

Řízení správy rolí v rozsáhlých organizacích

Michal Opatřil
Corinex Group

ca Forum

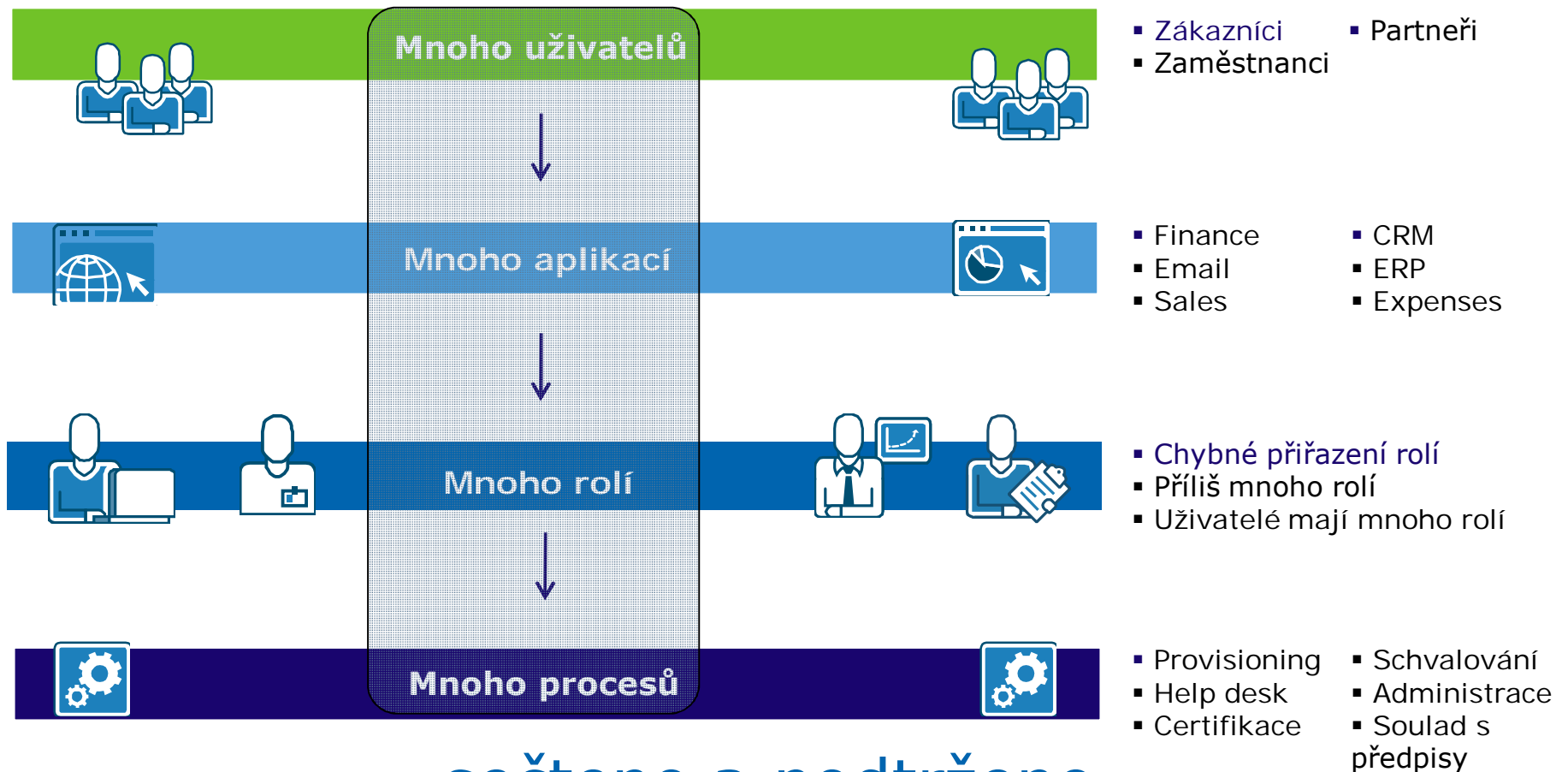
Bratislava
20. október

Agenda



- Popis typické situace v rozsáhlých organizacích
- Řešení Identity Lifecycle Management
- Úrovně vyspělosti integrace ILM
- Požadavky zákazníků pro postup na vyšší úroveň řízení
- CA Role & Compliance Manager
- Architektura
- Plánování projektu

Velké množství a komplexnost entit



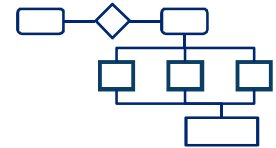
sečteno a podtrženo

Bezpečnostní rizika, nesoulad v auditu, provozní náklady

Plnění cílů projektu modelování rolí



- Cíl
 - 80% pokrytí oprávnění
- Oprávnění vůči business rolím
 - Top-down/bottom-up mining, modeling a rule discovery
- Párování a porovnávání
 - Efektivně porovnat a napárovat oprávnění k rolím na všech úrovních automaticky



Identity Lifecycle Management



Zlepšuje efektivitu businessu, bezpečnosti a souladu s předpisy automatizací životního cyklu Identity a Access Managementu

Role Management



- Kontrola, audit a čištění přístupových oprávnění
- Definování, přiřazení, adaptace, schvalování a certifikace modelu rolí

Identity Compliance



- Vybudování centrálního skladu identit
- Audit, definování, kontrola politik, certifikace oprávnění a jejich náprava
- Reporty a dashboard

User Provisioning



- Automatizace nástupu a výstupu zaměstnanců
- Nastavení účtů a přístupových oprávnění
- Okamžité ukončení přístup pro snížení rizika

Service Request Management



- Umožnění realizace požadavků ze strany business a IT s kontrolou Smart Provisioningu
- Umožnění správy hesel

Úrovně vyspělosti integrace ILM



Cíle ILM

- Identifikace rizik spojených se správou identit a správou souladu s předpsy
- Zvýšit provozní efektivitu

Smart Provisioning

Manuální

- Existující manuální procesy pro přidělování oprávnění
- Řízení oddělním IT a auditem

Automatizace

- Implementace nástrojů pro Identity Management a Provisioning pro automatizaci přidělování a kontroly oprávnění
- Synchronizované řešení pro přidělování rolí a provisioningu
- **Umožňuje měřitelnost z pohledu business**

Business Integrated

- Využití nástrojů pro IDM, Provisioning, Role modeling a Smart Provisioning
- Využívání analytických nástrojů pro podporu rozhodovacích procesů ILM
- Řízení z business pohledu na úrovni politik a analýzy
- Výrazně zvyšuje přizpůsobení uživatelů a procesů vyšší efektivitě
- **Umožňuje proaktivní řízení**

Požadavky zákoníků pro správu rolí



- Analýza aktuálního stavu rolí
- Stanovení nového modelu rolí
- Nový model reflektuje business pohled
- Nový model musí zjednodušit přehled rolí a oprávnění
- Soulad s předpisy a nařízenými (audit)
- Pravidelné kontrola stavu oprávnění a narovnávání vůči modelu
- Plná integrace vůči stávajícím provisioning procesům a nástrojům
- Modelování a přizpůsobení nového modelu rolí s pomocí analytických nástrojů
- Reporting s varováním o chybách, výjimkách a porušování pravidel

CA Identity Manager CA Role & Compliance Manager

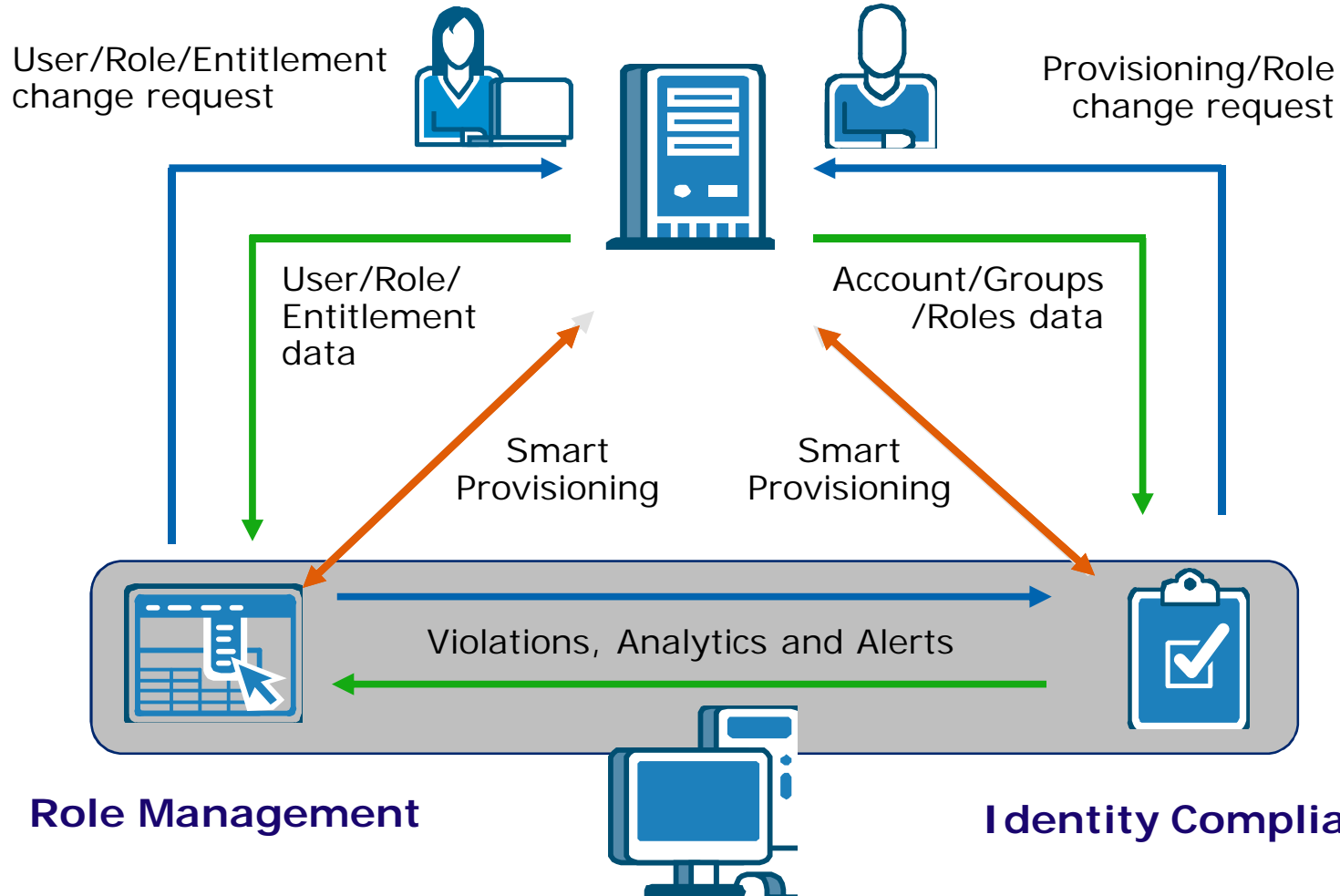


Architektura CA ILM



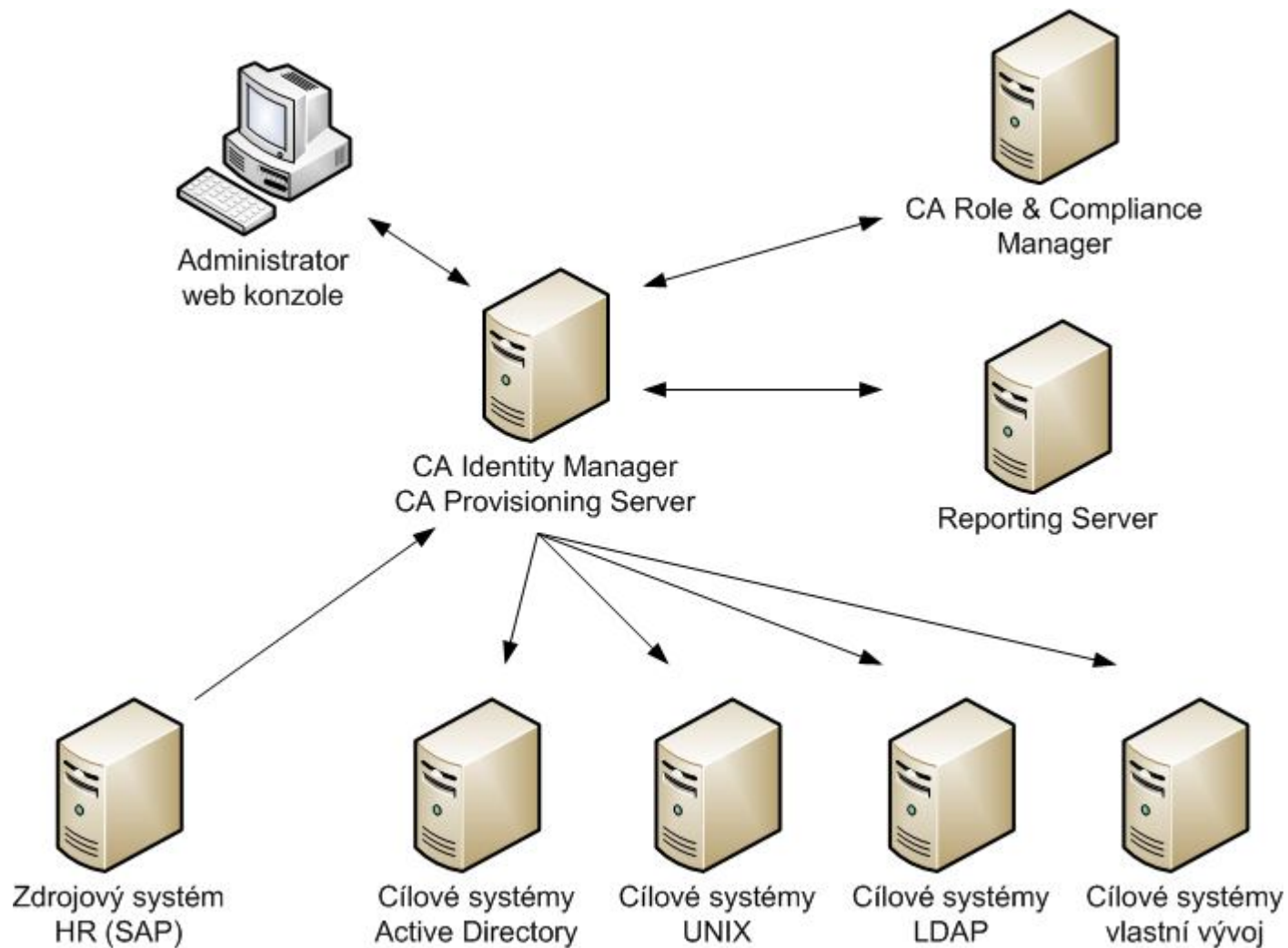
Service Request Management

User Provisioning



Architektura CA ILM

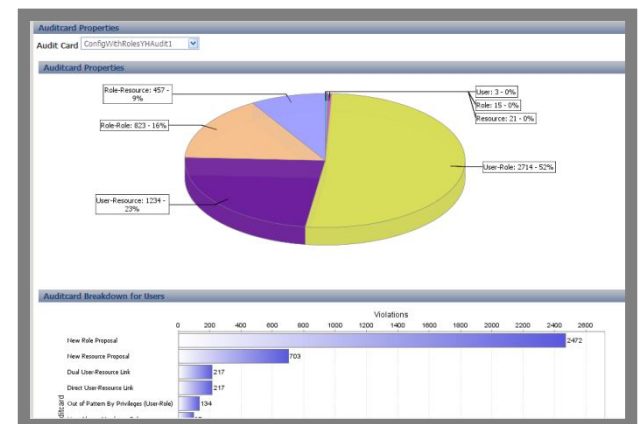
Implementační reálný pohled



CA Role & Compliance Manager



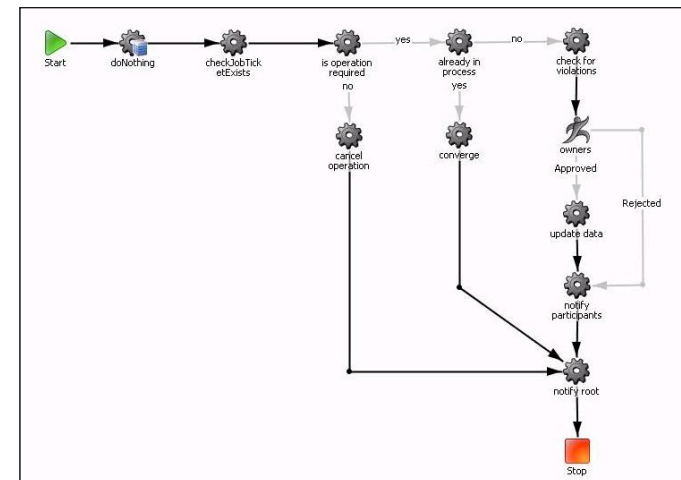
- **Kontrola kvality**
 - Identifikace nekonzistencí a výjimek uživatelských oprávnění pro potřeby řízení rolí a auditu
- **Policy Modeling & Management**
 - Definování a identifikování porušování business politik, SoD a dalších rizik
 - Modeluje změny politik a odhaduje dopad na aktuální stav
- **Role Modeling & Management**
 - Plánování, optimalizace a discovery modelu rolí
 - Kontrola změn modelu rolí, schvalovací procesy
- **Certifikace oprávnění a reporting**
 - Streamline managerial validation of entitlements
 - Privilege, Role and Policy reports and dashboards
- **Smart Provisioning**
 - Přímá integrace se systémy Identity Managementu, přímá automatická kontrola přiřazení rolí



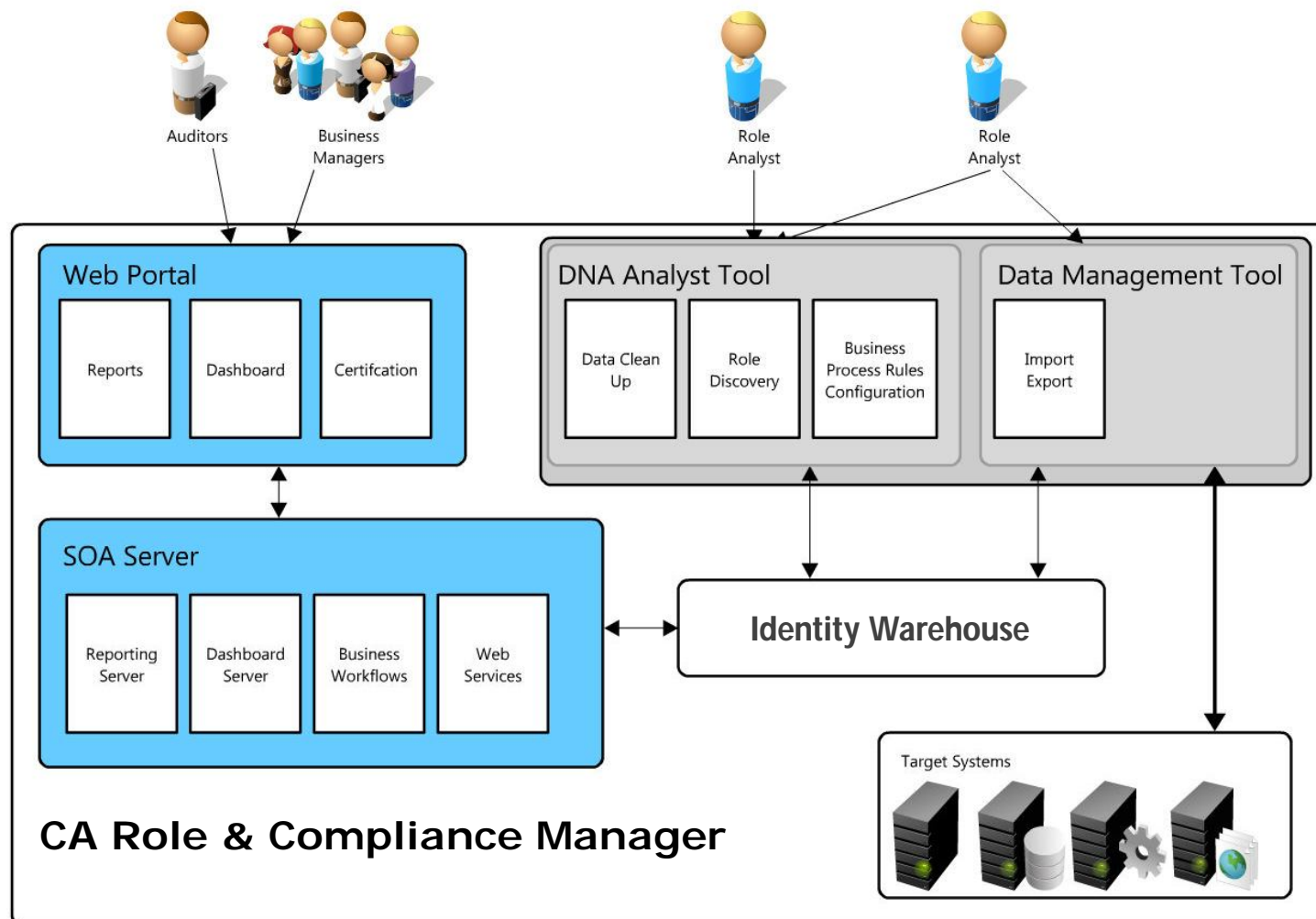
CA Role & Compliance Manager



- Patentované algoritmy pro analýzu rolí
 - Rychlé rozpoznání business struktur a vygenerování návrhu business rolí z velkého množství oprávnění
 - Rychlá detekce nekorektních oprávnění a porušení politik
 - Monitorování a adaptace modelu rolí podle business změn
- Analýza je integrována s workflow a reportingem



CA Role & Compliance Manager Bloková architektura

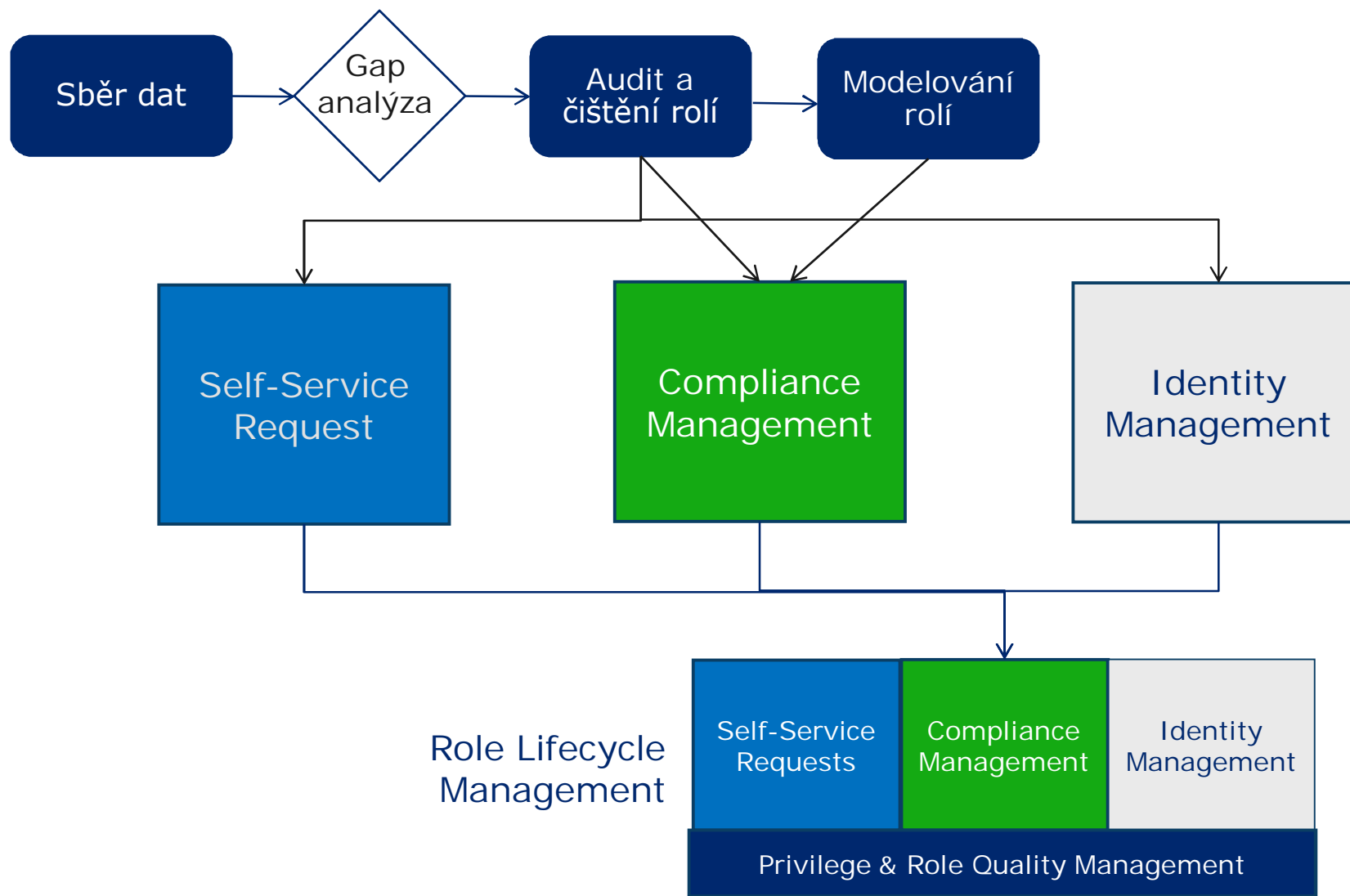


Jak dosáhnout projektového cíle

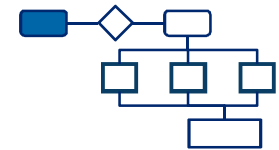


Ca Forum | Bratislava
20. október

Proces kontroly oprávnění a modelování rolí



Sběr dat Vybudování skladu identity

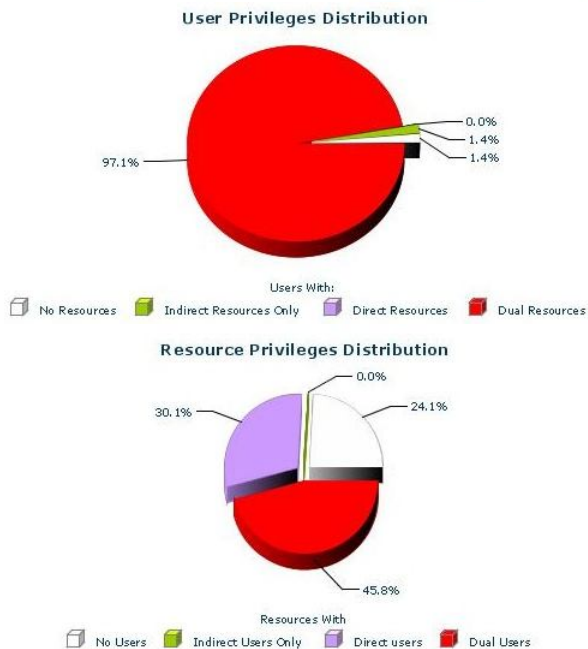


Created on: May 11, 2009 6:04

Configuration Properties Report

Configuration:	Company_model	Resources DB:	1
Create Date:	Mar 2, 2009 7:50 PM	Modified Date:	May 11, 2009 6:00 AM
Owner 1:	Ilan Sharoni	Owner 2:	
Organization 1:	Company	Organization 2:	
Read Only:	No	Parent Configuration:	No
Logged:	No		

Number of DB Users:	75	Users Statistics:	Average	STD
Number of DB Resources:	83	Resources Per User:	6.6	2.9
Number of Configuration Users:	69	Roles Per User:	2.8	1.2
Number of Configuration Resources:	83	Resources Statistics:	Average	STD
Number of Configuration Roles:	30	Users Per Resource:	3.4	10.7
Number of Direct User-Resource Links:	438	Roles Per Resource:	1.3	3.5
Number of User-Role Links:	190	Roles Statistics:	Average	STD
Number of Role-Resource Links:	108	Users Per Role:	6.4	11.4
Number of Role Hierarchy Links:	1	Resources Per Role:	3.7	1.5



- Sběr a agregace dat z jednotlivých systémů
- Libovolná úroveň detailu
 - Uživatelé, skupiny, oprávnění
 - Import rolí, kde je to možné
- Datové zdroje
 - Identity Management system
 - Přímý přístup k systémům nepokrytých systémy IDM

Gap analýza Plánování projektu a business case

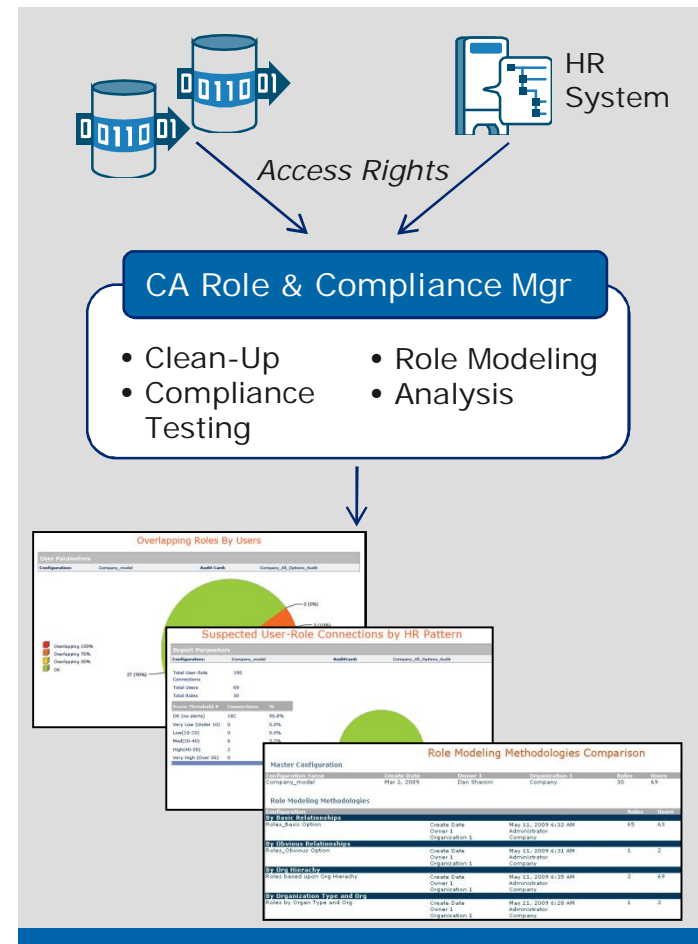
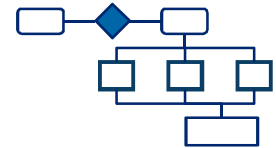


Objektivně a rychle

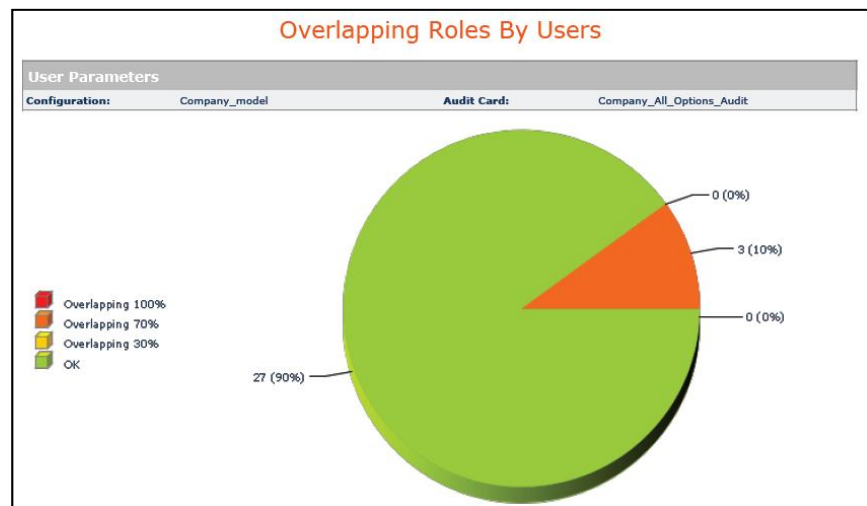
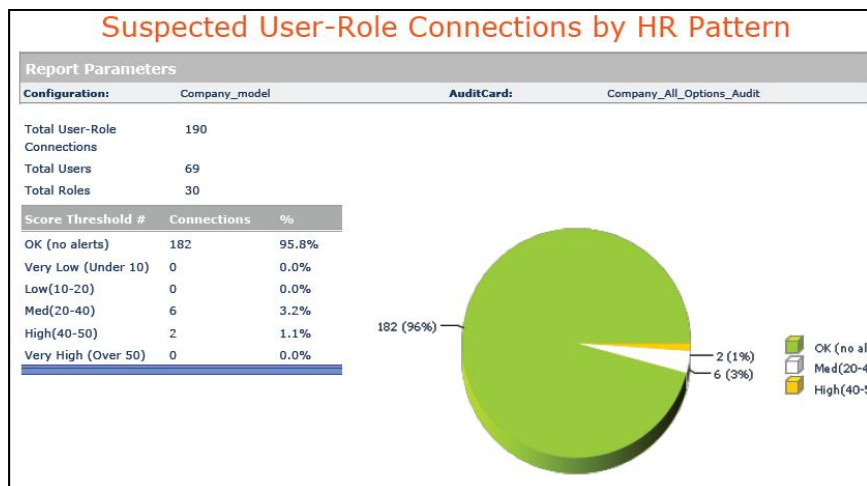
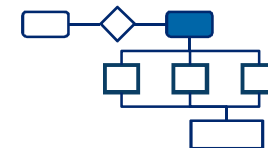
- Identifikace rizik, odhad času a úsilí
- Definice a určení cílů

Kroky procesu

1. Sběr oprávnění z klíčových systémů
2. Napárování vůči HR informacím
3. Vytvoření analytických reportů
 - Quality assessment: uživatelská přístupová oprávnění
 - Výjimky a narušení pravidel včetně SoD
 - Doporučení pro modelování rolí



Audit a vyčistění rolí



- Audit oprávnění
- Detekce výjimek a nenkonzistencí
- Korelace uživatelských UniqueID
- Vyčistění
 - Nastavení kvalitativních cílů (množství výjimek apod.)
 - Nepřiřazení uživatelé, zdroje, skupiny
 - HR chyby
 - Out-of-pattern oprávnění
 - Redundantní skupiny a role
 - Dual linky

Compliance Management

Určení rizik a řízení IT



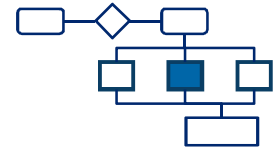
- Nastavení politik z pohledu businessu a nařízení
 - Politiky jsou nastaveny lidmi z vedení, IT a auditory
 - Určení omezení z pohledu zákona a norem (SoD, ochrana osobních údajů atd.)
 - Interní nařízení
- Pro všechny systémy a všechny úrovně
 - často nejsou zahrnuty všechny systémy (většinou jenom ty, které jsou v IDM)
 - často nejsou systémy automatizovány prostřednictvím IDM
 - často nejsou zahrnuty oprávnění nepokryté existujícími rolemi
- Stanovení úrovně rizik
 - Kontrola a následný report do jaké míry odpovídá aktuální stav vůči nastaveným politikám

Compliance Management

Kontrola oprávnění, certifikace

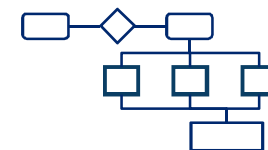


- Kampaně pro kontrolu rolí a oprávnění
 - Certifikováno manažery, vlastníky rolí a vlastníky zdrojů
 - Politiky pro kontrolu a schválení výjimek
 - Více souběžných kampaní
 - Automatické notifikace stavů
- Self Service administrace
 - Požadavky na změny v modelu rolí
- Kontrola a schvalování
 - Požadavky na změnu modelu rolí



Progress	Violations	Person ID	User Name	Organization	Comment
0/13		peral01	Alberto Pereira	HR	
0/3		allmi01	Michael Allen	Executive	
0/7	1	thaed01	Edgar Thain	HR	
0/6		nisku01	Kuniaki Nishikawa	HR	
0/7	2	arnju01	June Arnold	HR	

Efektivní Role Lifecycle Management



Definice rolí

Kontrola
uživatelských
přístupů a
oprávnění

Přiřazení rolí

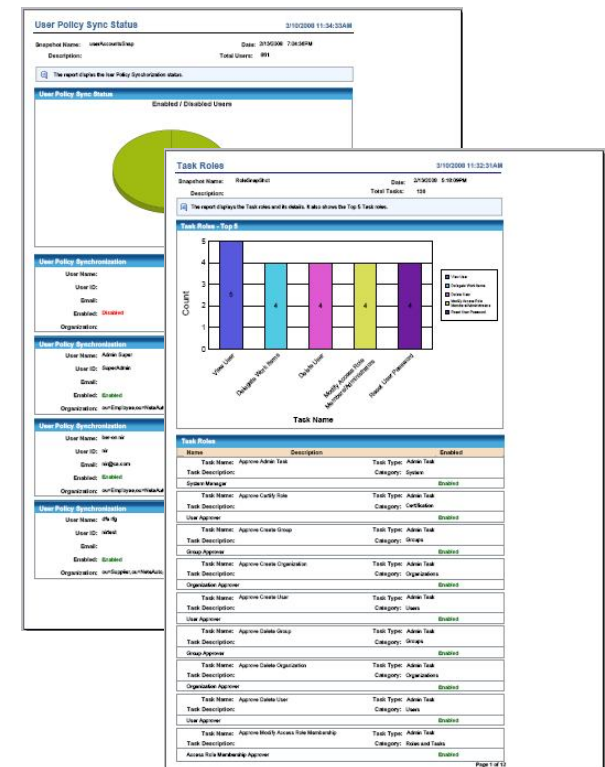
Správa rolí

Kontrola rolí a
certifikace

Plnění cílů projektu modelování rolí



- Integrace se SAP Business Objects
- Předdefinované reporty
 - End Point Accounts
 - Exception Account Trends
 - Policies
 - Role Members
 - Roles
 - Task Roles
 - User Policy Sync Status
 - User Roles
 - Exception Accounts
 - Orphan Accounts
 - Role Administrators
 - Role Owners
 - Snapshots
 - User Accounts
 - User Profile
 - User Entitlements



Plnění cílů projektu modelování rolí



- Nástroje pro analýzu a stanovení modelu rolí
- Vytvoření a správa modelu rolí z business pohledu vůči technickému pohledu
- Reporting jako podklad pro audit a soulad s předpisy
- Reporting jako monitoring plnění souladu s modelem rolí
- Pravidelná kontrola rolí, politik a oprávnění
- Analýza a vytváření nového modelu rolí
- Narovnávání a případné vynucení vůči modelu
- Smart Provisioning s integrací na stávající Provisioning nástroje



Otázky



Ca Forum | Bratislava
20. október