

# HRP Europe Kft.

Új biztonsági stratégiák  
Compliance megfeleléssel

2025



# Mi az a vállalati stratégia?



A vállalati stratégia központi eleme (pl. üzleti terv - jövőkép, küldetés, ütemterv)

Ebből a technológia:

- Versenyelőnyt biztosít,
- Valós idejű adatokat biztosít,
- Üzleti rugalmasságot biztosít

„A Z generáció számára a munka nem helyhez kötött tevékenység, hanem inkább a feladatokra és a teljesítményre koncentrálnak. Az otthoni munkavégzés és a rugalmas munkarend már elengedhetetlen elvárások a fiatal munkavállalók számára.”

# VÁLLALATVEZETŐK ÉS A DIGITÁLIS STRATÉGIA



## Mérés technológiai projekteknél

### **Időtáv**

Rövid táv:

Kezdeti megtakarítások?

Hosszú táv:

Versenyelőny, skálázhatóság=SLA,  
KPI

### **Költség**

Beruházás: Szoftver, hardver, tanácsadás, karbantartás és frissítések!

### **Nyereség**

Költségcsökkentés (pl. adminisztrációs költségek csökkenése).  
Növekvő bevétel az ügyfélmegtartás vagy új piacok által.

### **Kvantitatív:**

Közvetlen megtakarítások (pl. kevesebb munkaerő-ráfordítás).  
Termelékenység növekedés (pl. 20%-kal gyorsabb folyamatok).

### **Kvalitatív:**

Ügyfélélegedettségi növekedése.  
A „márka” piaci pozíciójának erősödése.

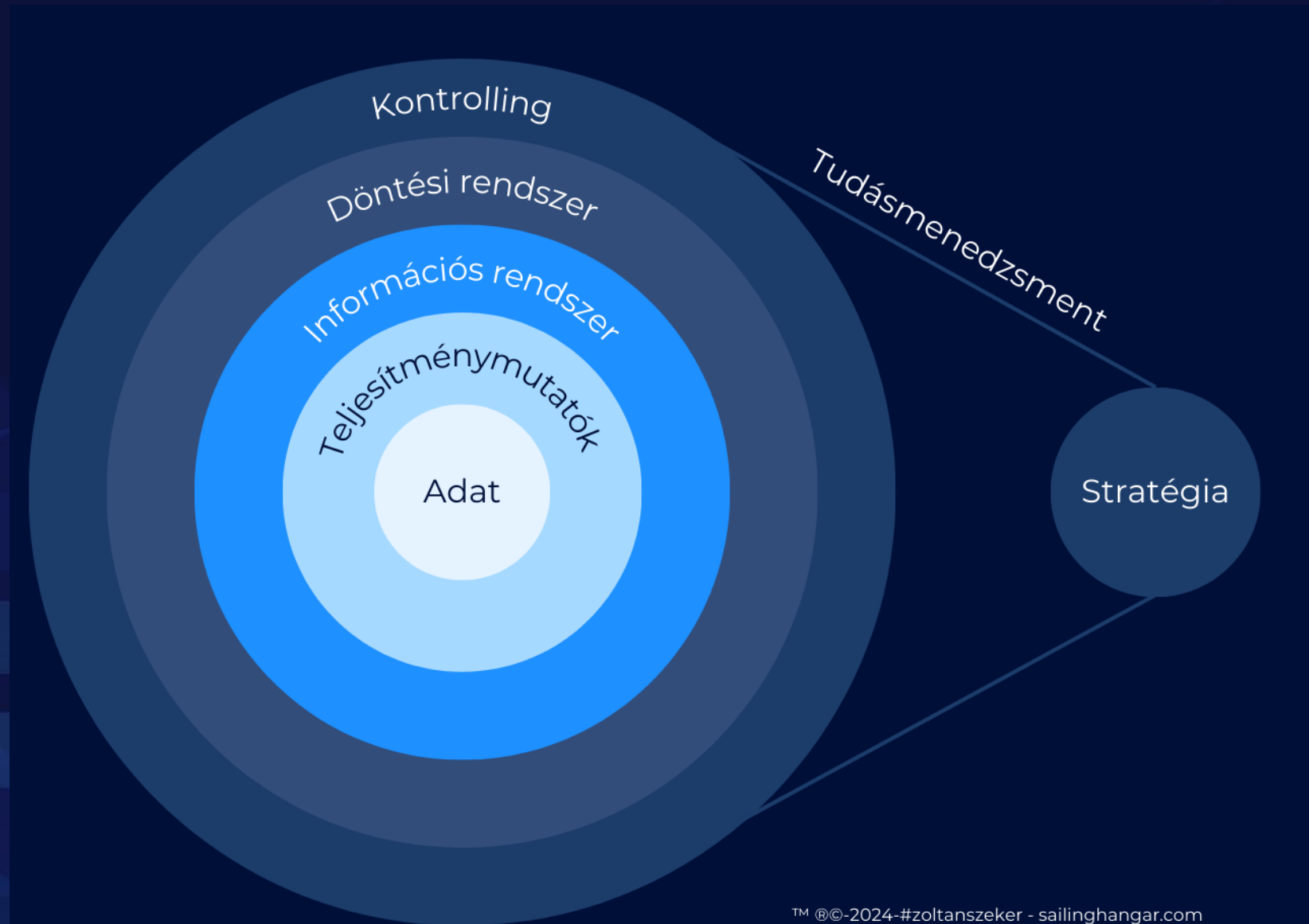
# VÁLLALATVEZETŐK ÉS A DIGITÁLIS STRATÉGIA



- „Működtetés” (az alapok fenntartása)
- Üzleti eredmények javítása
- Kommunikáció

-----

**2024-es PWC felmérés szerint az AI-t nem mint technológiai eszközt érdemes kezelni, hanem az üzleti stratégiák, termékek és szolgáltatások átalakításának alapvető elemeként.**



# Hogyan alakítja át a digitalizáció az üzleti modelleket és stratégiákat?



Compliance:

AI and Data Science

DORA - (EU) 2022/2554

NIS2

Kockázatmenedzsment

stratégia

ISO

új fogyasztói szokások megjelenése

automatizáció és hatékonyság

új kibertámadási szokások, AI segítségével

az üzleti átalakulása, digitális megoldások és az AI megjelenése – generációs változások

# Kockázatkezelés és irányítás:

## DORA / reziliencia képesség:

Operatív ellenállóképesség, intézkedések hatékonysága és értékelése

ICT SWOT azonosítás

Forgatókönyv-alapú tesztelés végrehajtása - zavarok szimulálása érdekében

A kritikus entitások esetében Threat-Led Penetration Testing (TLPT) végrehajtása - valós fenyegetések értékelése.

## Külső szolgáltatók kockázatkezelése:

- A DORA rendelet hangsúlyozza a **kritikus és fontos** funkciók kiszervezésekor a külső szolgáltatók kockázatainak aktív kezelésének a kikényszerítését.
- Stratégiai szerződések tárgyalása külső szolgáltatókkal.
- A szolgáltatás megszüntetésére, teljesítménykövetelményekre és kontrollmechanizmusokra vonatkozó elvárások rögzítése.
- Átlátható felügyeleti eszközök alkalmazása a partner biztonsági és működési kockázatainak kezelésére.
- A partner megfelelésének biztosítása a vállalati kockázatkezelési irányelvek mentén.

# ARCSEERVE MEGOLDÁSOK

A DORA előírja, hogy a pénzügyi szervezeteknek ki kell dolgozniuk és dokumentálniuk kell olyan biztonsági mentési szabályzatokat és eljárásokat, amelyek meghatározzák a mentésre kerülő adatok körét és a mentés minimális gyakoriságát, figyelembe véve az információk kritikus jellegét vagy az adatok bizalmassági szintjét.

Megfelelnek-e a mentési gyakorlataink a DORA által elvárt üzletmenet-folytonossági és incidens-ellenállósági elvárásoknak?

- Mentési gyakoriság.
- Visszaállítási célok.
- Tesztelés
- Képzés

Az Arcserve megoldásai biztosítják a kritikus üzleti adatok védelmét és helyreállíthatóságát a Microsoft és más felhőalapú alkalmazásokban – ezáltal támogatva a DORA által megkövetelt digitális működési ellenállóképességet és adatbiztonságot.

# FORTINET® MEGOLDÁSOK

Legyen szó technikai hibáról vagy biztonsági incidensről, a működés leállása mindenkire hat – az ügyfelek viszont nem várnak, hanem továbblépnek.

FortiSIEM®, FortiTester, FortiNAC

A DORA által előírt digitális működési ellenálló képesség biztosításához elengedhetetlen felgyorsítani a problémák elhárítását. (Adatvédelem és megfelelőség, hibák csökkentése, biztonsági kockázatok megelőzése. )

Miért fontos ez?

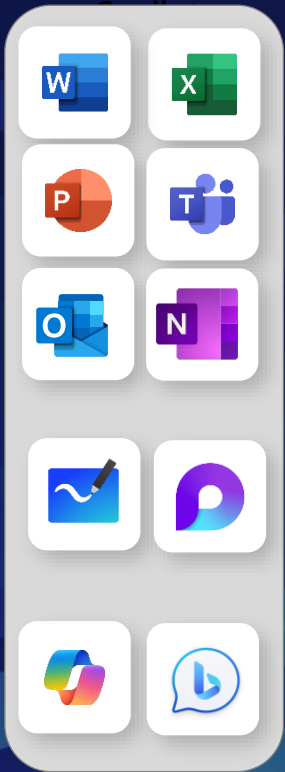
A Fortinet megoldásaival valós idejű eseménykezelése és automatizált válaszmechanizmusai révén minimalizálja a rendszerleállásokat

A Fortinet megoldások csökkentik a manuális feladatokat és növelik a hatékonyságot

Kiberbiztonsági tudatosság és a fejlett analitikai képességek lehetővé teszik a gyanús tevékenységek azonosítását és kezelését.

# COPILLOT (AI) és MICROSOFT

Microsoft



A Baby Boomer generáció tagjainak 73%-a, míg a Z generációs munkavállalók 85%-a használ olyan AI eszközöket a munkavégzés során, amelyeket nem a munkáltatójuk biztosított.

A „Digital Operational Resilience Act” (DORA) széles körű pénzügyi entitásokat érint, beleértve a bankokat, fizetési intézményeket, befektetési vállalkozásokat és kriptoeszköz-szolgáltatókat is. A mesterséges intelligencia egyre inkább beépül a pénzügyi szektor működésébe, miközben a szabályozások, mint a DORA, MiCA, AI Act igyekeznek biztosítani a digitális működési ellenálló képességet és a biztonságos AI-használatot.

## DORA szabályozás hatások:

Kiberbiztonság

Kockázatkezelés

Megfelelőségi intézkedések

## Miért érdemes a Microsoft 365 Copilotot használni?

Elemzés/ modellezés – **Integrálhatóság(!)**

PI. Call center panaszkezelés - **Megfelelőségi intézkedések**

Folyamat optimalizálás – **AI Agentek**

# Kockázatkezelés és irányítás:

- Hatékony kockázatkezelési stratégiák tervezése és végrehajtása.
- Folyamatos kockázatértékelések elvégzése a sebezhetőségek azonosítása érdekében.
- Megfelelő kiberbiztonsági védelmi intézkedések bevezetése.
- Az ICT kockázatok kezeléséért felelős szerepek és felelősségek meghatározása.

## **Incidentsreagálás és jelentéstétel**

Incidentsfigyelő rendszerek bevezetése az események gyors észlelésére és kezelésére.

Az események súlyosság és hatás alapján történő osztályozása.

Az események jelentése a szabályozó hatóságoknak és az érintett feleknek a meghatározott határidőkön belül.

Az események részleteinek dokumentálása a további elemzés és fejlesztés céljából.

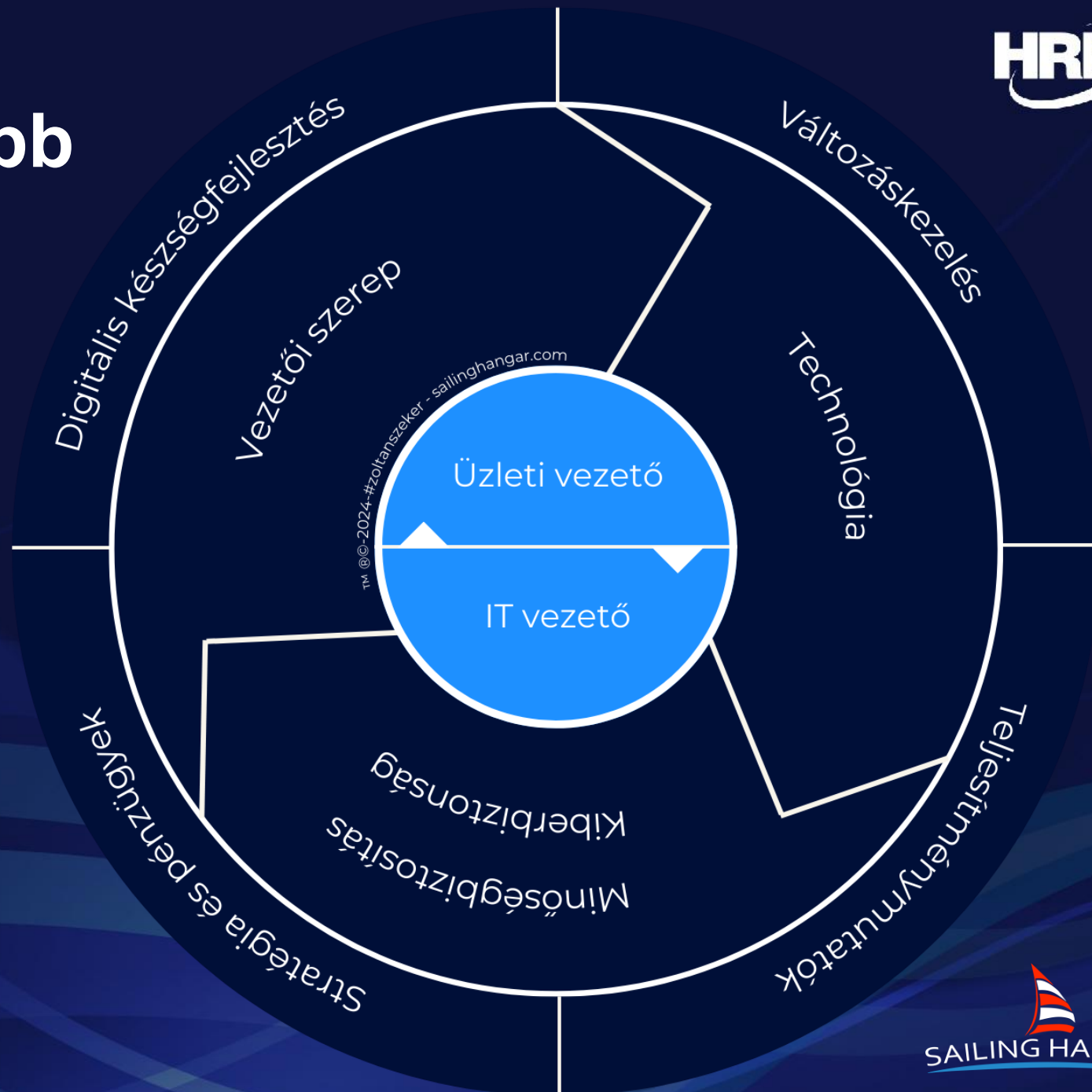
# A vezetőkre nagyobb felelősség hárul!

- Döntéshozatal alapja
- Forrásallokáció (ICT védelem)
- Teljesítménymutatók

-----

A digitalizációs projektek 81%-a nem haladt előre, vagy nem érte el a kitűzött üzleti célokat!

<https://fortinetatc.hrp.hu/>  
<https://www.oditsolutions.hu/>



# Köszönöm a figyelmet!

---

**Szekér Zoltán**

**Kiberbiztonsági és digitalizációs szakértő**

**+36305603158**



Konzultáció

# Achievements

