NewYork_2 through the account MEGAMART\AAAB Direct Comment required for No

Should Anthony Anderson have permission MEGAMART\Domain Users through the account MEGAMART\AAAB Direct Comment required for No

Should Anthony Anderson have permission MEGAMART\ManageInventoryDocument_US_NewYork_2 through the account MEGAMART\AAAB Direct Comment required for No

Should Anthony Anderson have account Anthony Anderson on system SAP01 (Megapart)

Person: Anthony Baker

Should Anthony Baker have account MEGAMART\ABAG on system Megamart.local (AD)

Should Anthony Baker have permission MEGAMART\ManageGoodsReceipt_US_NewYork_2 through the account MEGAMART\ABAG Direct Comment required for No

UID	Last updated	Joined with	Status	Similar	Type	Reason
ABAB	6/11/2012 2:46 PM	ABAB	Confirmed	1	Personal	Exact Match
ABAC	6/11/2012 2:46 PM	ABAC	Confirmed	1	Personal	Exact Match
ABAD	6/11/2012 2:46 PM	ABAD	Confirmed	1	Personal	Exact Match
ABAE	6/11/2012 2:46 PM	ABAE	Confirmed	1	Personal	Exact Match
ABAF	6/11/2012 2:46 PM	ABAF	Confirmed	1	Personal	Exact Match
ABAG	6/11/2012 2:46 PM	ABAG	Confirmed	1	Personal	Exact Match
ABAA	6/11/2012 2:46 PM	ABAA	Confirmed	1	Personal	Exact Match
ACAB	6/11/2012 2:46 PM	ACAB	Confirmed	1	Personal	Exact Match
ACAC	6/11/2012 2:46 PM	ACAC	Confirmed	1	Personal	Exact Match
ACAD	6/11/2012 2:46 PM	ACAD	Confirmed	1	Personal	Exact Match
ACAA	6/11/2012 2:46 PM	ACAA	Confirmed	1	Personal	Exact Match
ADAB	6/11/2012 2:46 PM	ADAB	Confirmed	1	Personal	Exact Match

Ausprägung 2: Rezertifizierung von Account, Entitlements, Rollen



Surveys zur Überprüfung von

- User Entitlementments
- Accounts
- Permission Entitlementments
- Permissions

The screenshot shows a web-based survey tool interface. At the top, there's a navigation bar with 'Site Actions' and 'Survey' tabs. Below this is a toolbar with icons for 'Navigation', 'Check All', 'Approve Checked', 'Delegate', 'Close Survey', 'Dashboard', 'Hide Answered', 'Show Answered', and 'Indicate Scopes'. The main content area displays a list of users with their account IDs and a question: 'Should [User Name] have permission Email through the account [Account ID]'. Each row has a 'Direct' link, a text input field for 'Comment required for No', and three buttons: 'Yes', 'No', and 'Don't Know'.

Person	Account ID	Question	Direct	Comment	Yes	No	Don't Know
Person : Gebert, Jan (b5400)	b5400	Should Gebert, Jan (b5400) have permission Email through the account b5400	Direct	Comment required for No	Yes	No	Don't Know
Person : Rutetzki, Regina (b2193)	b2193	Should Rutetzki, Regina (b2193) have permission Email through the account b2193	Direct	Comment required for No	Yes	No	Don't Know
Person : Saturno, Sven (b6796)	b6796	Should Saturno, Sven (b6796) have permission Email through the account b6796	Direct	Comment required for No	Yes	No	Don't Know
Person : Winter, Marco (b9880)	b9880	Should Winter, Marco (b9880) have permission Email through the account b9880	Direct	Comment required for No	Yes	No	Don't Know

Überprüfung der Qualität der Surveys

- Dashboard mit Antwortverteilung
- Zulassen der Antwort "Ich weiß nicht"
-> Business Description Survey



Jutta Cymanek
Country Manager DACH & BENELUX

[email: jcy@omada.net](mailto:jcy@omada.net)

Telefon: 06151 97197 58

Mobil: 0176 6125 8851