



NIS2 négy nélkül...

...avagy mire tanít minket
Bud Spencer és Terence Hill?

Rónaszéki Péter, ügyvezető, FORTIX Consulting Kft.



RÓNASZÉKI PÉTER

CISM, CDPSE, ISO 27001 LA, LI, ISO 22301 LA



Tapasztalat:

- BISO, Citibank
- CISO, Budapest Bank, (GE Money)
- OISRM, ING Bank
- CISO, Lufthansa Systems
- Partner, FORTIX Consulting, MySec

KIBEV alapító tag

ISACA Magyarországi Egyesület, elnökségi tag
25 év gyakorlati tapasztalat (10 év pü. szektor)



Napirend

- A dilemma
- Mi a BCM?
- PDCA BCM módra
- Mi a BIA?
- Mire tanít minket Bud Spencer és Terence Hill?



A dilemma

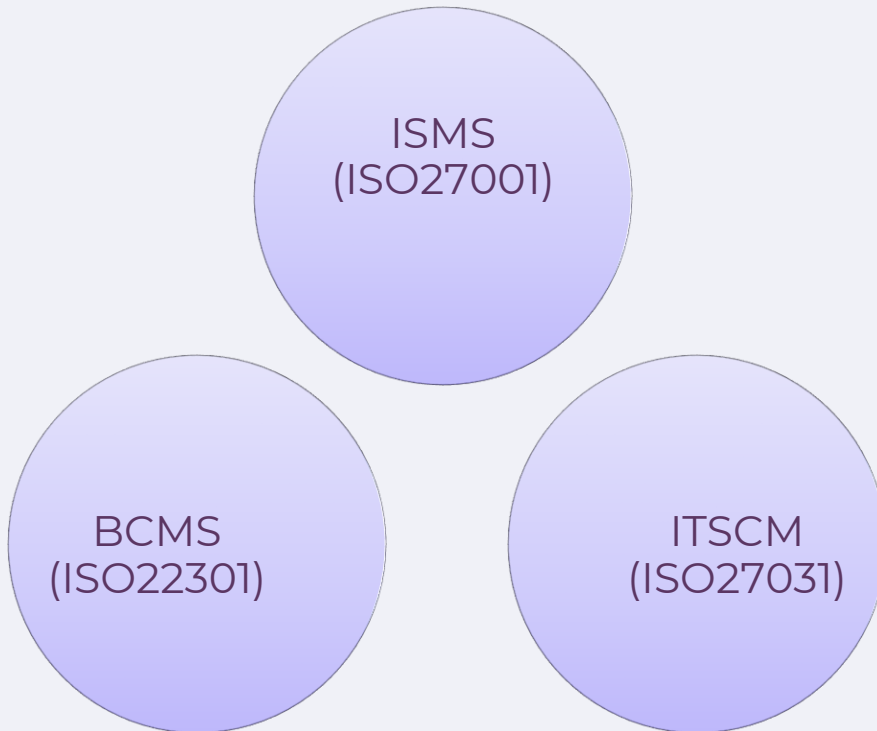
BCMS – ISMS

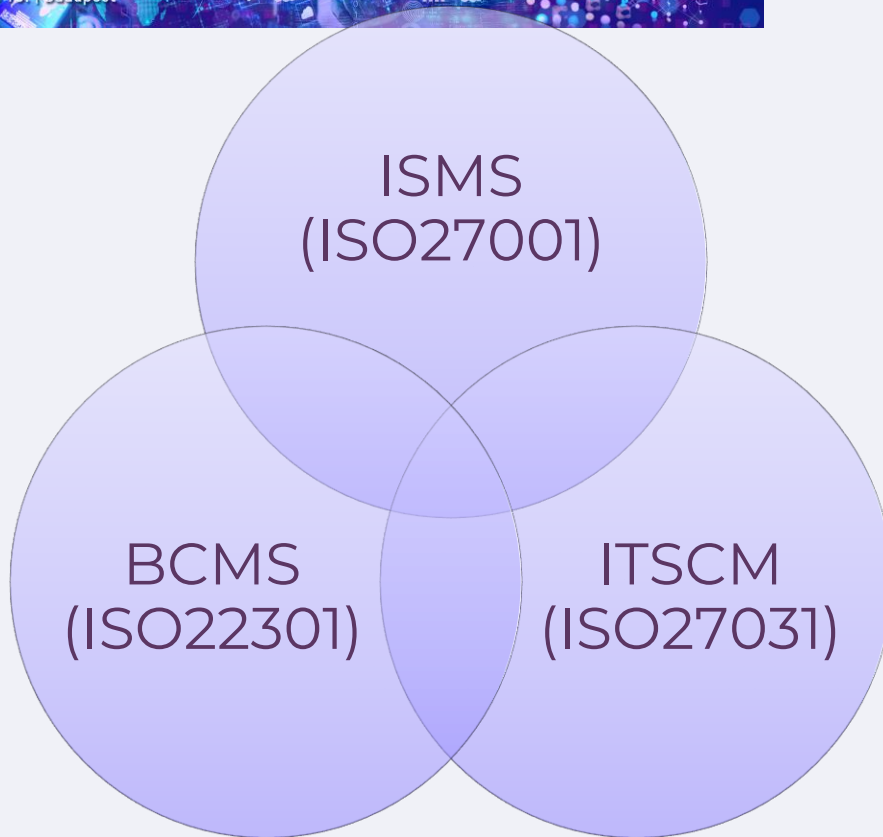


FORTIX

2024. 03. 21.

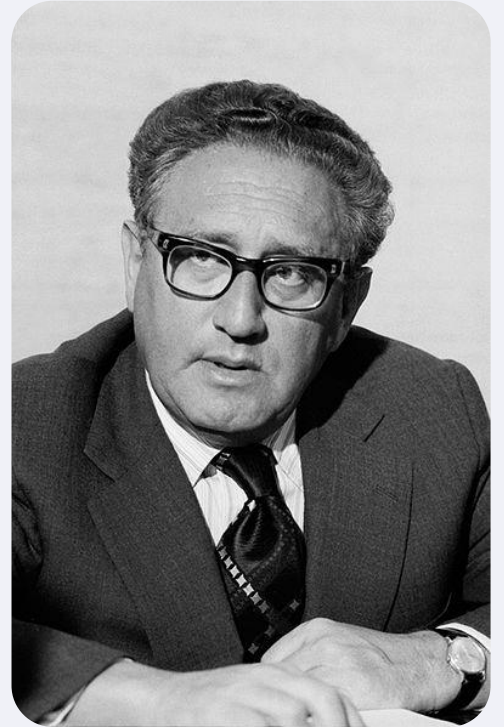
Bizalmas





„Jövő héten nem lehet semmilyen probléma, sem krízis.
Tele van a naptáram.”

Nem a „ha” hanem a „mikor” a kérdés



(Henry Kissinger)



Tények és adatok

- 20%-a a vállalatoknak még mindig nem veszi komolyan adatainak és rendszereinek védelmét.
- 88%-a a vállalatoknak beismerte, hogy komoly gondokkal kellett szembenézniük olyan rendszerterületeken, amiket nem fedtek le BC tervekkel.
- 92%-a a vállalatoknak miután átélte a komoly krízist, átvizsgálta a meglévő BC terveket és kiterjesztette a hatáskörüket
- 25%-a a vállalatoknak kevesebb mint két óra leállást képes tolerálni.
- 60%-a a vállalatoknak mondta azt, hogy a helyreállítási pontértékeket nem sikerült tartani a leállás vagy incidens ideje alatt

Mi a BCM?

Egy holisztikus irányítási rendszer, mely:

azonosítja a szervezet **kritikus** folyamatait, termékeit és szolgáltatásait, az ezeket fenyegető lehetséges hatásokat, keretrendszert biztosít az üzletmenet rugalmasságának kialakításához, így a hatékony válasz képessége lehetővé teszi

- az emberi életek,
- az érdekelt felek érdekeinek,
- a hírnév,
- a márka és
- az értékteremtő tevékenységek

védelmét.





Tervezés (PLAN)

Program követelmények

a BCMS hatályának és célkitűzéseinek azonosítása, figyelembe véve a szervezet stratégiai céljait, kockázattűrését és bármely jogszabályi, szerződéses vagy az érdekelt felektől származó kötelezettséget.

BCM üzletfolytonossági politika

a vezetőség BCMS-hez való hozzájárulásának és az azonosított céloknak és hatálynak a dokumentálása a szükséges felülvizsgálati intervallumok meghatározásával, valamint a politika kommunikációja a szervezet valamennyi alkalmazottja számára.

Erőforrások és személyzeti kompetenciák

A megfelelő erőforrások allokációja a BCMS bevezetéséhez, felügyeletéhez és fenntartásához, beleértve a hatáskörébe rendelt erőforrások kompetenciájának növelésére és fenntartására szolgáló képzéseket.



Tervezés (PLAN)

A BCMS beágyazása a szervezetbe

Folyamatos tudatosító és szerep-specifikus képzések beindítása annak érdekében, hogy minden dolgozó megértse a BCMS politikát, a célkitűzéseket és a saját szerepüket a szervezeti BCM célok elérésében.

Dokumentumok és feljegyzések

A folyamatok fejlesztése annak érdekében, hogy biztosítsuk a BCMS részeként elkészített dokumentumok és feljegyzések teljességét, elérhetőségét, időszerűségét és biztonságát.

Bevezetés és üzemeltetés (DO)

Üzleti hatáselemzés

Meg kell határozni a kritikus szervezeti tevékenységek (fenyegetés-független) megszakadásának hatását azért, hogy kijelöljük a visszaállítási célkitűzéseket.

Kockázatértékelés

Meg kell érteni a kritikus szervezeti tevékenységek fenyegetéseit és sérülékenységeit és biztosítani kell az erőforrásokat.

Kockázatcsökkentő intézkedések meghozatala

Azonosítani kell a kockázatkezelési intézkedéseket a kockázatok csökkentésére a folyamatok megszakadása valószínűségének csökkentésével, a hatásának csökkentésével vagy az időkeret korlátozásával.



Bevezetés és üzemeltetés (DO)

Az üzletfolytonossági stratégia meghatározása

Meg kell határozni, hogy a szervezet milyen válaszokat fog adni és hogyan fog helyreállni a tevékenységei megszakadásából.

Incidenskezelés

Azonosítani kell az incidensekre adandó üzletfolytonossági válaszokhoz szükséges személyzetet, terveket kell készíteni, az erőforrásokat allokálni és kommunikálni kell az érdekelt felekkel.

Üzletfolytonossági és incidenskezelési terv

Azt dokumentáljuk a tervben, hogy a szervezet hogyan fogja megoldani az incidenst és helyreállni, vagy a tevékenységeit egy előre meghatározott szinten fenntartani.



Bevezetés és üzemeltetés (DO)

Begyakorlás

Igazolni kell, hogy a tervek és intézkedések megfelelnek az üzleti követelményeknek. Akciókat kell kidolgozni és a terveket felül kell vizsgálni.

A BCM intézkedések fenntartása és átvizsgálása

Át kell vizsgálni a BCM intézkedéseket meghatározott intervallumokban annak érdekében, hogy biztosítsuk a folyamatos alkalmasságot, megfelelőséget és hatékonyságot.



Ellenőrzés és felülvizsgálat (CHECK)

Belső audit

Biztosítani kell, hogy a szervezet tervezett időszakonként független BCMS felülvizsgálatokon essen át annak érdekében, hogy megfeleljen a követelményeknek, a tervezett intézkedéseknek, a szervezeti politikának és célkitűzéseknek.

Vezetőségi átvizsgálás

Tervezett időszakonként felül kell vizsgálni a szervezet BCMS-ét az alkalmasság, megfelelőség, hatékonyság és a folyamatos fejlesztés biztosítása érdekében.



Fenntartás és fejlesztés (ACT)

Helyesbítő és megelőző intézkedések

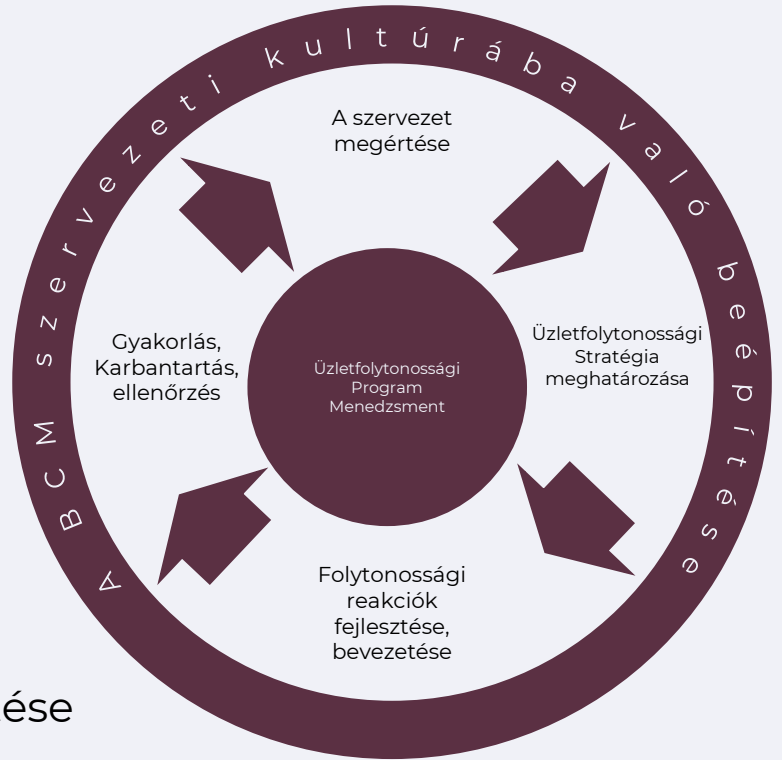
Az üzletfolytonossági irányítási rendszer (BCMS) fenntartása és javítása helyesbítő intézkedések meghozatalával, amelyek a vezetőségi átvizsgálások eredményein, valamint a BCMS hatályán, az üzletfolytonossági politika és célok újraértékelésén alapulnak.

Folyamatos fejlesztés

Folyamatosan fejleszteni kell a BCMS hatékonyságát a politika, a célkitűzések, az audit eredmények, a megfigyelt események elemzése, helyesbítő és megelőző intézkedések, valamint a vezetőségi átvizsgálások által.

A BCMS életrciklus

- I. BCM program menedzsment
- II. A szervezet megértése
- III. BCM stratégia meghatározása
- IV. Folytonossági reakciók bevezetése
- V. Gyakorlás, karbantartás, ellenőrzés
- VI. A BCM szervezeti kultúrába való beépítése



Fontos dátumok (BCM)...



A BCM célja

Az üzletfolytonossági kezdeményezésnek célja, hogy kifejlessze, bevezesse és fenntartsa az üzletfolytonossági programot és biztosítsa az alábbiak teljesülését:

- Az üzlet számára azonosítva vannak a kritikus folyamatok, a lehetséges veszélyek és a kiesések hatásai
- Kifejlesztésre, tesztelésre kerültek, a megfelelő üzleti helyreállítási tervek minden üzleti egység és minden helyszín részére
- A folytonossági előírások és a tervek rendszeresen átnézésre kerülnek, ezzel is biztosítva, hogy az üzleti szükségleteknek megfelelnek



BCM funkciók és hasznok

Funkciók

- A krízishelyzet alatti döntéshozatalt a minimumra csökkenti.
- Alternatívákat állít fel a kritikus üzleti folyamatok folytatására.
- A szervezet számára meghatározza a prioritásokat és az időkereteket.

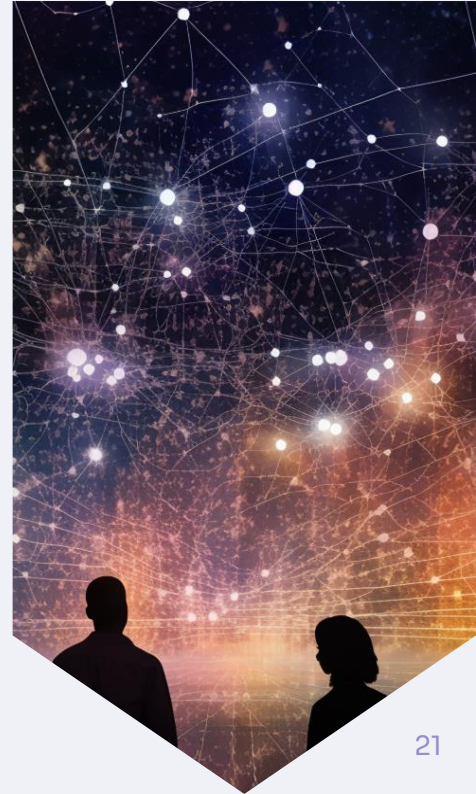
Hasznok

- A megelőzés költséghatékonyabb, mint a helyreállítás.
- A menedzsment és a munkatársak megismerkednek a kockázatkezelési gyakorlattal.
- A hírnevet, érintő negatív hatások megelőzése.
- A biztosítási díjak csökkenhetnek.

Az üzleti hatáselemzés (BIA) célja

A BIA célja, a folyamatok kiesése esetén a következmények felmérése.

- Azonosítani kell a **kritikus** folyamatokat és az egymásra épülő feladatokat (fel kell mérni a függőségi viszonyokat az üzletmenet során), majd ez alapján meg kell határozni a prioritásokat.
- Meg kell határozni a BCM mutatókat (RTO, RPO, MBCO, Lemaradás)
- Fel kell vázolni a folytonossági stratégiákat
- Meg kell határozni a helyreállításhoz szükséges dolgokat



Kritikus elemek azonosítása



Kettős szerepek – redundancia



Kockázatértékelés- és kezelés



Vészhelyzeti forgatókönyvek



Csapatmunka és kommunikáció



Alkalmazkodóképesség és rugalmasság



Proaktív megközelítés



Vidd el magaddal!

HTE
KIBERSZABÁLYOZÁSI
MINIKONFERENCIA
2024. március 19. - 20. Budapeszt

ISMS
≠
BCMS

BIA

ITSCM

2024. 03. 21.

Bizalmas

Iratkozz fel hírlevelünkre a
weboldalunkon!

<https://www.fortix.hu/hirlevel/>

Kapcsolat:

Rónaszéki Péter

+36 30 222 5585

peter.ronaszeki@fortix.hu



FORTIX

Magabiztonságot adunk!



Rónaszéki Péter, CISM, CDPSE, ISO27001 LA, LI, ISO22301 LA

Ügyvezető, partner
+3630 222 5585
peter.ronaszeki@fortix.hu

Köszönöm a figyelmet!

Kapcsolat:

FORTIX Consulting Kft.

1061 Budapest, Liszt Ferenc tér 2.

hello@fortix.hu