

euro one



# Cyber Summit Budapest 2025

## Életmentő GRC Platform

Peter Szigetvari

Governance, Risk Management and Compliance Advisor @ EURO ONE





# GRC papíron – Mi van a dobozokban?

## Governance

- Irányelvek, külső és belső kötelezettségek
- Szabályzatok, magas szintű követelmények, vezetői támogatással
- Tiltott gyakorlatok
- Utasítások
- Eljárások
- Szerepkörmeghatározások
- Felelősségi körök

## Risk Management

- Fenyjegetések
- Sebezhetőségek
- Vagyonelemek
- Izolált nyilvántartások
- Risk regiszterek (IT, Sec, TPRM, BCM)
- Intézkedési tervek

## Compliance

- Követelménykatalógusok
- Védelmi intézkedések design dokumentumai
- Check listák
- Bizonyítékok
- Jelentések
- Intézkedési tervek







# Meddig juthatunk papírral?

## Ahová nem

- Eseményvezérelt folyamatokig
- Számonkérhetőségig
- Valós idejű adatokhoz
- Objektív döntéshozásig
- Külső partnerek hatékony bevonásáig
- Változások automatikus észleléséig

## Ahová igen

- Autonóm rendszerekből kiexportált, és már nem a valóságot tükröző adatokhoz (pillanatfelvételek)
- Összelinkelt Excel táblákhoz
- Manuálisan készített jelentésekhez (ppt, excel charts)
- Kockázatos adathozzáféréshez
- Függőségeket nem kezelő nyilvántartásokhoz
- Kényszerű egyszerűsítésekig





# Hamis biztonságérzet

## Ahogy az lenni szokott

- Szabályzatok a polcon
  - Senki nem tudja, hogy hol vannak
- Eljárások a fiókba
  - Nem szokták kivenni
- Kinek mi a dolga
  - Mindenki csinál minden, vagy senki nem csinál semmit
- Rendszeres felülvizsgálat
  - Last modified: 2004.01.01
- Komplex és folyamatos feladat
  - Értéktelenségig egyszerűsített kivitelezés
  - Jó esetben évente megismételt
  - Excel risk register (bizalmas, de mindenki férjen hozzá aki felelős)
  - Kapcsolódó kockázatsökkentő akciótervek, projectek valahol máshol
  - Védelmi intézkedések értékelése valahol máshol
  - Sok a „szerintem” faktor a hiányzó vagy az ismeretlen információ miatt
- Célként van meghatározva
  - Nem a jó működés következményeként



**A megfelelés és nem megfelelés között van tolerancia: pontrendszer határérték, %, #.**

Van DR szabályzat? I, Van back-up stratégia? I, Ellenőriztük a back-up-ot? I, Hogy bizonyítjuk? Minden reggel megnézem. Visszatöltés tesztelve van? I A kisebb VM-eknél.  
És a nagyobbak? Azok ugyanúgy működnek mint a kisebbek. **Ups!!!**





# A strukturált adat irányába

| Nem Strukturált adat                             | Strukturált adat                       |
|--------------------------------------------------|----------------------------------------|
| Kereshetetlen vagy manuális feldolgozást igényel | Kereshető és lekérdezhető              |
| Nem automatizálható                              | Automatizálható                        |
| Nem biztosít konzisztenciát                      | Összehasonlítható és aggregálható      |
| Gyenge integritás védelem                        | Auditálható és bizonyítható            |
| „Előregedő” információ                           | Élő információként kezelhető           |
| File szintű access control (discretionary)       | Record vagy mező szintű access control |







# Eseményvezérelt reminder – Ez még nem GRC, de GRC eszköz

| Nélküle                                                   | Vele                                          |
|-----------------------------------------------------------|-----------------------------------------------|
| Szabad szöveg, e-mail, Word, Excel, verziók kavalkádja    | Táblázatszerű (DB), lekérdezhető, konzisztens |
| „Ki csinálta meg? Mikor? Hol van róla nyom?”              | Automatikus státusz, határidő, felelős        |
| PDF-ekből, e-mailekből manuális visszafejtés              | Naplózott, kereshető, visszakereshető         |
| „Valaki elfelejtette” vagy „nem szólt neki senki”         | Workflow, automatikus értesítés, dashboard    |
| Statikus Excel tábla, amit senki sem frissít hónapok óta  | Újraértékelhető, dinamikusan változó mátrix   |
| Személyes meggyőzés, e-mailek, „emlékszem hogy csináltuk” | Feladat-alapú, állapotalapú riport            |





# A tervezés

Aztán csináunk egy egységes control katalógust, a kontrollokat szerepkörökhöz És kockázatokhoz rendeljük! És a kontrol működésének bizonyítékát is

Abban biztos benne van a folyamatok és IT szolgáltatások kapcsolata is! Meg a felelősök is. Importáljuk be!

Előbb nézzük meg, hogy milyen követelményeknek kell megfelelnünk, aztán átnézzük a szabályzatainkat. Ez abban segít, hogy össze map-elhessük őket.

De mitől fog ez Működni?

A követelmények le vannak bontva feladatokká. A Feladatoknak vannak felelősei és határideje. Az elvégzett feladatnak van bizonyítéka. Csak a papíron definiált folyamatinkat kell egy workflow-ban automatizálni!

Határozzuk meg a szerepköröket. Az AD-ban benne van mindenki. Importáljuk be!

Az üzleti folyamatok listáját kérjük el a BCM-esektől. Biztos Van BIA. Importáljuk be!

Ez életmentő lehet!

És ez még nem Minden!

És az IT szolgáltatásokkal!

És a szolgáltatók a beszerzéstől. Összeköthetnénk a folyamatokkal!

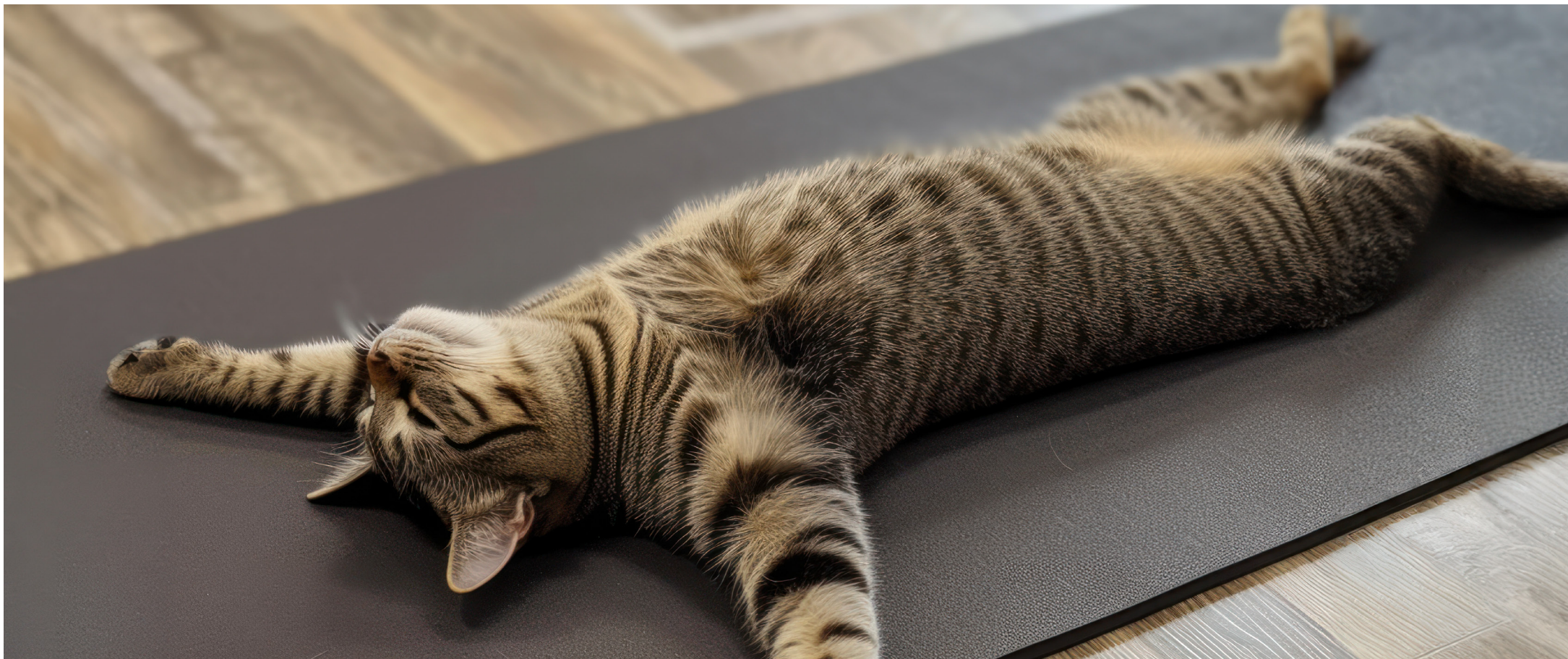
A Szabályzatokkal mi lesz? Abban vannak a követelménynek.







# Nem halott, csak gondtalan







Köszönjük!

euro one