Identity Management + Role Based Access Control

Hírközlési és Informatikai Tudományos Egyesület Számítástechnikai Szakosztálya, a European Organisation for Quality MNB Informatikai Szakbizottsága, és az ISACA Magyar Fejezete közös rendezvényén - 2010.05.07.

Az IDM

HumanoIT
IT Tuning

Mi az IDM?

- **Definíció szerint:**

Adminisztratív eszköz (**szoftver**), amely az egyéneket azonosítja egy adott rendszerben (pl. ország, hálózat, vállalat) és szabályozza az erőforrásokhoz való hozzáférésüket ezen rendszeren belül, azáltal, hogy összeköti a felhasználói jogosultságokat és tiltásokat a rendszerben létrehozott identitásokkal.

- **Management rendszer.**
  - ***Nem*** végez authentikációt
  - ***Nem*** végez authorizációt

- **Források**
  - Források lehetnek: LDAP, AD, OS, ERP-k, CSV fájlok
  - Konnektorok a forrásokhoz: gyári vagy fejlesztendő
  - Külső források (external resources): mobiltelefon, chipkártya

IDM eseteink

HumanoIT
IT Tuning

Két különleges IDM projekt tanulságai

1. **Nagyon sok gép – kevés felhasználó**
2. **Sok felhasználó (3000+ fő) – sok szolgáltatás**

Ügyfél elvárás:

- Komoly testreszabási igények (a rendszer feleljen meg 100%- ban a jelenlegi állapotnak

- Fejlesztés csak a legvégső esetben!

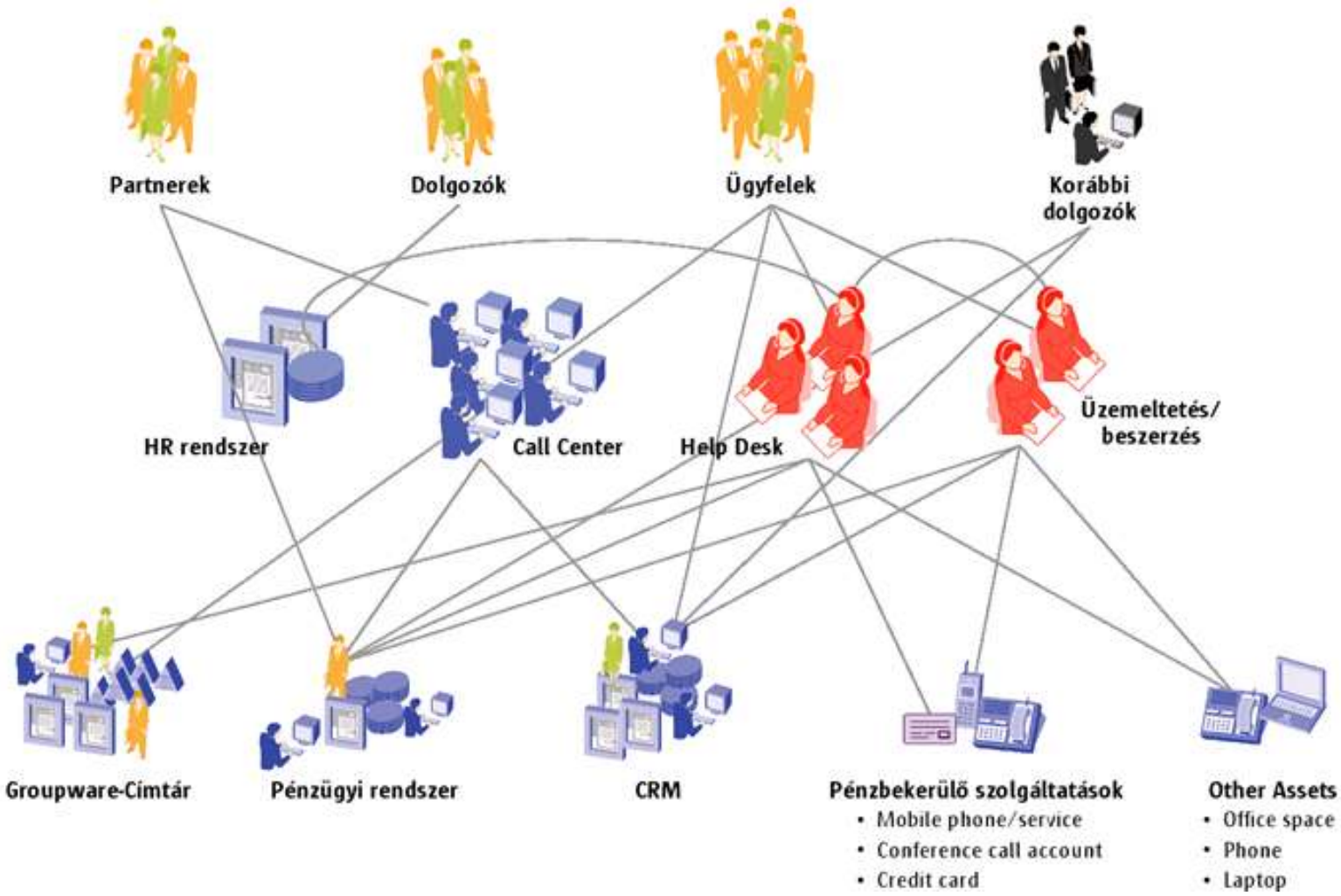
Az IDM rendszer:

- ≠ Sharepoint, Intranet: nehézkes a testreszabása
- Iparági szokványokat támogat

IDM nélkül

HumanoIT
IT Tuning

Anarchia



Az anarchia okai

HumanoIT
IT Tuning

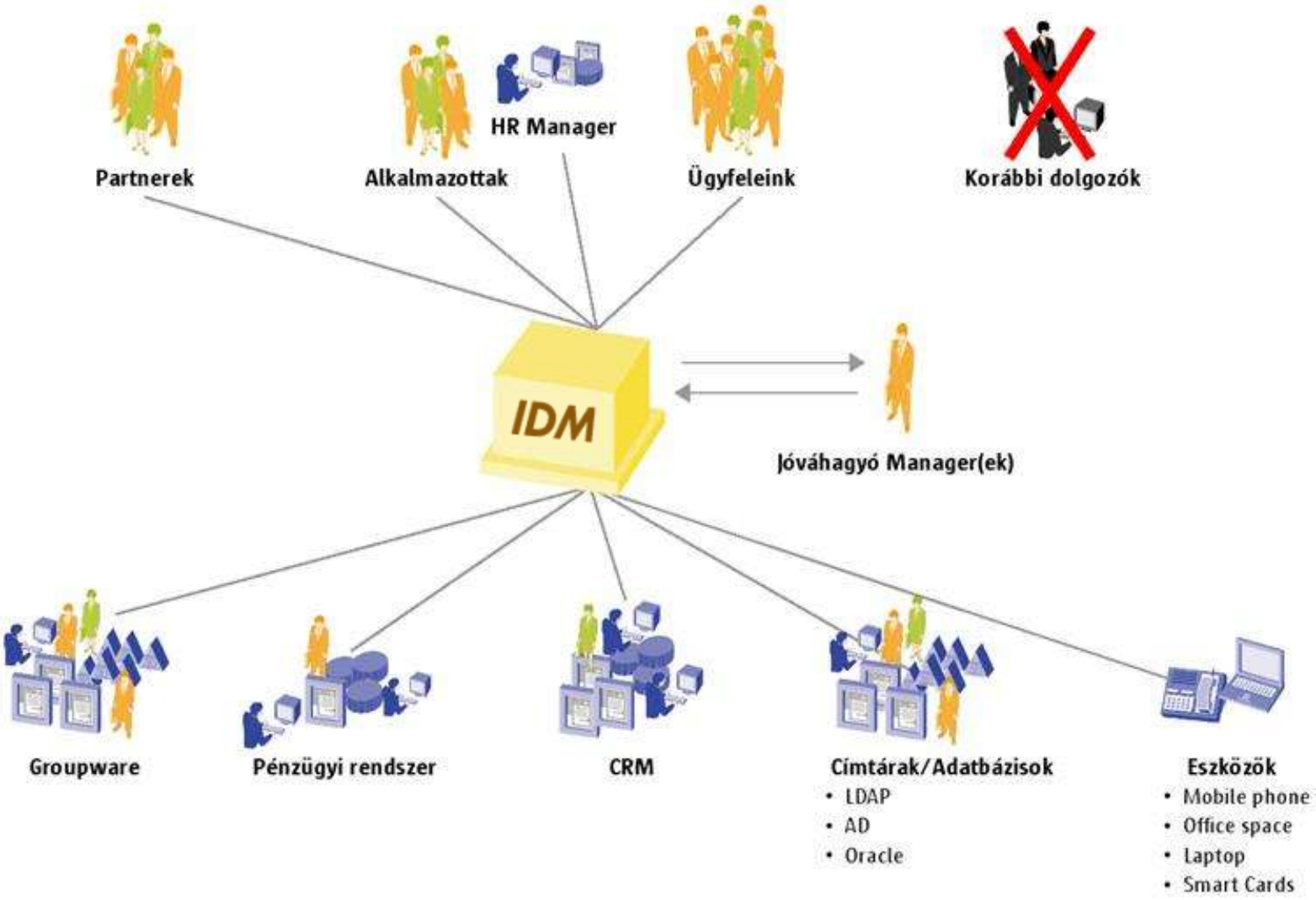
IDM előtt…

- IT rendszerek külön fejlődtek
  - így hézagok vagy átfedések keletkeztek.
- Ahány rendszer, annyi felhasználó-felviteli felület
  - (pl.: VPN-kapcsolat, chip-kártya, rendszerjogok), de ezek felhasználó-kezelése rendszerenként független
- A szerepkörök „maguktól” alakultak ki
- Felhasználó-kezelés ad-hoc
  - A szervezeti életút NEM reprodukálható.
- Az egységesítésre tett törekvések (pl. központi LDAP) tovább bonyolították az infrastruktúrát.

Rend

HumanoIT
IT Tuning

Anarchia helyett



IDM projekt

HumanoIT
IT Tuning

Az idő függvényében

1. Lépés

HumanoIT
IT Tuning

Felmérés

- Interjúk a forrásgazdákkal
- Folyamatok felmérése
  - Rendszerezettek-e
  - Működnek-e
  - Dokumentáltak-e

Eredménytermék:

Megvalósítási rendszerdokumentáció

2. Lépés

HumanoIT
IT Tuning

Role Management = szerepkörök kezelése

- **Általános Role Management:** a szerepkörök kezelésével, életciklusával foglalkozik
- **Role Mining:** szerepkör-bányászat, ami a role management része lehet.

  Céljai:

  - Szerepkörök összevonhatóságának vizsgálata
  - Szerepkör-anomáliák kutatása
  - Szerepkör-anomáliákra intézkedési terv kidolgozása

HumanoIT
IT Tuning

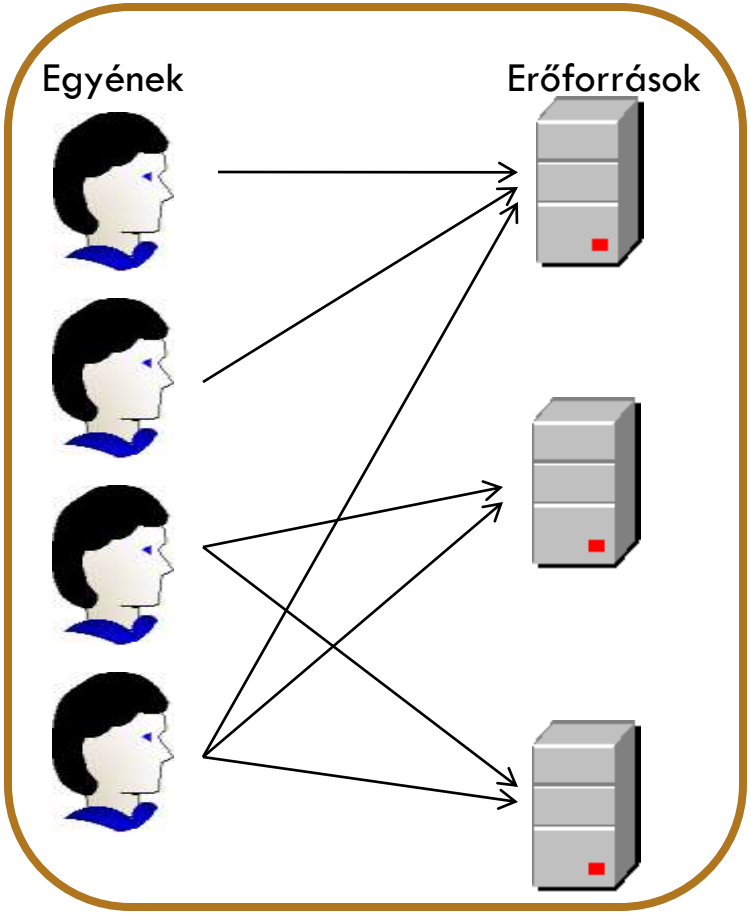
Kis kitérő közkívánatra

Role Management

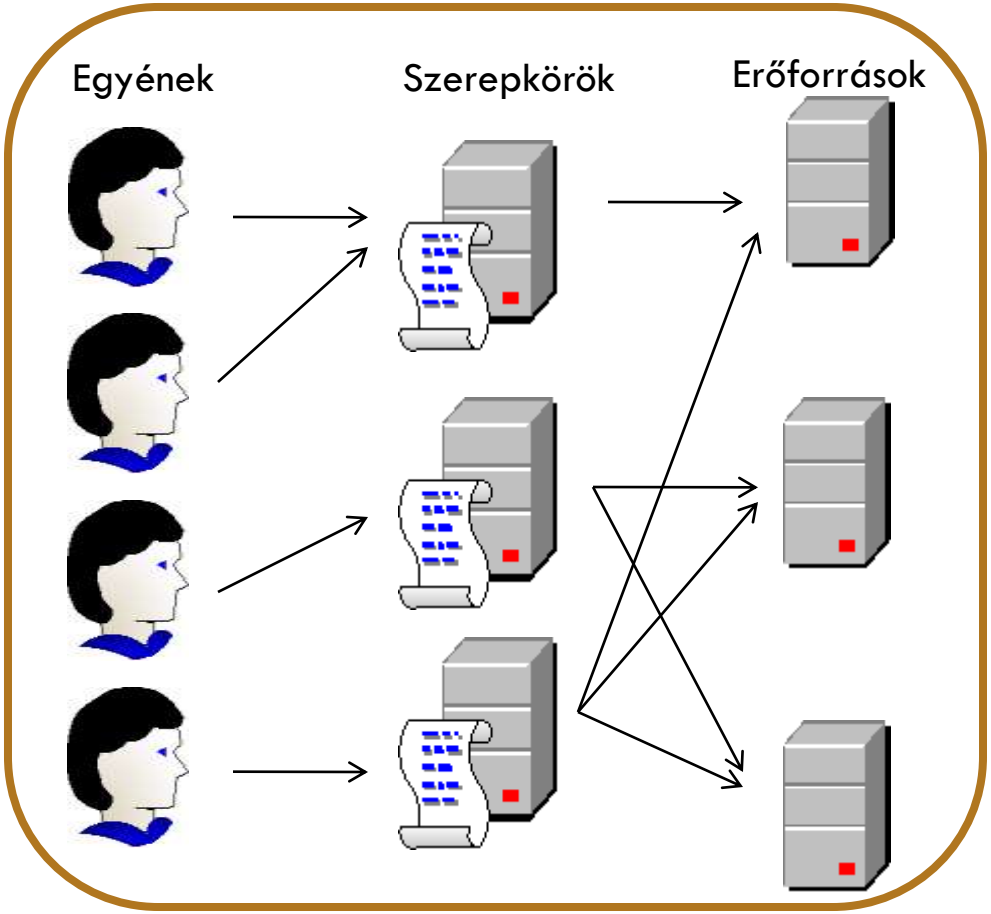
HumanoIT
IT Tuning

Role Engineering + Role Mining

Access Control Management (ACM)



Role-based Access Control (RBAC)



Role Management

HumanoIT
IT Tuning

A szerepkörök fajtái

- **Funkcionális szerepkörök:**
  - A vállalat alapvető üzleti funkcióinak kiszolgálását teszik lehetővé.
- **Szervezeti szerepkörök:**
  - A szervezet hierarchikus felépítését támogatják a meghatározott szervezeti struktúra alapján.

Az RBAC előnyei

HumanoIT
IT Tuning

Role Management = Role Engineering + Role Mining

- **Egyszerűsíti a biztonsági adminisztrációt**
  - a szerepkörök száma kevesebb, mint a felhasználók száma
  - A szerepkörök nagyjából statikusak, míg a felhasználók változnak
  - A legtöbb kereskedelemben lévő rendszer ma már támogatja az RBAC jogosultságkezelést

Az RBAC kialakítása

HumanoIT
IT Tuning

Megközelítési módok

- **Top-down megközelítés:**
  A valós szerepkörök azonosításával kezdünk
  - Körültekintő elemzést igényel, az üzleti folyamatok kisebb egységekre tagolásával
  - Figyelmen kívül hagyjuk a meglévő szerepköröket, jogosultságokat
- **Bottom-up megközelítés:**
  A meglévő jogosultságokat szerepkörökké aggregáljuk
  - Automatizálható
- **Hibrid megközelítés**
  - Erről kicsit később…

A Top-Down megközelítés

Top-Down megközelítés

HumanoIT
IT Tuning

A szervezet jogosultsági köreinek elemzése

1.

- **A funkcionális egységek az engedélyek alapján definiálódnak** *(pl. osztályok dolgozói + középvezetők + felsővezetők)*
- **Nem mindig jó:** *10^4 felhasználó, >10^6 jogosultság esetén → rendkívül nehéz lenne*

2.

- **'Use Case'-ek felhasználásával nyerünk információt**
  - A felhasználókat közvetlenül megkérdezzük, milyen interakciók vannak a rendszerben, majd a válaszokat speciális formátumban rögzítjük
- **A Use Case-ek kiterjesztése a jogosultságok specifikációjával**
- **Meghatározzuk az összes szerepkör jogosultságait:** az összes lehetséges Use Case-t felvázoljuk az adott rendszerre vonatkozóan. Rendszerenként ismételjük a műveletet.

Top-Down megközelítés

HumanoIT
IT Tuning

Előnyök, hátrányok

- **Előnyök**
  - Formális megközelítés: nincsenek egyediségekből adódó csúszások
  - Teljeskörű: az egész szervezetet felöleli
  - Nagy szervezeteknél is jól használható
- **Hátrányok**
  - Korlátozottan automatizálható
  - Nagyon drágává válhat


HumanoIT
IT Tuning
A Bottom-Up
megközelítés

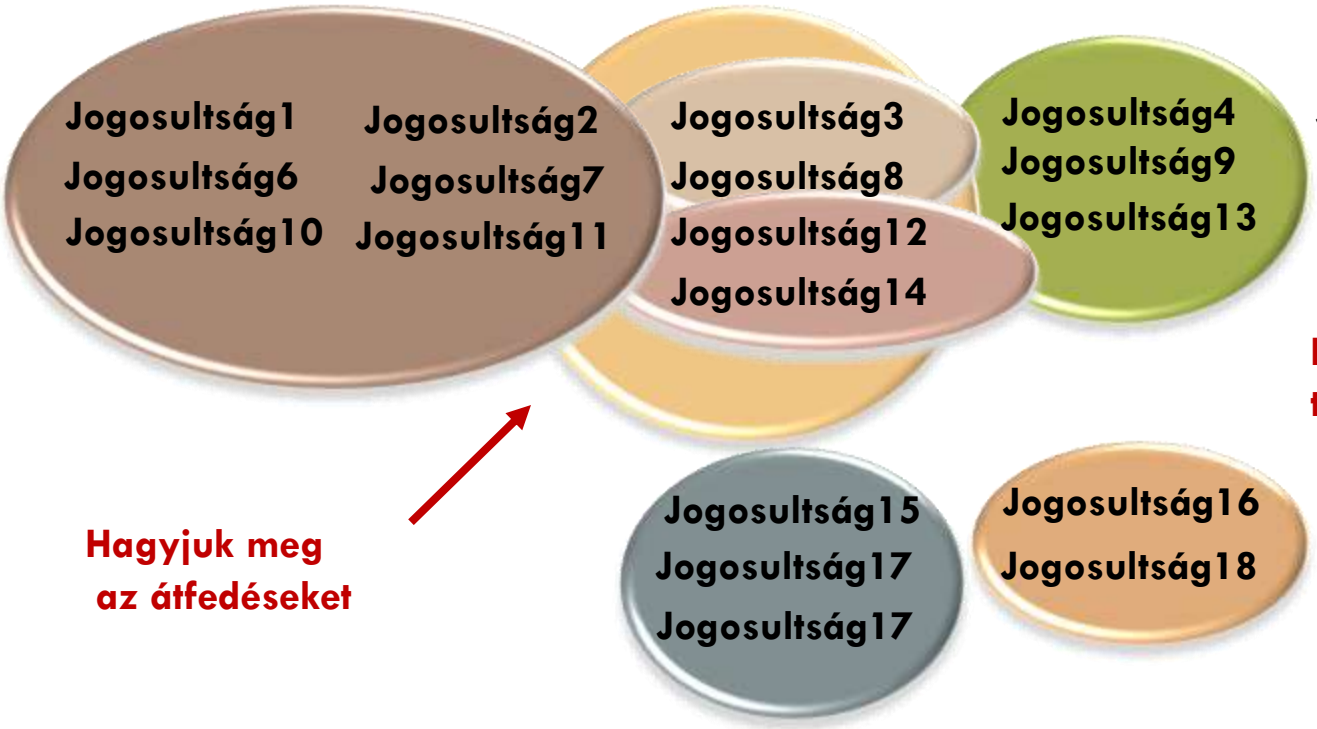
Jogosultságok feltérképezése

HumanoIT
IT Tuning

A meglévő jogosultságokból szerepkörök lesznek

Találjuk meg az összes létező jogosultságot

Ne akarjuk az összes jogosultságot szerepkörré tenni



Hagyjuk meg az átfedéseket

Ne dobjuk el a kevésbé támogatott szerepköröket

A szerepkörök ellenőrzése

HumanoIT
IT Tuning

Működőképes amit alkottunk?

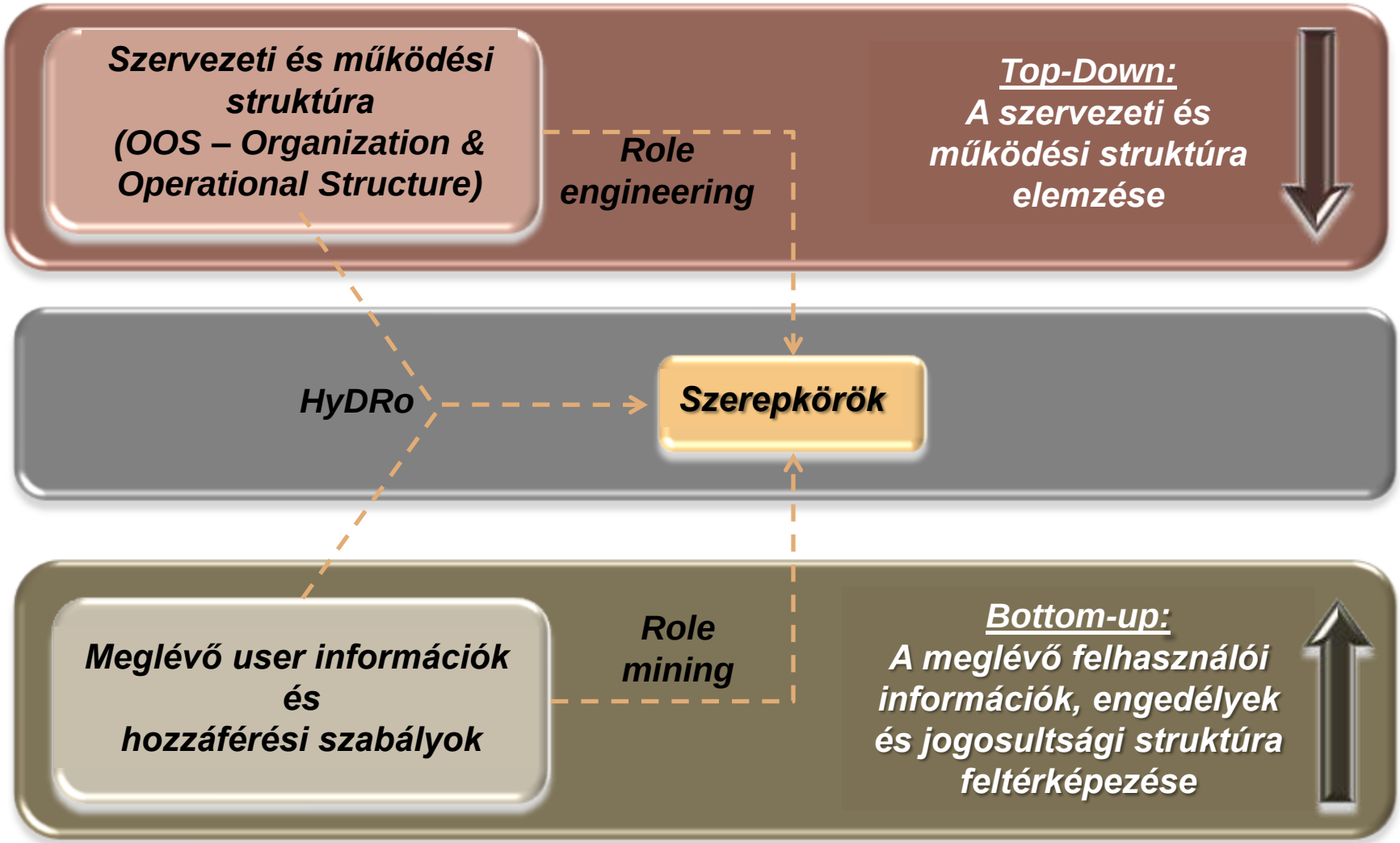
- **Ellenőrzést kíván:**
  - A szerepkörök viszonya, hierarchiája
  - Az anomáliák megléte – lehet, de tudjunk róla, és kezeljük!
  - A szerepkörök közös jogosultságai (átfedések)
- **Költségvezérelt megközelítés:**
  - A szerepköröket az engedélyek mentén azonosítsuk: alapvetően minden tiltott, kivéve amire szükség van
  - Töröljük azokat a szerepköröket, amelyekhez csak egyetlen/kevés user tartozik - ezeket a folyamatok átszervezésével is kiszolgálhatjuk


HumanoIT
IT Tuning
HyDRo:
A hibrid
megközelítés

HyDRo –
Hibrid módú szerepkörfejlesztés

HumanoIT
IT Tuning

Ötvözzük az előnyöket



A HyDRo fázisai

Fontos a sorrend


HumanoIT
IT Tuning
Kitérő után vissza a projekthez

3. lépés

HumanoIT
IT Tuning

Workflow implementálás, felület-testreszabás

- A felmért workflow-k rendszerbe építése
- A workflow-k implementálásának főbb szempontjai:
  - Eszkalációs pontok
  - Jogok delegálása (helyettesítés esetére)
  - Jóváhagyások
  - Jogok időbeli lejáratának kezelése (előtte figyelmeztetés, meghosszabbítási lehetőség, eszkaláció stb.)
- A felületen a használt funkciók megjelenítése, fejlesztések

4. lépés

HumanoIT
IT Tuning

Betöltés - Az igazság pillanata…

Fejlesztői rendszer

- Csak a HumanoIT fejlesztői dolgoznak benne
- A munkáról dokumentáció készül, mely a tesztelést segíti

Tesztrendszer

- Az ügyfél szakemberei dolgoznak benne, a HumanoIT szakértői támogatásával
- A fejlesztői dokumentációk szükség esetén módosíthatók

Éles rendszer

- A dokumentációk alapján az ügyfél szakemberei állítják be.
- A dokumentációk módosítása csak Change Management folyamaton keresztül

5. lépés

HumanoIT
IT Tuning

Projektzárás

- Dokumentáció véglegesítés
- Oktatás
- Online dokumentációk készítése:

  az oktatás ezzel még gyorsabban megvalósítható

- Üzemeltetés támogatás
- Road-map

Élet a projekt után

HumanoIT
IT Tuning

Az IDM használata

- **A rendszert folyamatosan karban kell tartani:**
  - Új felhasználókat könnyen kezelhetjük
  - Átszervezéssel, bővüléssel új szerepkörök keletkeznek: folyamatos role
  - Új rendszerek bevezetése után azok is forrásul szolgálhatnak, szerepkörök jogosultságait bővíthetik
  - Törvényi változásokkal módosulhatnak a workflow-k, szerepkörök (pl. jóváhagyás esetén)

Kiemelendő IDM funkció

IDM – megoldások a gyakorlatban

- **Jelszó management** - A helpdesk idejének 30-70%-a telik jelszavak visszaállításával* – Beállítási lehetőségek: biztonsági kérdések száma, elfogadás módja
- **Self-servicing** – a felhasználók saját maguknak, beosztottjaiknak igényelhetnek, vonhatnak vissza jogokat
- **Workflow -** jogosultság létrehozására, engedélyezésére, terítésére, jóváhagyásra, visszavonásra, eszkalációra)
- **Provisioning** – online változás-terjesztés, meghatározható terjesztési iránnyal

*Forrás: Forrester Research

Az IDM előnyei

HumanoIT
IT Tuning

Megoldás

- **Teljes körű megfelelés**
  - Központosított szabályozási és ellenőrzési funkciók (egyszerű auditálhatóság pl.: PSZÁF)
- **Nagyobb biztonság**
  - Strukturált erőforrás menedzsment
- **Javuló szolgáltatás minőség (Komfortosabb felhasználói rendszerek)**
  - Mérőpontok, átláthatóság
  - Önkiszolgáló funkciók (gyorsabb, biztonságosabb)
  - Átruházási funkciók
- **Üzlet és IT hatékony együttműködése**
  - Üzleti folyamatok és rendszerek integrációja
  - Címtár-szinkronizáció

IDM méretek

HumanoIT
IT Tuning

IDM – ahol érdemes bevezetni…

- **Segít a bevezetéskor:**
  - A forrásokhoz tartozó konnektorok megléte
  - Jól kidolgozott folyamatok
  - Jól dokumentált folyamatok

- **Az IDM rendszer lehetőségei:** Egyes IDM gyártók licensz-skálájában szerepelnek 10 milliós felhasználói körre ajánlott licenszcsomagok

Köszönjük a figyelmet!

HumanoIT
IT Tuning

HumanoIT Kft.

- **Hollósi Gábor**
  - Rendszermérnök, szakértő
  - gabor.hollosi@humanoit.hu
- **Fazekas Éva**
  - Account manager
  - eva.fazekas@humanoit.hu

HumanoIT

IT Tuning