GDPR:
AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) – GDPR

PDCA elv
Folyamatmodell az IR fejlesztésének, megvalósításának és hatékonyságának biztosítására
Lefedik a teljes tevékenységi ciklust.
Bármilyen műveletre, tevékenységre, folyamatra, rendszerre, működtetésre, koncepcióra, elgondolásra vonatkoztatható, zárt hatásláncú, folytonosan ismétlődő körfolyamat-elv.
első szakasz a Tervezés (Plan) – a fennálló helyzet tanulmányozása, adatgyűjtés, javítás megtervezése
második szakasz a Végrehajtás (Do) – a terv kipróbálása kísérleti jelleggel egy kisebb projekt vagy a felhasználók egy szűkebb körén belül alkalmazva
harmadik szakasz az Ellenőrzés (Check) – a változtatások hatásának elemzése és értékelése)
negyedik szakasz a Beavatkozás (Act) – a bevált módszer bevezetése és szabványosítása

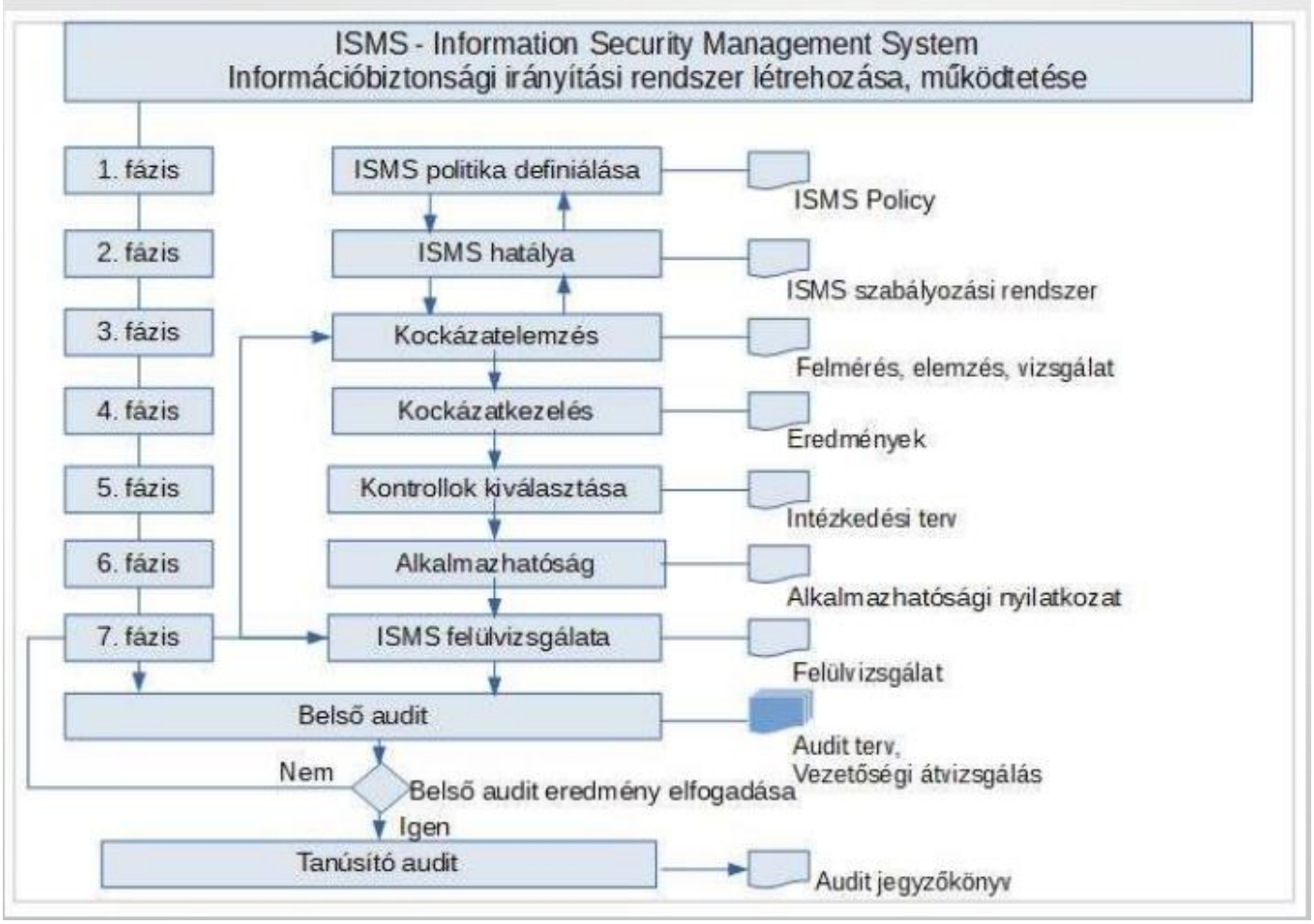
IBIR
MSZ ISO/IEC 27001:2014 (ISO/IEC 27001:2013) szabvány
Informatikai Biztonsági Irányítási Rendszer (IBIR)
(Information Security Management System, ISMS)
Általános irányítási rendszer, amely az üzleti kockázat elemzésén alapul.
Megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot.
Követelményrendszer az Információbiztonsági Irányítási Rendszer
tervezéséhez,
létrehozásához,
ellenőrzéséhez és
bevezetéséhez
az informatikai biztonsági rendszer teljes életciklusában bekövetkező tevékenységekre vonatkozólag.

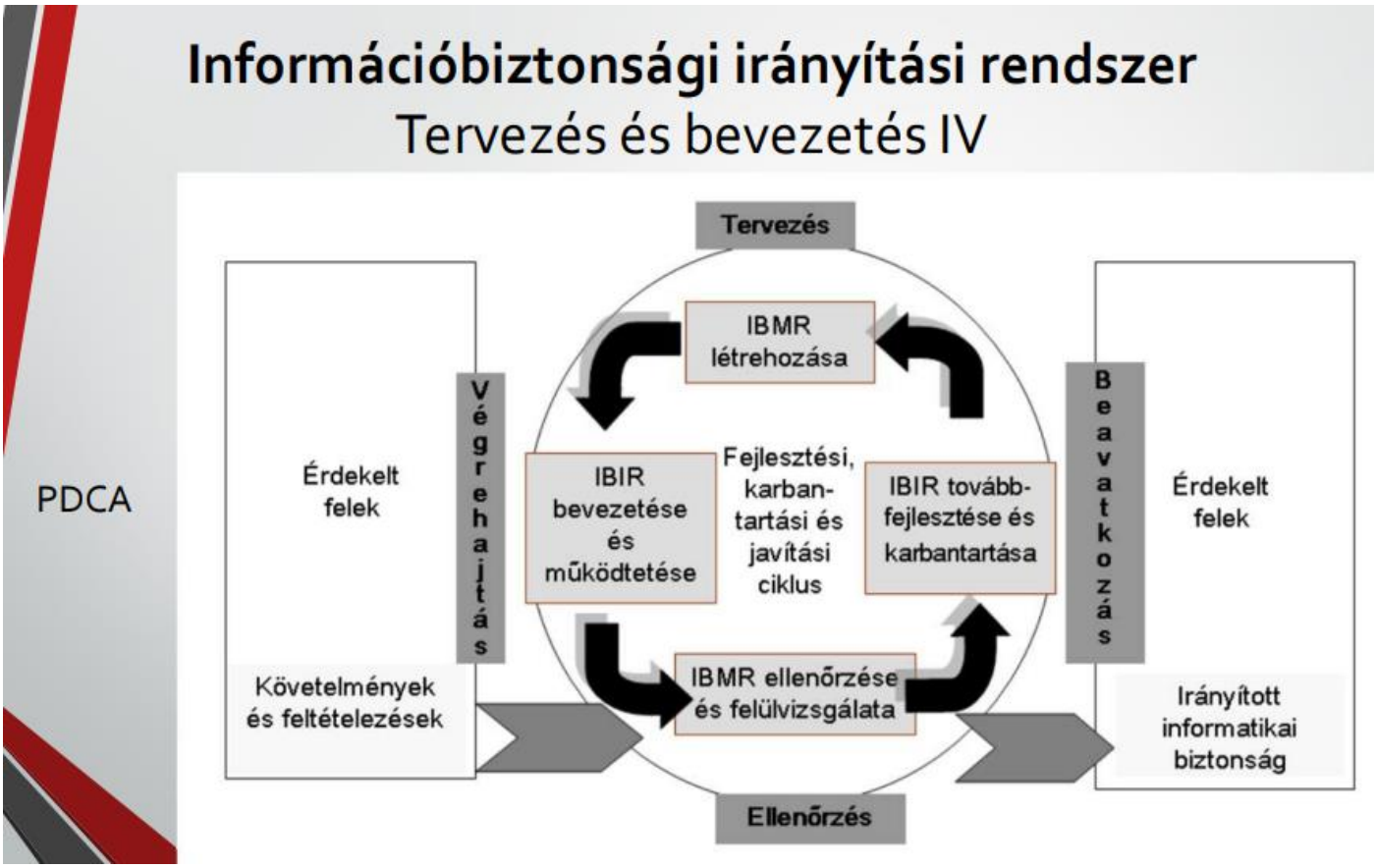
CIA
Rendelkezésre állás - A = Availability: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

Kockázat:
a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

ISMS
Információ biztonsági és irányítási rendszer

Kockázatelemzés (analysis)
működési hatás elemzés,
vagyonelemek kategorizálása,
vagyonelemek értékelése: fenyegetések, sebezhetőségek szempontjából,
veszély hatásának mértéke és skálája,
támogató folyamatok kritikussága, osztályozása,
kockázatkezelés határértéke.


ISMS - Information Security Management System
Információbiztonsági irányítási rendszer létrehozása, működtetése
1. fázis
ISMS politika definiálása
ISMS Policy
2. fázis
ISMS hatálya
ISMS szabályozási rendszer
3. fázis
Kockázatelemzés
Felmérés, elemzés, vizsgálat
4. fázis
Kockázatkezelés
Eredmények
5. fázis
Kontrollok kiválasztása
Intézkedési terv
6. fázis
Alkalmazhatóság
Alkalmazhatósági nyilatkozat
7. fázis
ISMS felülvizsgálata
Felülvizsgálat
Belső audit
Audit terv,
Vezetőségi átvizsgálás
Nem
Belső audit eredmény elfogadása
Igen
Tanúsító audit
Audit jegyzőkönyv


Információbiztonsági irányítási rendszer
Tervezés és bevezetés IV
PDCA
Tervezés
IBMR létrehozása
Végrehajtás
Érdekelt felek
IBIR bevezetése és működtetése
Fejlesztési, karbantartási és javítási ciklus
IBIR továbbfejlesztése és karbantartása
Bevezetés
Érdekelt felek
IBMR ellenőrzése és felülvizsgálata
Követelmények és feltételezések
Irányított informatikai biztonság
Ellenőrzés

A kockázatmenedzsment