

# Identity Management

Szabvány még nincs – Legjobb gyakorlat már van



**HumanoIT**  
IT Tuning

# Amiről szó lesz ma...



•2

## Napirend

- Bemutatkozás
- IDM „szabvány”
- Élet IDM nélkül...
- ... és vele
- IDM projekt lépései
- Az IDM rendszerek sajátosságai

## IT TUNING = MŰKÖDÉS OPTIMALIZÁLÁS, FINOMHANGOLÁS

- **2005 - megalakulás**
- **2009**
  - *Közel 0,5 Mrd HUF bevétel*
  - *Közel 85% szolgáltatás*
- **24 fő szakértő**
  - **5 projektvezető**
  - **4 CISA,**
  - **2 CISM**
  - **4 fő ITIL**

### Projekt

(valós cél, határidő, költség)

### IT Biztonság

(megfelelőség, használhatóság, költség)

### IT Működés

(üzleti elvárásoknak való megfelelés, használhatóság, költség)

optimalizálás

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

---

### ***Ügyfél elvárás:***

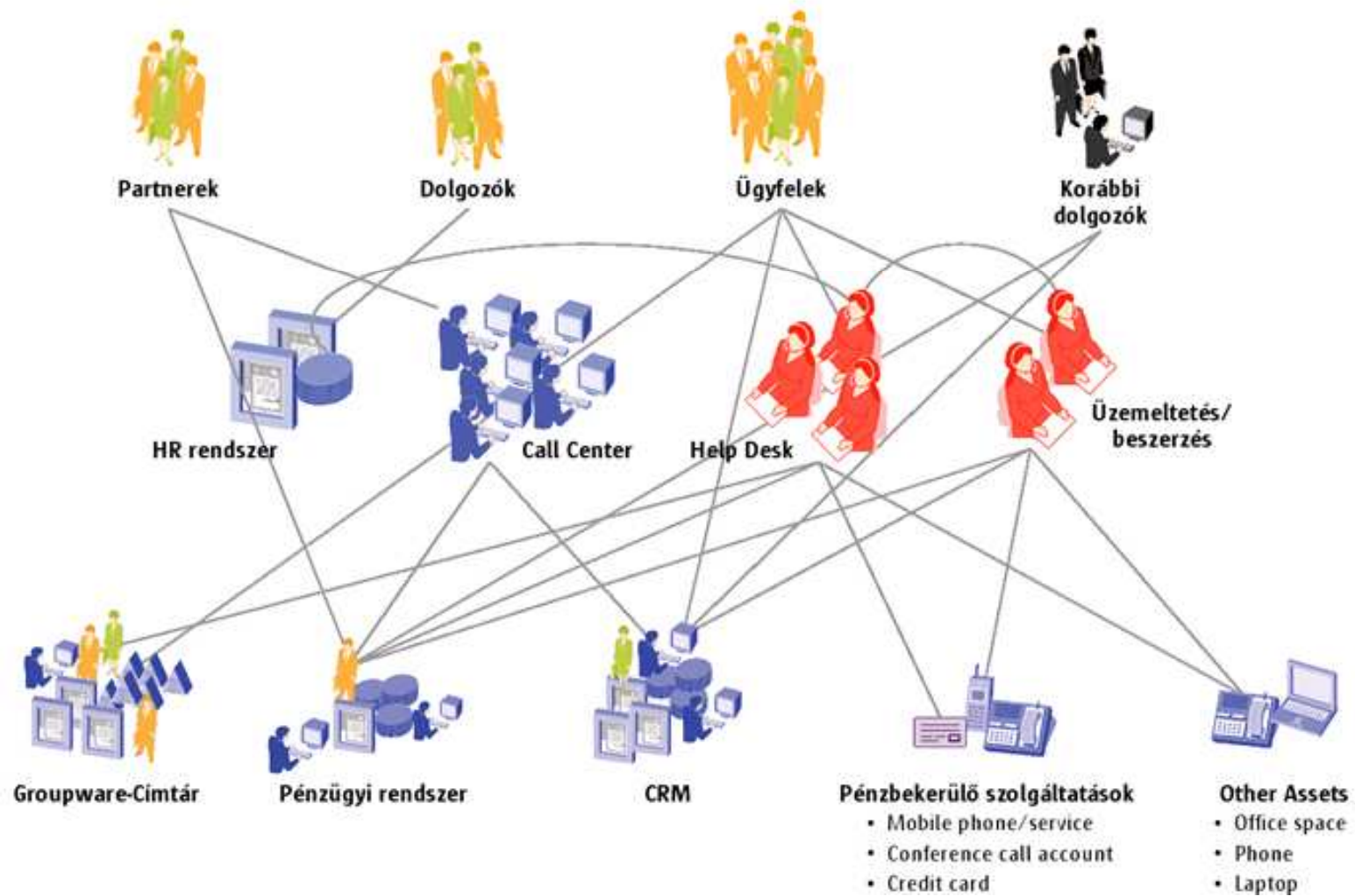
- ▣ Komoly testreszabási igények
- ▣ Fejlesztés csak a legvégső esetben!

### ***Az IDM rendszer:***

- ▣ Korlátozott fejlesztési lehetőségek
  - ▣ IDM  $\neq$  Sharepoint, Intranet...
-

# Anarchia

•5



# Az anarchia okai



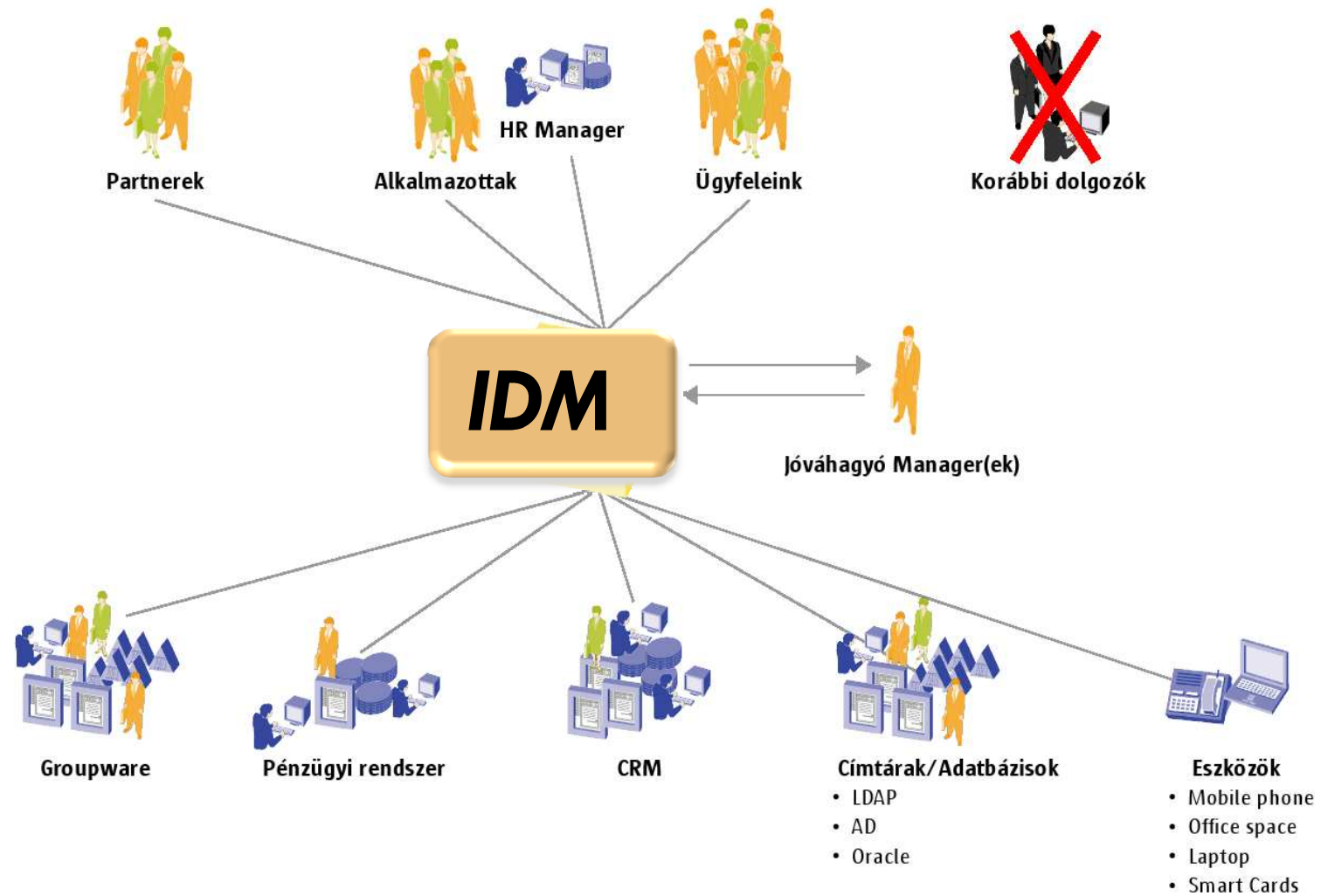
•6

IDM előtt...

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

# Rend

•7



# A vonatkozó szabvány



•8

## ISO/IEC CD 24760

ISO/IEC CD 24760 - Information Technology -- Security Techniques -- A Framework for Identity Management - Mozilla Firefox

http://www.iso.org/iso/catalogue\_detail.htm?csnumber=51625

International Organization for Standardization

International Standards for Business, Government and Society

Home Products Standards development News and media About ISO For ISO Members · FAQs · Fr ISO Store

Products > ISO Standards > By TC > JTC 1 Information technology > SC 27

ISO Store  
ISO Standards  
By ICS  
By TC  
How to use the ISO Catalogue  
Management standards  
The ISO portfolio  
FAQs  
Country codes (ISO 3166/MA)  
Directory of aerospace standards  
ISO Concept Database (ISO/CDB)  
Publications and e-products  
Copyright

### ISO/IEC CD 24760

Information Technology -- Security Techniques -- A Framework for Identity Management

General information

Number of Pages:

Edition: 1	ICS: 35.040
Status: Under development	Stage: 30_20 (2010-01-12)
TC/SC: JTC 1/SC 27	Target publication date: 2013-04-12

These standards could also interest you

- ISO/IEC 27003:2010 Information technology-- Security techniques -- Information security management system implementation guidance
- ISO/IEC 27033-1:2009 Information technology-- Security techniques -- Network security -- Part 1: Overview and concepts
- ISO/IEC 19792:2009 Information technology-- Security techniques -- Security evaluation of biometrics

© 2010 ISO Privacy Policy Name and logo Sitemap Contact ISO Guided tour of ISO-Online Print Increase text size News feeds

Kész

start ISO/IEC CD 24760 - I... 10:02



# Unified Threat Management



•9

Hálózatbiztonság



# Identity-based Unified Threat Management



•10

Hálózatbiztonság



A szabályokat nem IP címekhez, hanem auditált felhasználókhöz lehet kötni!

# Mire való az IDM?

•11

Az IDM maga – Amiért külön szabvány kell

## ▣ **ACM: Access Control Management**

- Csak jogosultságokkal foglalkozik, nem szerepkör szemléletű

## ▣ **RBAC: Role-based Access Control**

- Szerepkörökhöz rendelünk felhasználókat

## **Az IDM**

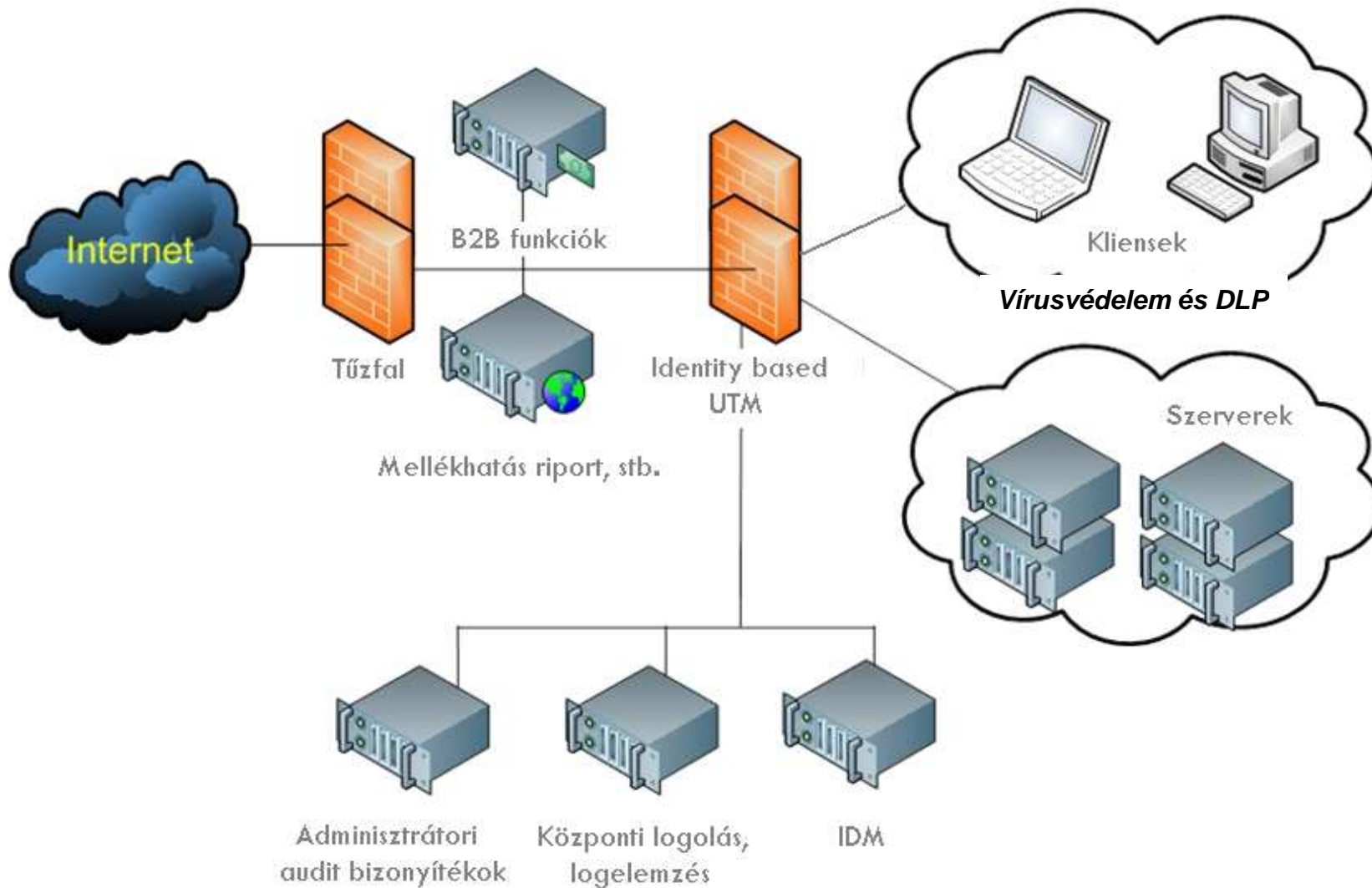
## ▣ **Management. Azaz:**

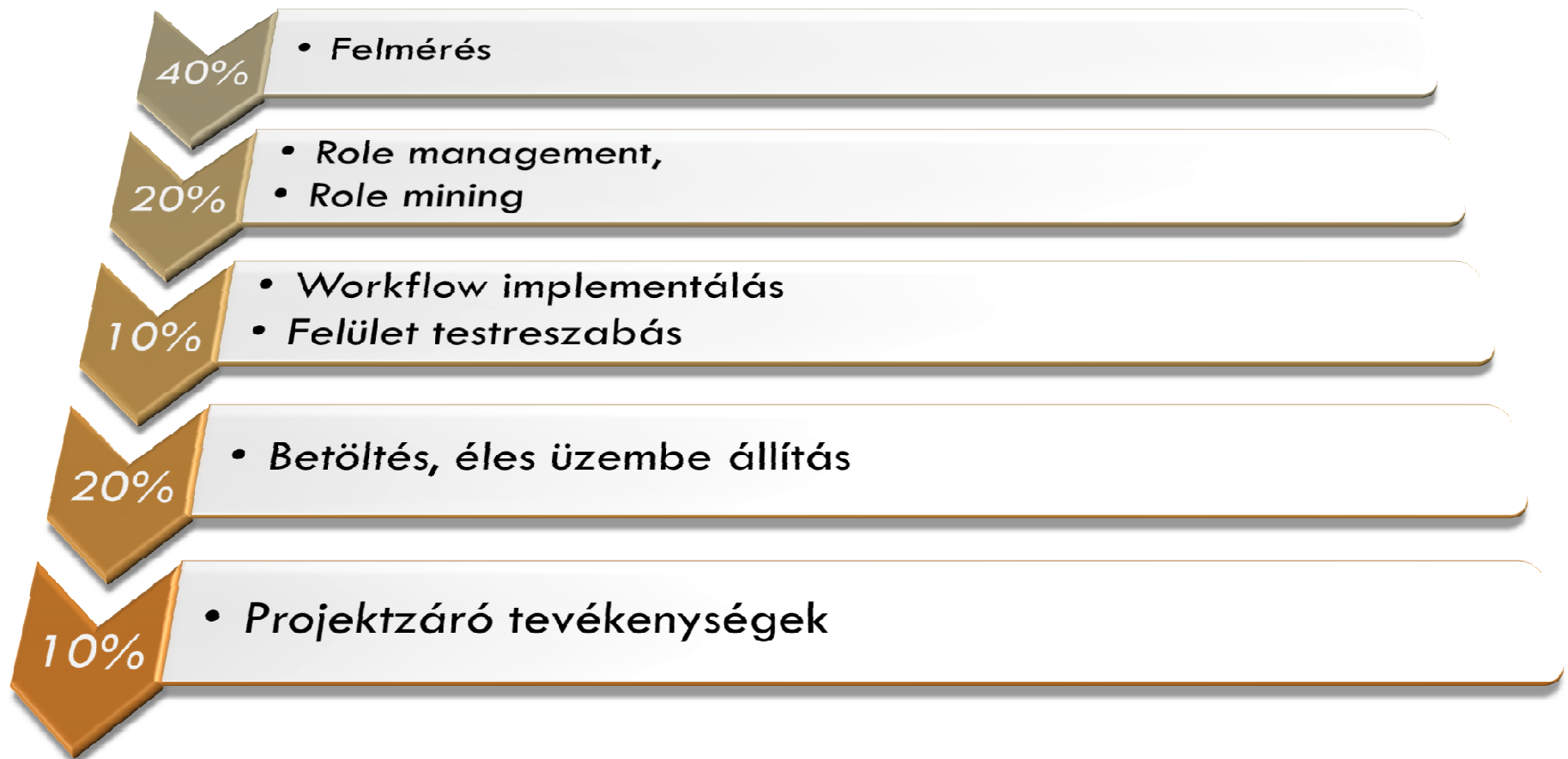
- **Nem** végez autentikációt
- **Nem** végez autorizációt

# IDM hálózati koncepció

•12

## Hálózatbiztonság





# 1. Lépés

•14

## Felmérés

- ▣ Interjúk az forrásgazdákkal
- ▣ Folyamatok felmérése
  - Rendszerezettek-e
  - Működnek-e
  - Dokumentáltak-e

---

***Eredménytermék:***

Megvalósítási rendszerdokumentáció

# 2. Lépés

= *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

# 3. lépés

## Workflow implementálás, felület-testreszabás

- ▣ A felmért workflow-k rendszerbe építése
- ▣ A workflow-k implementálásának főbb szempontjai:
  - Eszkalációs pontok
  - Jogok delegálása
  - Jóváhagyások
  - Jogok időbeli lejáráásának kezelése
- ▣ A felületen a használt funkciók megjelenítése, fejlesztések



# 4. lépés

•17

## Betöltés - Az igazság pillanata...

### Fejlesztői rendszer

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

### Tesztrendszer

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

### Éles rendszer

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

# 5. lépés

•18

## Projektzárás

- Dokumentáció véglegesítés
  - Oktatás
  - Online dokumentációk készítése:  
az oktatás ezzel még gyorsabban megvalósítható
- 



- Üzemeltetés támogatás
- Road-map

# Az IDM előnyei

•19

## 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

### ▣ Jelszó management

- A rendszergazdák idejének 20%-a telik jelszavak visszaállításával – Beállítási lehetőségek: biztonsági kérdések száma, elfogadás módja

### ▣ Források

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

### ▣ **Segít a bevezetéskor:**

- A forrásokhoz tartozó konnektorok megléte
- Jól kidolgozott folyamatok
- Jól dokumentált folyamatok

### ▣ **Az IDM rendszer lehetőségei:** Egyes IDM gyártók licenz-skálájában szerepelnek 10 milliós felhasználói körre ajánlott licenzcsomagok

# Köszönjük a figyelmet!

•22

HumanIT Kft.

## ▣ **Hollósi Gábor**

- Rendszermérnök, szakértő
- [gabor.hollosi@humanoit.hu](mailto:gabor.hollosi@humanoit.hu)

## ▣ **Fazekas Éva**

- Account manager
- [eva.fazekas@humanoit.hu](mailto:eva.fazekas@humanoit.hu)



**HumanIT**  
IT Tuning