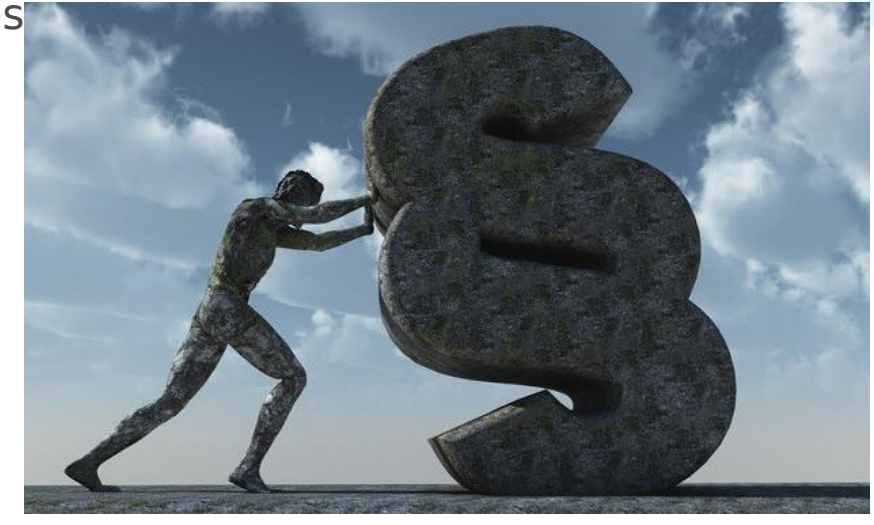
FELELŐSSÉGEK ÉS HATÁSKÖRÖK
A HAZAI SZABÁLYOZÁSBAN

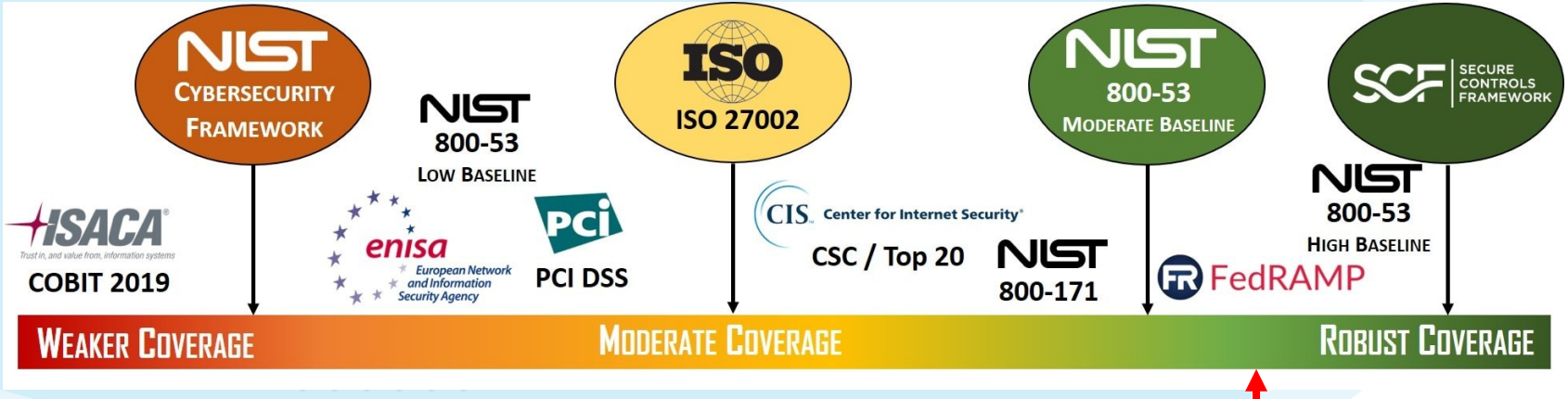
Fából vaskarika??? ☺

A TARTALOMBÓL

- Bemutatkozás
- Hazai szabályozás helyzete és megítélés
- A szabályozó betartásának helyzete
- Mi lehet a probléma
- Mitől lehet jobb



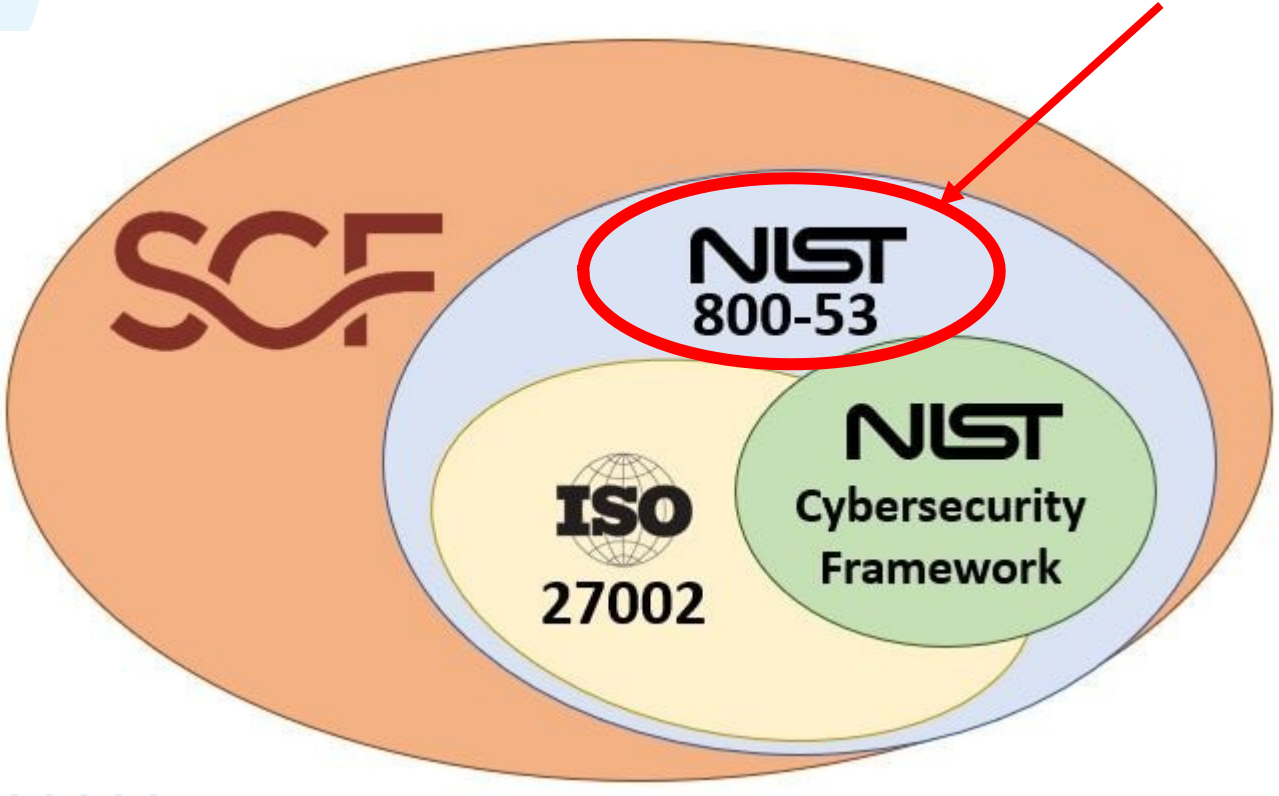
A HAZAI SZABÁLYOZÁS A NAGYVILÁGBAN



41/2015. (VII. 15.) BM rendelet

FORRÁS: HTTPS://WWW.COMPLIANCEFORGE.COM/

MÉGIS MIHEZ **HASONLÍT**



FORRÁS: HTTPS://WWW.COMPLIANCEFORGE.COM/

BETARTÁSÁNAK HELYZETE

- NINCS PONTOS ADAT, DE KOMOLY A LEMARADÁS (2015!!)
- ALACSONY ÉRETTSÉGI SZINT
- AZ ÚJ FEJLESZTÉSEKNÉL AZONNALI MEGFELELÉS!
- KEVÉS A TISZTÁN EGY KÉZBEN LEVŐ RENDSZER
- BONYOLULT ÜZEMELTETÉSI HÁTTÉRSZERVEZETEK
- ÖSSZETETT FEJLESZTŐ-PARTNERI VISZONYOK

MIT KELL TENNIE AKI BE AKARJA TARTANI?

- **(4)Ha az elektronikus információs rendszerrel rendelkező szervezet az elektronikus információs rendszernek csak egyes elemeit vagy funkcióit üzemelteti vagy használja - részben vagy teljesen -, a 4. mellékletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni.**

- **(5) Ha az elektronikus információs rendszert több szervezet használja, az elektronikus információs rendszer üzemeltetője az üzemeltetés elektronikus információbiztonságához szükséges követelményeket az elektronikus információs rendszeren tevékenységet végző minden, elektronikus információs rendszerrel rendelkező szervezet tekintetében érvényesíti.**

- **(6) … Az elektronikus információs rendszer üzemeltetője és az elektronikus információs rendszerrel rendelkező szervezetek az üzemeltetés elektronikus információbiztonságához szükséges követelményeket az elektronikus információs rendszer üzemeltetésére kötött szerződésben rögzítik.**

MI ALAPJÁN KÖSSÜNK SZERZŐDÉST?

- **Nincs egyértelmű ajánlás[1]**
- **Nehéz definiálni a határokat (technológiai lebontás)**
- **Nehéz definiálni a felelősségeket**
- **Sokszor közszolgáltatási szerződések szabályoznak**

[1]Kivétel talán a 3.3.11 Pont RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

JÓGYAKORLAT→ JÓ GYAKORLAT!

- PONTOS RENDSZERHATÁROK DEFINIÁLÁSA
- FELELŐSSÉGEK ELHATÁROLÁSA→ JOGSZABÁLY?
- NEMZETKÖZI SZABVÁNYOKNAK TÖRTÉNŐ MEGFELELTETÉS

41/2015. BM rendelet → ISO 27001/ NIST 800-53 → Cloud Controls Matrix[1]

A.13.2.2 Learning from information security incidents	IR-4
A.13.2.3 Collection of evidence	AU-9, IR-4
A.14 Business continuity management	
A.14.1 Information security aspects of business continuity management	
A.14.1.1 Including information security in the business continuity management process	CP-1, CP-2, CP-4
A.14.1.2 Business continuity and risk assessment	CP-2, PM-9, RA Family
A.14.1.3 Developing and implementing continuity plans including information security	CP Family
A.14.1.4 Business continuity planning framework	CP-2, CP-4
A.14.1.5 Testing, maintaining and reassessing business continuity plans	CP-2, CP-4
A.15 Compliance	
A.15.1 Compliance with legal requirements	
A.15.1.1 Identification of applicable legislation	XX-1 controls, IA-7
A.15.1.2 Intellectual property rights (IPR)	SA-6
A.15.1.3 Protection of organizational records	AU-9, AU-11, CP-9, MP-1, MP-4, SA-5, SI-12
A.15.1.4 Data protection and privacy of personal information	PL-5; SI-12
A.15.1.5 Prevention of misuse of information processing facilities	AC-8, AU-6, PL-4, PS-6, PS-8, SA-7
A.15.1.6 Regulation of cryptographic controls	IA-7, SC-13
A.15.2 Compliance with security policies and standards, and technical compliance	
A.15.2.1 Compliance with security policies and standards	XX-1 controls, AC-2, CA-2, CA-7, IA-7, PE-8,

CCM™ Cloud Controls Matrix

[1]CLOUD SECURITY ALLIANCE HTTPS://CLOUDSECURITYALLIANCE.ORG/RESEARCH/CLOUD-CONTROLS-MATRIX/

4G

KÖSZÖNÖM
A FIGYELMET!

Bánszki Zsolt
IT biztonsági üzletág igazgató