IT biztonság
2017/2018 tanév

A kockázatelemzés alapjai

security.hu

A kockázatelemzés alapjai

Botos Zsolt vezető tanácsadó, CGEIT, CRISC
Security.hu Kft.
zsolt.botos@security.hu
www.security.hu

security.hu

Bemutatkozás

Információbiztonsági megoldások már 15 éve

Szolgáltatások, megoldások

- Tanácsadói szolgáltatások
- Üzleti folyamat alapú megoldások
- Technológiai védelmi megoldások
- PKI megoldások
- Támogatás
- Oktatás

Auditok, vizsgálatok

- Üzleti folyamat alapú vizsgálatok
- Technológiai vizsgálatok
- Auditok

Botos Zsolt
ügyvezető, vezető tanácsadó,
CGEIT, CRISC
zsolt.botos@security.hu
www.securitiy.hu

A kockázatelemzés célja

Fő kérdések:

- Mi is az az információrendszer kockázatelemzés?
- Miért is kell kockázatelemzést végezni?

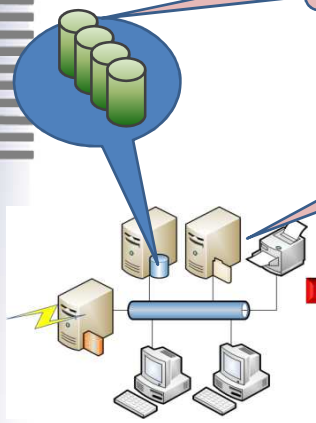
A kockázatelemzés célja

A szervezetek működése az adatvagyonuktól, elsődlegesen ennek rendelkezésre állásától, másodlagosan bizalmasságától és sértetlenségétől függ.

Az adatvagyont összetett, elosztott (diverzifikált) informatikai rendszereken kezelik és tárolják. Alapvetően e vagyonelemek felelnek a rendelkezésre állásért.

Az üzletmenet, a működés és a bevétel teljes körűen függ ezektől a vagyonelemektől

A szervezetnek tudnia kell; melyik vagyonelem fontos, melyik kevésbé fontos és melyik létfontosságú!

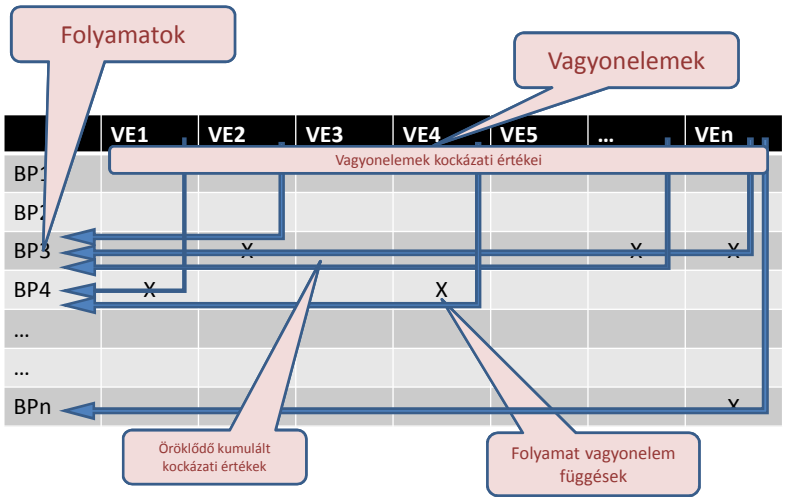


€, HUF, $

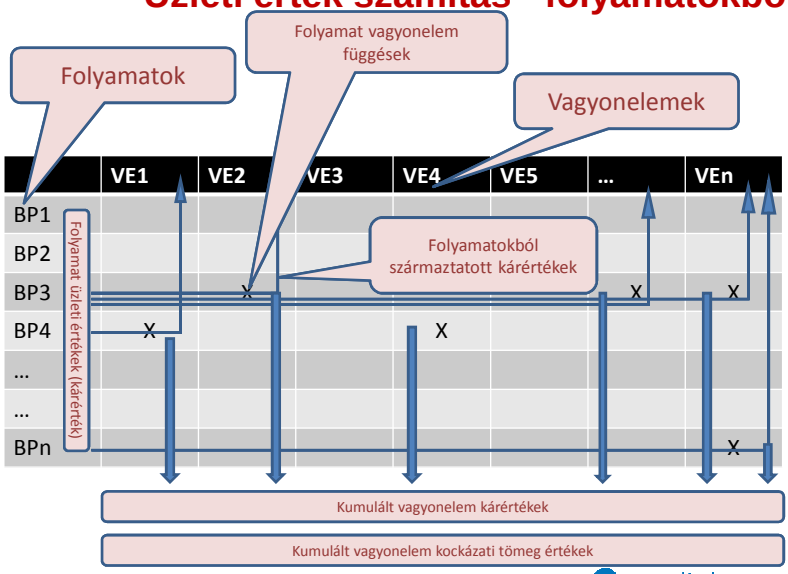
Rendszer 1	A
Rendszer 2	B
…	…
Rendszer 256	C

KOCKÁZATELEMZÉS

Alapkoncepció
Kockázati értékszámítás - vagyonelemekből



Alapkoncepció
Üzleti érték számítás - folyamatokból



Kockázatelemzés típusok

Kvalitatív kockázatelemzés, (üzleti hatáselemzés, BIA) főbb ismérvei

- Minőségi (kvalitatív), számszerűen nem mérhető ismérveken alapszik.
- Az informatikai rendszer üzletmenetre gyakorolt hatását csak minőségi jellemzők alapján veszi figyelembe.
- A szervezeti működést modelláló képessége erősen korlátozott.
- A kimenetei összetettebb szervezet és rendszer esetén kevéssé megbízhatók.
- Gyorsan, relatíve kevés erőforrás felhasználásával elvégezhető.

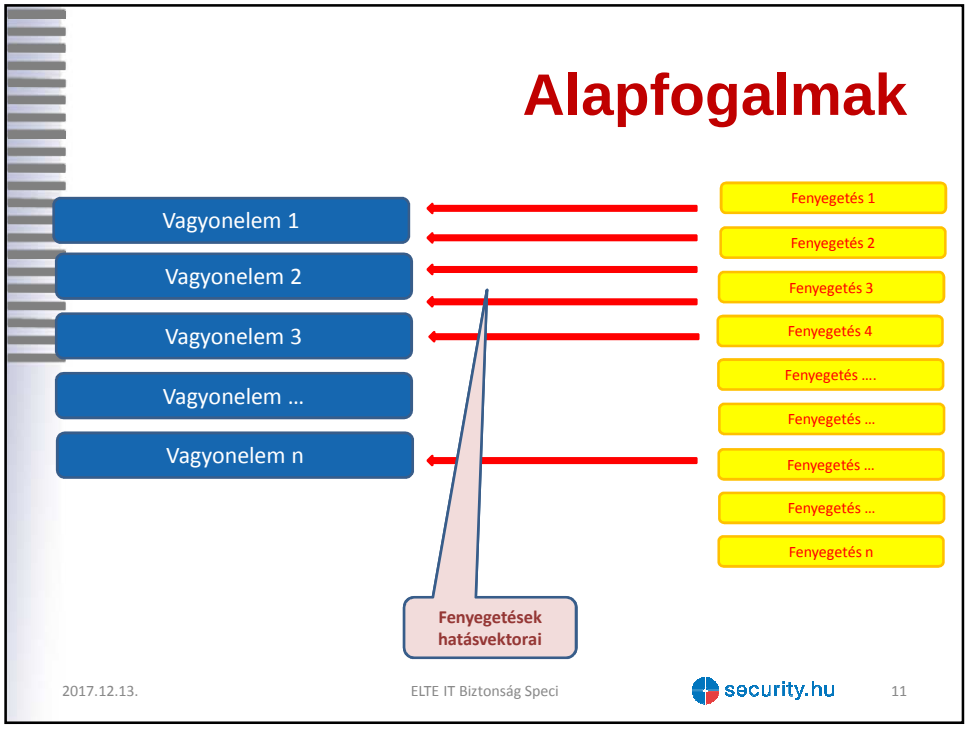
Kockázatelemzés típusok

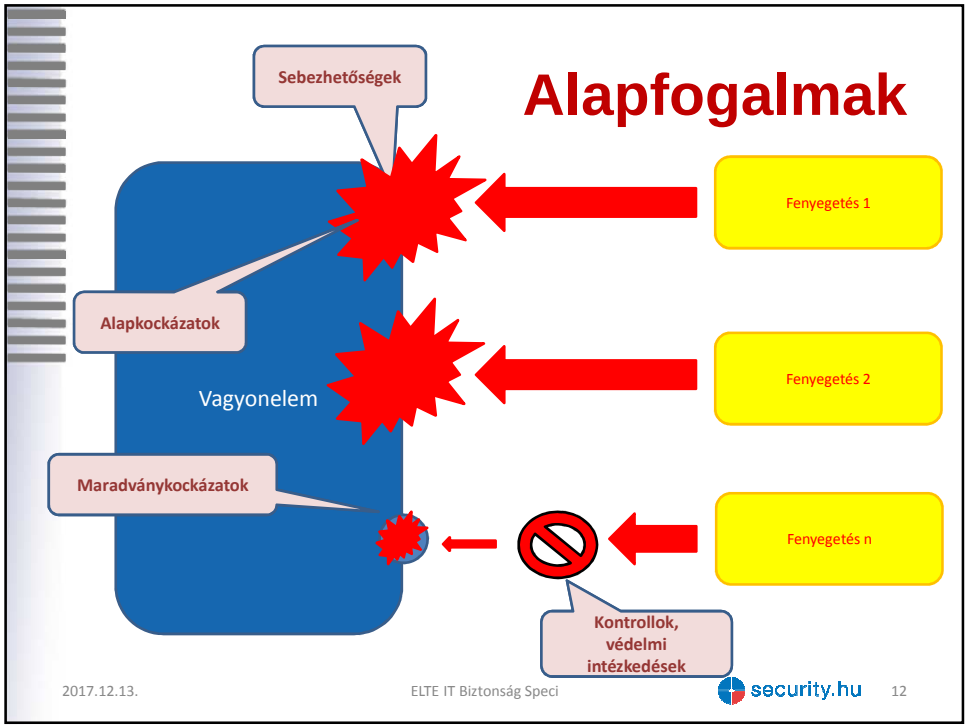
Kvantitatív (QN) kockázatelemzés főbb ismérvei

- Számszerű (kvantitatív), mérhető ***mennyiségi*** ismérveken alapszik.
  - Az informatikai rendszer üzletmenetre gyakorolt hatását elsődlegesen ***mennyiségi jellemzők*** alapján veszi figyelembe.
  - A nehezen számszerűsíthető, szubjektív jellemzők méréséhez a ***szubjektív skálák*** módszerét alkalmazza.
  - A szervezeti működést modelláló képessége kifejezetten erős.
  - A kimenetei nagyobb összetett szervezet és rendszer esetén is megbízhatóak.
  - Viszonylag sok erőforrást igényel.

Amiről most beszélünk

Kvantitatív (QN) kockázatelemzés


Alapfogalmak
Vagyonelem 1
Vagyonelem 2
Vagyonelem 3
Vagyonelem ...
Vagyonelem n
Fenyegetés 1
Fenyegetés 2
Fenyegetés 3
Fenyegetés 4
Fenyegetés ....
Fenyegetés ...
Fenyegetés ...
Fenyegetés ...
Fenyegetés n
Fenyegetések hatásvektorai
2017.12.13.
ELTE IT Biztonság Speci
security.hu
11


Sebezhetőségek
Alapfogalmak
Alapkockázatok
Vagyonelem
Maradványkockázatok
Fenyegetés 1
Fenyegetés 2
Fenyegetés n
Kontrollok, védelmi intézkedések
2017.12.13.
ELTE IT Biztonság Speci
security.hu
12

Kvatitatív kockázatelemzés folyamata

Információs vagyonleltár (Information Asset Inventory)

- Folyamatfelmérés
- Vagyonelem azonosítás
- Folyamat-vagyonelem függőségek felmérése

Fenyegetés katalógus (Threat Inventory)

- Fenyegetés katalógus
- Védelmi intézkedés katalógus
- Konvencionális értékmátrixok létrehozása

Kockázatelemzés (Risk Analisys)

- Kockázati mátrix prototípusok
- Vagyonelem kockázati mátrixok
- Folyamatok és vagyonelemek üzleti értékeinek számítása
- Folyamatok és vagyonelemek kockázati értékszámítása
- Kockázati besorolások készítése
- Kockázatkezelési terv készítése

Információs vagyonleltár

Információs vagyonleltár (Information Asset Inventory)

- Folyamatfelmérés
- Vagyonelem azonosítás
- Folyamat-vagyonelem függőségek felmérése

Fenyegetés katalógus (Threat Inventory)

- Fenyegetés katalógus
- Védelmi intézkedés katalógus
- Konvencionális értékmátrixok létrehozása

Kockázatelemzés (Risk Analisys)

- Kockázati mátrix prototípusok
- Vagyonelem kockázati mátrixok
- Folyamatok és vagyonelemek üzleti értékeinek számítása
- Folyamatok és vagyonelemek kockázati értékszámítása
- Kockázati besorolások készítése
- Kockázatkezelési terv készítése

Folyamatfelmérés

Információs vagyonleltár
Folyamatfelmérés

Folyamatmodell

- Elvi modell a folyamatok egymáshoz való viszonyának ábrázolásához

Folyamatok azonosítása

- A szer[illegible] konkrét üzleti-, működési folyamatainak azonosítása

Az elemzéshez mindenképp szükségesek

Folyamattérkép

- A konkrét folyamatok grafikus modellben való ábrázolása

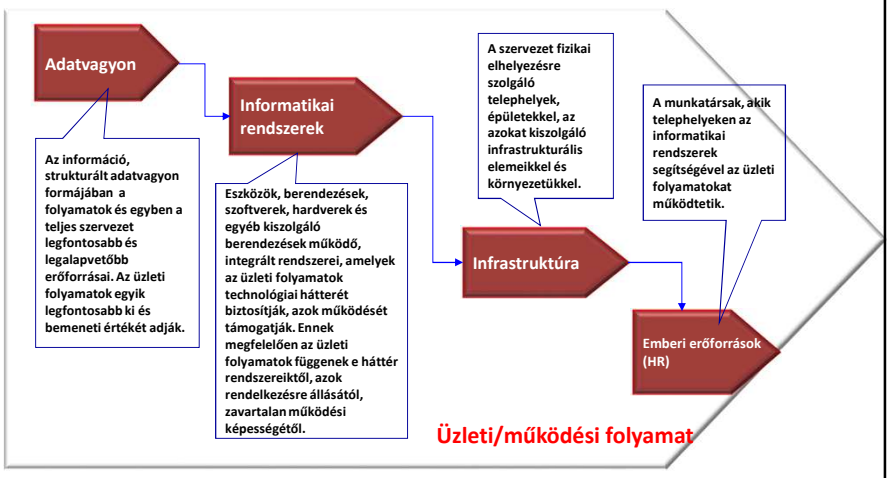
Folyamatábrák

- Az egyes folyamatok grafikus folyamatábráinak felvétele

Folyamatleírások

- Az egyes folyamatok narratív szöveges leírásai

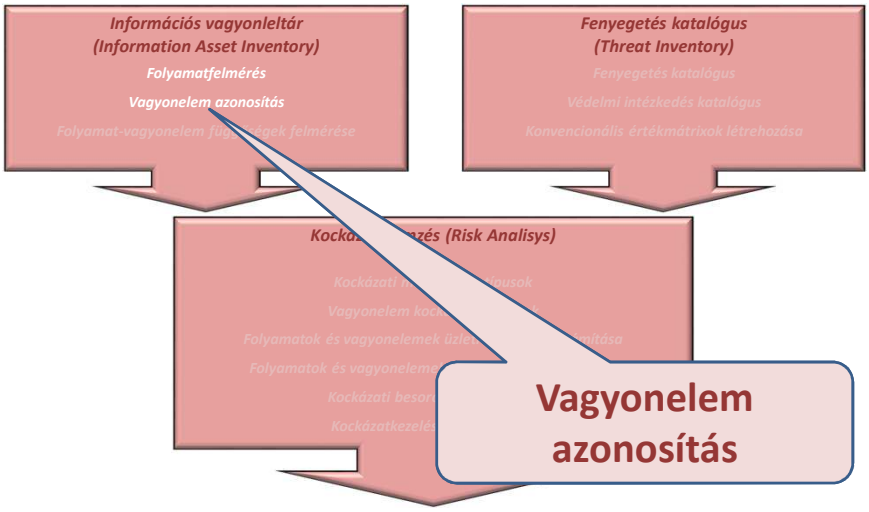
Információs vagyonleltár
Üzleti/működési folyamat vagyonelem osztályai



Információs vagyonleltár
Elvi folyamatstruktúra

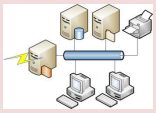
Folyamat		Alfolyamat	
Azonosító	**Folyamat név**	**Azonosító**	**Alfolyamat név**
BP 01	***Főfolyamat 1***	Azonosító	
		BP 01-01	Alfolyamat 1-1
		BP 01-02	Alfolyamat 1-2
		BP 01-03	Alfolyamat 1-3
		BP 01-04	Alfolyamat 1-4
BP 02	***Főfolyamat 2***		
		BP 02-01	Alfolyamat 2-1
		BP 02-02	Alfolyamat 2-2
		BP 02-03	Alfolyamat 2-3
		BP 02-04	Alfolyamat 2-4

Információs vagyonleltár



Információs vagyonleltár
Vagyonelemek azonosítása és osztályozása

Alapvető vagyonelem osztályok

Adat (D)	Rendszer (IT)
	
Munkaerő (HR)	**Infrastruktúra (I)**

Információs vagyonleltár

Információs vagyonleltár
(Information Asset Inventory)
Folyamatfelmérés
Vagyonelem azonosítás
Folyamat-vagyonelem függőségek felmérése

Fenyegetés katalógus
(Threat Inventory)
Fenyegetés katalógus
Védelmi intézkedés katalógus
Konvencionális értékmátrixok létrehozása

ázatelemzés (Risk Analisys)
ix prototípusok
mátrixok

Folyamat-vagyonelem függőségek felmérése

Információs vagyonleltár
Folyamat-vagyonelem függőségek modellezése

- Cél: annak felmérése, hogy az egyes folyamatok mely vagyonelemektől és milyen mértékben függenek.
  - Vagyonelem folyamat függőség modellezésére a folyamat-vagyonelem mátrixokat hozunk létre
    - A függést a vagyonelem hatásindex-szel modellezzük [%]
    - Elsősorban a vagyonelem rendelkezésre állását modellezzük.
- A vagyonelem-hatásindex konvencionális értékű. Értéke 0% és 100% közé eső számérték lehet a konvenció helyzet- és környezetfüggő értelmezése szerint.

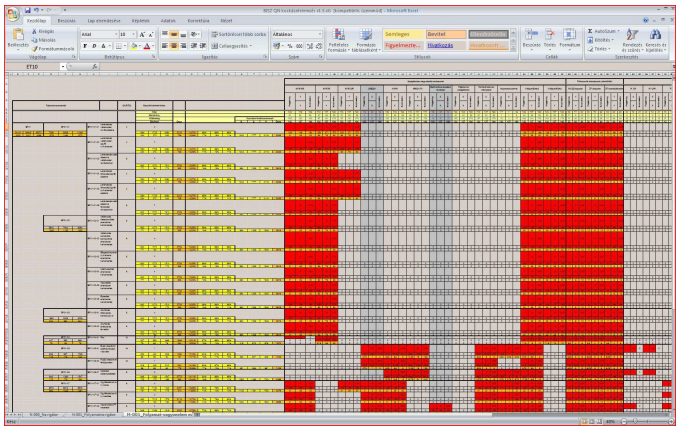
Információs vagyonleltár
Folyamat-vagyonelem függőségek feltérképezése

Folyamat-vagyonelem relevancia mátrix

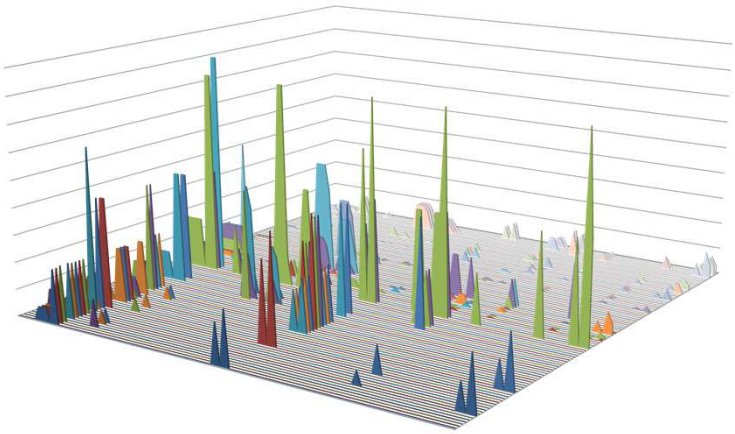
	VE1	VE2	VE3	VE4	VE5	…	VEn
BP1	45%				75%		
BP2							
BP3		50%			100%	25%	20%
BP4	25%			100%		100%	
…					25%		
…							
BPn		15%				100%	

Információs vagyonleltár
Folyamat-vagyonelem mátrix példa (részlet)

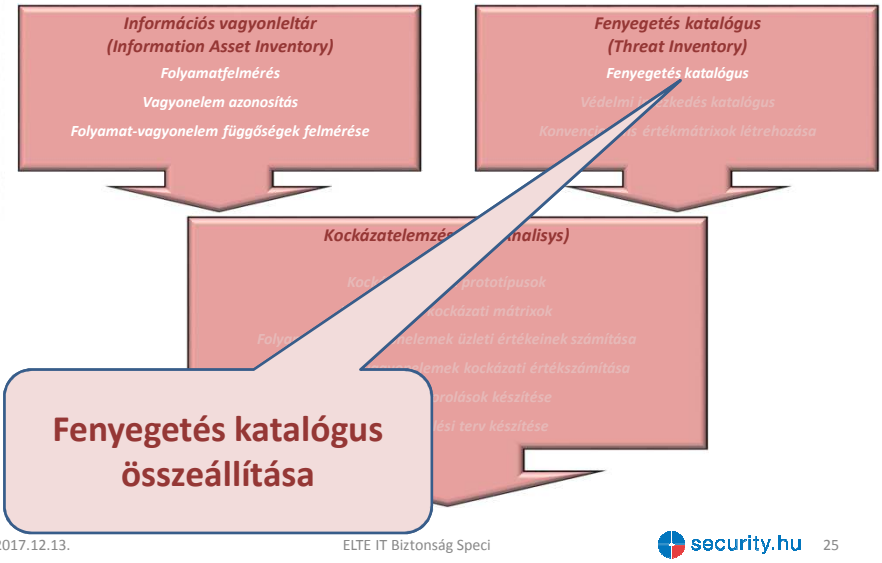
Folyamatok és vagyonelemek egymástól való függőségeinek felmérése



Információs vagyonleltár
Folyamat-vagyonelem függőségek



Fenyegetéskatalógus

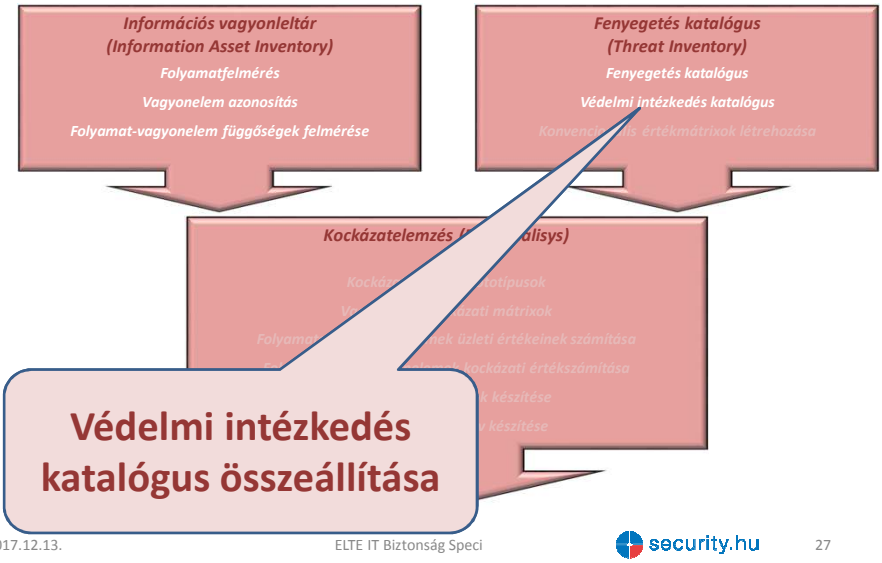


Fenyegetéskatalógus
Fenyegetés alapkatalógus elkészítése

Fenyegetés alapkatalógus elkészítése a különféle fenyegetés osztályokban:

- Természeti eredetű fenyegetések N[x]
- Infrastrukturális eredetű fenyegetések I[x]
- Akaratlan humán eredetű hibák AHH[x]
- Akaratlan humán eredetű információsértések AHI[x]
- Informatikai eredetű hibák IH[x]
- Akaratlagos informatikai támadások AIT[x]
- Akaratlagos információsértések AIS[x]
- Akaratlagos egyéb támadások AET[x]
- Dokumentációk hiánya, nem megfelelősége D[x]
- Kompetenciák hiánya, nem megfelelősége K[x]
- Életciklus kezelés hiánya, nem megfelelősége E[x]
- Szolgáltatás kiszervezés, kihelyezés fenyegetései KI[x]

Védelmi intézkedés katalógus



Védelmi intézkedés katalógus

A védelmi intézkedés katalógus az adott fenyegetésre vonatkozóan:

- alkalmazható védelmi intézkedések katalógusa,
- fenyegetésosztályonként tagolva,
- fenyegetésenkénti relevanciákkal,
- általános értelmezésben

Védelmi intézkedés katalógus

Védelmi intézkedés katalógus példa (részlet)

Védelmi intézkedés érettségi szintje (pl. COBIT alapján)

	Védelmi intézkedés megnevezése	Érettség (0-5)
		5
		4
		5
SF21	Átmeneti sz[illegible]tás (UPS, generátor)	5
SF22	Redundáns belső hálózat a [illegible]	4
SF23	Külső szállító rendelkezésre állása (SLA)	4
SF24	Túláram és impulzusok elleni védelem a megfelelő helyeken	5
SF25	Redundáns szolgáltató rendelkezésre tartása (BCP)	4
SF26	Átterhelési terv mobil kommunikációra (BCP)	3
SF27	Redundáns tartalék szolgáltató rendelkezésre tartása	4
SF28	DRP megléte és megfelelősége	4
SF29	Tartalék infrastruktúra rendelkezésre tartása	5
SF30	Infrastruktúra pótlása	5
SF31	Készenléti szolgáltatás rendelkezésre tartása (SLA)	5
SF32	Négyszem elv	4
SF33	Jogosultságok szükséges minimális szinten tartása	3
SF34	Szükséges, minimális kikényszerített eljárások alkalmazása	4
SF35	Rendszeres és ellenőrzött mentések	5
SF36	Szerepkörök szétválasztása	4
SF37	Naplógyűjtési és elemzési rendszer megléte és megfelelősége	3
SF45	Határvédelem megléte és megfelelő kialakítása	4
SF98	.....	4
SF99	Hibavisszacsatolási folyamatok tartalmi elemei megfelelőségének rendszeres ellenőrzése	4

Fenyegetéskatalógus
Konvencionális értékmátrixok

Információs vagyonleltár (Information Asset Inventory)

Folyamatfelmérés

Vagyonelem azonosítás

Folyamat-vagyonelem függőségek felmérése

Fenyegetés katalógus (Threat Inventory)

Fenyegetés katalógus

Védelmi intézkedés katalógus

Konvencionális értékmátrixok létrehozása

Kockázatelemzés (Risk Anali[illegible]

Kockázati mátri[illegible]

Vagyonek[illegible]ok

Folyamatok és v[illegible]tékelések számítása

[illegible]mítása

Konvencionális értékmátrixok létrehozása

Fenyegetéskatalógus
Konvencionális értékmátrixok

Konvencionális értékmátrixok:

- Bekövetkezési valószínűség (BV)
- Károkozási képesség (KK)
- Vagyonelem hatásindex
- Vagyonelem maradványkockázati tömeg szerinti besorolás
- Vagyonelemek üzleti érték szerinti kockázati besorolás
- Védelmi intézkedés hatékonyság
- Vagyonelem abszolút kockázati besorolása
- stb…

Fenyegetéskatalógus
Konvencionális értékmátrixok

Bekövetkezési valószínűség és károkozási képesség konvenciómátrix példák

	Bekövetkezési valószínűség érték - BV	Bekövetkezési valószínűség P	P értelmezés	Frekvencia értelmezés
Nem valószínű	0	0	Lehetetlen esemény bekövetkezés	100 évente egyszer bekövetkező esemény
Kismértékben valószínű	1	kisebb mint 0,5		10 évente egyszer bekövetkező esemény
Valószínű	2	nagyobb, mint 0,7		Évente legalább egyszer bekövetkező esemény
Erősen valószínű	3	1	Biztos esemény bekövetkezés	Évente 1-nél többször bekövetkező esemény

Károkozási képesség (KK) konvenció mátrix

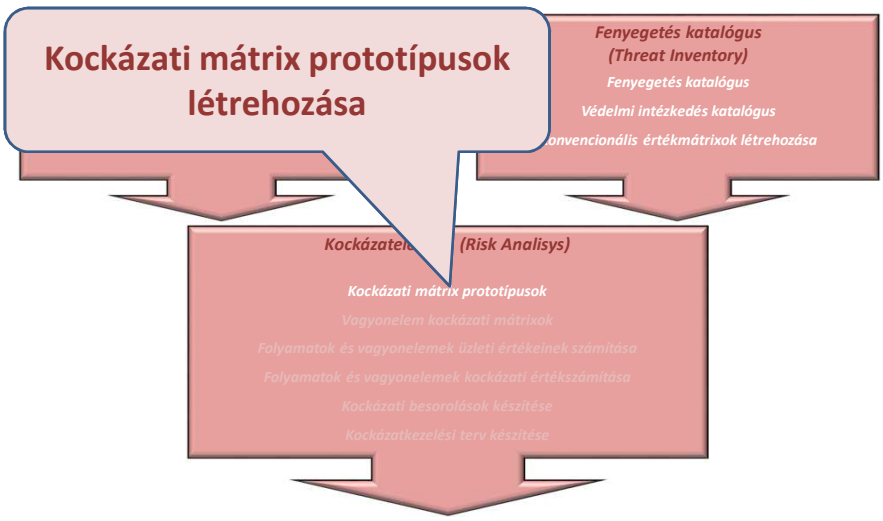
		B	S	R
Nincs károkozási képesség	0	A vagyonelem bizalmassága nem szenved kárt	A vagyonelem nem sérül	A vagyonelem teljes funkcionalitásával, tartalommal rendelkezésre áll
Enyhe károkozási képesség	1	A vagyonelem kevesebb, mint 20%-a kerül felfedésre és/vagy alacsony bizalmassági adatok felfedésre kerülnek	A vagyonelem és/vagy adat kevesebb, mint 20-a sérül, elvész, vagy megsemmisül	A vagyonelem funkcionalitásának 20%-nál kisebb része nem áll rendelkezésre
Közepes károkozási képesség	2	A vagyonelem több, mint 21-50%-a felfedésre kerül és/vagy közepes bizalmasság szintű adatok tömegesen felfedésre kerülnek	A vagyonelem és/vagy adat kevesebb, mint 21-50%-a sérül, elvész, vagy megsemmisül	A vagyonelem funkcionalitásának 21-50%-a nem áll rendelkezésre
Súlyos károkozási képesség	3	A vagyonelem 51-80%-ban felfedésre kerül és/vagy legmagasabb bizalmassági szintű adatok részlegesen felfedésre kerülnek	A vagyonelem és/vagy adat 51-80%-a sérül, elvész, vagy megsemmisül	A vagyonelem funkcionalitásának több, mint 80%-a nem áll rendelkezésre
Végzetes károkozási képesség	4	A vagyonelem 80-100%-os mértékben felfedésre kerül és/vagy legmagasabb bizalmassági szintű adatok tömegesen, vagy teljes mértékben felfedésre kerülnek	A vagyonelem 80-100%-ban megsemmisül	A vagyonelem funkcionalitásának 80-100%-a nem áll rendelkezésre

Fenyegetéskatalógus
Konvencionális értékmátrixok

KockázataránYos védelem konvenciómátrix példa

KockázataránYos védelem megvalósulása				
-1≤	VIH%-∑VÜÉ%	≤-0,5	A vagyonelem üzleti értékéhez képest az alkalmazott védelmi intézkedések bizonyosan elégtelenek.	Bizonyosan elégtelen
-0,5<	VIH%-∑VÜÉ%	≤-0,25	A vagyonelem üzleti értékéhez képest az alkalmazott védelmi intézkedések valószínűleg elégtelenek.	Valószínűleg elégtelen
-0,25<	VIH%-∑VÜÉ%	≤0,25	A vagyonelem üzleti értékéhez képest az alkalmazott védelmi intézkedések vélhetően megfelelőek.	Megfelelő
0,25<	VIH%-∑VÜÉ%	≤0,5	A vagyonelem üzleti értékéhez képest az alkalmazott védelmi intézkedések valószínűleg túlzottak.	Valószínűleg túlzó
0,5<	VIH%-∑VÜÉ%	≤1	A vagyonelem üzleti értékéhez képest az alkalmazott védelmi intézkedések nagy valószínűséggel erősen túlzottak.	Bizonyosan túlzó

Kockázatelemzés

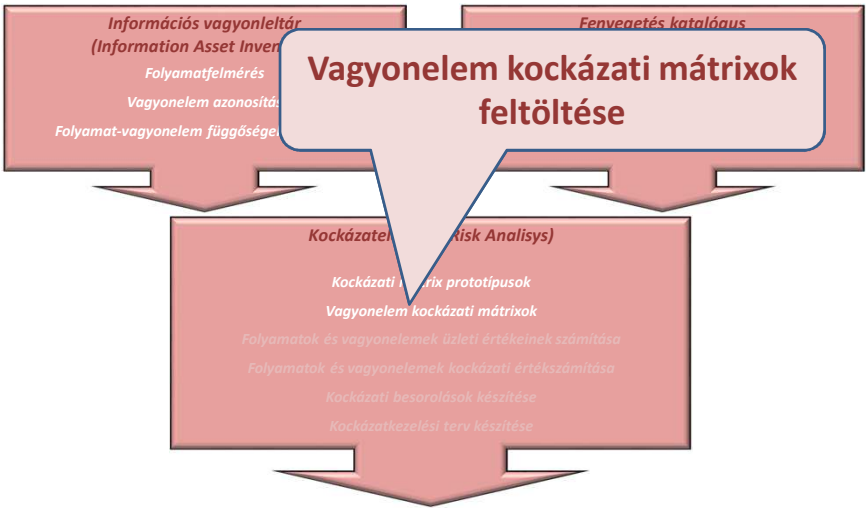


Kockázatelemzés
Kockázati mátrix prototípusok elkészítése

Kockázati mátrix prototípusok készítése az összes vagyonelem osztályra:

- Rendszer prototípus(ok)
- Adat prototípus(ok)
- Munkaerő prototípus(ok)
- Infrastruktúra prototípus(ok)
- Stb…

Kockázatelemzés



Kockázatelemzés
Vagyonelem kockázati mátrixok feltöltése

Bekövetkezési valószínűség - BV

	Bekövetkezési valószínűség érték - BV	Bekövetkezési valószínűség P	Frekvencia értelmezés
Nem valószínű	0	0	100 évente egyszer bekövetkező esemény
Kismértékben valószínű	1	kisebb mint 0,5	10 évente egyszer bekövetkező esemény
Valószínű	2	nagyobb, v. egyenlő mint 0,5	Évente legalább egyszer bekövetkező esemény
Erősen valószínű	3	1	Évente 1-nél többször bekövetkező esemény

Károkozási képesség- KK

Károkozási képesség (KK) konvenció mátrix

		B	S	R
Nincs károkozási képesség	0	A vagyonelem bizalmassága nem szenved kárt	A vagyonelem nem sérül	A vagyonelem teljes funkcionalitással, tartalommal rendelkezésre áll
Enyhe károkozási képesség	1	A vagyonelem kevesebb, mint 20%-a kerül felfedésre és/vagy alacsony bizalmassági adatok felfedésre kerülnek	A vagyonelem és/vagy adat kevesebb, mint 20-a sérül, elvész, vagy megsemmisül	A vagyonelem funkcionalitásának 20%-nál kisebb része nem áll rendelkezésre
Közepes károkozási képesség	2	A vagyonelem több, mint 21-50%-a felfedésre kerül és/vagy közepes bizalmassági szintű adatok tömegesen felfedésre kerülnek	A vagyonelem és/vagy adat kevesebb, mint 21-50%-a sérül, elvész, vagy megsemmisül	A vagyonelem funkcionalitásának 21-50%-a nem áll rendelkezésre
Súlyos károkozási képesség	3	A vagyonelem 51-80%-ban felfedésre kerül és/vagy legmagasabb bizalmassági szintű adatok részlegesen felfedésre kerülnek	A vagyonelem és/vagy adat 51-80%-a sérül, elvész, vagy megsemmisül	A vagyonelem funkcionalitásának több, mint 50%-a de kevesebb, mint 80%-a nem áll rendelkezésre
Végzetes károkozási képesség	4	A vagyonelem 80-100%-os mértékben felfedésre kerül és/vagy legmagasabb bizalmassági szintű adatok tömegesen, vagy teljes mértékben felfedésre kerülnek	A vagyonelem 80-100%-ban megsemmisül	A vagyonelem funkcionalitásának 80-100%-a nem áll rendelkezésre

Kockázatelemzés
Vagyonelem kockázati mátrixok feltöltése

Vagyonelem kockázati mátrixok feltöltése

- Alap kockázati értékek meghatározása
  AK=BVA(B,S,R)*KKA(B,S,R)

		Bekövetkezési valószínűség (BV)			
		0	**1**	**2**	**3**
Károkozási képesség (KK)	**0**	0	0	0	0
	1	0	1	2	3
	2	0	2	4	6
	3	0	3	6	9
	4	0	4	8	12

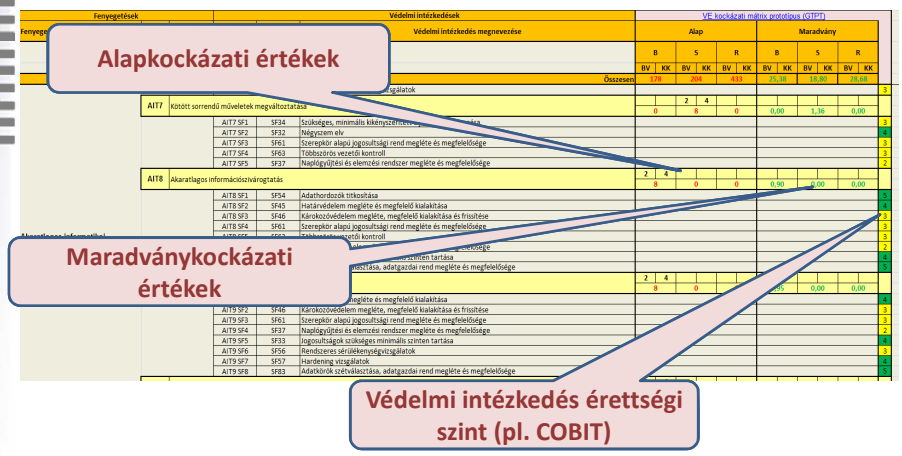
Kockázatelemzés
Vagyonelem kockázati mátrixok feltöltése

Vagyonelem kockázati mátrixok feltöltése:

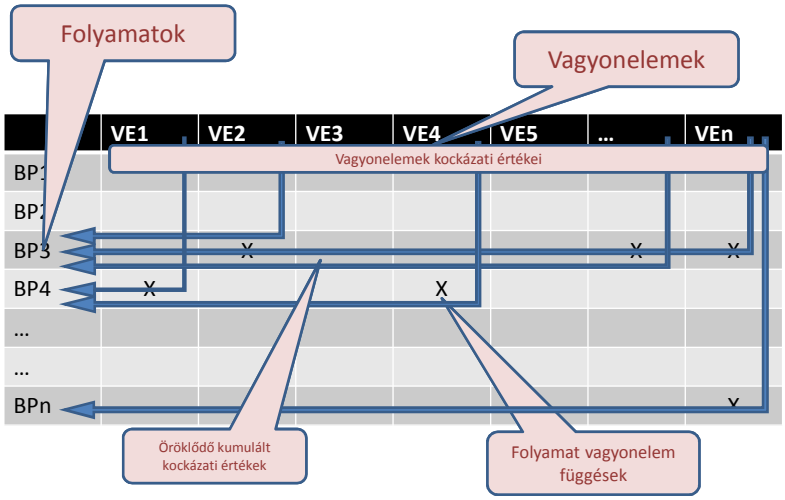
- Védelmi intézkedés (safeguard, countermeasure) relevanciák meghatározása
- Maradványkockázati értékek (MK) meghatározása védelmi intézkedés érettségi szintek megadásával

Kockázatelemzés
Vagyonelem kockázati mátrixok feltöltése

Vagyonelem kockázati mátrixok feltöltés példa (részlet)



Kockázatelemzés
Vagyonelem kockázati mátrixok feltöltése



Kockázatelemzés

Kockázatelemzés
Folyamatok üzleti értékeinek számítása

Pézügyi kár (PK):

- A folyamat által éves szinten termelt bevétel, a szolgáltatás kieséséből adódó elmaradt haszon.
- A folyamat pótlásának és újraindításának költségei.
- …

Közvetett kár (PK):

- A folyamat kieséséből származó harmadik felek számára fizetendő károk értéke.
- A jó hírnév elvesztéséből, csorbulásából származó reputációs károk és ebből eredő jövőbeli elmaradó haszon.
- A személyes adatok, banktitkok, stb. napvilágra kerüléséből, jogok és törvényi előírások megsértéséből származó járulékos károk.
- …

Kockázatelemzés
Folyamatok üzleti értékeinek számítása

Teljes kárérték, vagy üzleti érték (TK):

a pénzügyi károkokból (PK) és a közvetett károkból (KK) áll össze, vagyis

TK = PK + KK

Kockázatelemzés
Folyamatok üzleti értékeinek számítása

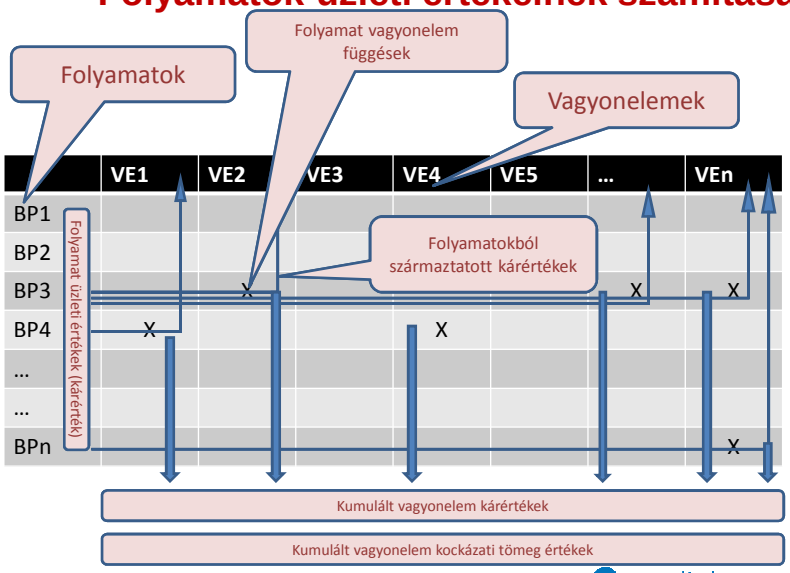
		TK	PK: A folyamat által éves szinten termelt bevétel, a szolgáltatás kieséséből adódó elmaradt haszon	PK: A folyamat pótlásának és újraindításának költségei	KK: A folyamat kieséséből származó harmadik felek számára fizetendő károk értéke	KK: A jó hírnév elvesztéséből, csorbulásából származó reputációs károk és ebből eredő jövőbeli elmaradó haszon	KK: A személyes adatok, banktitkok, stb. napvilágra kerüléséből, jogok és törvényi előírások megsértéséből származó járulékos károk	FKI
BP 01	*Szolgáltatástámogatás*	**5 888 555 000 Ft**	**1 371 355 000 Ft**	**2 032 200 000 Ft**	**600 000 000 Ft**	**30 000 000 Ft**	**55 000 000 Ft**	
BP 01-01	Folyamat 1	3 260 000 000 Ft	1 140 000 000 Ft	1 800 000 000 Ft	300 000 000 Ft	- Ft	20 000 000 Ft	4
BP 01-02	Folyamat 2	2 320 000 000 Ft	200 000 000 Ft	1 800 000 000 Ft	300 000 000 Ft	- Ft	20 000 000 Ft	4
BP 01-03	Folyamat 3	7 000 000 Ft	- Ft	6 000 000 Ft	- Ft	- Ft	1 000 000 Ft	2
BP 01-04	Folyamat 4	18 400 000 Ft	- Ft	8 400 000 Ft	- Ft	- Ft	10 000 000 Ft	3
BP 01-05	Folyamat 5	139 355 000 Ft	1 355 000 Ft	136 000 000 Ft	- Ft	- Ft	2 000 000 Ft	4
BP 01-06	Folyamat 6	60 800 000 Ft	- Ft	58 800 000 Ft	- Ft	- Ft	2 000 000 Ft	3
BP 01-07	Folyamat 7	83 000 000 Ft	30 000 000 Ft	23 000 000 Ft	- Ft	30 000 000 Ft	- Ft	3
BSP 01	*Szolgáltatástámogatás*	**1 498 550 000 Ft**	**375 000 000 Ft**	**1 115 550 000 Ft**	**- Ft**	**- Ft**	**8 000 000 Ft**	
BSP 01-01	Folyamat 8	736 000 000 Ft	350 000 000 Ft	386 000 000 Ft	- Ft	- Ft	- Ft	4
BSP 01-02	Folyamat 9	260 000 000 Ft	- Ft	260 000 000 Ft	- Ft	- Ft	- Ft	4
BSP 01-03	Folyamat 10	155 000 000 Ft	- Ft	155 000 000 Ft	- Ft	- Ft	- Ft	4
BSP 01-04	Folyamat 11	175 500 000 Ft	- Ft	173 500 000 Ft	- Ft	- Ft	2 000 000 Ft	4
BSP 01-05	Folyamat 12	64 000 000 Ft	- Ft	59 000 000 Ft	- Ft	- Ft	5 000 000 Ft	3
BSP 01-06	Folyamat 13	22 000 000 Ft	- Ft	22 000 000 Ft	- Ft	- Ft	- Ft	3
BSP 01-07	Folyamat 14	61 000 000 Ft	- Ft	60 000 000 Ft	- Ft	- Ft	1 000 000 Ft	3
BSP 01-08	Folyamat 15	25 050 000 Ft	25 000 000 Ft	50 000 Ft	- Ft	- Ft	- Ft	3

Teljes kárérték

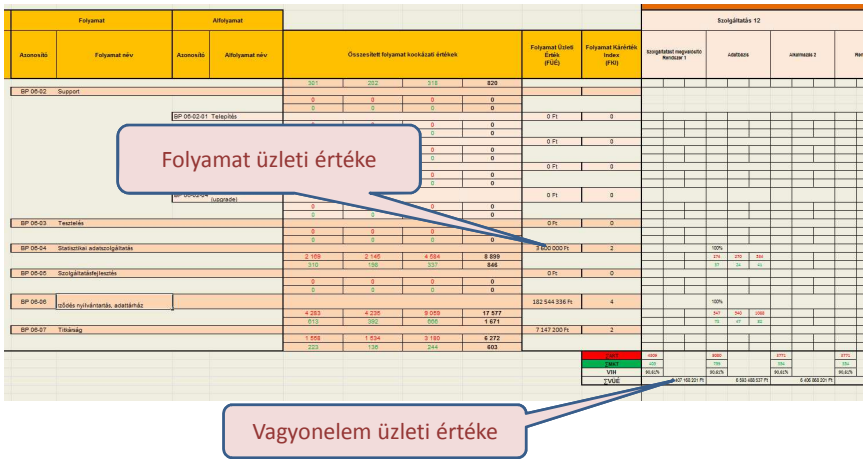
Pénzügyi kár

Közvetett kár

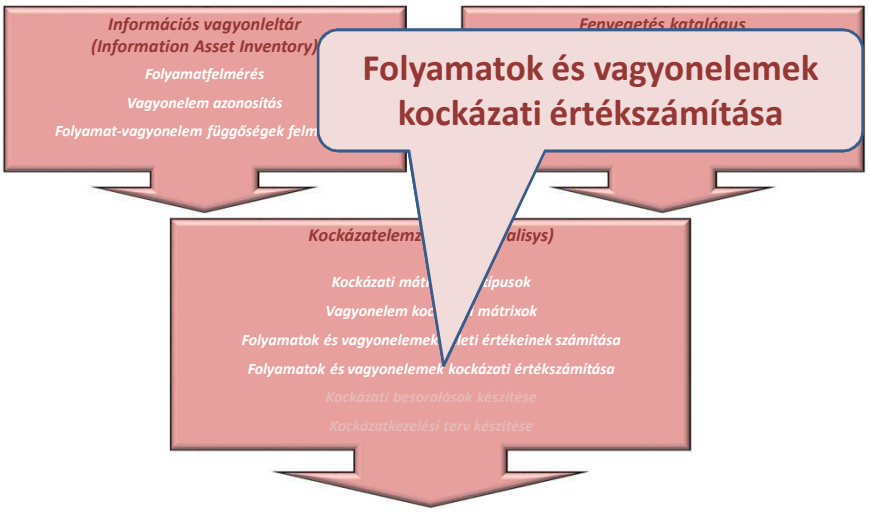
Kockázatelemzés
Folyamatok üzleti értékeinek számítása



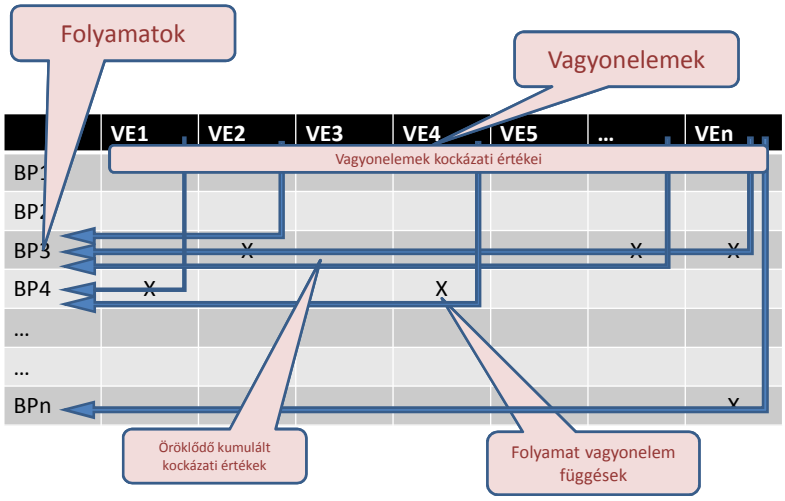
Kockázatelemzés
Vagyonelemek üzleti értékeinek számítása



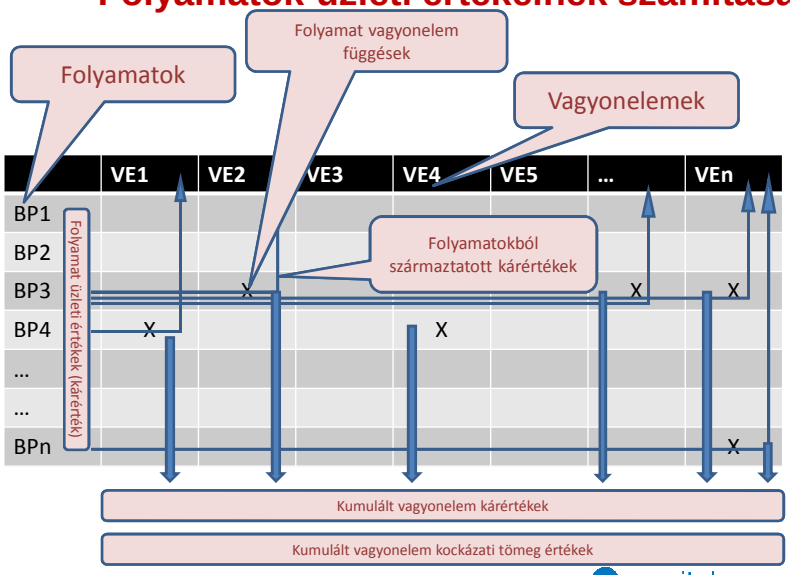
Kockázatelemzés
Folyamatok és vagyonelemek kockázati értékszámítása



Kockázatelemzés
Vagyonelem kockázati mátrixok feltöltése

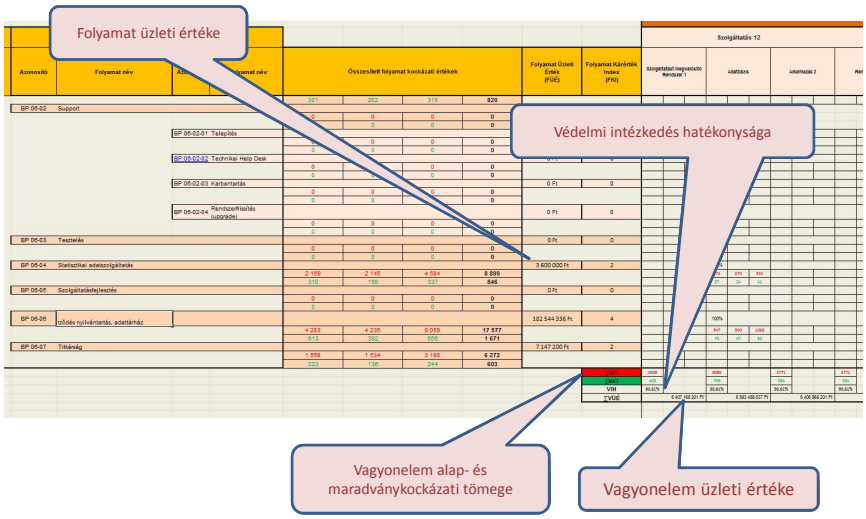


Kockázatelemzés
Folyamatok üzleti értékeinek számítása



Kockázatelemzés

Folyamatok és vagyonelemek kockázati értékszámítása



Kockázatelemzés

Elemzés, kockázati besorolások készítése

Fenyegetés katalógus (Threat Inventory)

Fenyegetés katalógus

Védelmi intézkedés katalógus

Konvencionális értékmátrixok létrehozása

Kockáz (Risk Analisys)

Kockázat rototípusok

Vagyonelem ati mátrixok

Folyamatok és vagyonelemek eti értékeinek számítása

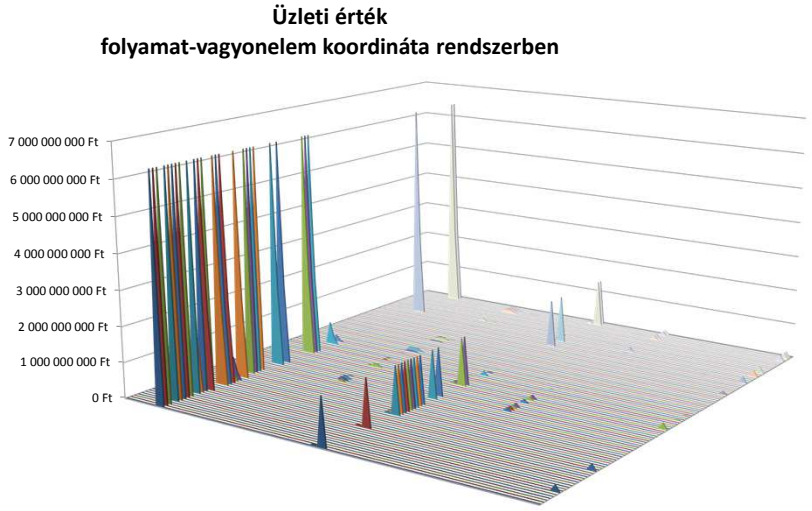
Folyamatok és vagyonelemek kázati értékszámítása

Kockázati besorolás készítése

Kockázatkezelési terv készítése

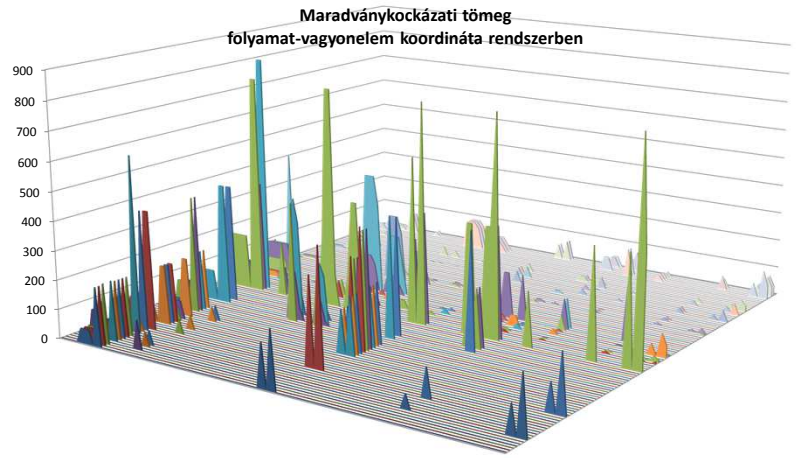
Kockázatelemzés

Folyamatok és vagyonelemek üzleti értékeinek elemzése



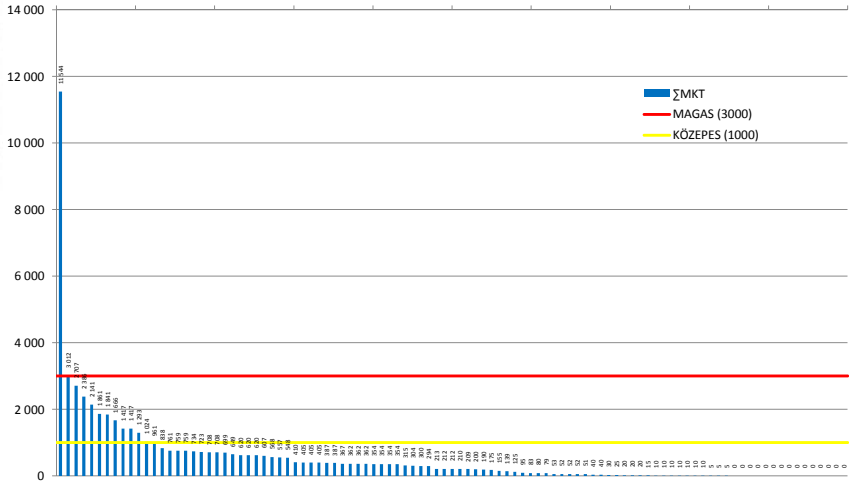
Kockázatelemzés

Folyamatok és vagyonelemek kockázati értékeinek elemzése



Kockázatelemzés
Vagyonelemek kockázatelemzése

Vagyonelemek maradványkockázati össztömeg értéke



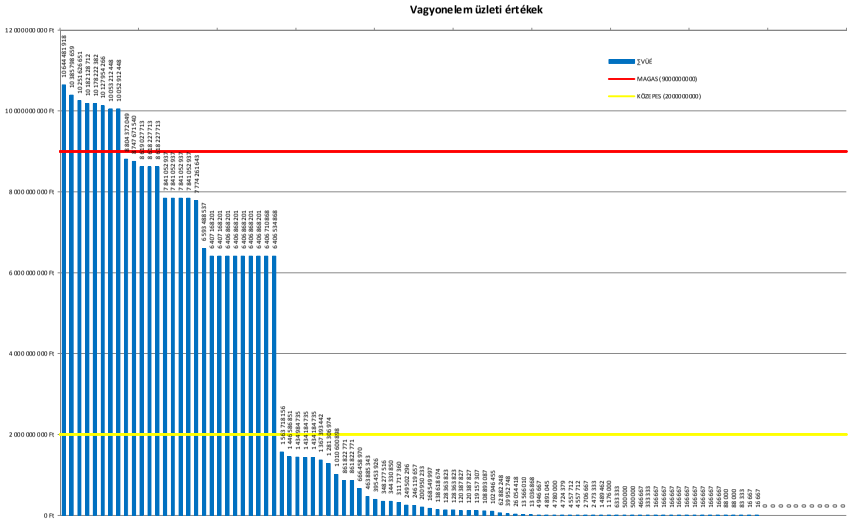
Kockázatelemzés
Vagyonelemek kockázati besorolása

Vagyonelem maradványkockázati tömeg érték szerinti kockázati besorolása

Besorolás	∑MKT érték		Kockázati érték
MAGAS	>	3 000	3
KÖZEPES	<=	3 000	2
ALACSONY	<	1 000	1

Kockázatelemzés

Vagyonelemek üzleti érték szerinti elemzése



Kockázatelemzés

Vagyonelemek üzleti érték szerinti besorolása

Vagyonelem üzleti érték szerinti kockázati besorolása

Besorolás	∑VÜÉ érték		Kockázati érték
MAGAS	>	9 000 000 000 Ft	3
KÖZEPES	<=	9 000 000 000 Ft	2
ALACSONY	<	2 000 000 000 Ft	1

Kockázatelemzés
Vagyonelemek abszolút kockázati besorolása

Vagyonelemek abszolút kockázati besorolása

Vagyonelem kockázati tömeg szerinti besorolása	Vagyonelem üzleti érték szerinti besorolása		
	3	2	1
3	MAGAS (9)	MAGAS (6)	KÖZEPES (3)
2	MAGAS (6)	KÖZEPES (3)	ALACSONY (2)
1	KÖZEPES (3)	ALACSONY (2)	ALACSONY (1)

Kockázatelemzés
Vagyonelemek kockázati besorolása

Vagyonelem kockázati besorolás						
				Kockázati besorolás		
VE típus	VE	∑MKT	∑VÜÉ	Maradvány-kockázati tömeg szerint	Üzleti érték szerint	Abszolút
	Vagyonelem 0	708	7 841 052 937 Ft	1	2	2
	Vagyonelem 1	354	6 406 868 201 Ft	1	2	2
	Vagyonelem 2	362	6 406 868 201 Ft	1	2	2
	Vagyonelem 3	304	633 333 Ft	1	1	1
	Vagyonelem 4	362	6 406 868 201 Ft	1	2	2
	Vagyonelem 5	405	6 407 168 201 Ft	1	2	2
	Vagyonelem 6	759	6 593 488 537 Ft	1	2	2
	Vagyonelem 7	354	6 406 868 201 Ft	1	2	2
	Vagyonelem 8	354	6 406 868 201 Ft	1	2	2
	Vagyonelem 9	52	166 667 Ft	1	1	1
	Vagyonelem 10	759	6 406 534 868 Ft	1	2	2
	Vagyonelem 11	52	1 281 306 974 Ft	1	1	1
	Vagyonelem 12	620	6 406 710 868 Ft	1	2	2
	Vagyonelem 13	1841	10 052 912 448 Ft	2	3	6
	Vagyonelem 14	405	6 407 168 201 Ft	1	2	2
	Vagyonelem 15	315	500 000 Ft	1	1	1
	Vagyonelem 16	155	500 000 Ft	1	1	1
	Vagyonelem 17	607	8 619 027 713 Ft	1	2	2
	Vagyonelem 18	708	8 804 372 049 Ft	1	2	2
	Vagyonelem 19	405	8 618 227 713 Ft	1	2	2
	Vagyonelem 20	79	861 822 771 Ft	1	1	1
	Vagyonelem 21	125	861 822 771 Ft	1	1	1
	Vagyonelem 22	354	1 434 184 735 Ft	1	1	1
	Vagyonelem 23	961	10 053 212 448 Ft	1	3	3
	Vagyonelem 24	557	1 434 984 735 Ft	1	1	1
	Vagyonelem 25	734	1 434 184 735 Ft	1	1	1
	Vagyonelem 26	1417	7 841 052 937 Ft	2	2	4

Kockázatelemzés

Kockázatelemzés

Védelmi intézkedés hatékonyságelemzés

Védelmi intézkedés hatékonyság elemzése

			VÜÉ%			
			0-25	26-50	51-75	76-100
			1	2	3	4
VIH%	91-100	4	41	42	43	44
	81-90	3	31	32	33	34
	26-80	2	21	22	23	24
	0-25	1	11	12	13	14

Kockázatelemzés
Védelmi intézkedés hatékonyság elemzése

Alkalmazott védelmi intézkedések hatékonysága

Kockázatarányos védelem megvalósulása				
-1≤	VIH%-∑VÜÉ%	≤-0,5	A vagyonelem üzleti értékéhez képest az alkalmazott védelmi intézkedések bizonyosan elégtelenek.	Bizonyosan elégtelen
-0,5<	VIH%-∑VÜÉ%	≤-0,25	A vagyonelem üzleti értékéhez képest az alkalmazott védelmi intézkedések valószínűleg elégtelenek.	Valószínűleg elégtelen
-0,25<	VIH%-∑VÜÉ%	≤0,25	A vagyonelem üzleti értékéhez képest az alkalmazott védelmi intézkedések vélhetően megfelelőek.	Megfelelő
0,25<	VIH%-∑VÜÉ%	≤0,5	A vagyonelem üzleti értékéhez képest az alkalmazott védelmi intézkedések valószínűleg túlzottak.	Valószínűleg túlzó
0,5<	VIH%-∑VÜÉ%	≤1	A vagyonelem üzleti értékéhez képest az alkalmazott védelmi intézkedések nagy valószínűséggel erősen túlzottak.	Bizonyosan túlzó

Kockázatelemzés
Védelmi intézkedés hatékonyság elemzése

			25%	50%	75%	100%
			VÜÉ%			
			0-25	25-50	50-75	75-100
			1	2	3	4
VIH%	90-100	4	41	[illegible]	43	44
	80-90	3	31	[illegible]	33	34
	26-80	2	21	22	23	24
	0-25	1	11	12	13	14

Érték	Hatékonyság
11	Megfelelő
12	Valószínűleg elégtelen
[illegible]	Nagy valószínűséggel elégtelen
[illegible]	Nagy valószínűséggel elégtelen
[illegible]	Megfelelő
[illegible]	Megfelelő
[illegible]	Valószínűleg elégtelen
24	Nagy valószínűséggel elégtelen
31	Valószínűleg túlzó
32	Megfelelő
33	Megfelelő
34	Valószínűleg elégtelen
41	Nagy valószínűséggel túlzó
42	Valószínűleg túlzó
43	Megfelelő
44	Megfelelő

Kockázatelemzés
Védelmi intézkedés hatékonyság besorolás

Érték	Hatékonyság
11	Megfelelő
12	Valószínűleg elégtelen
13	Nagy valószínűséggel elégtelen
14	Nagy valószínűséggel elégtelen
21	Megfelelő
22	Megfelelő
23	Valószínűleg elégtelen
24	Nagy valószínűséggel elégtelen
31	Valószínűleg túlzó
32	Megfelelő
33	Megfelelő
34	Valószínűleg elégtelen
41	Nagy valószínűséggel túlzó
42	Valószínűleg túlzó
43	Megfelelő
44	Megfelelő

Kockázatelemzés
Védelmi intézkedés hatékonyság besorolás

Vagyonelem típus	Vagyonelem	Védelem hatékonysága szerinti besorolás	ΣVÜÉ%	ΣVÜÉ	VIH%
IT	Vagyonelem 27	Megfelelő	80,30%	7 841 052 937 Ft	90,61%
	Vagyonelem 28	Megfelelő	80,30%	7 841 052 937 Ft	90,61%
	Vagyonelem 29	Megfelelő	78,70%	7 774 261 643 Ft	90,61%
	Vagyonelem 30	Megfelelő	57,50%	1 367 393 442 Ft	90,61%
	Vagyonelem 31	Megfelelő	0,00%	0 Ft	0,00%
	Vagyonelem 32	Valószínűleg túlzó	37,80%	108 893 087 Ft	90,61%
	Vagyonelem 33	Valószínűleg túlzó	46,90%	200 950 233 Ft	90,61%
	Vagyonelem 34	Megfelelő	98,40%	10 182 128 712 Ft	90,61%
	Vagyonelem 35	Megfelelő	0,00%	0 Ft	0,00%
	Vagyonelem 36	Megfelelő	95,40%	10 127 954 266 Ft	90,61%
	Vagyonelem 37	Valószínűleg elégtelen	40,90%	120 387 827 Ft	0,00%
	Vagyonelem 38	Valószínűleg túlzó	43,90%	128 363 823 Ft	90,61%
	Vagyonelem 39	Valószínűleg túlzó	43,90%	128 363 823 Ft	90,61%
	Vagyonelem 40	Megfelelő	0,00%	0 Ft	0,00%
	Vagyonelem 41	Megfelelő	0,00%	0 Ft	0,00%
	Vagyonelem 42	Valószínűleg elégtelen	40,90%	120 387 827 Ft	0,00%
	Vagyonelem 43	Megfelelő	0,00%	0 Ft	0,00%
	Vagyonelem 44	Megfelelő	100,00%	10 644 481 918 Ft	90,73%
	Vagyonelem 45	Megfelelő	96,90%	10 178 222 382 Ft	90,80%
	Vagyonelem 46	Megfelelő	86,30%	8 618 227 713 Ft	90,65%
	Vagyonelem 47	Valószínűleg elégtelen	28,70%	4 946 667 Ft	0,00%
	Vagyonelem 48	Megfelelő	21,20%	466 667 Ft	0,00%
	Vagyonelem 49	Valószínűleg túlzó	33,30%	39 952 748 Ft	90,61%
	Vagyonelem 50	Valószínűleg túlzó	34,80%	62 882 248 Ft	90,61%
	Vagyonelem 51	Megfelelő	0,00%	0 Ft	0,00%
	Vagyonelem 52	Megfelelő	54,50%	1 010 600 898 Ft	90,61%
	Vagyonelem 53	Valószínűleg túlzó	31,80%	26 054 418 Ft	90,62%
	Vagyonelem 54	Valószínűleg túlzó	48,40%	311 717 360 Ft	90,61%
	Vagyonelem 55	Valószínűleg túlzó	30,30%	13 566 010 Ft	90,63%
	Vagyonelem 56	Valószínűleg túlzó	27,20%	1 176 000 Ft	90,61%

Kockázatelemzés
Kockázatkezelés

- Kockázatkezelési terv javaslat készítése
- Üzletfolytonossági rendszer (BCM) bemenetek számítása
- Naplómenedzsment rendszer kockázatokkal arányos megvalósítása
- Stb…

Kockázatkezelés
Kockázati helyzetjavító hatás maximalizálása

A fejlesztendő vagyonelemek és/vagy védelmi intézkedések kiválasztásának alapelvei:

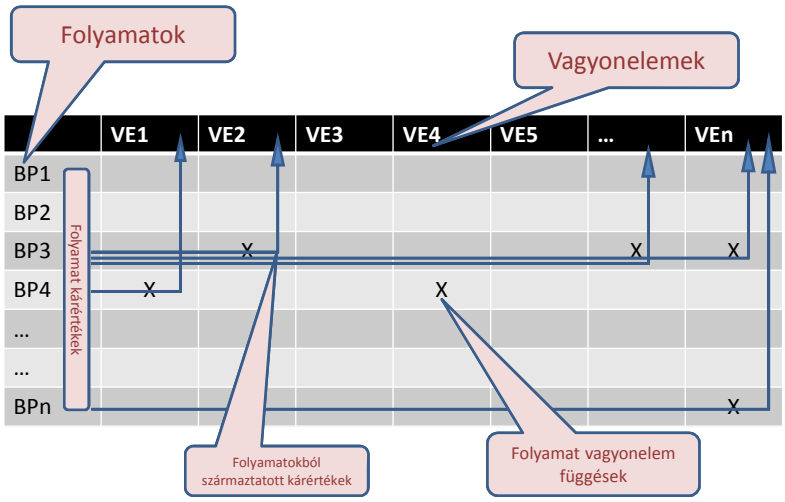
- **ÉRTÉK:** a legértékesebb folyamatokat és/vagy vagyonelemeket érintő fenyegetések
- **KOCKÁZAT:** a szervezet kockázati helyzetet, összképet leginkább javító fenyegetések
- **HATÓKÖR:** a szervezetben és/vagy a rendszerben legszerteágazóbb hatókörrel bíró vagyonelemek fenyegetései
- **SZÁMOSSÁG:** a legtöbb vagyonelemet és/vagy folyamatot érintő fenyegetések

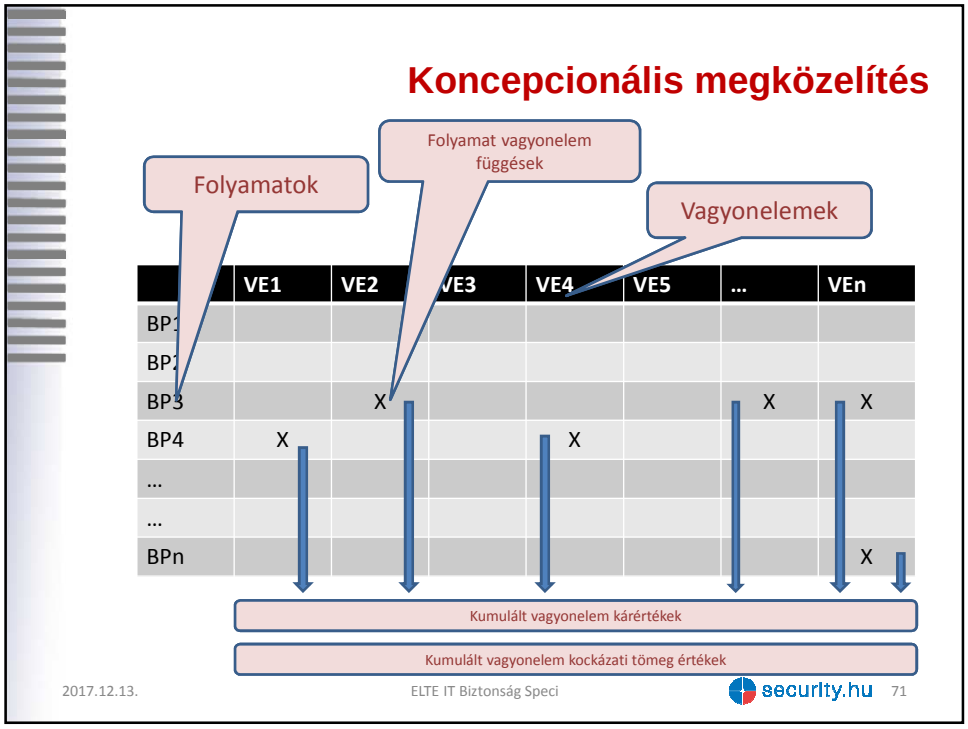
Kérdések

Köszönöm a figyelmet.

security.hu

Koncepcionális megközelítés




Koncepcionális megközelítés
Folyamat vagyonelem függések
Folyamatok
Vagyonelemek
VE1
VE2
VE3
VE4
VE5
...
VEn
BP1
BP2
BP3
BP4
...
...
BPn
X
X
X
X
X
X
Kumulált vagyonelem kárértékek
Kumulált vagyonelem kockázati tömeg értékek
2017.12.13.
ELTE IT Biztonság Speci
security.hu
71