A NIST SP 800-53 szabvány áttekintése, és alkalmazása a 2013. L. törvény kapcsán

Lengré Tamás CISA

asc
Save it easy

A 2013. évi L. törvény

- Törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
  - Az Országgyűlés 2013. április 15-én fogadta el
  - Hatályba 2013. július 1.-én lépett
  - Már 2013 évre is meghatározott határidőket
    - *melyeket az adott szervezetek nem igazán tartottak be azóta sem!* 😊
  - Végrehajtási rendeletek késve készültek el, azóta módosították:

77/2013 (XII.19.) NFM rendelet helyett 41/2015. (VII.15.) BM rendelet

A 2013. évi L. törvény

- Módosította a 2015. évi CXXX. törvény:
  - az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról

Kikre vonatkozik?

- Állami és önkormányzati szervek
  (Kormány és kormánybizottságok kivételével)
  - Köztársasági Elnöki Hivatal
  - Országgyűlés Hivatala
  - Alkotmánybíróság Hivatala
  - Országos Bírósági Hivatal és a bíróságok, az Ügyészség
  - Alapvető Jogok Biztosának Hivatala
  - Állami Számvevőszék
  - MNB
  - Fővárosi és megyei kormányhivatalok
  - Helyi és nemzetiségi Önkormányzatok képviselő testületének hivatala
  - Magyar Honvédség

…és az apróbetűs rész… 😊

- Akikre még vonatkozik:
  - Aki az állam és az önkormányzatok számára adatkezelést végez.
  - Aki a nemzeti adatvagyon adatfeldolgozója.
  - Aki/Ami kritikus információs rendszerelem (infrastruktúra (üzemeltetője)), illetve ennek minősített szervezet.

Felelős

Az intézmény vezetője!!

ALAPVETŐ BIZTONSÁGI KÖVETELMÉNYEK

- Az EIR-ek teljes életciklusában meg kell valósítani, és biztosítani kell:
  - az EIR-ben kezelt adatok és információk
    - bizalmasságát (B)
    - Sértetlenségét (S)
    - Rendelkezésre állását (R)
  - Az EIR-ek és rendszerelemeinek
    - zárt, teljes körű, folytonos
    - kockázatokkal arányos védelmét

CIA=BSR

ALAPVETŐ BIZTONSÁGI KÖVETELMÉNYEK

A meghatározott követelményeket biztosítani kell:

- fizikai
- adminisztratív
- logikai

védelmi intézkedésekkel, amelyek támogatják:

- a megelőzést és a korai figyelmeztetést
- az észlelést
- a reagálást
- a biztonsági események kezelését.

BIZTONSÁGI SZINT, BIZTONSÁGI OSZTÁLY

- Az intézményre, és az egyes szervezeti egységekre meg kell határozni, melyik biztonsági szintbe tartozik (1-5)
- Az EIR-eket biztonsági osztályokba kell sorolni (1-5)

	A	B	C	D	E	F	G	H
1		**Szervezet neve:**						*Kötelező*
2		**Szervezet törzsszáma:**						*Kötelező*
3		**Rendszer neve:**						*Kötelező*
4		**Kitöltő neve:**						*Kötelező*
5		**Kitöltés dátuma:**						*Kötelező*
6	*Űrlap biztonsági osztályba soroláshoz és a védelmi intézkedések kiválasztásához, a 41/2015. (VII. 15.) BM rendelet alapján*		**A rendszer biztonsági osztálya (ezt kell elérni):**			**A rendszer aktuálisan megfelel:**		
7			**Hiányos adat**			**0**		
8	*Verzió:*	*3.15*	**Bizalmasság**	**Sértetlenség**	**Rendelkezésre állás**	**Bizalmasság**	**Sértetlenség**	**Rendelkezésre állás**
9	*Készült:*	*2015.11.02*	**Hiányos adat**	**Hiányos adat**	**Hiányos adat**	**0**	**0**	**0**
10	*Szerzők:*	*Szilárd Zoltán, Benyó Pál, Juhász György, Simonyi Gyula*		**Megfelelt/Nem felelt meg**			**Teljesített osztály**	
14	*3.1.3.*	*Rendszer és szolgáltatás beszerzés*		*Hiányos adat*				
15	*3.1.4.*	*Üzletmenet- (ügymenet-) folytonosság tervezése*		*Hiányos adat*				
16	*3.1.5.*	*A biztonsági események kezelése*		*Hiányos adat*				
17	*3.1.6.*	*Emberi tényezőket figyelembe vevő - személy - biztonság*		*Hiányos adat*				
18	*3.1.7.*	*Tudatosság és képzés*		*Hiányos adat*				
19		**FIZIKAI VÉDELMI INTÉZKEDÉSEK**		**Hiányos adat**			**1**	
20			**Bizalmasság**	**Sértetlenség**	**Rendelkezésre állás**	**Bizalmasság**	**Sértetlenség**	**Rendelkezésre állás**
21		**LOGIKAI VÉDELMI INTÉZKEDÉSEK**	**Hiányos adat**	**Hiányos adat**	**Hiányos adat**			
22	*3.3.1.*	*Általános védelmi intézkedések*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			
23	*3.3.2.*	*Tervezés*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			
24	*3.3.3.*	*Rendszer és szolgáltatás beszerzés*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			
25	*3.3.4.*	*Biztonsági elemzés*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			
26	*3.3.5.*	*Tesztelés, képzés és felügyelet*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			
27	*3.3.6.*	*Konfigurációkezelés*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			
28	*3.3.7.*	*Karbantartás*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*	**1**	**1**	**1**
29	*3.3.8.*	*Adathordozók védelme*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			
30	*3.3.9.*	*Azonosítás és hitelesítés*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			
31	*3.3.10.*	*Hozzáférés ellenőrzése*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			
32	*3.3.11.*	*Rendszer- és információsértetlenség*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			
33	*3.3.12.*	*Naplózás és elszámoltathatóság*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			
34	*3.3.13.*	*Rendszer- és kommunikációvédelem*	*Hiányos adat*	*Hiányos adat*	*Hiányos adat*			

	A	B	C	D	E	F	G	H	I
1	**3.1.**	**ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK**	**Elvárt osztály:**	**Hiányos adat**	**Követelmény**				
2	**3.1.1.**	**SZERVEZETI SZINTŰ ALAPFELADATOK**	**Megfelelt? (I/N)**	**Ki kell tölteni?**	**1**	**2**	**3**	**4**	**5**
3	**3.1.1.1.**	**Informatikai biztonsági szabályzat**	**Hiányos adat**		X	X	X	X	X
4	*3.1.1.1.1.*	*Az érintett szervezet:*	-		-	-	-	-	-
5	3.1.1.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági szabályzatot;			N	N	N	N	N
6	3.1.1.1.1.2.	más belső szabályozásában, vagy magában az informatikai biztonsági szabályzatban meghatározza az informatikai biztonsági szabályzat felülvizsgálatának és frissítésének gyakoriságát;			N	N	N	N	N
7	3.1.1.1.1.3.	gondoskodik arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.			N	N	N	N	N
8	*3.1.1.1.2.*	*Az informatikai biztonsági szabályzatban meg kell határozni:*	-		-	-	-	-	-
9	3.1.1.1.2.1.	a célokat, a szabályzat tárgyi és személyi (a szervezet jellegétől függően területi) hatályát;			N	N	N	N	N
10	3.1.1.1.2.2.	az elektronikus információbiztonsággal kapcsolatos szerepköröket;			N	N	N	N	N
11	3.1.1.1.2.3.	a szerepkörhöz rendelt tevékenységet;			N	N	N	N	N
12	3.1.1.1.2.4.	a tevékenységhez kapcsolódó felelősséget;			N	N	N	N	N
13	3.1.1.1.2.5.	az információbiztonság szervezetrendszerének belső együttműködését.			N	N	N	N	N
14	*3.1.1.1.3.*	*Az informatikai biztonsági szabályzat elsősorban a következő elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza:*	-		-	-	-	-	-
15	3.1.1.1.3.1.	kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz);			N	N	N	N	N
16	3.1.1.1.3.2.	biztonsági helyzet-, és eseményértékelés eljárási rendje;			N	N	N	N	N
17	3.1.1.1.3.3.	az elektronikus információs rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás beszerzés (amennyiben az érintett szervezet ilyet végez, vagy végezhet);			N	N	N	N	N
18	3.1.1.1.3.4.	biztonsággal kapcsolatos tervezés (például: beszerzés, fejlesztés, eljárásrendek kialakítását);			N	N	N	N	N
19	3.1.1.1.3.5.	fizikai és környezeti védelem szabályai, jellemzői;			N	N	N	N	N
20	3.1.1.1.3.6.	az emberi erőforrásokban rejlő veszélyek megakadályozása (pl.: személyzeti felvételi- és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése, stb.);			N	N	N	N	N
21	3.1.1.1.3.7.	az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében;			N	N	N	N	N
22	3.1.1.1.3.8.	az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvárások, jogok (amennyiben az érintett szervezetnél ez értelmezhető);			N	N	N	N	N
23	3.1.1.1.3.9.	üzlet-, ügy- vagy üzemmenet folytonosság tervezése (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása, stb.);			N	N	N	N	N
24	3.1.1.1.3.10.	az elektronikus információs rendszerek karbantartásának rendje;			N	N	N	N	N
25	3.1.1.1.3.11.	az adathordozók fizikai és logikai védelmének szabályozása;			N	N	N	N	N
26	3.1.1.1.3.12.	az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárás, és a hozzáférési szabályok betartásának ellenőrzése;			N	N	N	N	N
		amennyiben az érintett szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszerbejegyzések értékelése, az							

Kötelező

B) 3.2. FIZIKAI VÉDELMI INTÉZKEDÉSEK

	A	B	C	D	E	F	G
1.	**Sorszám**	**Intézkedés típusa**	**Biztonsági osztály**				
2.			**1**	**2**	**3**	**4**	**5**
3.	3.2.1.2.	Fizikai védelmi eljárásrend	0	X	X	X	X
4.	3.2.1.3.	Fizikai belépési engedélyek	0	X	X	X	X
5.	3.2.1.4.	A fizikai belépés ellenőrzése	0	X	X	X	X
6.	3.2.1.4.2.	Hozzáférés az információs rendszerhez	0	0	0	0	X
7.	3.2.1.5.	Hozzáférés az adatátviteli eszközökhöz és csatornákhoz	0	0	0	X	X
8.	3.2.1.6.	A kimeneti eszközök hozzáférés ellenőrzése	0	0	0	X	X
9.	3.2.1.7.	A fizikai hozzáférések felügyelete	0	0	X	X	X
10.	3.2.1.7.2.	Behatolás riasztás, felügyeleti berendezések	0	0	0	X	X
11.	3.2.1.7.3.	Az elektronikus információs rendszerekhez való hozzáférés felügyelete	0	0	0	0	X
12.	3.2.1.8.	A látogatók ellenőrzése	0	0	X	X	X
13.	3.2.1.8.2.	Automatizált látogatói információkezelés	0	0	0	0	X
14.	3.2.1.9.	Áramellátó berendezések és kábelezés	0	0	0	X	X
15.	3.2.1.9.1.	Tartalék áramellátás	0	0	0	X	X
16.	3.2.1.9.2.	Hosszú távú tartalék áramellátás a minimálisan elvárt működési képességhez	0	0	0	0	X
17.	3.2.1.10.	Vészkikapcsolás	0	0	0	X	X
18.	3.2.1.11.	Vészvilágítás	0	0	X	X	X
19.	3.2.1.12.	Tűzvédelem	0	0	X	X	X
20.	3.2.1.12.2.	Automatikus tűzelfojtás	0	0	0	X	X
21.	3.2.1.12.3.	Észlelő berendezések, rendszerek	0	0	0	0	X
22.	3.2.1.12.4.	Tűzelfojtó berendezések, rendszerek	0	0	0	0	X
23.	3.2.1.13.	Hőmérséklet és páratartalom ellenőrzés	0	0	X	X	X
24.	3.2.1.14.	Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	0	0	X	X	X
25.	3.2.1.14.2.	Automatizált védelem	0	0	0	0	X
26.	3.2.1.15.	Be- és kiszállítás	0	0	X	X	X
27.	3.2.1.16.	Az elektronikus információs rendszer elemeinek elhelyezése	0	0	0	X	X
28.	3.2.1.17.	Ellenőrzés	0	0	0	X	X
29.	3.2.1.18.	Szállítási felügyelet	0	0	0	0	X
30.	3.2.1.19.	Karbantartók	0	0	X	X	X
31.	3.2.1.19.2.	Karbantartás fokozott biztonsági intézkedésekkel	0	0	0	0	X
32.	3.2.1.19.3.	Időben történő javítás	0	0	0	X	X

A) 3.1. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

	A	B	C	D	E	F	G
1.	**Sorszám**	**Intézkedés típusa**	**Biztonsági osztály**				
2.			**1**	**2**	**3**	**4**	**5**
3.	**3.1.1.**	**Szervezeti szintű alapfeladatok**					
4.	3.1.1.1.	Informatikai biztonsági szabályzat	X	X	X	X	X
5.	3.1.1.2.	Az elektronikus információs rendszerek biztonságáért felelős személy	X	X	X	X	X
6.	3.1.1.3.	Az intézkedési terv és mérföldkövei	0	X	X	X	X
7.	3.1.1.4.	Az elektronikus információs rendszerek nyilvántartása	X	X	X	X	X
8.	3.1.1.5.	Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás	X	X	X	X	X
9.	**3.1.2.**	**Kockázatelemzés**					
10.	3.1.2.1.	Kockázatelemzési és kockázatkezelési eljárásrend	X	X	X	X	X
11.	3.1.2.2.	Biztonsági osztályba sorolás	X	X	X	X	X
12.	3.1.2.3.	Kockázatelemzés	X	X	X	X	X
13.	**3.1.3.**	**Rendszer és szolgáltatás beszerzés**					
14.	3.1.3.1.	Beszerzési eljárásrend	0	0	X	X	X
15.	3.1.3.2.	Erőforrás igény felmérés	0	0	X	X	X
16.	3.1.3.3.	Beszerzések	0	0	X	X	X
17.	3.1.3.3.2.	A védelem szempontjainak érvényesítése a beszerzés során	0	0	0	X	X
18.	3.1.3.3.3.	A védelmi intézkedések terv-, és megvalósítási dokumentációi	0	0	0	X	X
19.	3.1.3.3.4.	Funkciók – protokollok – szolgáltatások	0	0	0	X	X
20.	3.1.3.4.	Az elektronikus információs rendszerre vonatkozó dokumentáció	0	0	X	X	X
21.	3.1.3.5.	Biztonságtervezési elvek	0	0	0	X	X
22.	3.1.3.6.	Külső elektronikus információs rendszerek szolgáltatásai	0	X	X	X	X
23.	3.1.3.7.	Független értékelők	0	0	0	X	X
24.	3.1.3.8.	Folyamatos ellenőrzés	0	0	X	X	X

C) 3.3. LOGIKAI VÉDELMI INTÉZKEDÉSEK

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1.	**Sorszám**	**Intézkedés típusa**	**Alapelvek**											
2.			**Bizalmasság**				**Sértetlenség**				**Rendelkezésre állás**			
3.			**Biztonsági osztályok**											
4.			**2**	**3**	**4**	**5**	**2**	**3**	**4**	**5**	**2**	**3**	**4**	**5**
5.	**3.3.1.**	**Általános védelmi intézkedések**												
6.	3.3.1.3.	Az elektronikus információs rendszer kapcsolódásai	0	X	X	X	0	X	X	X	0	X	X	X
7.	3.3.1.3.2.	Belső rendszer kapcsolatok	0	X	X	X	0	X	X	X	0	X	X	X
8.	3.3.1.3.3.	Külső kapcsolódásokra vonatkozó korlátozások	0	X	X	X	0	X	X	X	0	X	X	X
9.	3.3.1.4.	Személybiztonság	X	X	X	X	X	X	X	X	X	X	X	X
10.	**3.3.2.**	**Tervezés**												
11.	3.3.2.1.	Biztonságtervezési szabályzat	0	0	X	X	0	0	X	X	0	0	X	X
12.	3.3.2.2.	Rendszerbiztonsági terv	X	X	X	X	X	X	X	X	X	X	X	X
13.	3.3.2.3.	Cselekvési terv	X	X	X	X	X	X	X	X	0	0	0	0
14.	3.3.2.4.	Személyi biztonság	X	X	X	X	0	0	0	0	0	0	0	0
15.	3.3.2.5.	Információbiztonsági architektúra leírás	0	0	X	X	0	0	0	0	0	0	0	0
16.	**3.3.3.**	**Rendszer és szolgáltatás beszerzés**												
17.	3.3.3.2.	A rendszer fejlesztési életciklusa	X	X	X	X	0	0	0	0	0	0	0	0
18.	3.3.3.3.	Funkciók, portok, protokollok, szolgáltatások	0	X	X	X	0	X	X	X	0	X	X	X
19.	3.3.3.4.	Fejlesztői változáskövetés	0	0	X	X	0	0	X	X	0	0	X	X

3. VÉDELMI INTÉZKEDÉS KATALÓGUS

3.1. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK
3.1.1. SZERVEZETI SZINTŰ ALAPFELADATOK
3.1.1.1. Informatikai biztonsági szabályzat
3.1.1.1.1. Az érintett szervezet:
3.1.1.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági szabályzatot;
3.1.1.1.1.2. más belső szabályozásában, vagy magában az informatikai biztonsági szabályzatban meghatározza az informatikai biztonsági szabályzat felülvizsgálatának és frissítésének gyakoriságát;
3.1.1.1.1.3. gondoskodik arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.
3.1.1.1.2. Az informatikai biztonsági szabályzatban meg kell határozni:
3.1.1.1.2.1. a célokat, a szabályzat tárgyi és személyi (a szervezet jellegétől függően területi) hatályát;
3.1.1.1.2.2. az elektronikus információbiztonsággal kapcsolatos szerepköröket;
3.1.1.1.2.3. a szerepkörhöz rendelt tevékenységet;
3.1.1.1.2.4. a tevékenységhez kapcsolódó felelősséget;
3.1.1.1.2.5. az információbiztonság szervezetrendszerének belső együttműködését.
3.1.1.1.3. Az informatikai biztonsági szabályzat elsősorban a következő elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza:
3.1.1.1.3.1. kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz);
3.1.1.1.3.2. biztonsági helyzet-, és eseményértékelés eljárási rendje;

3.3.9.2.2. Hálózati hozzáférés privilegizált fiókokhoz

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött - úgynevezett privilegizált - felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

3.3.9.2.3. Hálózati hozzáférés nem privilegizált fiókokhoz

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

3.3.9.2.4. Helyi hozzáférés privilegizált fiókokhoz

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.

3.3.9.2.5. Visszajátszás-védelem

Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

3.3.9.5.2.1. Az érintett szervezet:

3.3.9.5.2.1.1. a jelszóra a következő elvárásokat érvényesíti: kis- és nagybetűk megkülönböztetése; a karakterek számának meghatározása; a kisbetűk, nagybetűk, számok és speciális karakterek, és minimális jelszóhosszúság;

3.3.9.5.2.1.2. meghatározott szám karakterváltozást kényszerít ki új jelszó létrehozásakor;

3.3.9.5.2.1.3. a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást), és nem továbbítja;

3.3.9.5.2.1.4. a jelszavakra minimális és maximális élettartam korlátozást juttat érvényre úgy, hogy meghatározott számú új jelszóig megtiltja a jelszavak ismételt felhasználását, és a rendszerbe első lépést lehetővé tevő ideiglenes jelszó lecserélésére kötelez.

3.3.11.8.6. Végrehajtható kód

Az elektronikus információs rendszer megtiltja az olyan bináris vagy gépi kód használatát, amely nem ellenőrzött forrásból származik, vagy amelynek forráskódjával nem rendelkezik.


De eltekintve az Iseumtól,
a karneváltól és a városalapítástól...

…AVAGY MIT SEGÍTHET A NIST?

- **Framework for Improving Critical Infrastructure Cybersecurity**
  - Framework Core
  - Framework Implementation Tiers
  - Framework Profile

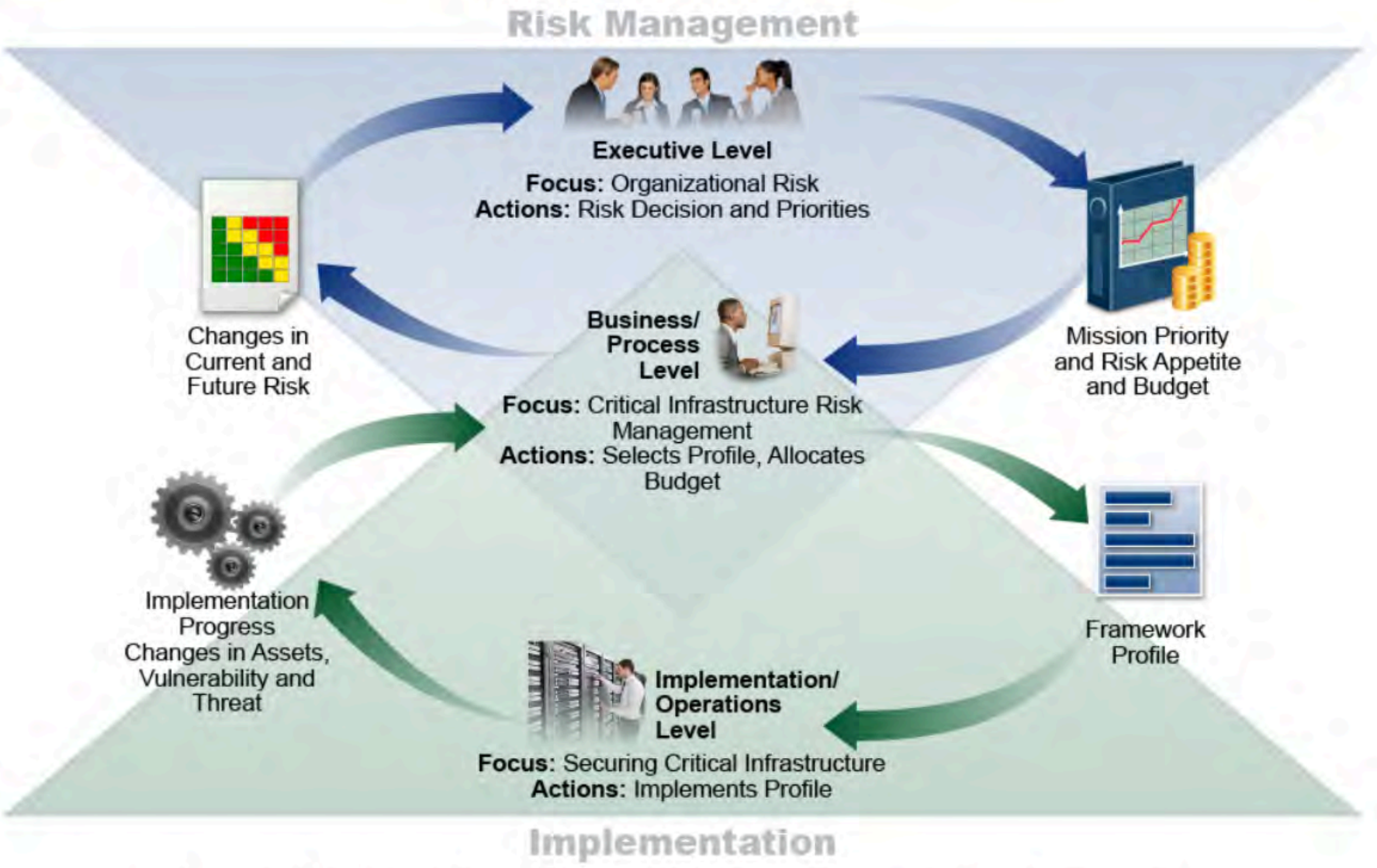

Figure 2: Notional Information and Decision Flows within an Organization

Figure 1: Framework Core Structure

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

NIST SP 800-53 REV4.

Security and Privacy Controls for Federal Information Systems and Organizations

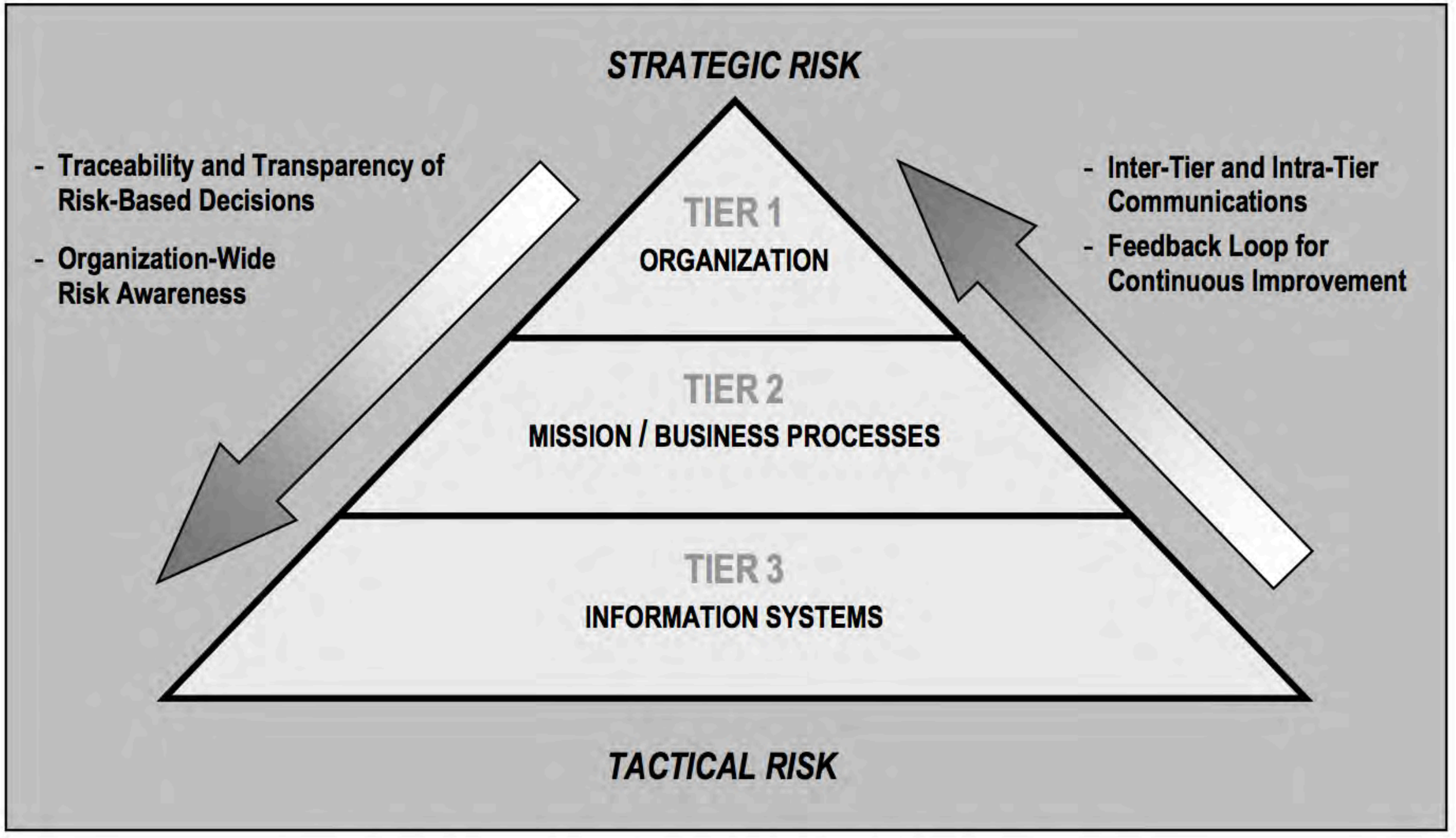

FIGURE 1: THREE-TIERED RISK MANAGEMENT APPROACH

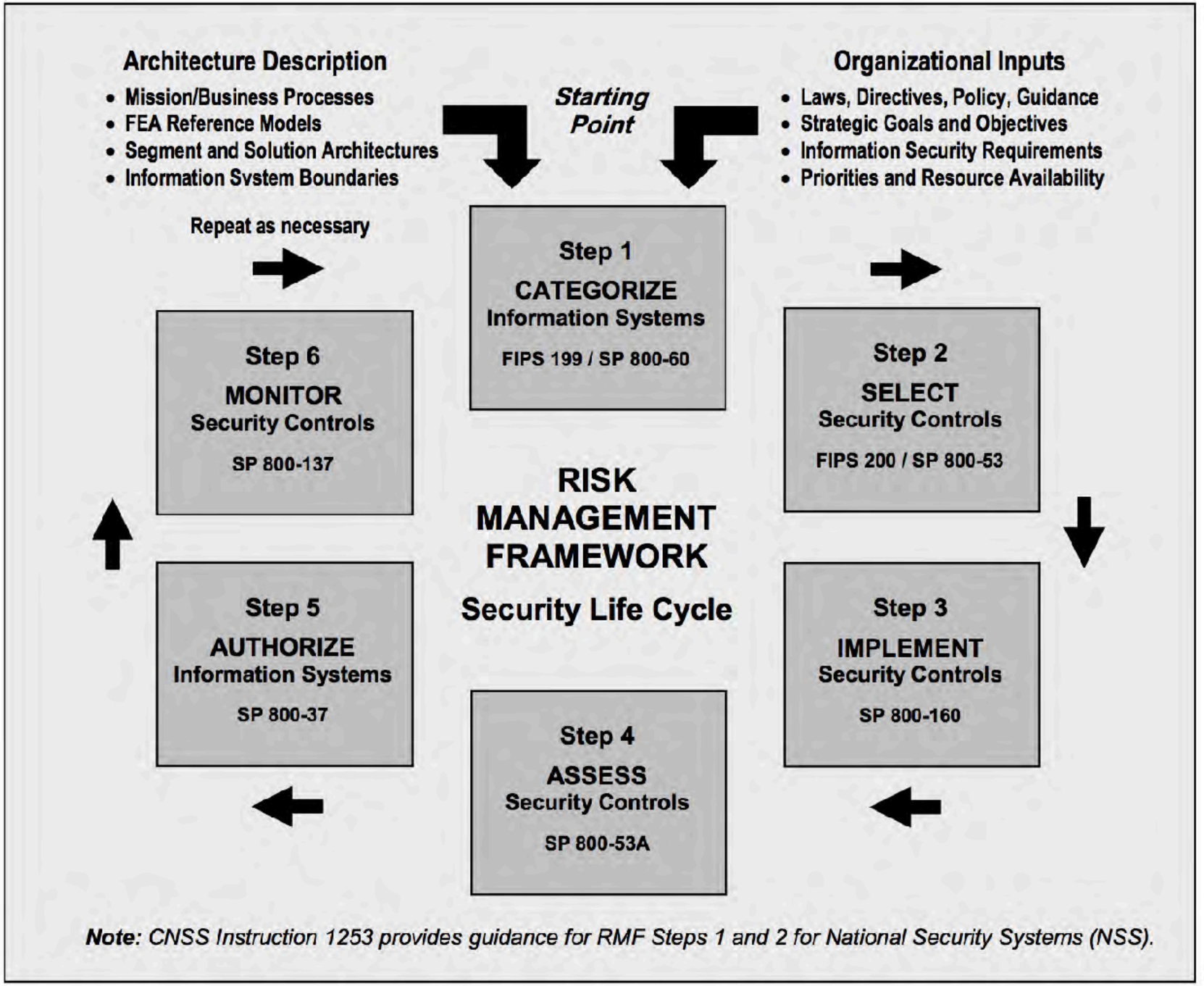

FIGURE 2: RISK MANAGEMENT FRAMEWORK

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

3.3.10.7. Sikertelen bejelentkezési kísérletek

3.3.10.7.1. Az elektronikus információs rendszer:

3.3.10.7.1.1. az érintett szervezet által meghatározott esetszám korlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire;

3.3.10.7.1.2. ha a sikertelen bejelentkezési kísérletekre felállított esetszám korlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot, vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control: The information system:

a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and

b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next logon prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.

Control Enhancements:

(1) *UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK*

[Withdrawn: Incorporated into AC-7].

(2) *UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE*

The information system purges/wipes information from [*Assignment: organization-defined mobile devices*] based on [*Assignment: organization-defined purging/wiping requirements/techniques*] after [*Assignment: organization-defined number*] consecutive, unsuccessful device logon attempts.

Supplemental Guidance: This control enhancement applies only to mobile devices for which a logon occurs (e.g., personal digital assistants, smart phones, tablets). The logon is to the mobile device, not to any one account on the device. Therefore, successful logons to any accounts on mobile devices reset the unsuccessful logon count to zero. Organizations define information to be purged/wiped carefully in order to avoid over purging/wiping which may result in devices becoming unusable. Purging/wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms. Related controls: AC-19, MP-5, MP-6, SC-13.

References: None.

Priority and Baseline Allocation:

P2	**LOW** AC-7	**MOD** AC-7	**HIGH** AC-7

3.3.10.8. A rendszerhasználat jelzése
3.3.10.8.1. Az érintett szervezet az elektronikus információs rendszer felhasználásával:
3.3.10.8.1.1. az érintett szervezet által meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést küld a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt, mely jelzi, hogy:
3.3.10.8.1.1.1. a felhasználó az érintett szervezet elektronikus információs rendszerét használja;
3.3.10.8.1.1.2. a rendszer használatot figyelhetik, rögzíthetik, naplózhatják;
3.3.10.8.1.1.3. a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár;
3.3.10.8.1.1.4. a rendszer használata egyben a felhasználó előbbiekbe történő beleegyezését is jelenti.
3.3.10.8.2. Az elektronikus információs rendszer a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez.
3.3.10.8.3. Az elektronikus információs rendszer a nyilvánosan elérhető rendszerek esetén:
3.3.10.8.3.1. kijelzi a rendszer használat feltételeit, mielőtt további hozzáférést biztosít;
3.3.10.8.3.2. ha felügyelet, adatrögzítés vagy naplózás történik, kijelzi, hogy ezek megfelelnek az adatvédelmi szabályoknak;
3.3.10.8.3.3. leírást biztosít a rendszer engedélyezett felhasználásáról.

AC-8 SYSTEM USE NOTIFICATION

Control: The information system:

a. Displays to users [*Assignment: organization-defined system use notification message or banner*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

1. Users are accessing a U.S. Government information system;
2. Information system usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
4. Use of the information system indicates consent to monitoring and recording;

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

c. For publicly accessible systems:

1. Displays system use information [*Assignment: organization-defined conditions*], before granting further access;
2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Includes a description of the authorized uses of the system.

Supplemental Guidance: System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-8	**MOD** AC-8	**HIGH** AC-8

ÖSSZEFOGLALÁS

- A 2013 évi L. törvény és a 41/2015 BM rendelet
  - hiánypótló, mindenképp szükség volt rá
  - önmagában majdhogynem pilótavizsgás
  - az intézmények még mindig nem szembesültek azzal, hogy belső erőforrásból nem, vagy nem teljes mértékben képesek megfelelni
- A NIST publikációi
  - magyarázatot, implementálási segédletet és iránymutatást adnak
  - használjuk tehát! 😊

asc
Save it easy

Lengré Tamás CISA
lengret@asc.hu