Horváth István

Az új ISO/IEC 27001 szabvány követelményeinek bevezetése

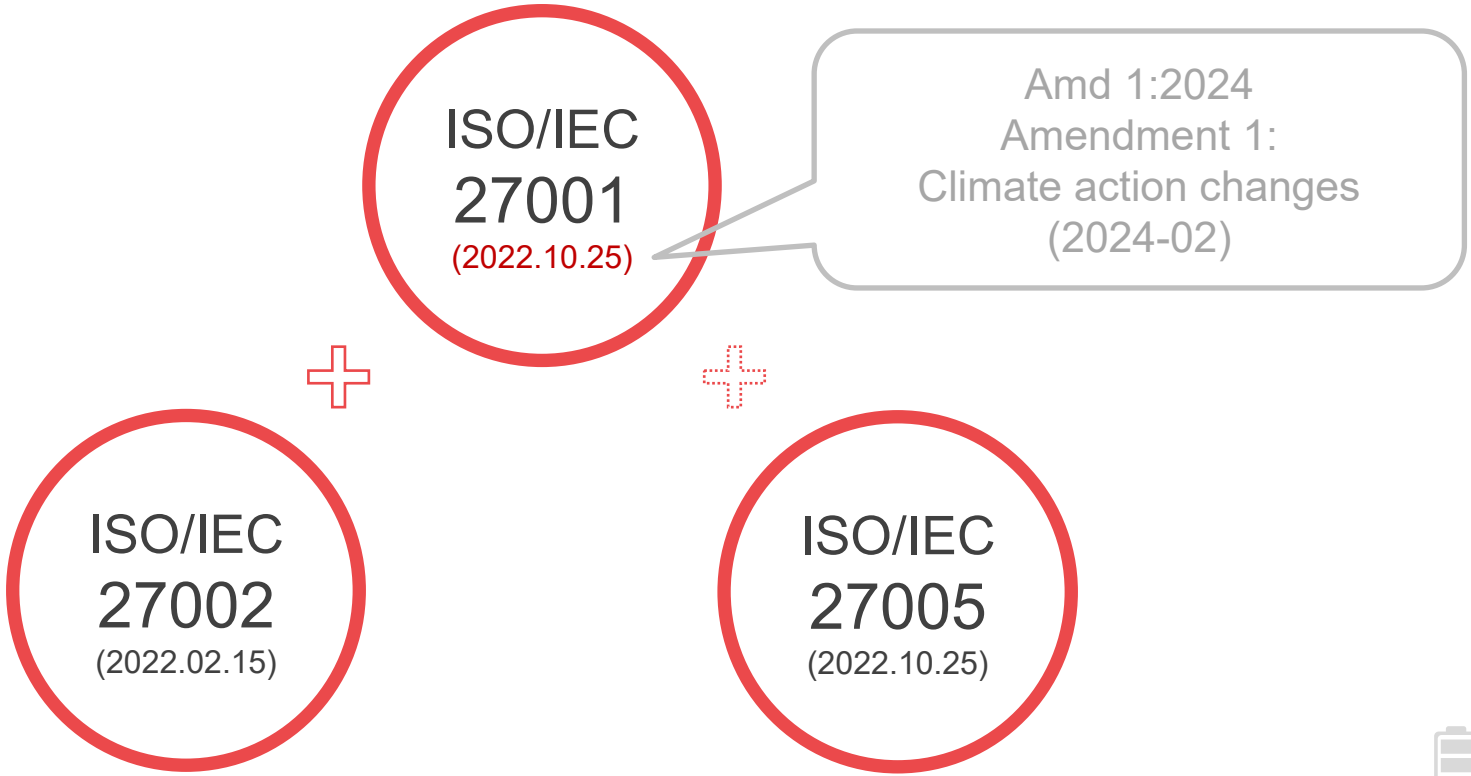
Az információbiztonsági követelményrendszerek aktuális változásai

(EOQ MNB Egyesület rendezvénye)

2024.03.26

ISO 27000 szabványcsalád változások

Releváns szabványok



ISO 27001 (2022) változások

Cím és tartalom

2013

Cím:

„Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek.”

Tartalom:

- Szabványtörzs (4-10).
- A mellékletben 13 intézkedés csoport (A5 - A18).
- Az intézkedések 3 szintű bontása.
- Az intézkedések a célt is tartalmazzák.

2022

Cím:

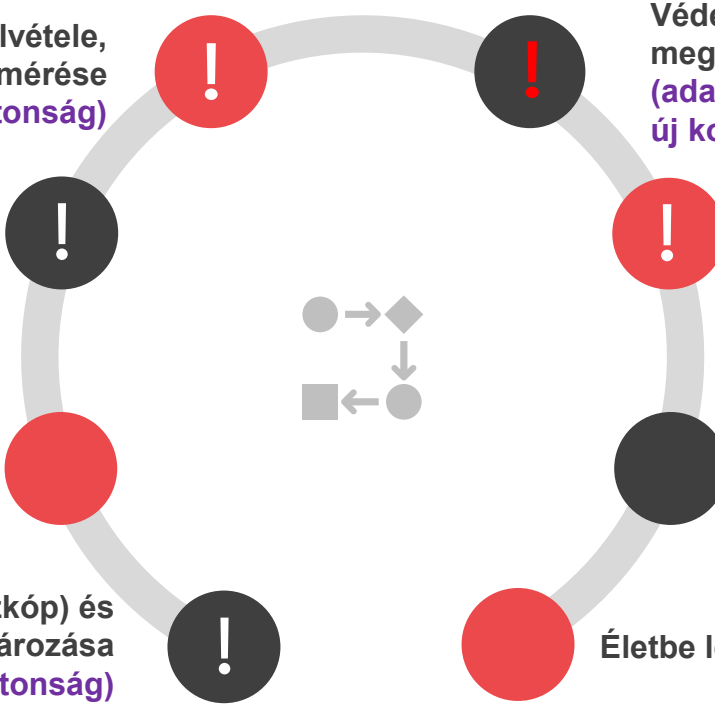
„Információbiztonság, kiberbiztonság és a magánélet védelme. Információbiztonság-irányítási rendszerek.”

Tartalom:

- Szabványtörzs (4-10), van változás.
- Az A mellékletben 4 intézkedés csoport (A5–A8) és 93 intézkedés.
- Az intézkedések 2 szintű bontása.
- Az intézkedések NEM tartalmaznak célt.

IBIR bevezetés lépései

(Spoiler Alert)



Fenyegetettségek felvétele, kockázatok felmérése (adatvédelem és kiberbiztonság)

A védendő (információs) vagyon felmérése (adatvédelem)

A szervezeti keretek és erőforrások tisztázása

Alkalmazási terület (szkóp) és politika meghatározása (adatvédelem és kiberbiztonság)

Védelmi intézkedések, kontrollok meghatározása (adatvédelem, kiberbiztonság, új kontrollok)

Védelmi intézkedések és IBIR folyamatok dokumentálása (változáskezelés új intézkedések)

Állomány oktatása, tudatosítás

Életbe léptetés

ISO 27001 (2024) változások

Amd 1:2024 - Szabványtörzs (4.1, 4.2)

4.1 A szervezet és környezetének megértése

\+ *„A szervezetnek meg kell határoznia, hogy az éghajlatváltozás releváns kérdés-e.”*

4.2 Az érdekelt felek szükségleteinek és elvárásainak megértése

\+ *„MEGJEGYZÉS 2. Az érintett érdekelt feleknek lehetnek az éghajlatváltozással kapcsolatos követelményei.*

ISO 27001 (2022) változások

Szabványtörzs (6 - 7)

6. Tervezés
„6.2 Információbiztonsági célok és az elérésük megtervezése…
Az információbiztonsági célok:
d) legyenek figyelemmel kísérve;”

Célok elérésének támogatása.
Nem csak a vezetőségi témája!

6. Tervezés
„6.3. A változtatások tervezése
…a változtatásokat tervezetten és módszeresen kell végrehajtani.”

Nem csak ledokumentálás az audit előtt!
Szervezeti és technológiai változtatások!

7. Erőforrás
7.4. Kommunikáció
„A szervezetnek meg kell határoznia…
d) hogyan kommunikáljanak.
~~*d) hogy kinek kell kommunikálnia; és*~~
~~*e) azokat a folyamatokat, amelyekkel a kommunikációt meg kell valósítani.”*

Egy gonddal kevesebb ☺.

ISO 27001 (2022) változások

Szabványtörzs (8 - 10)

8. Működés

8.1 Működéstervezés és –felügyelet

„...követelmények teljesítéséhez és a 6. fejezet szerinti tevékenységek megvalósításához szükségesek azáltal, hogy

– meghatározza a folyamatokra vonatkozó kritériumokat;

– megvalósítja a folyamatok felügyeletét, összhangban a kritériumokkal.;”

Folyamatok: tervezés, bevezetés, felügyelet alatt tartás, dokumentálás.
Az irányítási rendszer eredményeinek biztosítása.

9. Teljesítményértékelés

„9.3.2 A vezetőségi átvizsgálás bemenetei…

c) az érdekelt felek azon elvárásainak változásai, amelyek az információbiztonság-irányítási rendszer szempontjából lényegesek;”

Kik az érdekelt felek? (4.2)
Mi változott (pl. jogszabályok)?
Mit kell változtatni?

ISO 27001 (2022) változások

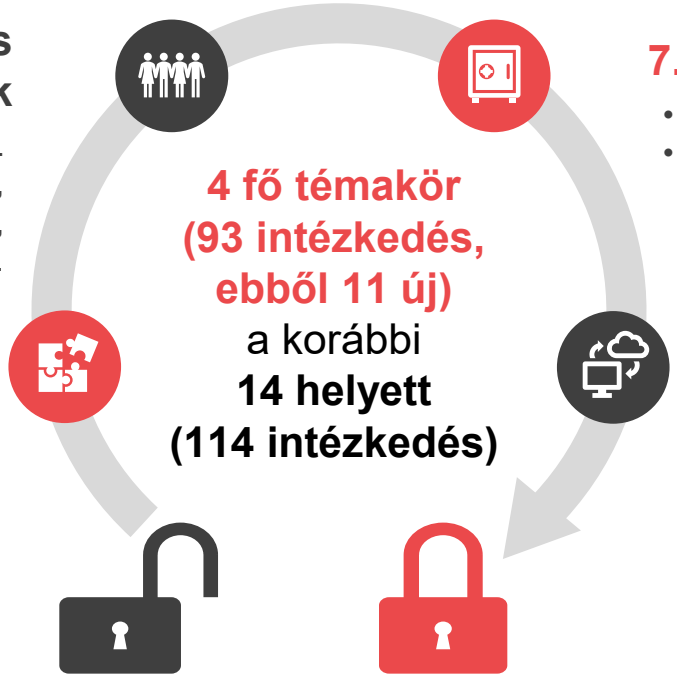
Az A melléklet (szakmai területek csoportosítása)

6. Emberekkel kapcsolatos intézkedések

- **8 db** intézkedés (A6.1 – A6.8).
- Humánerőforrás biztonsága, átvilágítás, tudatosság, képzés, fegyelmi eljárás, távmunka…

5. Szervezeti intézkedések

- **37 db** intézkedés (A5.1 - A5.37).
- Irányelvek, szabályok, folyamatok, eljárások, szervezeti struktúra…



4 fő témakör (93 intézkedés, ebből 11 új)
a korábbi
14 helyett
(114 intézkedés)

7. Fizikai intézkedések

- **14 db** intézkedés (A7.1 – A7.14).
- Fizikai hozzáférés, vendégek, eszközök biztonsága, adathordozók, környezeti fenyegetések, közműszolgáltatások…

8. Technológiai intézkedések

- **34 db** intézkedés (A8.1 – A8.34).
- IT-infrastruktúra védelme, szoftver- és rendszerfejlesztés, tesztelés…

ISO 27002 (2022) változások

Mit nem adtak nekünk a rómaiak (elég csak az ISO 27001)?

Célok és útmutatás

- A intézkedés és a hozzá tartozó cél.
- A gyakorlati végrehajtásra vonatkozó útmutatás.

Attribútumok

- Az intézkedések kategorizálásának eszköze.
- Kapcsolat a kockázatértékeléssel.

„Mapping” (2013 <> 2022)

- Összerendelés a 2013-as verzió felől.
- Összerendelés a 2022-es verzió felől.

ISO 27002 (2022), kell ez nekem?

Attribútumok

Mik azok az „attribútumok”?

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_access_management	#Governance_and_Ecosystem

- (Újra) csoportosíthatók a kontrollok.
- Holisztikus megközelítés.
- Több attribútum is lehet.
- Saját attribútumot is használhatunk.

Identitás- és hozzáférés-kezelés

5.3	Feladatkörök szétválasztása
5.15	Hozzáférés-felügyelet
5.16	Személyes azonosítók kezelése
5.17	Hitelesítési információk
5.18	Hozzáférési jogosultságok
5.37	Dokumentált működési eljárások
7.2	Fizikai belépés
8.2	Kiemelt hozzáférési jogosultságok
8.3	Az információhoz való hozzáférés korlátozása
8.4	Hozzáférés a forráskódhoz
8.5	Biztonságos hitelesítés

A5.7 Fenyegetésfelismerő képesség

Elmélet

Cél:

A szervezet **fenyegetettségi környezetének tudatosítása** annak érdekében, hogy a **megfelelő védekezési intézkedéseket** meg lehessen **valósítani**.

Intézkedés:

„Az információbiztonsági fenyegetésekkel kapcsolatos információkat össze kell gyűjteni és elemezni kell fenyegetést felismerő képesség kialakítása érdekében.”

Gyakorlat

- Meglévő és új fenyegetések (pl. AI).
- Stratégia: támadók, támadások típusai.
- Taktika: információk a támadók módszertanáról, eszközeiről és technológiáiról.
- Operatív: konkrét támadásokkal kapcsolatos részletek, beleértve a technikai jellemzőket is.
- TTP: Tactics, Techniques and Procedures (https://attack.mitre.org).
- Beépítés a kockázatkezelésbe.

A5.23 Felhőszolgáltatások használatára vonatkozó információbiztonság

Elmélet

Cél:

A felhőszolgáltatások használatához szükséges információbiztonság **meghatározása** és **menedzselése**.

Intézkedés:

*„A felhőszolgáltatások megszerzésének, használatának, kezelésének és befejezésének **folyamatait** a szervezet információbiztonsági **követelményeivel** összhangban kell kialakítani.”*

Gyakorlat

- Teljes életciklus!
- Tervezés (hol?, mit?, mennyiért?).
- Kockázatok elemzése és kezelése.
- Lokáció, sávszélesség, SLA?
- Ki és mire használja (Google Drive)?
- Megosztott felelősség (adatfeldolgozás).
- Kitől vesszük (disztribútor)?
- Kell mentés és hova?
- Incidensek kezelése.
- Felhő Elhagyási Stratégia (CES).

A5.30 IKT-felkészültség az üzletmenet-folytonossághoz

Elmélet

Cél:

Az IKT üzletmenet-folytonossági **felkészültsége**, **menedzsmentje** és az **információbiztonság** biztosítása a zavarok idején (szervezet célkitűzései).

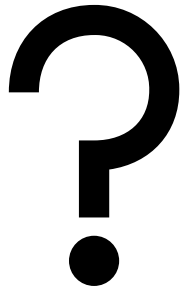
Intézkedés:

*„Az IKT-készültséget az üzletmenet-folytonossági célok és az IKT folytonossági követelmények alapján kell megtervezni, megvalósítani, karbantartani és **tesztelni**.”*

Gyakorlat

- A szervezet céljainak elérése a zavarok idején is.
- A követelmények az üzleti hatáselemzésből (BIA), ez nem (csak) IT.
- Helyreállítási időcél (RTO), helyreállítási pont (RPO).
- RTO/RPO-nál érdekelt felek igényei (és amit vállaltunk!).
- ISO 22301 és az ISO 22313 szabványok.
- ISO/TS 22317 útmutató az üzleti hatáselemzéshez (BIA).

A 6.1-6.8 Emberekkel kapcsolatos intézkedések (NINCS VÁLTOZÁS)



A7.4 A fizikai biztonság figyelemmel kísérése

Elmélet

Cél:

Az illetéktelen fizikai hozzáférés észlelése és megakadályozása.

Intézkedés:

*„Folyamatosan figyelemmel kell kísérni a telephelyeket az illetéktelen **fizikai** bejutás észlelése érdekében.”*

Gyakorlat

- Őrök, behatolásjelzők, videómegfigyelő rendszerek.
- Érintés- és nyitásérzékelők, hang- és mozgásérzékelők.
- A központi vezérlés és az érzékelők manipulációvédelme.
- Rendszerek kialakítása bizalmas információ (de van GDPR!).
- Adatvédelmi jogszabályok, megfigyelés, megőrzési idők.

A8.9 Konfigurációkezelés

Elmélet

Cél:

A hardverek, szoftverek, szolgáltatások és a **hálózatok** megfelelő és biztonságos beállítása és a konfiguráció felügyelet alatt tartása.

Intézkedés:

„A hardver, a szoftver, a szolgáltatások és a hálózatok konfigurációit, beleértve a biztonsági konfigurációkat létre kell hozni, dokumentálni kell, meg kell valósítani, felügyelni kell és át kell vizsgálni.”

Gyakorlat

- Konfigurációk egységes sablonjainak meghatározása (azonos eszközök).
- Gyártók és független biztonsági szervezetek ajánlásai.
- Sablonok rendszeres felülvizsgálata (verzióváltások).
- Változtatás a változáskezelési folyamat alapján (A8.32. pontot).
- Központosított felügyelet kialakítása (szoftvertámogatás).

A8.10 Információtörlés

Elmélet

Cél:

Az érzékeny információk nemkívánatos hozzáférhetővé tételének megelőzése, jogi, törvényi, szabályozási és szerződéses előírásoknak való megfelelés érdekében.

Intézkedés:

„Az információs rendszerekben, eszközökben vagy bármely más adathordozón tárolt információkat törölni kell, ha már nincs szükség rájuk.”

Gyakorlat

- Érzékeny információk tárolása csak a szükséges ideig (nem csak GDPR).
- Adatmegőrzési irányelvek a jogszabályokkal összhangban.
- Törlési módszer (felülírás, kriptográfia).
- Felhőszolgáltató által biztosított törlési módszer megfelelősége (ISO/IEC 27017).
- Másolatok és ideiglenes fájlok törlése.
- Biztonságos ártalmatlanítás („tanúsított” szolgáltatók és igazolás).
- ISO/IEC 27555 szabvány a személyes adatok törléshez.

A8.11 Adatmaszkolás

Elmélet

Cél:

Az érzékeny adatok (PII is) kitettségének korlátozása és a jogi, törvényi, szabályozási és szerződéses előírásoknak való megfelelés.

Intézkedés:

„Az adatmaszkolást kell használni a szervezet témaspecifikus hozzáférés-felügyeleti és egyéb kapcsolódó témaspecifikus politikáival, valamint üzleti követelményeivel összhangban, figyelembe véve a vonatkozó jogszabályokat.”

Gyakorlat

- Maszkolás, álnevesítés, anonimizálás.
- Megfelelő és hatékony módszerek alkalmazása (adatok nullázása, törlése, cseréje [****, hash, titkosítás]).
- Jogosultsághoz vagy tevékenységhez kötött adatelérés.
- Adatbázisok (*„Dynamic Data Mask”*).
- Adatfeldolgozók hozzáférése.
- Adatok más információkkal történő összekapcsolása!
- Nem csak a személyes adatok!

A8.12 Az adatszivárgás megelőzése

Elmélet

Cél:

Az információk jogosulatlan nyilvánosságra hozatalának és megszerzésének észlelése és megakadályozása.

Intézkedés:

*„Adatszivárgás-megelőző intézkedéseket kell alkalmazni olyan rendszerekre, hálózatokra és minden más eszközre, amely **érzékeny információkat** dolgoz fel, tárol vagy továbbít.”*

Gyakorlat

- Információk azonosítása és osztályozása (védelmi szint).
- Csatornák felügyelete (e-mail, adathordozók, stb.).
- Azonosítani, észlelni, blokkolni.
- Adatkezelési műveletek tiltása (másolás, beillesztés), DLP rendszerek.
- A mobileszközök, képernyőfotók, tudatosság.
- Szándék észlelése (honeypots), megtévesztés.

A8.16 Figyelemmel kísérési tevékenysége

Elmélet

Cél:

Az rendellenes viselkedés és a potenciális információbiztonsági incidensek észlelése.

Intézkedés:

„A hálózatokat, rendszereket és alkalmazásokat figyelemmel kell kísérni a rendellenes viselkedés szempontjából, és meg kell tenni a megfelelő intézkedéseket a lehetséges információbiztonsági események értékelésére.”

Gyakorlat

- A figyelemmel kísérési követelmények (üzleti, IB, törvényi).
- A figyelemmel kísérés terjedelme, szintje.
- IDS, IPS, DLP, vírusvédelem, tűzfalak…
- Normális viselkedés és küszöbértékek, riasztások meghatározása.
- Hozzáférési időpont, viselkedés, performancia esemény, stb.
- Napló tárolási idő (szükséges <> elégséges).
- Eljárások a időben történő reagálásra (incidensek A5.26.).

A8.23 Webszűrés

Elmélet

Cél:

A rendszerek védelme a rosszindulatú szoftverektől és a nem kívánt webes erőforrások elérésének megakadályozása.

Intézkedés:

„A külső webhelyekhez való hozzáférést úgy kell kezelni, hogy csökkentsék a rosszindulatú tartalomnak való kitettséget.”

Gyakorlat

- Webforgalom korlátozása (illegális, vírus, adathalász).
- IP cím vagy domain (DNS) blokkolása, tartalomszűrés (A5.7 kimenete).
- Weboldalak elérésére fehér (munkához) és fekete lista.
- Bevezetés előtt a szabályok meghatározása (kommunikálása).
- Tudatosítás a biztonságos és megfelelő használatáról.

A8.28 Biztonságos kódolás

Elmélet

Cél:

A szoftver biztonságos megírásának biztosítása, ezáltal a szoftverben lévő potenciális információbiztonsági sebezhetőségek számának csökkentése.

Intézkedés:

„A szoftverfejlesztés során biztonságos kódolási elveket kell alkalmazni.”

Gyakorlat

if (true) {

- Tervezés, kódolás, tesztelés, felülvizsgálat, karbantartás (teljes életciklus).
- Szervezeti szintű folyamatok kialakítása (fejlesztésre).
- A minimális követelmények meghatározása („open-source”, „third-party” is).
- Naprakész információk fenyegetésekről, sebezhetőségekről (OWASP).
- Statikus (SAST) és dinamikus (DAST) vizsgálat.

}

Köszönöm a figyelmet!