„Információvédelem menedzselése”
IC. vagy XCIX. Szakmai Fórum
Budapest, 2022. március 16.

Mi újság a 27000-es családban?
ISO/IEC 27002:2022

Móricz Pál
Hétpecsét Információbiztonsági Egyesület, alapító tag

www.szenzor-gm.hu

Dr. Tarján Gábor
Hétpecsét Információbiztonsági Egyesület, al-elnök

www.hetpecset.hu

Szabványcsalád fejlesztő

A 27000-es szabványcsalád fejlesztője:

- ISO/IEC *nemzetközi szabványügyi szervezetek*
- JTC1 Information Technology
- SC27 Information security, cybersecurity and privacy protection
  (SC27 korábbi neve: IT Security technics)
  - *216 publikált szabvány*
  - *72 szabvány fejlesztés alatt*
  - *48 P(articipating) és 34 O(bserving) member*
- (MSZT MB 819 műszaki bizottság: Informatika)

ISO 27000 szabványcsalád fő elemei

27000 Áttekintés és szótár

27001
Követelmények

Útmutatók
27002 Code practice
27003 Bevezetés
27037 Digitális bizonyíték
27038 Digitális redukció

27033-x Hálózat bizt
27034-x Alkalmazás bizt.
27036-x Szállító kapcs.

Biztonság területek
27004 Mérés
27005 Kockázat mgmt
27035 Incidens mgmt
27031 Folytonosság
27032 Kiberbiztonság
27039 IDS
27040 Storage bizt.
27016 Szerv. gazdálk.

Ágazatonkénti biztonság
27015 Pénzügyi szolg.
27011 for telecom
27010 Szervezetek közti komm.
27013 ISMS+ITSMS
27014 IS Govermnance
27019 Energiaipari foly.kontroll
27799 ISM eü-ben
27017 Cloud kontroll útmutató
27018 Public cloud sz.azon.info

Auditorok, auditálás
27006 ISMS tanúsító köv
27007 ISMS auditálás útmutató
27008 IS kontroll audit útmutató

27000 család szabványai

65 publikált szabvány
(+ 7 db 291xx privacy szabvány)

- Ezek között követelményszabvány:
  27001, 27701 (privacy kieg.), tanúsítóknak 27006

➢ 2020 január óta 28 új szabványkiadás, pl.

- 27006 tanúsító testületek követelményei (AMD)
- 27006-2 privacy tanúsító követelmények
- 27014 IS Governance
- 27013 Integrált ISMS és IT SMS
- 27021 ISMS tanácsadó kompetencia
- 27022 ISMS folyamatok
- 27100 Cybersecurity

Szabványok fejlesztés alatt

- Folyamatban lévő fejlesztések
  - *13 új szabvány fejlesztés, pl*
    27046 Big data security and privacy
    27109 Cybersecurity education and training
    2740x IoT security and privacy
    27033-7 Network virtualization security
  - *13 új szabványverzió fejlesztés, pl.*
    27005 IS kockázatmenedzsment
    27011 Kontrollok Telekom szervezetekre
    27021 Tanácsadó kompetencia
    27031 Folytonosság
    27032 Internet security (korábban cybersecurity)
    27035-x Incident management
    27036-x Supplier relationships

ISO/IEC 27002:2022

- korábbi cím:
  ISO/IEC 27002:2013
  Information technology — Security techniques — Code of practice for information security controls
- új szabvány cím:
  ISO/IEC 27002:2022
  Information security, cybersecurity and privacy protection — Information security controls

2022.02.15.
157 oldal

ISO/IEC 27002:2022 változások

Fő változások

- szabvány célt jobban tükröző cím (IS kontroll referenciakészlet nemzetközileg elfogadott legjobb gyakorlat alapján)
- kontrollokra attribútumok, osztályba sorolás (több szempont szerint csoportosíthatósághoz)
- új struktúra, összevonások, új kontrollok

- *Bevezetésben:*
  - *lehetnek ágazatspecifikus kiegészítések, példaként említ néhány szabványt is*

ISO/IEC 27001:2013

- Az ötéves felülvizsgálat lezárult, megerősítve változatlanul de:

- Módosítás (Amd) folyamatban
  - 27002 hivatkozás pontosítás
  - fogalmazás finomítás:
    kontrollok „átfogó listája” helyett „lehetséges listája”
    az A melléklet
  - „A” melléklet kontroll listája lecserélve új 27002 szerint
- Kiadás állása:
  - szabványmódosítás tervezet (draft) szavazás alatt
  - kiadás gyorsított eljárással várhatóan 2022. 2. félév
  - átállásra várhatóan kiadás után 2 évet fognak adni.

Változások az ISO 27002-es szabványban

- *Ha még emlékszünk:* ISO 2700**1**:2013 „A” melléklet = 114 kontroll, 14 témakörben és
- ISO 2700**2**:2013 = 114 kontroll magyarázatokkal (control + implementation guidance) a 14 témakörben
- ISO 2700**2**:20**22** = 114 kontroll összevonva 93-ba, és kiegészítve, átformálva néhány „hot topic”-kal **pl.:**
  - Threat Intelligence
  - Felhőbiztonság
  - Távmunka biztonsága
  - Adatszivárgás megelőzése
  - Adatmaszkolás

A lényegi változások az ISO 27002-es szabványban

- *A kontrollok 14 (A5-A18) helyett négy csokorba szedve*
- *114 kontroll helyett 93*
- *57 kontroll 24-be összevonva*
- *23 átnevezett kontroll*
- *11 „új” kontroll*
- *1 kettéosztott (szétválasztott kontroll)*
- *0 db kizárt kontroll*

Változások az ISO 27002-es szabványban

14 témakör helyett **négy kontroll kategória**:

5. **Szervezeti** Kontrollok
   (Organizational Controls – 37 db)
6. **Személyi** Kontrollok (People Controls – 8 db)
7. **Fizikai** Kontrollok (Physical Controls – 14 db)
8. **Technológiai** Kontrollok
   (Technological Controls – 34 db)

Annex A = a kontroll attribútumok leírása (mátrix)

Annex B = kereszt-referencia táblázat

(régi versus új verzió)

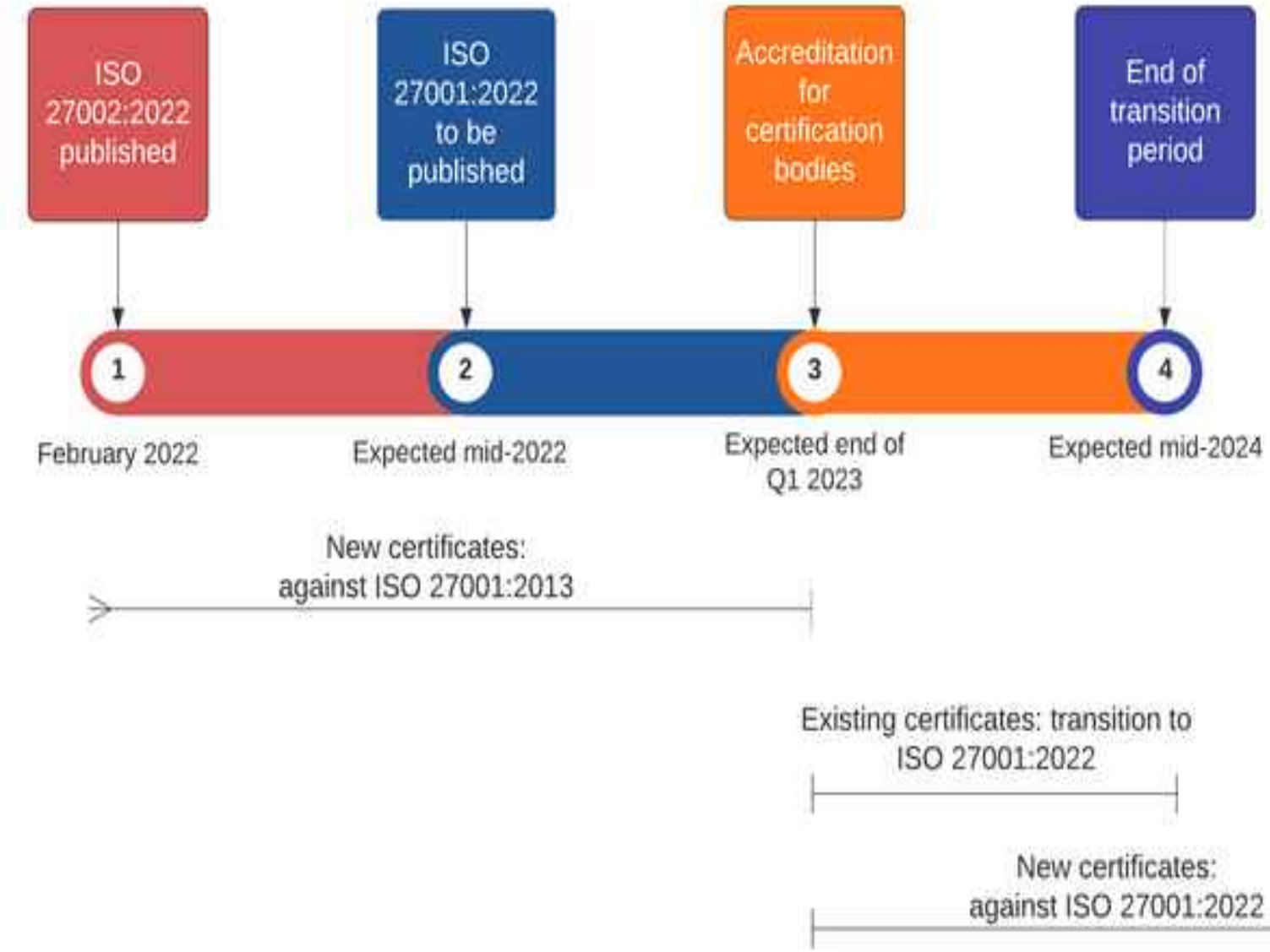
…és IGEN, lesz ún. **átmeneti időszak!**

…

Az „új” kontrollok (csak ízelítő gyanánt)

- 5.7 Threat intelligence
- 5.23 Information security for use of cloud services
- 5.30 ICT readiness for business continuity
- 7.4 Physical security monitoring
- 8.9 Configuration management
- 8.10 Information deletion
- 8.11 Data masking
- 8.12 Data leakage prevention
- 8.16 Monitoring activities
- 8.23 Web filtering
- 8.28 Secure coding

Az átmenet (transition) szabályai!



Az átmenet javasolt stratégiái

Ha még csak most van a céged az első tanúsítás (initial assessment) előtt:

- Ha tudod, hogy **2023.03.31. előtt** lesz a tanúsítási esemény, akkor alkalmazd a „régi” 114 kontrollt, és fuss neki így a tanúsításnak,
- Ha tudod, hogy **2023.04.01. után** lesz a tanúsítási esemény, akkor alkalmazd az „új” 93 elemű kontroll-készletet

Ha már tanúsítva van a céged, akkor készülj fel **2023.03.31.-ig** a változásokra, és a dátum után esedékes felügyeleti auditon mutasd be az „új” 93 elemű kontroll-készletre optimalizált működésedet!

Mi az amiben (valószínűleg) nem kell változtatni?

Ha van egy működő IBIR, akkor ehhez ne nyúlj (feltétlenül):

- Az IBIR (ISMS) terjedelme (scope)
- Érdekelt felek (és igényeik)
- IBSZ *(ha ez egy átfogó dokumentum és az egyes kontrollok külön szabályozásban vannak)*
- Kockázatértékelési módszertan
- Képzés & tudatosítás
- Kommunikáció
- Dokumentum kezelés (document control)
- Megfigyelés és mérés
- Belső audit
- Vezetőségi átvizsgálás
- Javító, helyesbítő, megelőző intézkedések

Köszönjük a figyelmet!
(és találkozunk a 200. Fórumon is!)