ADAPTO

GDPR-
INFORMATIKAI MEGOLDÁSOK A JOGI MEGFELELÉS BIZTOSÍTÁSÁNAK ÉRDEKÉBEN

Pflanzner Sándor – ADAPTO Solutions

Kockázatelemzés követelménye

Az adatkezelő és az adatfeldolgozó ... a változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja .. :

- a személyes adatok álnevesítését és titkosítását
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

ADAPTO

Hatáselemzés

- Érintett adatok köre (az összes adatok közül)
  - nem érintett
  - személyes
  - különleges személyes
- Érintett adatelemek
  - célhoz kötöttségi elemzés
  - érdekmérlegelési teszt
- Adatkezelésbe bevontak köre
  - adat kezelése (adatkezelő és feldolgozó)
  - adatmegosztás

ADAPTO

Kockázat = Hatás * Valószínűség

Hatás csökkentése
- Csak a legszükségesebb adatkategóriák gyűjtése
- A lehető legkevesebb érintett bevonása (adatmegosztás)
- A kockázatok megosztása az adatfeldolgozókkal

Keretrendszer: GDPR

} Jogi szakterület

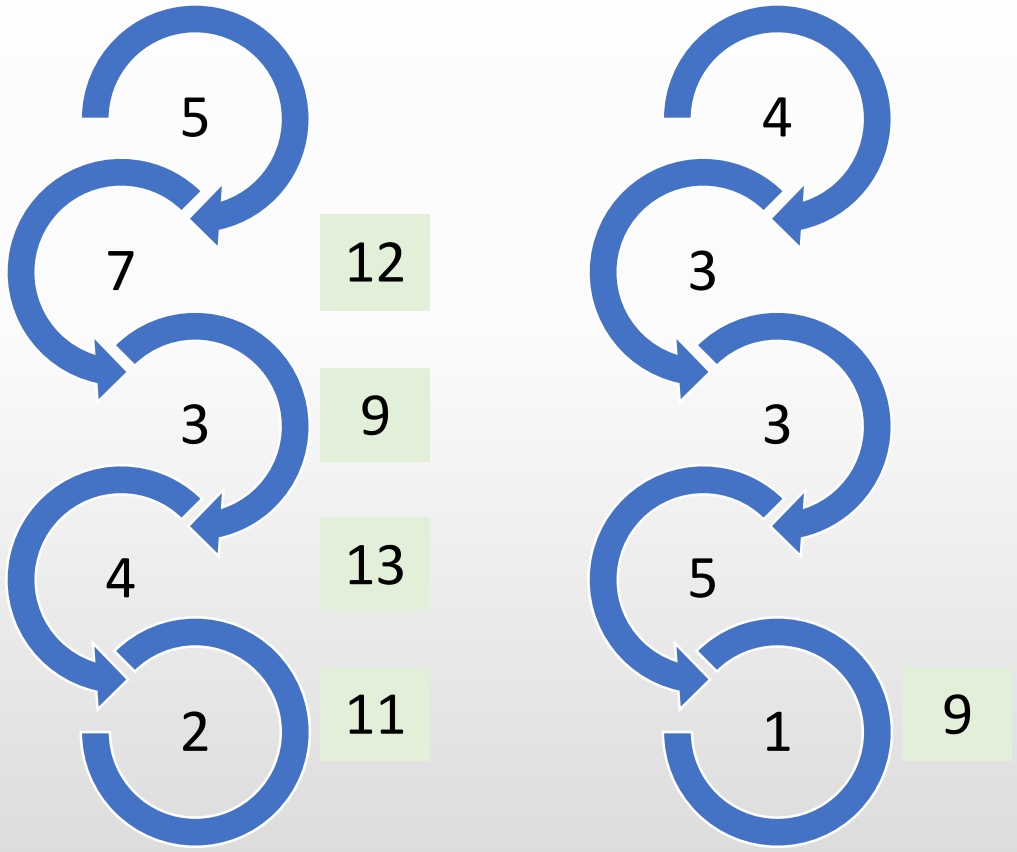
Valószínűség csökkentése
- Az adatot kiszolgáló infrastruktúra védelme

Keretrendszer: ISO 27001

} Informatikai szakterület

ADAPTO

Módszeres elemzés képessége

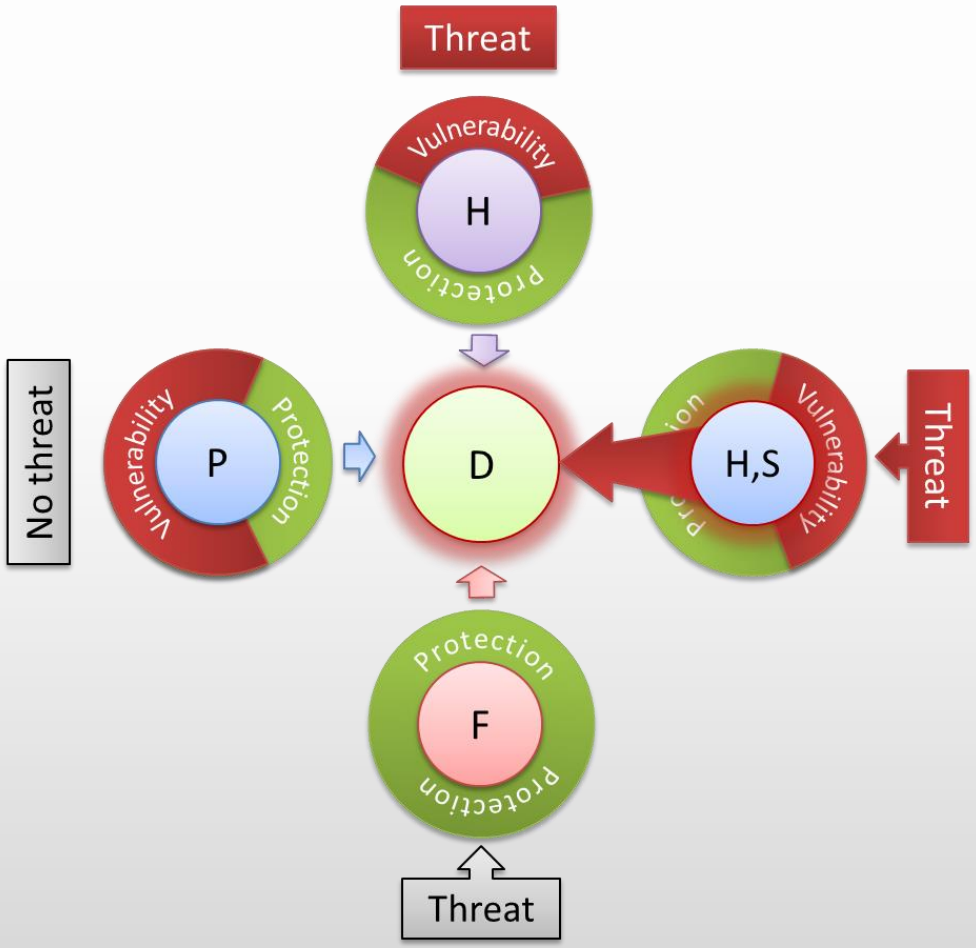


Jó az eredmény?

Honnan tudja?
Hogyan derítette ki?

ADAPTO

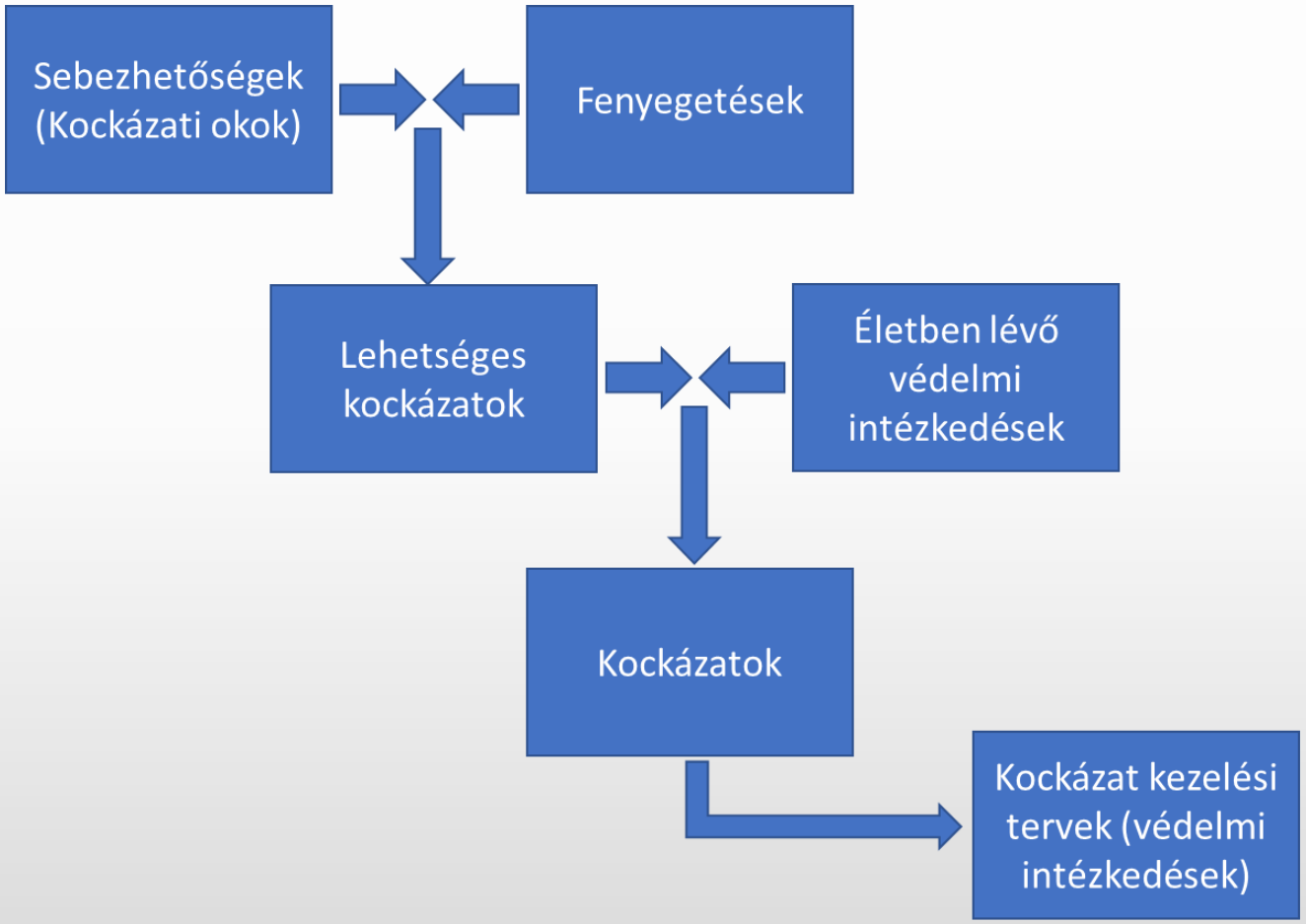
Sérülékenységek módszeres elemzése (COBIT)



Folyamatok
Kiszolgáló személyzet
Hardverek, szoftverek
Létesítmények

ADAPTO

Kockázatelemzés CRAMM módszertan szerint



Védelmi intézkedések

Adminisztratív

Logikai

Fizikai

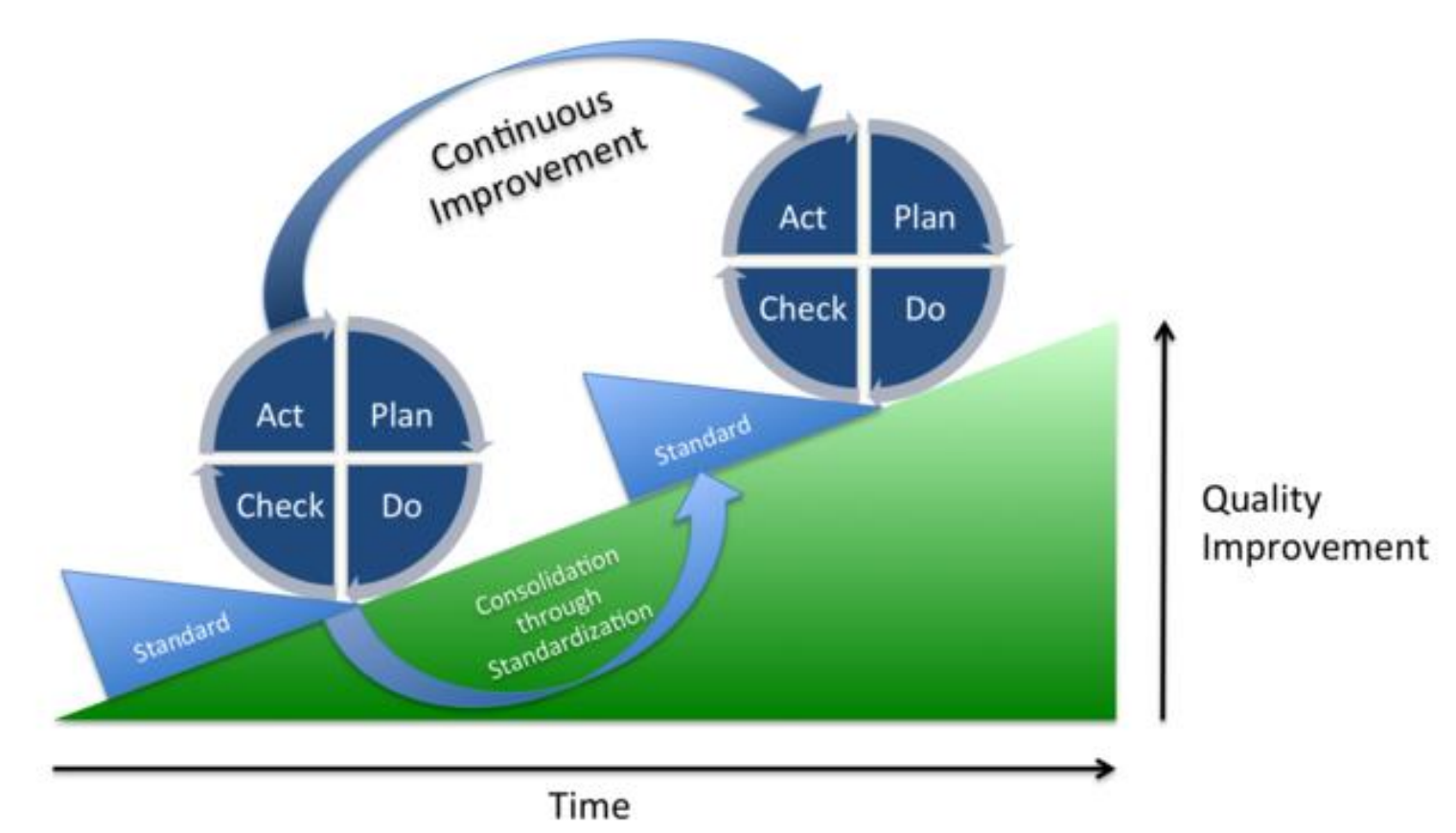
ADAPTO

Szempontok az információbiztonsági vizsgálathoz

- fejlesztés
- fizikai biztonság
- hálózat hozzáférés, - biztonság, kábelbiztonság
- hozzáférés szabályozás
- incidenskezelés
- információ továbbítás, kommunikáció
- információ biztonsági szabályozás különböző területekre
- információhordozók
- jelszókezelés
- kapacitáskezelés
- külső felek, kapcsolat
- mobil eszköz szabályzat
- naplózás
- szellemi tulajdonjog, titoktartás
- szerepkörök megfelelése
- távmunka
- üzemeltetés
- üzletmenet folytonosság
- vagyonelemek
- változáskezelés

ADAPTO

Információbiztonság folyamatos fejlesztése

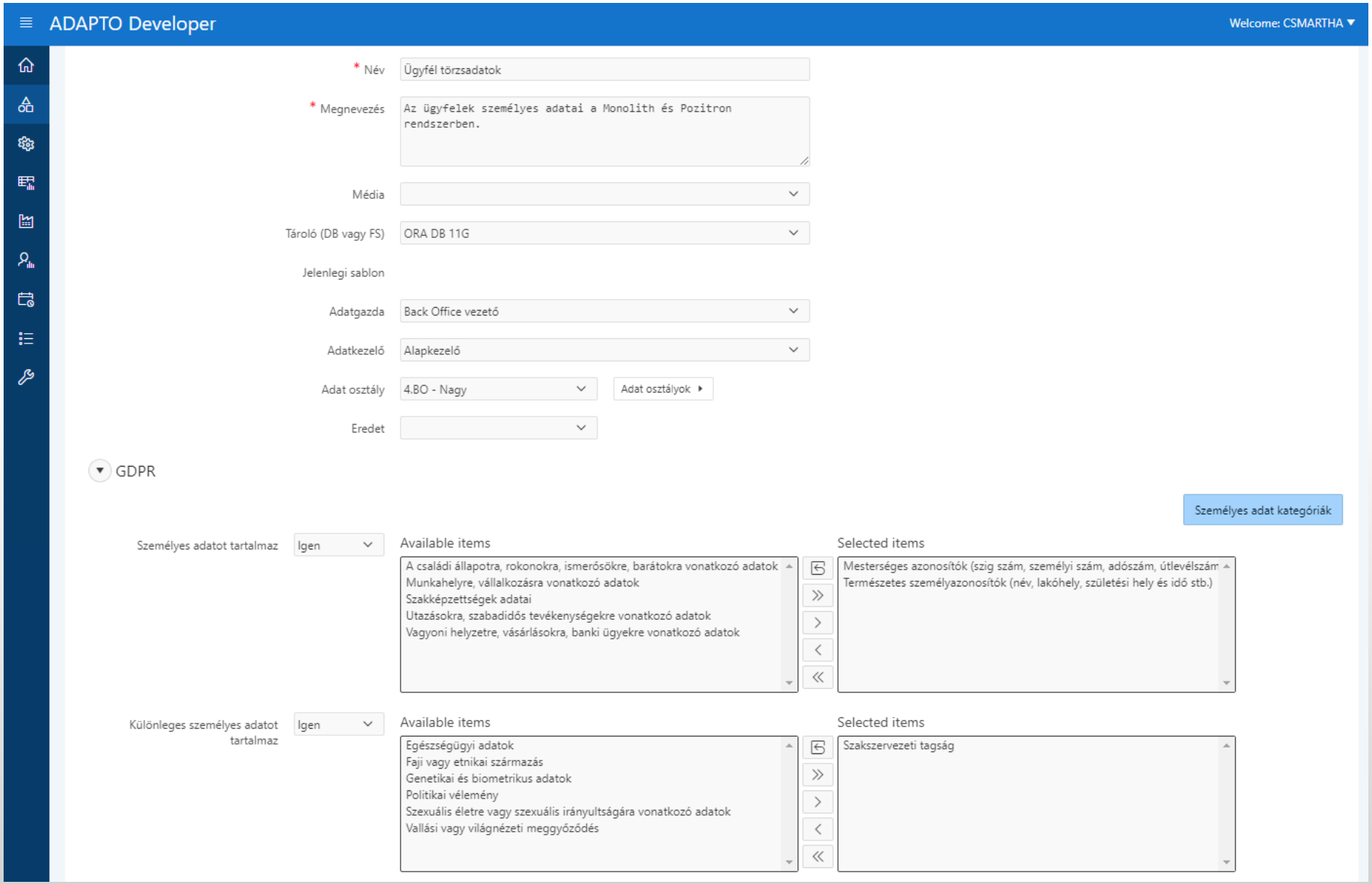


Összefoglalás – ADAPTO módszertan

1. Adatköröket összegyűjteni a vállalatban
2. Adatvagyon infrastruktúrát összeállítani
3. Adatköröket tovább elemezni:
   Személyes adat-e (ha igen, melyik kategóriákba tartozik)
   Különleges személyes adat-e (ha igen, melyik kategóriákba tartozik)
   Adatkezelés célja, jogalapja, megtartási idő, szabályzat
   Adatkezelő, Adatfeldolgozó
4. Hatás csökkentése
   Célhoz kötöttségi audit, érdekmérlegelés, adatmegosztási audit
5. Kockázat felmérés (kár bekövetkezési valószínűségének csökkentése)

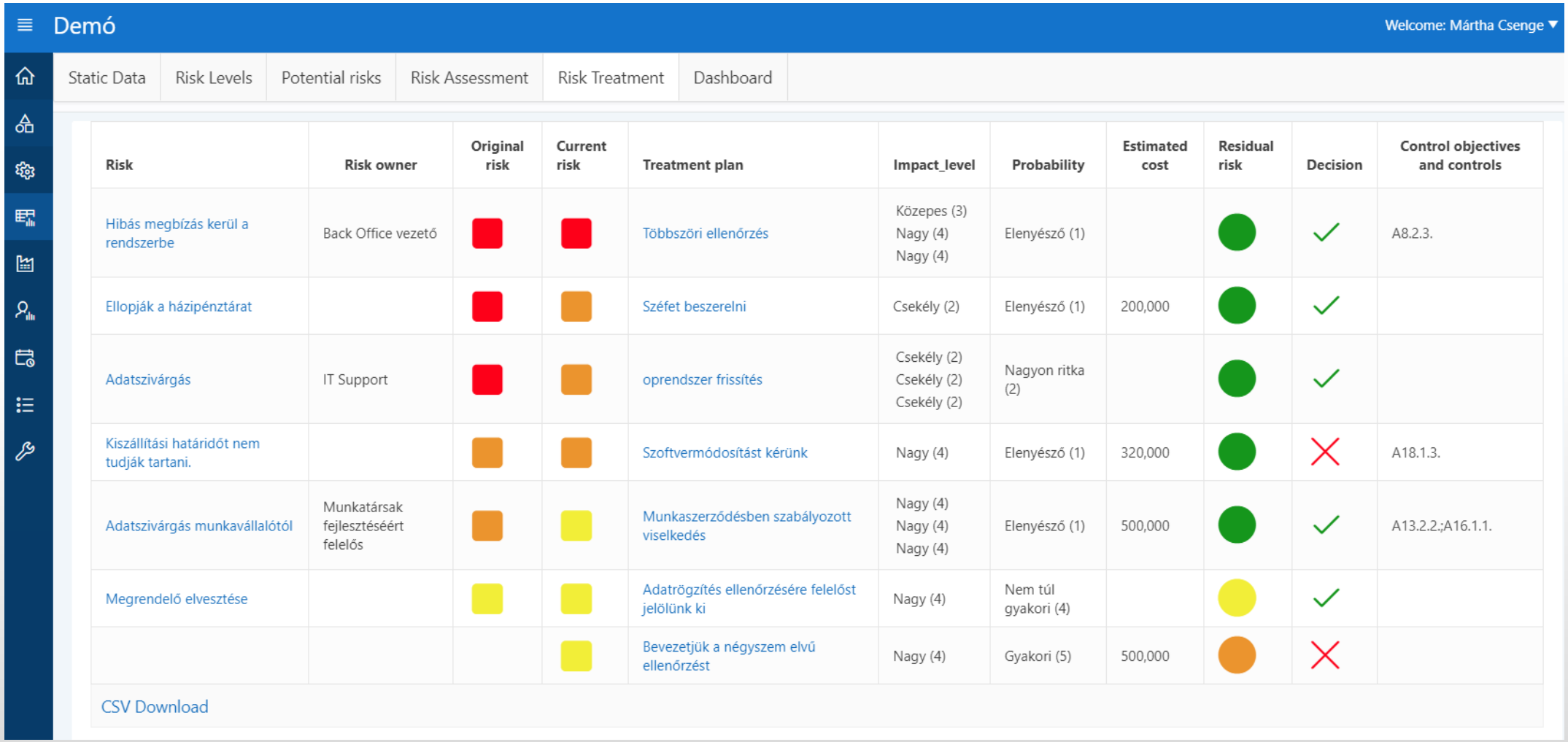
ADAPTO

Adatok kiegészítő nyilvántartása



ADAPTO

Kockázatelemzés és kezelés



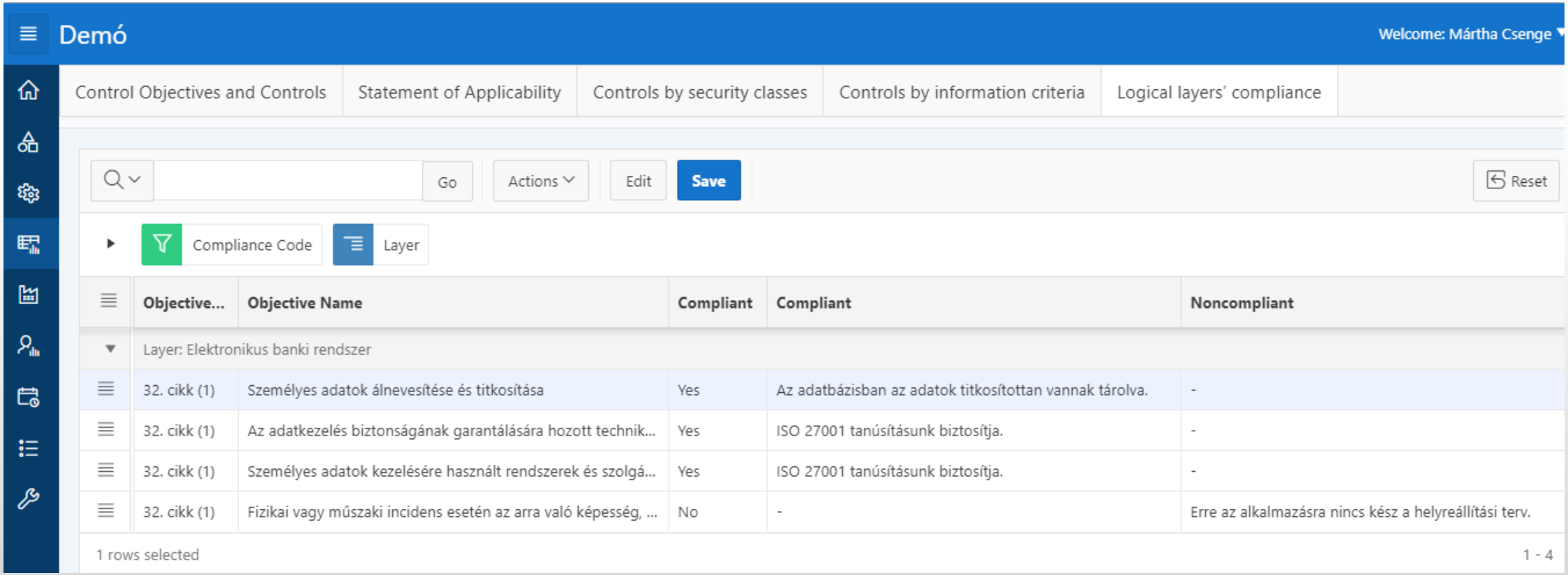
Risk	Risk owner	Original risk	Current risk	Treatment plan	Impact_level	Probability	Estimated cost	Residual risk	Decision	Control objectives and controls
Hibás megbízás kerül a rendszerbe	Back Office vezető			Többszöri ellenőrzés	Közepes (3) Nagy (4) Nagy (4)	Elenyésző (1)			✓	A8.2.3.
Ellopják a házipénztárat				Széfet beszerelni	Csekély (2)	Elenyésző (1)	200,000		✓	
Adatszivárgás	IT Support			oprendszer frissítés	Csekély (2) Csekély (2) Csekély (2)	Nagyon ritka (2)			✓	
Kiszállítási határidőt nem tudják tartani.				Szoftvermódosítást kérünk	Nagy (4)	Elenyésző (1)	320,000		✗	A18.1.3.
Adatszivárgás munkavállalótól	Munkatársak fejlesztéséért felelős			Munkaszerződésben szabályozott viselkedés	Nagy (4) Nagy (4) Nagy (4)	Elenyésző (1)	500,000		✓	A13.2.2.;A16.1.1.
Megrendelő elvesztése				Adatrögzítés ellenőrzésére felelőst jelölünk ki	Nagy (4)	Nem túl gyakori (4)			✓	
				Bevezetjük a négyszem elvű ellenőrzést	Nagy (4)	Gyakori (5)	500,000		✗	

CSV Download

ADAPTO

Alkalmazhatósági nyilatkozat

1. Kockázatkezelési tervek végrehajtása
2. Megfelelőségi nyilatkozat



ADAPTO