# ADAPTO

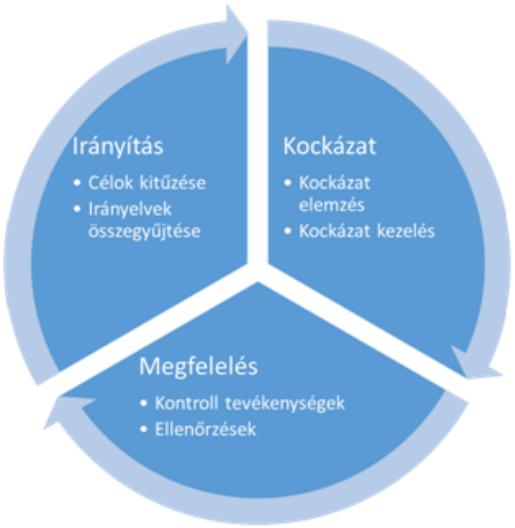
tisztánlátás egyszerűen

## A tökéletes BIA receptje

Pflanzner Sándor

# Egy vállalat átvilágításakor használható szabványok

- ISO 9001
  - Folyamatmodellezés
  - Vizsgálandó erőforrások: folyamat bemenetei (beszállítói)
- ISO 27001
  - Vizsgálandó erőforrások: COBIT irányelvek
- Közös a GRC alapú megközelítés
  - Célkitűzések
    - 9001 – a vevő minőségi követelményei
    - 27001 – A. melléklet szabályozási céljai
  - Kockázatelemzés
  - Megfelelési nyilatkozat
- ISO 22301
  - Folyamatmodellezés részletezettsége





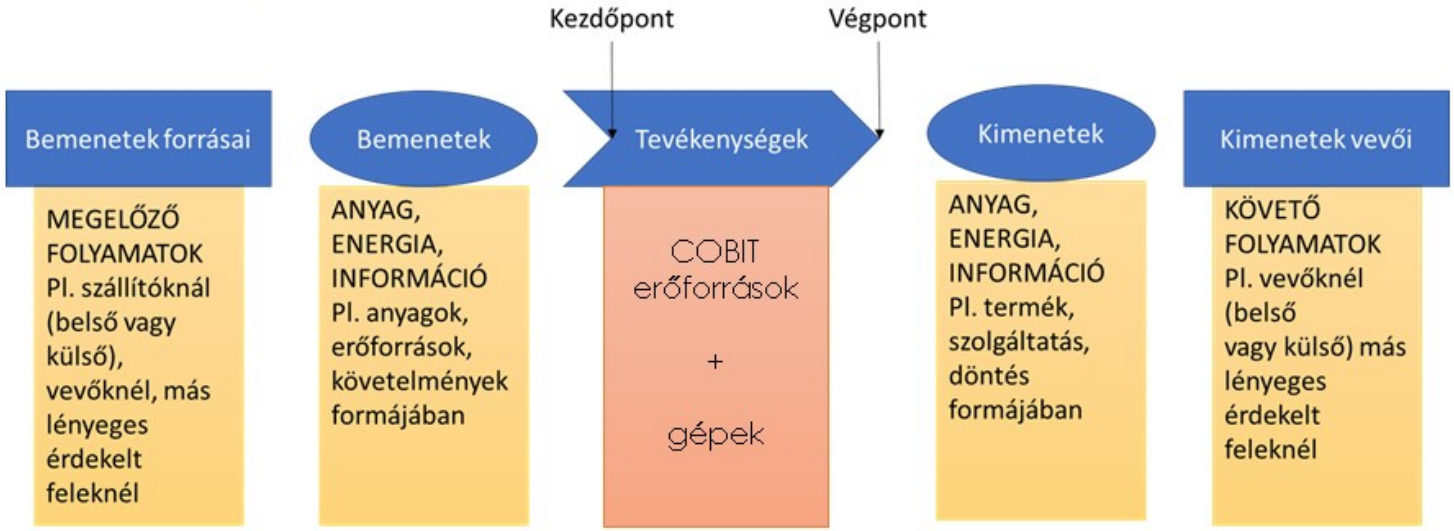

ADAPTO

# 1. Axióma

Olyan átvilágítást kell készíteni, amelyik kiszolgálja a minőségirányítási (környezetirányítási), információ biztonsági és üzletmenet folytonossági igényeket is.

# Milyen modelleket használunk a BIA elkészítéséhez?

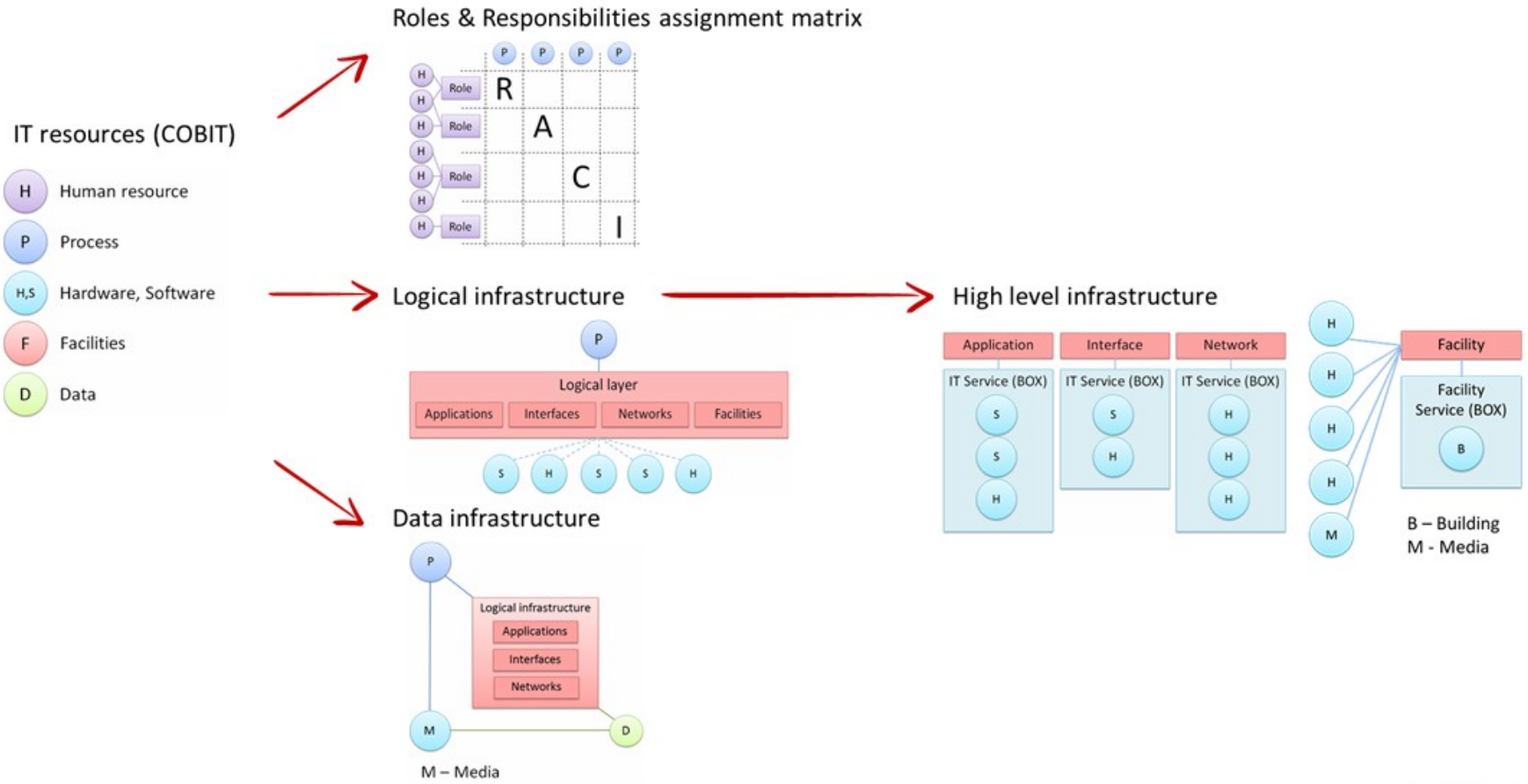
- ISO 9001 folyamatmodell
- COBIT erőforrások (ipar 4.0)
  - + gépek
  - + bemenetek (szállítók)



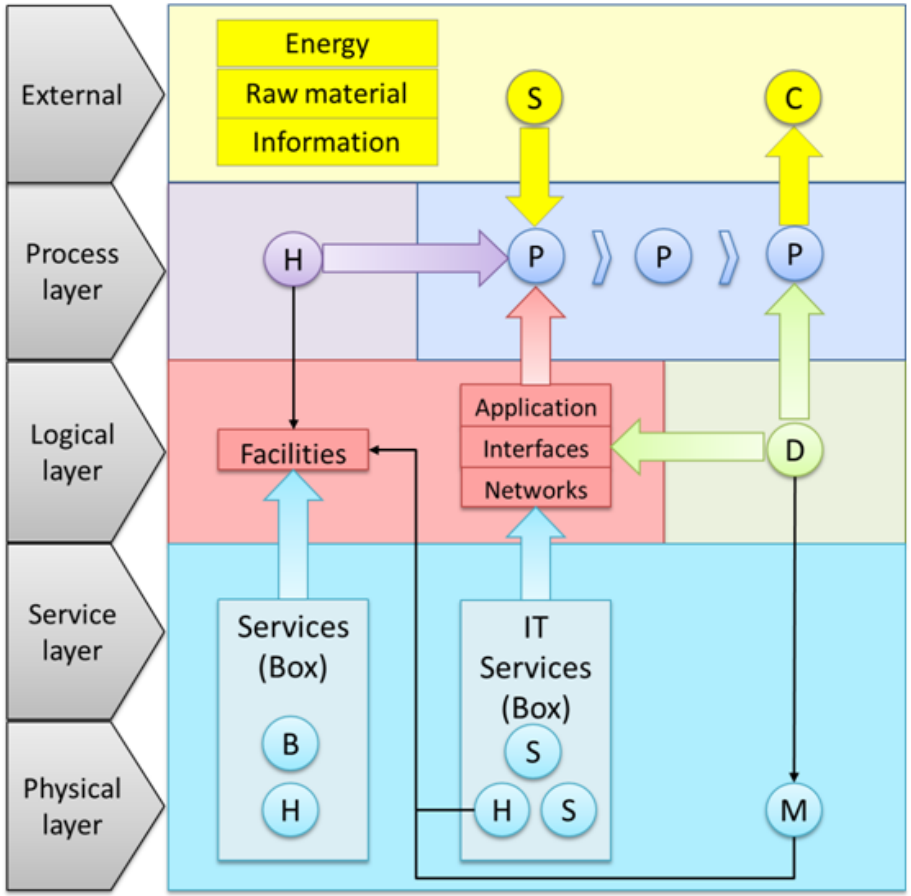



ADAPTO

# Vállalati erőforrások kapcsolatai



# Vállalati erőforrások egységes modellezése




- Vállalati felépítmény modell
  - folyamathoz és
  - az adathoz

  vezető út kijelölhető
- Kiértékelése
  - BCP: Folyamatok leállásának költsége
  - RA: Kárérték osztályozás
    - Működési károk
    - Adatvagyon károk



ADAPTO

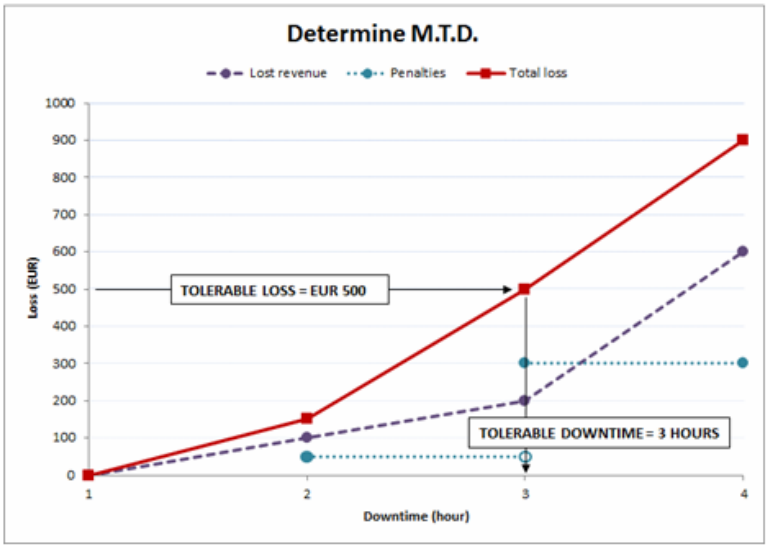
# Kárérték becslés a BCM tevékenységhez

- Folytonosság tervezés célja:
  rangsorolni az üzleti folyamatokat, a leállás okozta veszteség szerint

- Lehetőleg megszakítás nélküli kárérték függvényt kell használni
  - Sokkal pontosabb
  - Forrása: E2E process kiesésének vizsgálata (kontrolling)

- A nem pénzügyi károk szintenkénti besorolása felesleges
  - Fáj vagy nem fáj? Mennyi idő múlva fáj?

- Folyamatok megengedett leállási idejének kiszámítása
  - Mert az erre vonatkozó becslések mindig pontatlanok és konfliktusok forrásai






ADAPTO

# Kárérték osztályozás a kockázatkezeléshez

- Kockázatelemzés
  - A hagyományos kárérték osztályozás (időhöz nincs kötve)

- Kockázat-típusonként eltérő kiértékelési metódus
  - Információ-biztonság
  - Szállítói kockázat
  - Emberi tevékenység kockázata
  - Létesítmény-biztonság

- Összehasonlíthatóság: minden kockázattípusra
  - egységes kárérték osztályozás



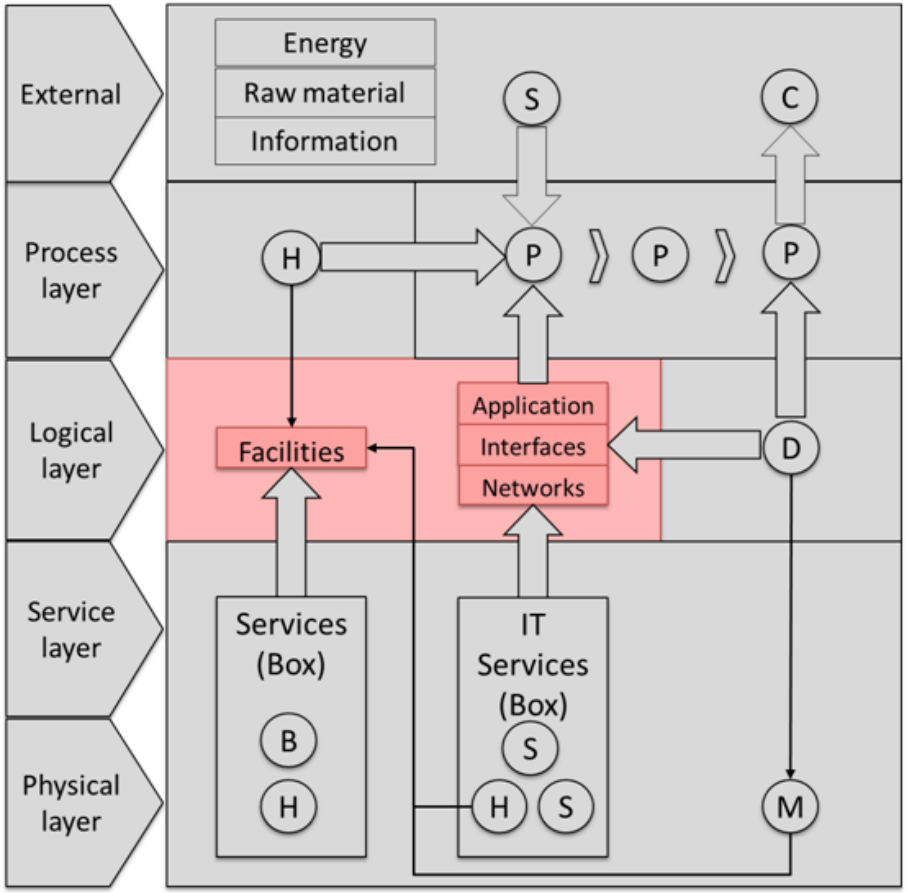
ADAPTO

# 2. Axióma

Az átvilágítást a lehető legkevesebb emberi erőforrás igénybe vételével kell elkészíteni mind a megbízó, mind a konzulens részéről.

Folyománya: a CMDB import felesleges.

# A kidolgozottság (részletezettség) problémája

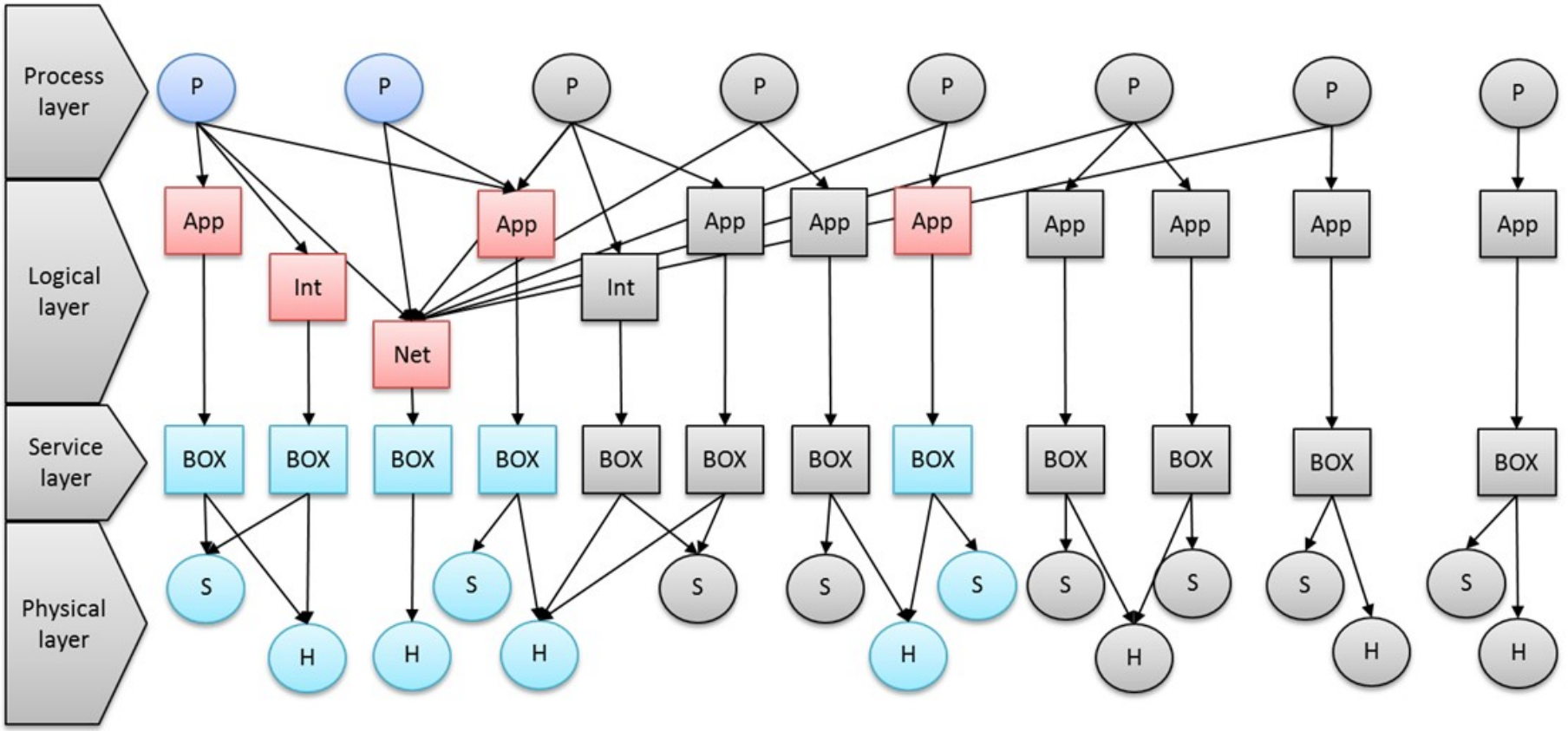



- A logikai réteg önállóan megjelenik a szabályozási célokban:
  - Hálózatok védelme
  - Alkalmazások hozzáférései
  - Munkavégzés helyszíne
- Fontos logikai rétegek
  - Magas biztonsági osztályú adatokat kezelő információs rendszerek
  - Fontos folyamatokat kiszolgáló információs rendszerek



ADAPTO

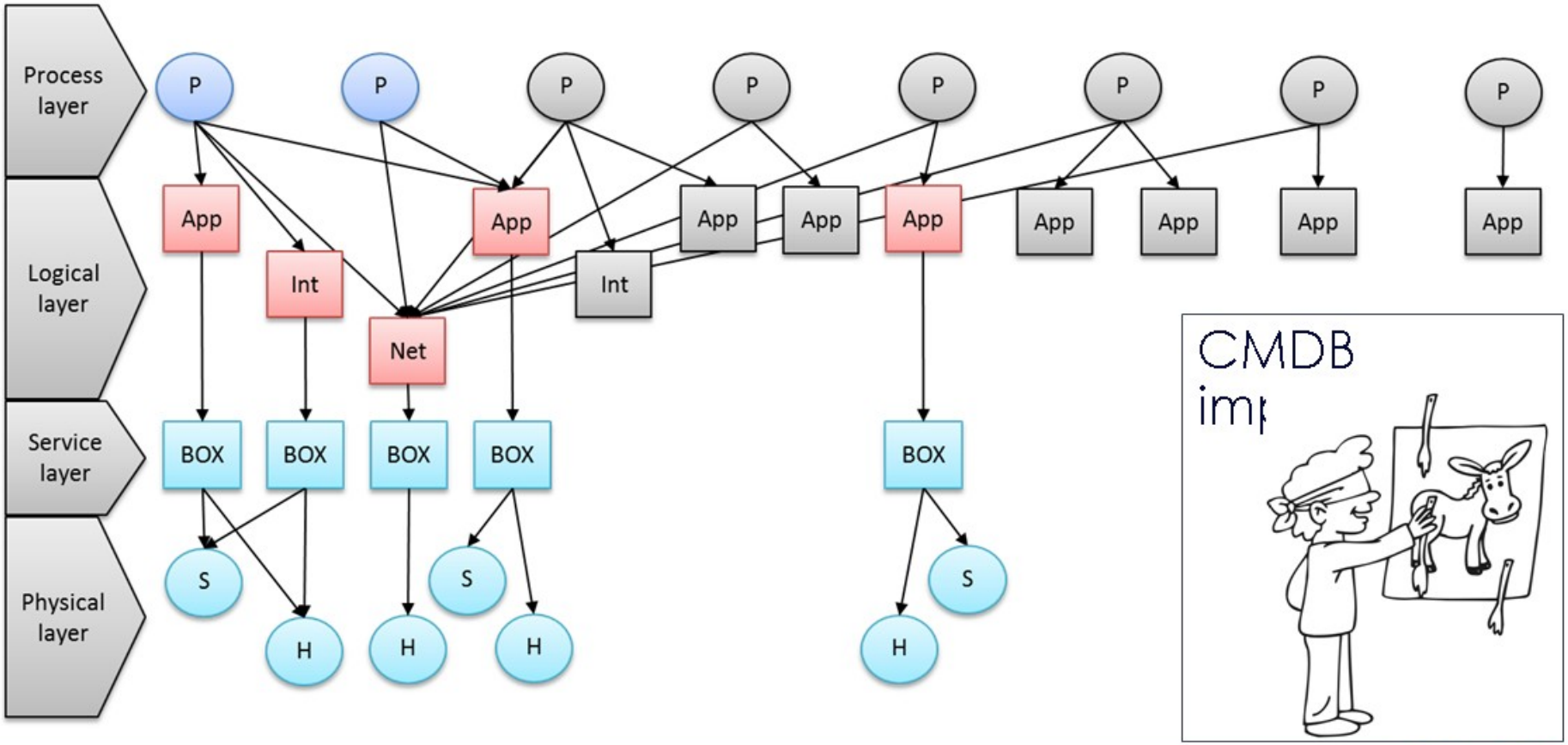
# Folyamatokat támogató erőforrások






ADAPTO

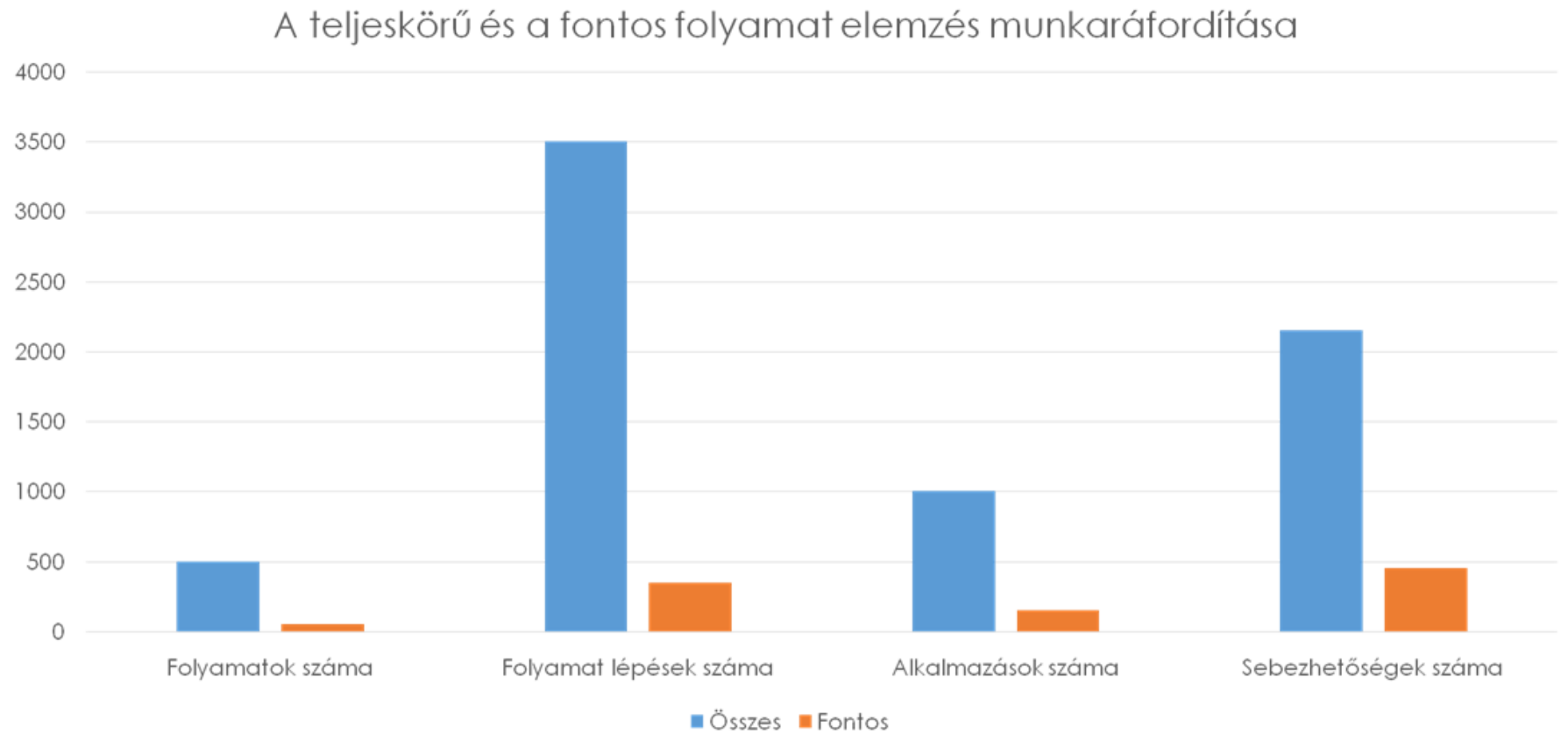
# Fontos erőforrások






ADAPTO

# Célzott kockázatelemzés






ADAPTO