A megújult ISO/IEC 27001 információbiztonsági szabványra való átállás követelményei

Dr. Horváth Zsolt, Horváth István

Előzmények

Az információbiztonsági irányítási rendszer követelményeit meghatározó szabvány, az ISO/IEC 27001 megújult, és 2022 októberében megjelent az új kiadása. A szabványban a szabványtörzsben lévő követelmények kisebb mértékben, míg az információbiztonsági kontrollok követelményeit tartalmazó A melléklet jelentős mértékben változott. Jelen publikáció célja a szabvány főbb újdonságainak bemutatása, valamint az új szabvány használatára való átállásban a szabványt alkalmazó szervezetek számára útmutatás adása.

1. Bevezetés

Az International Organization for Standardization (ISO) általi irányítási rendszerszabványok az adott szabvány tárgyának megfelelő működés legjobb gyakorlatának alapelveit tartalmazzák. Azonban a legjobb gyakorlatok az idő, és vele együtt a technika, technológia változásával jelentősen megváltoznak. Emiatt ezeket a szabványokat rendszeres időközönként felülvizsgálják, és a kor követelményeihez igazítva újra kiadják.

Ez történt most az információbiztonsági irányítási rendszer szabványával, az ISO/IEC 27001-gyel is. A szabvány megelőző kiadása 2013 óta volt érvényben, és az azóta eltelt majdnem egy évtizedben a világban jelentős változások mentek végbe. Ezek a változások különösen az információbiztonságra, és azon belül is kiemelten az informatikai biztonságra voltak nagy hatással. Csak néhány példa ezekre a változásokra: rohamosan megnövekedett a kibertér használatának volumene és jelentősége, általánosabb lett a felhő-alapú szolgáltatások használata, nagyobb szerepet kapott a virtualizáció és a dockerizáció, a munkavégzés módjában elterjedtebb lett a home office, sőt már rohamos mértékben terjed a 'digitális nomád' életmódhoz kapcsolódó online munkavégzési stílus is. A változásokat sokáig lehetne még sorolni.

Az információbiztonsági szakma többi szabványrendszereiben, illetve az egyes ágazatok speciális információbiztonsági követelményrendszereiben egyre inkább kialakult egy újfajta rendszerezési szemlélet, amelyet a legtöbb szakmai helyen nagyjából egységesen használnak. Logikus elvárásként adódik, hogy az illeszkedő ISO-szabványrendszer követelményeinek is célszerű ezt a struktúrát alkalmaznia.

Mindez azonban magával hozza, hogy az információbiztonsági működésnek újabb kihívásokkal kell szembe nézni, ami gyakorlatilag kikényszerítette az ezek megfelelő működését előíró követelményszabvány megújítását is. Az ISO/IEC 27001:2022 szabványt [1] 2022. október 25-én adták ki, a szabvány 'A mellékeltében' lévő információbiztonsági kontrollok értelmezésére és magyarázatára vonatkozó ISO/IEC 27002:2022 szabványt [2] pedig már korábban, 2022. februárjában.

2. Az ISO/IEC 27001:2022 szabvány főbb újdonságai

A) Általános alapelvek

Már a szabvány címének módosulása is előre jelzi, hogy jelentős változásokra lehet számítani. Az információbiztonság mellett a cybersecurity (kiberbiztonság) és a privacy protection (magánélet védelme) szavak is megjelentek. Ez előrevetíti azt a törekvést, hogy a szabvány és az általa kiépített irányítási rendszer megfeleljenek a kor információbiztonsági és adatvédelmi elvárásainak. A címben szerelő két terület az információs társadalom rohamos fejlődésével, az online tér és szolgáltatásainak robbanásszerű növekedésével és a különböző generációk általi intenzív használatával vált egyre hangsúlyosabbá. Ez jól nyomon követhető a törvényi és jogszabályi környezet változásán is, amely reagálni próbált az új kihívásokra. A kiberbiztonság és a kibervédelem kiemelt és önálló terület lett a hazai és nemzetközi jogban is. Például 2013-as évben fogadták el Magyarország első Nemzeti Kiberbiztonsági Stratégiáját, 2019-ben pedig megszületett a modern, a valódi fenyegetésekre reagáló európai uniós kiberbiztonsági törvény (EU Cybersecurity Act). Az adatvédelem és ezen keresztül a magánélet fokozott védelmének az igénye is folyamatosan erősödött, amit a 2016-ban megjelent GDPR rendelet is világosan tükröz. Tehát már a címből sejthető, hogy a szabványalkotók globális szinten jogi és szakmai elvárásoknak megfelelő szabványt kívántak megalkotni. Ez vonatkozik mind a ISO/IEC 27001:2022-es, mind a ISO/IEC 27002:2022-es szabványra is.

B) Szabványtörzs tartalmi újdonságai

A ISO/IEC 27001 szabvány sajátossága, hogy az irányítási rendszer követelményeit leíró szabványtörzs (5-10 fejezet) mellett a konkrét információbiztonsági intézkedési célok és intézkedések a szabvány 'A mellékletében' találhatóak. Ennek felépítése összhangban van a ISO/IEC 27002-es szabvánnyal, amely az intézkedések megvalósításához nyújt végrehajtási útmutatót. Ez a felépítés és kapcsolat az új 2022-es kiadásban sem változott, és a végrehajtási útmutatóként már az új ISO/IEC 27002:2022-es szabványra hivatkozik.

Természetesen az új szabványtörzs is követi a HLS-t (High Level Structure), ami az ISO irányítási rendszerek fontos strukturális jellemzője. Ez az egységes felépítés nagyban megkönnyíti az integrált irányítási rendszerek kialakítását és auditálását. A HLS-hez történő pontosabb illeszkedés érdekében – követve az előző verzió óta megjelent irányítási rendszerszabványokat –finomhangolások történtek. Ezek többségében a szövegstruktúra jobb illeszkedését szolgáló szövegformázási (pl. sorszámozási, tördelési) módosítások, de vannak köztük kisebb változtatások is,

amelyek tartalmi szempontból nem elhanyagolhatóak. Ilyen tartalmi változások a következők:

A 6. Tervezés c. fejezetben két érdemi változtatás történt.

- A 6.2 Célok és elérésük megtervezése c. alfejezetbe d) alpontként megjelent a „figyelemmel kísérés" követelménye is, ezzel támogatva a célok elérésének hatékonyságát.
- Az újonnan megjelenő 6.3 Változások megtervezése c. alfejezet a változtatások tervezésének követelményét fogalmazza meg. Ez garantálja, hogy az információbiztonsági rendszeren végrehajtott változtatás tervezett és módszeres tevékenység legyen.

A 7. Erőforrások c. fejezetben csak a 7.4 Kommunikáció c. alfejezetben történt változás. A frissített d) pont alapján a szervezetnek meg kell határoznia, hogyan kommunikál a belső és külső kommunikáció tekintetében. Kikerült viszont a szabványból két másik kommunikációs követelmény, így már nem kell kötelezően meghatározni sem azt, hogy kinek kell kommunikálnia, sem azt, hogy melyek a kommunikációt megvalósító folyamatok.

A 8. Működés c. fejezetben is csak a 8.1 Működéstervezés és –felügyelet c. alfejezet változott. Azoknál a folyamatoknál, amelyek a követelmények teljesítését vagy kockázatokkal és lehetőségekkel kapcsolatos tevékenységek elvégzését szolgálják, meg kell határozni a kritériumokat ezekre a folyamatokra, és meg kell valósítani a folyamatok felügyeletét a kritériumokkal összhangban.

A 9. Teljesítményértékelés c. fejezetben az átstrukturáláson kívül (igazodva ezzel például a ISO 9001-es szabványhoz) csak a vezetőségi átvizsgálás bemenetei követelménynél történt érdemi módosítás. Itt új követelménypontként jelenik meg az információbiztonsági irányítási rendszer szempontjából releváns érdekelt felek igényeiben és elvárásaiban bekövetkezett változások figyelembevétele.

A 10. Fejlesztés c. fejezet érdekessége, hogy felcserélésre került a két alfejezet, így a 10.1. alfejezet tartalmazza a folyamatos fejlesztés és 10.2. alfejezet pedig a nemmegfelelőségek és helyesbítő tevékenységek követelményeit. Utóbbiban némi nyelvi pontosítás is történt, így a tevékenység bizonyítékairól a dokumentált információnak rendelkezésre kell állnia („shall be available"), a korábbi dokumentált információt kell fenntartani („shall retain") megfogalmazás helyett.

A szabványtörzs változtatása tehát nem jelentős, de érdemes odafigyelni az új megfogalmazásokra és a beszúrt új követelmények megfelelő megvalósítására, kiemelten a Tervezésnél a célok figyelemmel kisérésére, a Működés tervezésnél a folyamatok kritériumainak meghatározására és ezek figyelembevételével történő ellenőrzésére, illetve a vezetőségi átvizsgálás bemeneteinek változására.

C) Az információbiztonsági kontrollok jelentősebb újdonságai

A 27001-es és 27002-es szabványok leírt szoros kapcsolatából adódóan már a ISO/IEC 27002:2022 szabvány 2022. februári megjelenésekor lehetett tudni, hogy az ISO/IEC 27001:2022 szabvány A mellékletében, – vagyis az információbiztonsági intézkedésekben – jelentős strukturá-

lis és tartalmi változások várhatóak. Érdekesség, hogy míg a régi A melléklet főfejezetei tartalmazták az adott tématerület célkitűzését, az új verzióban már csak az intézkedések jelennek meg, ezzel az értelmezés és kiépítés szempontjából nagyobb szerepet szánva az ISO/IEC 27002-es szabványnak.

Az 'A melléklet' változásait átvizsgálva elsőre szembetűnő, hogy az intézkedések számossága 114-ről 93-ra csökkent és ezek is már az újfajta követelmény-rendszerezési szemléletnek megfelelően, közvetlenül 4 fő tématerület köré csoportosulnak (az előző 14-gyel szemben):

- szervezeti intézkedések (Organizational) 37 db intézkedéssel;
- humán erőforrásokkal kapcsolatos intézkedések (People) 8 db intézkedéssel;
- fizikai védelemmel kapcsolatos intézkedések (Physical) 14 db intézkedéssel;
- technológiai intézkedések (Technological) 34 db intézkedéssel.

Az új ISO/IEC 27001 szabvány információbiztonsági kontrolljainak számosságából (93 db) könnyű azt a téves következtetést levonni, hogy az új szabványverzió lényegesen kevesebb követelményt fogalmaz meg. A valóság az, hogy a 93 intézkedés úgy tartalmaz 11 új követelménypontot, hogy érdemben egy régi követelmény sem került törlésre. A szabványalkotók ezt úgy oldották meg, hogy több követelmény összevonásra került. Ez jellemzően a régi szabvány 3. szintű kontroll pontjait érinti, de vannak eltérő kontrollterületekről származó összevonások is. Szerencsére az új ISO/IEC 27002-es szabvány B mellékletének táblázatai mindkét szabványverzió irányából tartalmazzák a megfeleltetést, így könnyű átlátni a változtatásokat.

A követelmények tekintetében az igazi újdonság természetesen a 11 új információbiztonsági témakör bevezetése, noha a régi, illetve összevont kontrollok is tartalmaznak részben új követelményeket. A teljesen új 11 kontroll közül 3 a szervezeti (adminisztratív biztonsági) intézkedéseket, 1 a fizikai védelemmel kapcsolatos (fizikai biztonsági) intézkedéseket, 7 pedig a technológiai (logikai biztonsági) intézkedéseket erősíti. Ezek a következők:

#	Kontroll neve	Terület
5.7	Fenyegetettségi információk (Threat intelligence)	szervezeti
5.23	Információbiztonság a felhőszolgáltatások használatakor (Information security for use of cloud services)	szervezeti
5.30	IKT felkészültség az üzletmenet folytonosságához (ICT readiness for business continuity)	szervezeti
7.4	Fizikai biztonság felügyelete (Physical security monitoring)	fizikai
8.9	Konfigurációkezelés (Configuration management)	technológiai
8.10	Információk törlése (Information deletion)	technológiai
8.11	Adatmaszkolás (Data masking)	technológiai
8.12	Az adatszivárgás megelőzése (Data leakage prevention)	technológiai
8.16	Monitoring tevékenységek (Monitoring activities)	technológiai
8.23	Webszűrés (Web filtering)	technológiai
8.28	Biztonságos fejlesztés (Secure coding)	technológiai

Az ISO/IEC 27002:2022 számos meglévő kontrollt egészít ki további részletekkel, illetve szempontokkal. A jelen publikáció terjedelmi korlátai miatt azonban itt csak a teljesen új intézkedéseknek a célját és használatukra vonatkozó néhány fontosabb gondolatot mutatunk be:

5.7 Fenyegetettségi információk (Threat intelligence)

Az adminisztratív intézkedés célja a szervezet fenyegetettségi környezetének feltárása és tudatosítása, hogy a megfelelő védekezési intézkedéseket lehessen megvalósítani. Ez 3 szinten értelmezendő:

- Stratégiai szint: A lehetséges támadók és támadástípusok azonosítása.
- Taktikai szint: Információk gyűjtése a támadók módszertanáról, eszközeiről és technológiáiról.
- Operatív szint: Konkrét támadásokkal kapcsolatos részletek, beleértve a technikai jellemzőket is.

A vállalatok a fenyegetésekkel kapcsolatos információkat felhasználhatják a fenyegetések megelőzésére, észlelésére vagy az azokra való reagálásra. A vállalatok előállíthatnak maguk is fenyegetettségi információkat, de jellemzőbb, hogy ezeket más forrásokból kapják meg és használják fel. Ilyen más források lehetnek például független szolgáltatók vagy tanácsadók, kormányzati ügynökségek vagy együttműködő, fenyegetésekkel foglalkozó szakmai szervezetek vagy csoportok.

5.23 Információbiztonság a felhőszolgáltatások használatakor (Information security for use of cloud services)

Az intézkedés célja a felhőszolgáltatások használatához szükséges információbiztonság meghatározása és felügyelete a szervezet követelményeivel összhangban. Ez a teljes életciklusra vonatkozik, így a felhőszolgáltatások beszerzésére, használatára, menedzselésére és elhagyására vonatkozó folyamatokra is meg kell határozni valamennyi releváns információbiztonsági követelményt. Ebben fontos szerep jut a felhőszolgáltatást nyújtó és azt igénybe vevő szervezetek közötti megállapodásban a szerepek és felelősségek meghatározásának, az incidensek kezelésének, valamint a kockázatok és a működés folyamatos nyomon követésének.

A felhőszolgáltatási megállapodások gyakran a szolgáltató Általános Szolgáltatási Feltételek dokumentumán keresztül előre meghatározottak, és nem képezik tárgyalás alapját. A felhőszolgáltatást igénybe vevő szervezetnek minden esetben felül kell vizsgálnia ezeket a felhőszolgáltatási megállapodásokat a saját információbiztonsági követelményei szempontjából, és a felhőszolgáltatás használatával kapcsolatos megfelelő kockázatértékelést is előre el kell végeznie.

A terület összetettségét a megvalósítást segítő, kapcsolódó témájú szabványok (ISO/IEC 17788, ISO/IEC 17789, ISO/IEC 22123-1, ISO/IEC 19941, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27036-4, ISO/IEC 19086, ISO/IEC 19086-4) számossága is jelzi.

5.30 IKT felkészültség az üzletmenet folytonosságához (ICT readiness for business continuity)

Az intézkedés célja a szervezet által birtokolt információk és egyéb kapcsolódó eszközök rendelkezésre állásának biztosítása az esetlegesen fellépő zavarok ideje alatt is.

Először is a szervezetnek meg kell határoznia az üzletmenet-folytonossági célkitű-

zéseit és követelményeit. Ehhez illeszkedve kell az információs és kommunikációs technológiával (IKT) összefüggő területeinek felkészültségét megtervezni, megvalósítani, fenntartani és tesztelni. Az IKT folyamatosságának kezelése tehát a rendelkezésre állásra vonatkozó üzletmenet-folytonossági követelmények kulcsfontosságú részét képezi.

Az ISO/IEC 27002:2022 szabvány a konkrét megvalósításhoz referenciaként további szabványhivatkozásokat tartalmaz. Ezek alapul szolgálhatnak az üzletmenet folytonosság kiépítéséhez (ISO 22301 és ISO 22313), illetve az üzleti hatáselemzés (BIA) végrehajtásához (ISO/TS 22317).

7.4 Fizikai biztonság felügyelete (Physical security monitoring)

Az intézkedés célja az illetéktelen fizikai hozzáférés észlelése és megakadályozása, a védendő területek és helyiségek folyamatos ellenőrzésével. Ez – többek közt – magába foglalja a kritikus rendszereknek otthont adó épületekben a kockázatokkal arányos felügyeleti intézkedéseket. Ilyenek például az őrszolgálat, behatolásjelzők, videómegfigyelő rendszerek, érintés- és nyitásérzékelők, hang- és mozgásérzékelők.

Fontos szempont az ezeket irányító központi vezérlők és az érzékelők manipulációvédelme és a rendszerek kialakításának részleteire vonatkozó információk bizalmas kezelése, megnehezítve ezzel a védelem megkerülését vagy kiiktatását.

A kialakításnál és működtetésnél nem szabad megfeledkezni a törvényi és jogszabályi környezet szabta korlátokról és előírásokról, különös tekintettel a megfigyelésre és a megőrzési időkre.

8.9 Konfigurációkezelés (Configuration management)

Az intézkedés célja annak biztosítása, hogy a használt hardverek, szoftverek, szolgáltatások és hálózatok folyamatosan a megkövetelt biztonsági szintnek megfelelően működjenek. Ezt nem csak a megfelelő biztonsági beállításokat jelenti, hanem a konfigurációk jogosulatlan vagy helytelen módosításának elkerülését is. Ezért fontos ezeket előzetesen meghatározni, megfelelően dokumentálni és alkalmazni, gondoskodva a felügyeletről és a rendszeres felülvizsgálatról. A konfigurációk módosításának a változáskezelési folyamatot kell követnie.

Mindehhez folyamatokat és eszközöket kell meghatározni és bevezetni a hardver, a szoftver, a szolgáltatások (pl. felhőszolgáltatások) és a hálózatok meghatározott konfigurációinak (beleértve a biztonsági konfigurációkat is) érvényesítésére, mind az újonnan telepített rendszerek, mind az üzemeltetett rendszerek esetében azok élettartama alatt. A kialakított konfigurációkezelési folyamatokon belül szerepköröket, felelősségi köröket és eljárásokat szükséges kialakítani a konfigurációs változások megfelelő ellenőrzésének biztosítására.

8.10 Információk törlése (Information deletion)

Az intézkedés célja, hogy megelőzzük az érzékeny adatok nem kívánt hozzáférhetőségét / nyilvánosságra hozatalát, valamint hogy biztosítsuk az információk törlésére vonatkozó törvényi, jogszabályi, szabályozási és szerződéses követelményeknek való megfelelést. Ennek megvalósítását segíti az említett követelményekkel összhangban kialakított tárolási idők szükséges minimumra történő korlátozása. Kiemelten fontos szempont a megfelelő törlési módszerek alkalmazása, figyelve a másolatok

és ideiglenes fájlok törlésére is. Javasolt odafigyelni a különböző (központi és végponti) eszközökön tárolt adatok törlésére is, figyelembe véve az adott eszközök által biztosított technikai lehetőségeket.

A felhasználói adatok felhőszolgáltatásokban történő törlésével kapcsolatos információk az ISO/IEC 27017 szabványban találhatók. A személyes adatok biztonságos adattörléséhez és az ártalmatlanítás megvalósításához további támpontot biztosít az ISO/IEC 27555 szabvány.

8.11 Adatmaszkolás (Data masking)

Az intézkedés célja az érzékeny adatok, köztük a személyes adatok kitettségének csökkentése, valamint a törvényi, jogszabályi, szabályozási és szerződéses követelményeknek való megfelelés biztosítása. Ezt a hozzáférés-ellenőrzésre vonatkozó irányelvekkel és az üzleti követelményekkel összhangban kell megvalósítani, figyelembe véve az alkalmazandó törvényi és jogszabályi környezetet.

A konkrét megvalósításhoz alkalmazhatóak az ismert technikák és technológiák (pl. titkosítás, hashelés, maszkolás, álnevesítés, anonimizálás, többkörös adat-felülírás), valamint az adatelérések jogosultsághoz vagy tevékenységhez kötött korlátozása. A megfelelő megvalósítási technológia kiválasztásakor figyelembe kell venni az eltakarandó (védendő) adat illetéktelenek általi megismerésének kockázatát, valamint azt a tényt is, hogy az adatkezelés során azt az adatot szükséges-e visszaállítani tudni vagy sem.

Figyelmet érdemel a felhőhasználatból és a személyes adatok más információkkal történő összekapcsolásából eredő kockázatok kezelése, amelyhez további segítséget nyújtanak a hivatkozott ISO szabványok (ISO/IEC 27018, ISO/IEC 20889).

8.12 Az adatszivárgás megelőzése (Data leakage prevention)

Az intézkedés célja annak felderítése és megakadályozása, hogy személyeken vagy rendszereken keresztül adatszivárgás történjen. Ezeket az intézkedéseket alkalmazni kell az érzékeny információkat feldolgozó, tároló vagy továbbító rendszerekre, hálózatokra és egyéb eszközökre. A megvalósítás alappillére az információk megfelelő azonosítása és biztonsági osztályba sorolása, a kapcsolódó védelmi szint meghatározásával. Kiemelt jelentőségű az adatáramlási csatornák felügyelete (pl. e-mail, adathordozók, stb.), a jogosulatlan hozzáférések azonosítása, észlelése és blokkolása.

Az adatszivárgás megelőzése érdekében külön ajánlott figyelembe venni mindegyik adattároló és adatkezelő eszközön tárolt adatok védelmét, valamint a kommunikációs csatornákon továbbított adatok biztonságát is. A különböző adattároló eszközök és kommunikációs csatornák gyengeségei, kockázatai eltérőek, és mindegyik esetben az adott helyzetnek megfelelő kockázatarányos megoldást kell választani. Itt külön érdemes odafigyelni az informatikai megoldásokon túlmenően az analóg eszközök kockázataira, illetve a humán kockázatokra is.

8.16 Monitoring tevékenységek (Monitoring activities)

Az intézkedés célja a rendellenes működés és a potenciális információbiztonsági incidensek felderítése a hálózatok, rendszerek és alkalmazások monitorozásával. Ezen

felül fontos szempont a megfelelő intézkedések kialakítása a lehetséges információbiztonsági incidensek kiértékelésének érdekében. Ehhez legelőször a (törvényi, jogszabályi, szabályozási és szerződéses) követelmények előzetes meghatározása szükséges, és a normális működéssel összefüggő, valamint az ettől eltérő (pl. hozzáférésre, performanciára, viselkedésre, eseményekre vonatkozó) küszöbértékek definiálása. Az automatizált monitoring szoftvereket úgy kell konfigurálni, hogy előre meghatározott küszöbértékek alapján riasztásokat generáljanak. A riasztásokra való reagálásra ki kell alakítani a megfelelő folyamatokat.

A monitoring tevékenységeket célszerű kiterjeszteni az informatikai infrastruktúra üzemeltetési paramétereinek monitoringján túlmenően a biztonsági kérdések monitoringjára is, amelyek az információbiztonsági események és incidensek előrejelzésében, esetleges elkerülésében és a gyors reagálásban jelenthetnek nagy segítséget.

A későbbi visszakövethetőség és bizonyíthatóság érdekében a monitoring feljegyzéseket meghatározott megőrzési időig meg kell őrizni.

8.23 Webszűrés (Web filtering)

Az intézkedés célja a külső webhelyek hozzáférésfelügyeletén keresztül, a rendszerek megfelelő védelmének kialakítása a kártékony szoftverek károkozásával szemben (pl. vírus, adathalászat), valamint a nem engedélyezett webes erőforrásokhoz (pl. illegális tartalom) történő hozzáférés megakadályozása. Ez a megfelelő technikák és technológiák alkalmazásával érhető el. Ilyenek például az IP címek vagy domainek blokkolása, tartalomszűrés, weboldalak elérésére (munkához) fehér listák és tiltására fekete listák kialakítása. Szintén kiemelkedő jelentőségű a felhasználók tudatosítása a biztonságos és megfelelő webhasználatáról.

8.28 Biztonságos fejlesztés (Secure coding)

Az intézkedés célja annak a garantálása, hogy a fejlesztett szoftvereket a biztonságos fejlesztés elveit alkalmazva megfelelően írják meg, ezáltal csökkentve a szoftverben rejlő potenciális információbiztonsági sebezhetőségek számát. A kialakítás fontos sarokköve a szervezeti szintű folyamatok kialakítása a szoftverfejlesztésre, meghatározva a minimális követelményeket (pl. open-source, third-party komponensek használata). Emellett fontos a naprakész információk biztosítása és elemzése a fenyegetések, sebezhetőségek tekintetében. Mivel a szoftverfejlesztés önálló és komplex terület, érdemes az ISO/IEC 27002:2022 szabvány a teljes szoftverfejlesztés életciklust lefedő (tervezés, kódolás, tesztelés, felülvizsgálat, karbantartás) javaslatait megfontolni. További segítséget kínál még a területhez az ISO/IEC 15408 szabványsorozat is, ami a szoftvertermékek IT-biztonság értékelési kritériumainak meghatározásával foglalkozik.

D) Az attribútumok jelentősége

Az újdonságok tekintetében az ISO/IEC 27002:2022 szabvány további érdekessége az attribútumok bevezetése.

De mik is azok az attribútumok?

A szabvány minden intézkedéshez (táblázatos formában) hozzárendel különböző kategóriákba sorolt attribútumokat (címkéket), amelyeket a kereshetőség érdekében "#" előtaggal jelöltek. Ezek segítségével kategorizálhatóak az intézkedések, le-

hetővé téve különböző nézetek kialakítását, azaz egyfajta holisztikus megközelítés alkalmazását. Először érdemes megvizsgálni ezeket a kategóriákat:

- Az intézkedés típusa (Control types): A „PreDeCo" elvnek megfelelő (#Preventive, #Detective, #Corrective) csoportosítást tesz lehetővé, ezzel jelezve, hogy az intézkedés milyen típus(ok)ba (megelőző, felderítő vagy javító) sorolható. Általánosan elfogadott az a nézet, hogy az információbiztonsági kontrollok kialakítása során meg kell tartani az egészséges egyensúlyt a megelőző, a felderítő és a javító intézkedések arányában.
- Az információbiztonsági tulajdonság (Information security properties): Ez a szempont a CIA elvnek (#Confidentiality, #Integrity, #Availability) megfelelő csoportosítást segíti, rámutatva arra, hogy az adott intézkedés az adat mely védendő információbiztonsági tulajdonságának (bizalmasság, integritás, rendelkezésre állás) védelmére irányul.
- A kibervédelmi koncepció (Cybersecurity concepts): Ez a csoportosítás az ISO/IEC TS 27110:2021 Cybersecurity framework-ben meghatározott 5 lépéséhez (#Identify, #Protect, #Detect, #Respond, #Recover) illeszti az adott intézkedést, meghatározva, hogy az adott intézkedés a kibervédelem melyik szakaszában (azonosítás, védelem, felderítés, reagálás, helyreállítás) alkalmazható.
- A működési képességek (Operational capabilities): Ez a kategorizálás a védelem alkalmazójának szemszögéből egyfajta szakértői nézőpont, mintegy alkalmazási terület vagy témakör (#Governance, #Asset_management, #Information_protection, #Human_resource_security, #Physical_security, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Threat_and_vulnerability_management, #Continuity, #Supplier_relationships_security, #Legal_and_compliance, #Information_security_event_management, #Information_security_assurance) szerint csoportosítja az intézkedéseket. Ezek a területek a következők: a Vezetés, Vagyonkezelés, Információvédelem, Emberi erőforrás biztonság, Fizikai biztonság, Rendszer- és hálózatbiztonság, Alkalmazásbiztonság, Biztonságos konfiguráció, Identitás- és hozzáférés-kezelés, Fenyegetések és sebezhetőségek kezelése, Folyamatosság, Beszállítói kapcsolatok biztonsága, Jogi és jogszabályi megfelelőség, Információbiztonsági események kezelése és az Információbiztonság biztosítása.
- Biztonsági területek (Security domains): Ez a szakterületi megközelítés a biztonsági intézkedés hatásának jellege (#Governance_and_Ecosystem, #Protection, #Defence, #Resilience) szerinti csoportosítást tesz lehetővé. Ezek a kategóriák a következők: Vezetés és környezet (ökoszisztéma), Védelem, Védekezés, Ellenállóképesség.

Az attribútumok felhasználása sokrétű lehet. Alkalmasak az intézkedések szűrésére, csoportosítására és rendezésére. Az ISO/IEC 27002:2022-es szabvány 'A melléklete' maga is ajánlja a vállalatoknak saját attribútumokat létrehozását, hogy jobban átláthassák a kialakított intézkedési

struktúráikat. A könnyebb megértésért még egy példát is bemutat a kockázatkezelési terv támogatására, a negatív eseményeket, mint attribútumokat használva. Ezen felül további attribútumok definiálásához kapunk további ötleteket (pl. érettségi szint, megvalósítási állapot, prioritás, érintett szervezeti területek, érintett eszközök, stb.)

3. Mit jelent az átállás az új szabvány követelményeinek való megfelelésre?

Az ISO/IEC 27001:2022 szabvány kiadási dátuma: 2022. október 25. Ennek a szabványnak a magyar fordítása várhatóan 2023 év folyamán jelenik meg, MSZ ISO/IEC 27001:2023 jelzettel.

Az újonnan kiadott szabvány bevezetésének, és persze vele együtt a régi verziójú szabvány kivezetésének menetrendjét egységesen az akkreditáló hatóságok előírják. A tanúsító szervezetek számára a központi irányelvet a Nemzetközi Akkreditációs Fórum (IAF – International Accreditation Forum) az IAF MD 26:2022 Transition Requirements for ISO/IEC 27001:2022 (Az ISO/IEC 27001:2022-re vonatkozó átállási követelmények) című dokumentumában [3] tette közzé. Ennek Magyarországon érvényes előírásait a NAH (Nemzeti Akkreditálási Hatóság) Áttérési Ütemterv az IAF MD 26:2022 c. dokumentuma [4] tartalmazza.

Ezek alapján a tanúsító testületek által tanúsított szervezetek átállásának határideje: 2025. október 31., azaz ezután már ISO/IEC 27001:2013 (MSZ ISO/IEC 27001:2014) szerinti tanúsítások nem lehetnek érvényben.

Ennek részletei az akkreditáló szervezetek (Magyarországon a NAH) vonatkozásában:

- Az ISO/IEC 27001:2022 szerinti NAH általi akkreditációra a NAH felkészülésének határideje: 2023. április 30.
- A tanúsító testületek ISO/IEC 27001:2022 szerinti tanúsításra történő átállások NAH általi ellenőrzésének határideje: 2023. október 31. Ezután a NAH már csak ISO/IEC 27001:2022 szerint végez akkreditálási eljárást.

Ennek részletei az akkreditált tanúsító testületek és az akkreditáltan tanúsított szervezetek vonatkozásában:

- 2023. október 31. után kezdeti (azaz első) tanúsító audit már csak az ISO/IEC 27001:2022 szerint folytatható le.
- Az akkreditált tanúsító testületek általi tanúsítások ISO/IEC 27001:2022-re történő átállításának befejezési határideje: 2025. október 31. (Az ISO/IEC 27001:2013 szabványon alapuló valamennyi tanúsítás az ezután az időpont után hatályát veszti vagy visszavonásra kerül.)

Az ISO/IEC 27001:2013 (MSZ ISO/IEC 27001:2014) szerint tanúsított szervezeteknek az átállásra, az új szabvány szerinti átállást igazoló auditra előzetesen alaposan fel kell készülniük, ami legalább a következő lépéseket foglalja magába:

- az ISO/IEC 27001:2022 (vagy MSZ ISO/IEC 27001:2023, ha már megjelent) szabvány beszerzése, megismerése, valamint ajánlott még az ISO/IEC 27002:2022 szabvány beszerzése és megismerése is, hiszen ez segít az ISO/IEC 27001:2022 szabvány 'A melléklete' kontrolljainak értelmezésében;
- a saját információbiztonsági irányítási rendszer felmérése (pl. belső audit formában), ahol az auditkövetelmények már az új, az ISO/IEC 27001:2022 szabvány kö-

vetelményei alapján kerültek meghatározásra, és a felmérés alapján a hiányok meghatározása;
- az információbiztonsági kockázatfelmérés aktualizálása, kiemelt hangsúllyal az új/módosult követelmények és a felmérés során feltárt hiányok tekintetében;
- intézkedési terv meghatározása és végrehajtása a felmérés feltárt hiányosságai, illetve a kockázatfelmérés eredményei alapján;
- a végrehajtott intézkedéseknek megfelelően a dokumentált szabályozások aktualizálása, és az Alkalmazhatósági nyilatkozat módosítása (illeszkedve az ISO/IEC 27001:2022 követelményekhez, és megfelelve a bevezetett új információbiztonsági intézkedéseknek és kontrolloknak);
- az információbiztonsági irányítási rendszer bevezetett módosításainak képzése a szervezet érintett állománya részére;
- megfelelő idejű működés után a már az új verziójú szabvány szerint működő információbiztonsági irányítási rendszer működésének felülvizsgálata belső audittal, majd ajánlott egy vezetőségi felülvizsgálat keretében az átállás sikerességét értékelni, és meghatározni az elkövetkező időszakra vonatkozó további információbiztonsági célkitűzéseket és feladatokat;
- felkészülés a tanúsító általi következő auditra, amelyen már az új szabvány szerinti tanúsításra való átállás történik meg.

Ez az új információbiztonsági szabványverzióra való átállási forgatókönyv gyakorlatilag megfelel az eddig is ismert, bármely irányítási rendszer szabványváltozásakor alkalmazott forgatókönyvnek. Ennek végrehajtása azonban az egyes szervezetek számára különböző nehézséget, kihívást jelent majd. Lesznek vállalatok, amelyek működése már eddig is nagy többségében megfelelt az új információbiztonsági rendszerszabvány követelményeinek, számukra várhatóan könnyen megy majd az átállás. Azonban vannak olyan vállalatok is, amelyeknél az információbiztonsági irányítási rendszer csak részben vagy teljes egészében formálisan működött. Az átállás az ő esetükben sokkal nagyobb kihívást jelent, különösen ha az új követelmények érdemi működését is kell tudni bizonyítani.

Az átállás és az új követelményeknek való megfelelés nehézségének mértéke több tényezőtől is függ. Ilyenek például:

- a szervezet mérete és működésének összetettsége;
- a meglévő biztonsági kontrollok egyszerű és áttekinthető vagy bonyolult működése;
- a szabályozó dokumentációk struktúrájának szabványalapú vagy működés-alapú leképezése;
- a meglévő információbiztonsági irányítási rendszer csak formális vagy érdemi, testreszabott működése;
- az információbiztonságért felelősök, illetve annak működésében résztvevő kollégák tapasztalata;
- a (régi és új) információbiztonsági szabványkövetelmények ismerete, tapasztalat azok értelmezésében;

Összefoglalás

A 2022. október 25-én megjelent ISO/IEC 27001:2022 információbiztonsági irányítási rendszer követelményeit tartalmazó rendszerszabvány jelentős változáson ment keresztül, és az elmúlt évtized változásaihoz és fejlődéséhez igazítva egy aktuális és hatékony információvédelmi szabvánnyá vált. Ezek a követelmények egy rendszerbe foglalták a fontosabb je-

lenlegi információbiztonsági, kibervédelmi, személyes adatvédelmi és egyéb kapcsolódó jogszabályi előírásokat és irányelveket, megfelelve a szakma által kialakult jó gyakorlatoknak.

Jelen publikációban ennek a szabványnak néhány kiemelt, fontos aspektusát és az új szabvány alkalmazására való áttéréshez szükséges út lépéseit mutattuk be.

Látható, hogy az ISO/IEC 27001:2022 szabvány legnagyobb változásának, az 'A mellékletben' megújult információbiztonsági kontrollok-nak a magyarázata és értelmezése az ISO/IEC 27002:2022 szabványban található. Miután a szabványkövetelmények teljesítése érdekében azok sokrétűsége miatt szükséges a kontrollok címén és egymondatos összefoglalásán túlmenően azok célját, tartalmát és értelmezését is megismerni, ezért nagyon ajánlott minden vállalatnak az ISO/IEC 27002:2022 szabvány megismerése és használata is.

Felhasznált források

[1] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements; Third Edition, ISO/IEC 2022

[2] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls; Third Edition, ISO/IEC 2022

[3] IAF MD 26:2022 IAF Mandatory Document: Transition Requirements for ISO/IEC 27001:2022, Issue 1.; International Accreditation Forum, Inc. 2022

[4] Áttérési Ütemterv az IAF MD 26:2022, Issue 1.; 1. kiadás, Nemzeti Akkreditálási Rendszer 2022.11.30; https://nah.gov.hu/admin/staticmedia/Oldalakhoz_csatolt_dokumentumok/%C3%81tt%C3%A9r%C3%A9si%20%C3%BCtemterv/IAF_MD_26-2022_ISO_27001_2022-atteresi_utemterv_a.pdf (letöltés: 2023.01.06.)

Dr. Horváth Zsolt az INFOBIZ Informatikai, Információbiztonsági és Vezetési Tanácsadó Kft. tulajdonosa és ügyvezetője 2006 óta. EOQ MNB által regisztrált minőségirányítási és információbiztonsági rendszermenedzser és auditor. Tíz évig látta el a SIEMENS magyarországi szoftverházának, a SIEMENS PSE Kft-nek a minőségirányítási igazgatói feladatait. Több, mint húsz éve dolgozik a minőségirányítás és az információbiztonsági irányítás területén, több akkreditált tanúsító szervezet vezető auditoraként, valamint tanácsadóként és szakmai oktatóként. Számos szakmai konferencián elhangzott előadás és megjelent publikáció szerzője és társszerzője.

Horváth István 2006 óta az immunIT Információbiztonsági Tanácsadó Kft. tulajdonosa és ügyvezetője. Az INFOBIZ Kft. tanácsadói csapatának oszlopos tagja. Mérnök-informatikus és adatvédelmi jogi szakember, valamint az EOQ MNB által regisztrált információbiztonsági rendszermenedzser és auditor. Komoly szerepet töltött be az első magyarországi digitális cafeteria kártya és elszámoló rendszer tervezésében, fejlesztésében és üzemeltetésében. Több, mint tizenöt éve foglalkozik az informatika különböző területével és tanácsadóként, oktatóként és auditorként vesz részt irányítási rendszerek kiépítésében. Több akkreditált tanúsító szervezetnél számos irányítási rendszer vezető auditora.