HORVÁTH ZSOLT, ügyvezető igazgató, INFOBIZ Kft., Budapest

Az információbiztonsági követelmények változása a megújult ISO/IEC 27002 szabvány alapján

Az információbiztonsági irányítási rendszer követelményeit meghatározó szabványpár, az ISO/IEC 27001 és ISO/IEC 27002 megújultak, és 2022-ben jelent meg az új kiadásuk. Az ISO/IEC 27001 szabványtörzsében lévő követelmények kisebb mértékben, míg az információbiztonsági kontrollok követelményeit tartalmazó 'A melléklet' jelentős mértékben változott. Az ISO/IEC 27001 'A mellékletében' szereplő kontrollok értelmezését és a kapcsolódó alkalmazási útmutatót az ISO/IEC 27002 tartalmazza, amely így lényegesen megváltozott.

Publikációm célja áttekinteni a fenti szabványok információbiztonsági kontrolljaiban bekövetkezett újdonságokat, elsősorban az ISO/IEC 27002:2022 szabvány fontosabb változásaira fókuszálva.

1. Bevezetés

Az International Organization for Standardization (ISO) az International Electrotechnical Commission (IEC) szervezettel közösen az információbiztonság témakörében számos szabványt adott ki, legtöbbjük az ISO/IEC 270xx szabványcsoportba tartozik. Ezek központi alapszabványa az ISO/IEC 27001, ami az információbiztonsági irányítási rendszer követelményeit tartalmazza. Az ISO/IEC 27001 [1] legújabb kiadása 2022. októberében jelent meg, követelményeinek struktúrája két részből áll: a szabványtörzsből és az 'A mellékletben' található információbiztonsági kontrollok felsorolásából. A kontrollok értelmezését és a kapcsolódó alkalmazási útmutatót az ISO/IEC 27002 szabvány [2] tartalmazza, legutolsó (és frissített) kiadása 2022 márciusában jelent meg. Az ISO/IEC 27001 és ISO/IEC 27002 szabványok mindig párban jelennek meg és kiegészítik egymást.

A megelőző, 2013. évi kiadáshoz képest számos változás történt, amelyekre szükség is volt, hiszen az elmúlt évtizedben mind az információs technológia, mind a felhőszolgáltatások elterjedése, mind a munkavégzési módok és kultúrák nagy mértékben fejlődtek. A kibertér használata sokkal dominánsabb lett, és ezen keresztül a kiberbűnözés is egyre komolyabb és nagyobb fenyegetést jelent a vállalatok számára. Erre választ adva jelent meg az információvédelem során alkalmazott kontrollok bővítése és értelmezésük kiterjesztése, hogy az új kockázatok kezelésére is alkalmassá váljanak.

Az ISO/IEC 27001 szabványtörzse továbbra 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 való pontosabb illeszkedés érdekében – követve az előző verzió óta megjelent irányítási rendszerszabványokat – csak kisebb módosítások történtek. Azonban az 'A mellékletben' található információbiztonsági kontrollok struktúrájában és tartalmában jelentősek a változások. Az ebben felsorolt információbiztonsági kontrollok magyarázata megtalálható az ISO/IEC 27002 szabványtörzsében, ugyanabban a számozási struktúrában, ahogy azt az ISO/IEC 27001 'A melléklete' tartalmazza. Ebből látszik az is, hogy az ISO/IEC 27002 szabvány lényeges átalakuláson ment keresztül: megváltozott a kontrollok strukturálása, száma, belső tartalmi felépítése, és a tartalma is jelentős részben. Miután az ISO/IEC 27001:2022 szabvány 'A mellékletének' változásai tartalmukban az ISO/IEC 27002:2022 szabványon, az abban lévő magyarázatokon keresztül érthetők, ezért a publikációmban annak a változásairól adok egy áttekintést.

2. Az ISO/IEC 27002:2022-ben a követelmények strukturálásának változása

Az információbiztonságot megvalósító szabályozásokat önálló biztonsági szabályok és operatív működésbe beépített biztonsági szempontok alkotják. Az azonos témakörön belül a szűkebb biztonsági célokat megvalósító intézkedéseket nevezzük átfogóan információbiztonsági kontrolloknak, és a szabvány ezekre csak, mint 'kontroll' hivatkozik.

Az ISO/IEC 27002:2022 a következőképp definiálja a kontrollt: „A kontroll a kockázatok fenntartására és/vagy módosítására irányuló gyakorlat. A kontrollok többek közt magukban foglalnak bármely olyan folyamatot, vezérlőelvet, eszközt, gyakorlatot vagy egyéb körülményeket és/vagy tevékenységeket, amelyek fenntartják és/vagy módosítják a kockázatot. A kontrollok azonban nem mindig érik el a kívánt vagy feltételezett mértékű módosító hatást." (Az ISO/IEC 27002:2022, 3.1.8. pontja szerint.)

A szabványban az egyes kontrollok mérete és tartalma is eltérő lehet. Vannak olyan kontrollok, amelyek önmagukban is egy nagyobb témakört fognak át, és azon belül számos önálló szabályozást tartalmazhatnak. (Például ilyenek a „Távmunka, a „Hálózatok biztonsága", a „Hálózati szolgáltatások biztonsága" vagy a „Kriptográfia használata".) Ugyanakkor vannak olyan kontrollok is, amelyek egy folyamatnak csak egy-egy elemét, lépését tartalmazzák, és több kontroll használata ad ki együttesen egy információbiztonsági folyamatot. (Például az információbiztonsági incidens- és eseménykezelés életciklusa egyes lépéseinek megvalósítását külön-külön kontrollok írják le.) Látható, hogy egy-egy kontroll nem igazán egy konkrét intézkedést követel meg, hanem az információbiztonság egy-egy megvalósítandó szempontját, ami lehet egy folyamat része, lehet önálló intézkedés vagy szabály vagy akár ezekből egyszerre több is. A kontroll követelményeinek a megvalósításakor mindig a működési módhoz, a védendő információhoz és vagyonelemekhez, illetve a felmért kockázatokhoz mérten testre szabva kell eljárni.

Az egyes információbiztonsági intézkedések többféle szempont szerint csoportosíthatók, és ezek a csoportosítások az intézkedések célorientált, tudatos kiválasztásában nyújtanak nagy segítséget. A legfontosabb csoportosítási szempontokat a megújult ISO/IEC 27002:2022 a kontrollok szintjén tartalmazza, és ezeket nevezte el az egyes kontrollok attribútumainak. Az attribútumok értelmezését a publikációm 3. fejezete ismerteti.

A megelőző verziójú, az ISO/IEC 27002:2013 szabvány az információbiztonsági kontrollokat 14 fejezetre bontotta, és ez sorszámozásban az 5. fejezettől a 18. fejezetig tartott. Ezek a nagyobb, önálló témaköröket jelentették, amelyen belül az egyes kontrollok alábontása további két szintre tagozódott: A nagyobb, önálló témakörök (első szint) alatt az ahhoz tartozó szabályozási célok (második szint) alkottak egy-egy témakör szűkítését, majd azok alatt a szabályozási kontrollok (harmadik szint) jelentették a további szabályozandó területek további szűkítését. Ilyen módon a szabvány összesen 114 szabályozási kontrollt tartalmazott.

Az új ISO/IEC 27002:2022 szabvány a kontrollok csoportosítását és tartalmát is átalakította. A régi szabvány 114 kontrollja helyett az új szabvány összesen 93 kontrollt tartalmaz. Ez azonban nem jelenti a követelményrendszer csökkentését, mert számos kontroll összevonásra került, valamint meglévő kontrollok tartalmi követelményei is kibővültek, továbbá megjelentek teljesen új kontrollok is.

Az új ISO/IEC 27002:2022 szabványban a kontrollok csoportosítása csak két szintű, azaz a 4 főfejezet (első szint) alatt közvetlenül maguk az ahhoz tartozó kontrollok (második szint) találhatók. A kontrollok csoportosításában az első rendű szempont, ami ebbe a 4 főfejezetbe való besorolást alkotja, az intézkedések végrehajtási jellege. Ezek alapján az intézkedések lehetnek

- szervezeti (vagy más néven adminisztratív) biztonsági kontrollok;
- humán biztonsági kontrollok;
- fizikai biztonsági kontrollok;
- technológiai (vagy más néven logikai) biztonsági kontrollok.

Az ISO/IEC 27002:2022 szabvány 11 új kontrollt vezetett be, amelyek 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-folytonossághoz (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 új ISO/IEC 27002:2022 szabványban a kontrollok leírásának struktúrája egységes:

- A kontroll címe alatt a rá jellemző tulajdonságokat az attribútumok foglalják össze, egységes táblázatos formában. Ezek az attribútumok 5 szempont szerint vannak csoportosítva, amelyek a kontrollok értelmezésében és tudatos használatában segítenek.
- Ezután következik a kontroll tartalmára utaló egymondatos összefoglalás, majd a kontroll céljának szintén egymondatos leírása.
- A kontrollhoz tartozó használati útmutató lényegében a kontroll részletes értelmezését tartalmazza, ami felfogható a kontrollhoz tartozó követelményrendszer leírásának is.
- A kontroll végén „Egyéb információk" alcím alatt legtöbbször további hasznos magyarázatok találhatók, amelyek szintén a megértést segítik. Sok esetben a kontrollok általi követelményrendszer és a már alkalmazott szakmai jó gyakorlatok részletesebb bemutatása más szakmaspecifikus szabványokban is megtalálható. Ilyen estekben ez a fejezet tartalmazza ezeknek a külső szabványoknak az ajánlásként történő meghivatkozását is.

3. Az attribútumok és értelmezésük

Az ISO/IEC 27002:2022 szabvány minden kontrollhoz (táblázatos formában) hozzárendel különböző kategóriákba sorolt attribútumokat (címkéket), amelyeket a kereshetőség érdekében „#" előtaggal jelöltek. Ezek segítségével kategorizálhatóak és csoportosíthatók a kontrollok, lehetővé téve különböző nézetek kialakítását, azaz egyfajta holisztikus megközelítés alkalmazását.

Az attribútumok használata nem kötelező, de sokat segíthet. Az attribútumok felhasználása sokrétű lehet. Alkalmasak a kontrollok szűrésére, csoportosítására és rendezésére.

A szabványban megadott attribútumokat példaként mutatták be. Létrehozhatunk saját attribútumokat is, hogy jobban átlássuk és értékelhessük a kialakított intézkedési struktúránkat. Ennek a megértését segíti még az ISO/IEC 27002:2022-es szabvány 'A melléklete', ami ennek szemléltetésére egy példát is bemutat. Ezen felül további attribútumok definiálásához kapunk ötleteket (pl. érettségi szint, megvalósítási állapot, prioritás, érintett szervezeti területek, érintett eszközök stb.)

A szabványban megadott attribútum-kategóriák a következők:

- **Az intézkedés típusa (Control types)**
  Ez az attribútum-kategória azt mutatja meg, hogy milyen az adott intézkedés jellege a „PreDeCo" elv (#Preventive, #Detective, #Corrective) szempontjából, azaz, hogy az információk biztonsága szempontjából az adott intézkedés egy kockázati esemény (vagy biztonsági esemény vagy incidens) megelőzését, felderítését vagy annak bekövetkezése után a kijavítást teszi lehetővé. Látható az is, hogy noha ez az attribútum a szabványban a kontrollokhoz van hozzárendelve, de miután egy kontrollhoz tartozó terület több konkrét intézkedést is tartal-

mazhat, így igazából ezt az attribútumot magukhoz az intézkedésekhez rendelhetjük hozzá. Általánosan elfogadott az a nézet, hogy az információbiztonsági intézkedések kialakítása során meg kell tartani az egészséges egyensúlyt a megelőző, a felderítő és a javító intézkedések arányában.

- **Információbiztonsági tulajdonságok (Information Security Properties)**
  Ez a szempont az információbiztonság CIA elvének (#Confidentiality, #Integrity, #Availability) megfelelő csoportosítást segíti, rámutatva arra, hogy az adott intézkedés az adat mely védendő információbiztonsági tulajdonságának (bizalmasság, integritás, rendelkezésre állás) védelmére irányul. Ez a szempontrendszer hasznos segítség lehet például azokban az esetekben is, amikor feltárt információbiztonsági kockázatokra kell kockázatkezelési tervet készíteni. Tudatosabban és könnyebben lehet a megfelelő biztonsági intézkedéseket megkeresni, ha tudjuk, hogy a csökkenteni kívánt kockázat a védendő információ melyik információbiztonsági tulajdonságának veszélyeztetésével okozhat kárt. Itt is igaz az az állítás, hogy ezt az attribútumot elsősorban magukhoz a konkrét intézkedésekhez célszerű hozzárendelni.
- **Kibervédelmi koncepciók (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. Hasznos lehet ez a csoportosítás különösen olyan információbiztonsági rendszerek esetén, amelyeknél az informatikai infrastruktúrával szembeni kibervédelmi követelmények kiemelten jelentősek, illetve ahol elvárás a kibervédelem rendszerszintű működtetése is. Ott a 2 rendszer egymáshoz való illesztésében is jelentős segítséget adhat ennek a szempontrendszernek az alkalmazása.
- **Működési képességek (Operational Capabilities)**
  Ez az attribútum-kategória az információbiztonsági kontrollok/intézkedések alkalmazási területének egy csoportosítását adja, és azt mutatja meg, hogy mely kontrollok megvalósítása tartozik ugyanannak a szakmai területnek a szabályozásai közé. Természetesen itt sem egy az egyhez történik a kontrollok besorolása az attribútum kategóriába, hiszen több kontroll is tartozhat ugyanannak a témakörnek a szabályozásához; ugyanakkor egy kontroll szempontjai egyszerre több terület szabályozásához is kapcsolódhatnak. (Megjegyzés: tulajdonképpen ez az attribútum-kategória látja el azt a funkciót, amit a ISO/IEC 27002:2013 szabványban a kontrollok 14 főfejezetbe sorolt első szintű csoportosítása lát el.) Az attribútum-kategória lehetséges értékei a következők: #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. Ezek a területek magyarul a következők: a Vezetés, Vagyonkezelés, Információvédelem, Emberi erőforrás biztonság, Fizikai biztonság, Rendszer- és hálózatbiztonság, Alkalmazásbiztonság, Biztonságos konfiguráció, Identitás- és hozzáférés-kezelés, Fenyegetések és sebezhetőség kezelése, Folyamatosság, Beszállítói kapcsolatok biztonsága, Jog és megfelelőség, Információbiztonsági események kezelése és Információbiztonság biztosítása.
- **Biztonsági területek (Security Domains)**
  Ez az attribútum-kategória a biztonsági intézkedések hatásának jellege (#Governance_and_Ecosystem, #Protection, #Defence, #Resilience) szerinti csoportosítást tesz lehetővé. Ez abban adhat támogatást, hogy megmutatja az alkalmazott kontrollok az irányítás és szabályozás, a védelem vagy a védelmi képességek, vagy a rendszer rugalmassága, illetve ellenálló képessége erősítésén keresztül fejtik ki hatásukat. Ezen attribútumok figyelésével képet nyerhetünk az intézkedések hatásmechanizmusai közötti egyensúlyról is. Ezek a kategóriák magyarul a következők: Vezetés és környezet (ökoszisztéma), Védelem, Védekezés, Ellenálló képesség.

4. A nagyobb szakmai témakörök követelményeinek áttekintése

- A szakmai területek szerinti csoportosítás alapjának az ISO/IEC 27002:2022 szabványban megadott **A működési képességek** (Operational Capabilities) c. attribútum kategóriáit választottam, ezzel is bemutatva a szabványban ennek az attribútumnak a használatát.
- A szabványon belüli hozzárendelésekből látható, hogy egy-egy kategóriához több kontroll is tartozik, ugyanakkor a szabvány több kontrollhoz is ennek az attribútum-kategóriának több elemét is hozzárendelte.
- Az egyes témaköröket nem kívánom teljes részletezettségében bemutatni, csupán áttekintést szeretnék nyújtani a legfontosabb szempontokról és legjelentősebb újdonságokról.

4.1. Vezetés/Irányítás

- Kapcsolódó kontrollok:
  - 5.1. Információbiztonsági irányelvek
  - 5.2. Információbiztonsági szerepek és felelősségi körök
  - 5.3. A feladatok elkülönítése
  - 5.4. A vezetés felelősségei
  - 5.5. Kapcsolat a hatóságokkal
  - 5.6. Kapcsolat a speciális érdekcsoportokkal
  - 5.8. Információbiztonság a projektmenedzsmentben
  - 5.24. Információbiztonsági incidensek kezeléséphez tervezése és előkészítése
- Szabályozandó területek, témakörök:
  - A Vezetés/Irányítás alkalmazási terület teljes egészében az adminisztratív kontrollok közé tartozik, és az információbiztonság szervezeti működtetésének követelményeit fogja össze. Noha az itt bemutatott témák szabályozási kötelezettségei az ISO/IEC 27001:2022 szabvány szabványtörzsében is szerepelnek, mégis érdemes ezeknek a kontrolloknak a leírását is elolvasni, mert további hasznos szempontokat kaphatunk a gyakorlati megvalósításukhoz.
  - Ide tartoznak többek közt az információbiztonsági irányítási rendszer (IBIR) kialakításához, működtetéséhez és fejlesztéséhez szükséges politikák és irányelvek, dokumentált szabályozások (5.1.), valamint azok végrehajtásáért, irányításáért és számonkéréséért szükséges feladatkörök és felelősségek meghatározása (5.2.). Kiemelt elvárás, hogy az egymással összeférhetetlen feladatkörök (pl. jogosultságok igénylése – eldöntése – beállítása, bármilyen feladat végrehajtása és ellenőrzése) különböző független személyekhez legyenek hozzárendelve (5.3.). Külön kontrollok foglalkoznak a vezetőség IBIR-ben betöltött feladatainak meghatározásával (5.4.), és a hatóságok és egyéb külső érdekcsoportokkal való kapcsolat szempontjaival (5.5. és 5.6.).
  - A projektek információbiztonsági követelményei kontroll (5.8.) nem új elem, ennek ellenére az ide tartozó információbiztonsági elvárások érezhetően szigorúbbak lettek. Alapvetően meg kell határozni már a projekt kezdetekor a működése során kezelt adatokat és azok biztonsági besorolását, valamint alkalmazni kell a projekt teljes életciklusa során az adathozzáférések és adatkezelések információbiztonsági kockázatai alapján meghatározott biztonsági intézkedéseket. Ez természetesen a projekt teljes életciklusa során alkalmazott projektkockázat-felmérési és -kezelési folyamatba az információbiztonsági projektkockázatok integrálását is jelenti.
  - Noha az információbiztonsági események és incidensek kezelése egy önálló működési terület, annak ellenére az arra való felkészülés és készültség szabályozásainak kialakítása, megtervezése (5.24.) az adminisztratív kontrollok között is helyet kapott.
  - Ez a szakmai terület nem tartalmaz új kontrollt, ezek a témák már szerepeltek a régi szabvány követelményei között is.

4.2. Vagyonelemek kezelése

- Kapcsolódó kontrollok:
  - 5.9. Az információk és egyéb kapcsolódó eszközök nyilvántartása

- 5.10. Az információk és egyéb kapcsolódó eszközök elfogadható használata
- 5.11. Az eszközök visszaszolgáltatása
- 5.14. Információátadás
- 5.33. A feljegyzések védelme
- 5.37. Dokumentált működési eljárások
- 6.5. Felelősségek a munkaviszony megszűnése vagy megváltozása után
- 6.7. Távmunka
- 7.8. A berendezések elhelyezése és védelme
- 7.9. A telephelyen kívüli eszközök biztonsága
- 7.10. Adathordozók
- 7.13. A berendezések karbantartása
- 7.14. A berendezések biztonságos ártalmatlanítása és újrafelhasználása
- 8.1. Felhasználói végberendezések
- 8.14. Az információfeldolgozó létesítmények redundanciája

- Szabályozandó területek, témakörök:
  - A Vagyonelemek kezelése alkalmazási terület, noha elsősorban adminisztratív kontrollokat tartalmaz, de már megjelennek az adott szabályozást megvalósító operatív intézkedéseket tartalmazó humán, fizikai és logikai kontrollok is.
  - Ennek a témakörnek a célja az információs vagyonelemek biztonságos használata, aminek részei az érintett vagyonelemek nyilvántartása, az azokra vonatkozó biztonsági szabályok meghatározása és dokumentált szabályozása, majd azoknak a betartása és betartatása. Ezek ilyen módon vonatkoznak minden fajta olyan eszköz, berendezés, illetve folyamat kezelésére, amelyek adatokat tárolnak, használnak, illetve feldolgoznak, vagy amelyeken keresztül az adatok biztonsága veszélyeztethető.
  - Fontos szempont, hogy az egyes vagyonelemekre vonatkozó használati, illetve kezelési szabályok és kapcsolódó felelősségek egyértelműek legyenek, valamint a kialakított használati vagy kezelési mód integráltan tartalmazza az adott vagyonelemhez rendelt biztonsági osztálynak megfelelő információbiztonsági intézkedéseket is.
  - Ez a szakmai terület nem tartalmaz új kontrollt, ezek a témák alapvetően már szerepeltek a régi szabvány követelményei között is.

4.3. Információvédelem

- Kapcsolódó kontrollok:
  - 5.10. Az információk és egyéb kapcsolódó eszközök elfogadható használata
  - 5.12. Az információk osztályozása
  - 5.13. Az információk címkézése
  - 5.14. Információátadás
  - 5.33. A feljegyzések védelme
  - 5.34. Adatvédelem és PII (személyes adatok) védelme
  - 5.37. Dokumentált működési eljárások
  - 6.6. Bizalmassági vagy titoktartási megállapodások
  - 6.7. Távmunka
  - 8.1. Felhasználói végberendezések
  - 8.7. Védelem a rosszindulatú szoftverek ellen
  - 8.10. Információk törlése
  - 8.11. Adatmaszkolás
  - 8.12. Az adatszivárgás megelőzése
  - 8.33. Tesztelési információk
  - 8.34. Az információs rendszerek védelme az audittesztelés során
- Szabályozandó területek, témakörök:
  - Az Információvédelem alkalmazási terület az adatvagyon, mint a megvédendő információ védelmére szolgáló szempontokat és az ahhoz kapcsolódó biztonsági intézkedéseket foglalja össze.

- Kiindulási alap a védendő információk és azok védelmi igényének a meghatározása. Ezt a követelményt valósítja meg Az információk osztályozása c. kontroll (5.12.), amely alapján minden szervezetnek az elsődleges kiindulási pont az adatvagyonának a felmérése, és az adatvagyon biztonságának (bizalmassága, integritása és rendelkezésre állása) sérülése vagy elvesztése esetén a lehetséges kár meghatározása. Ezek alapján szükséges az adatvagyont biztonsági osztályba sorolni, majd a biztonsági osztályokhoz meghatározni a szükséges védelmi szintet meghatározó követelményeket.
- Az adatvagyon védelmének követelményei – megfelelve a meghatározott biztonsági szinteknek, – a különböző információs vagyonelemek és felhasználói csoportok vonatkozásában a többi, ehhez a fejezethez tartozó kontrollban jelennek meg. Ezek kiterjednek a szükséges biztonsági intézkedések meghatározására és szabályozására, valamint az azokat megvalósító technikai intézkedésekre is. Elsősorban adminisztratív, humán és logikai biztonsági kontrollokat tartalmaznak.
- Ez a szakmai terület, noha többségében olyan kontrollt tartalmaz, amelyek már szerepeltek a régi szabvány követelményei között, de itt megjelenik néhány teljesen új kontroll is: 8.10. Információk törlése, 8.11. Adatmaszkolás, 8.12. Az adatszivárgás megelőzése. Látható, hogy ezek mind logikai informatikai biztonsági követelmények, és mindegyik kontroll célja az információ bizalmasságának hatékonyabb megvédése.

4.4. Emberi erőforrás-biztonság

- Kapcsolódó kontrollok:
  - 6.1. Átvilágítás
  - 6.2. A foglalkoztatás feltételei
  - 6.3. Információbiztonsági tudatosság, oktatás és képzés
  - 6.4. Fegyelmi eljárás
  - 6.5. Felelősségek a munkaviszony megszűnése vagy megváltozása után
  - 6.6. Bizalmassági vagy titoktartási megállapodások
- Szabályozandó területek, témakörök:
  - Az Emberi erőforrás biztonsága alkalmazási terület kizárólag a humán biztonság területét öleli fel, célja az információbiztonságon belül a humán eredetű kockázatok csökkentése. Noha ebben a csoportban szám szerint relatíve kevesebb kontroll jelenik meg, a jelentősége mégis kiemelkedő. Elég csak arra gondolni, hogy ma is változatlanul reális állítás, hogy az információbiztonság egyik leggyengébb láncszeme a humán tényező.
  - A kontrollok használata kiterjed a munkatársak foglalkoztatásának biztonságára az elejétől a végéig, azaz a munkatárs felvételét megelőző akvizíciós szakasztól az alkalmazáson keresztül egészen a munkaviszony megszűnése során alkalmazandó információbiztonsági intézkedésekig, sőt a titoktartás tekintetében még azt követően is.
  - Ez a szakmai terület nem tartalmaz új kontrollt, ezek a témák már szerepeltek a régi szabvány követelményei között is.

4.5. Fizikai biztonság

- Kapcsolódó kontrollok:
  - 5.37. Dokumentált működési eljárások
  - 6.7. Távmunka
  - 7.1. Fizikai biztonsági peremterületek
  - 7.2. Fizikai belépés
  - 7.3. Irodák, helyiségek és létesítmények biztosítása
  - 7.4. Fizikai biztonsági felügyelet
  - 7.5. Fizikai és környezeti fenyegetések elleni védelem
  - 7.6. A biztonsági területeken való munkavégzés
  - 7.7. Tiszta asztal és tiszta képernyő

- 7.8. A berendezések elhelyezése és védelme
- 7.9. A telephelyen kívüli eszközök biztonsága
- 7.10. Adathordozók
- 7.11. Támogató közművek
- 7.12. A kábelezés biztonsága
- 7.13. A berendezések karbantartása
- 7.14. A berendezések biztonságos ártalmatlanítása és újrafelhasználása

- Szabályozandó területek, témakörök:
  - A Fizikai biztonság alkalmazási terület – hasonlóan a korábbi szabvány fizikai biztonsági fejezetéhez – két nagy területet ölel fel: a fizikai védelem területét, valamint az infrastruktúra üzemeltetésének fizikai biztonsági kérdéseit.
  - A fizikai védelem magában foglalja a munkavégzési területek fizikai határvédelmét, őrzésvédelmi feladatait, a beléptetések szabályozását beleértve a vendégek és egyéb idegenek fogadását és felügyeletét, illetve a különböző 'vis major' helyzetek vagy egyéb környezeti fenyegetések elleni védelmét.
  - Az infrastruktúra üzemeltetésének fizikai biztonsági kérdéseit az infrastruktúra elhelyezése és védelme, a berendezések megbízható és folyamatos fizikai működési feltételeinek biztosítása adja. Ebbe beleértendők többek közt az üzemeltetés fizikai körülményeinek biztosítása, megfelelő áramellátás, klimatizálás, kábelezés, kapcsolódó közművek biztonsága, tűzvédelem, a berendezések karbantartása és biztonságos selejtezése is. A berendezések alatt nemcsak a központi, illetve nagyméretű IKT (infokommunikációs technológiai) berendezések értendők, hanem figyelembe kell venni a mobil eszközöket és adathordozókat, valamint a papíralapú és egyéb hagyományos adathordozókat is.
  - A fizikai biztonság e követelményei – egy kivétellel – alapvetően mind megtalálhatóak a régi szabvány követelményei között, azok néhány részletének pontosításával illetve kiegészítésével kerültek át az új szabványba.
  - A kontrollokból is látszik, hogy az alkalmazási terület domináns részét a szabvány 6. fejezete maga adja, amihez két másik kontrollnak is van kapcsolódó része. Ezek:
    - 5.37. Dokumentált szabályozási eljárások: a fizikai biztonságot is megvalósító követelmények dokumentált szabályozások elkészítése és karbantartása;
    - 6.7. Távmunka: a távmunka (és ez a gyakorlatban legtöbbször a home office jellegű munkavégzést takarja) jellegű munkavégzés biztonságos feltételeinek kialakítása során a fizikai biztonság szempontjai;
  - Egy új követelmény mint új kontroll jelenik meg itt: Ez a 7.4. Fizikai biztonsági felügyelet c. kontroll. Az intézkedés célja az illetéktelen fizikai hozzáférés észlelése és megakadályozása, a védendő területek és helyiségek folyamatos ellenőrzésével. Ez – többek közt – magában foglalja a kritikus rendszereknek otthont adó épületekben a kockázatokkal arányos felügyeleti intézkedéseket. Ilyenek például az őrszolgálat, behatolás jelzők, videó megfigyelő rendszerek, érintés- és nyitásérzékelők, hang- és mozgásérzékelők stb. 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.

4.6. Rendszer- és hálózatbiztonság

- Kapcsolódó kontrollok:
  - 5.37. Dokumentált működési eljárások
  - 6.7. Távmunka
  - 8.7. Védelem a rosszindulatú szoftverek ellen
  - 8.18. A kiváltságos segédprogramok használata
  - 8.20. A hálózatok biztonsága
  - 8.21. A hálózati szolgáltatások biztonsága

- 8.22. A hálózatok elkülönítése
- 8.23. Webszűrés
- 8.25. Biztonságos fejlesztési életciklus
- 8.26. Az alkalmazások biztonsági követelményei
- 8.27. Biztonságos rendszerarchitektúra és műszaki elvek
- 8.28. Biztonságos kódolás
- 8.29. Biztonsági tesztelés a fejlesztés és elfogadás után
- 8.30. Kiszervezett fejlesztés
- 8.31. A fejlesztési, tesztelési és termelési környezetek elkülönítése
- 8.32. Változáskezelés
- 8.34. Az információs rendszerek védelme az audittesztelés során

- Szabályozandó területek, témakörök:
  - A Rendszer- és hálózatbiztonság alkalmazási terület önmagában is az információbiztonság egyik legnagyobb területét fogja össze: az informatikai infrastruktúra üzemeltetésének logikai biztonsági követelményeit. Ez kiterjed az informatikai infrastruktúra központi elemeinek (szerverek, központi hálózati elemek), végpontjainak és perifériáinak a biztonságos üzemeltetési követelményeire, beleértve már a felhőalapú szolgáltatások és egyéb interneten igénybe vett szolgáltatások szempontjait is.
  - Általános követelmény mindenfajta működés dokumentált szabályozottságának elvárása (5.37.), valamint minden változás végrehajtásának csak dokumentált változáskezelési eljárás keretében történő előírása (8.32.) is.
  - Külön követelményként szerepel a távmunka biztonsága (6.7.), beleértve annak fizikai biztonsági, humán biztonsági és informatikai biztonsági elvárásait is.
  - A központi szerver-oldali üzemeltetés biztonságát szolgálják a vírusvédelmi kontrollok (8.7.), a kiemelt jogokkal bíró segédprogramok biztonságos használatának kontrollja (8.18.). Noha a szabvány ehhez a ponthoz nem sorolja fel ezeket a témákat, de véleményem szerint ide tartoznak a következők: a biztonságos mentési eljárások (8.13.); a naplózás (8.15.) és monitorozás (8.16.); a konfigurációkezelés (8.9.); az információk törlése (8.10.); a kriptográfiai eljárások (8.24.) kontrolljai, valamint a Fenyegetések kezelése témakör kontrolljainak egyes elvárásai is.
  - A hálózatok és hálózati szolgáltatások biztonságos működésére sokkal nagyobb súlyt fektet a szabvány jelen verziója, ami meglátszik azon is, hogy ezt több önálló kontroll szabályozza. A hálózatok biztonsági szempontjait a 8.20. kontroll, és a hálózati szolgáltatások biztonsági elvárásait pedig a 8.21. kontroll foglalja össze. A hálózatok szegmentálásának (8.22.) követelményei ebben a szabványban önálló kontrollt alkotnak, és új önálló kontrollként jelent meg a Web-szűrés is.
  - A 8.23. Web-szűrés kontroll célja a rendszerek védelme a rosszindulatú szoftverek által történő veszélyeztetéstől, valamint megakadályozni a jogosulatlan webes erőforrásokhoz való hozzáférést.
  - Az informatikai infrastruktúra üzemeltetésének követelményein túlmenően megjelennek itt a szoftverfejlesztéshez kapcsolódó információbiztonsági követelmények is. Ezek azoknál a szervezeteknél bírnak jelentőséggel, ahol saját szoftverfejlesztéssel foglalkoznak, és a fejlesztett alkalmazások, rendszerek a saját, alkalmazott infrastruktúrájuk részét képezik.
  - A 8.25. Biztonságos fejlesztési életciklus tulajdonképpen egy összefoglalót ad a használandó további kontrollokra (8.26. – … – 8.34.). Ezek a követelmények lényegében megtalálhatók a megelőző verziójú ISO/IEC 27002:2013 szabványban, egy kivétellel.
  - A 8.28. Biztonságos kódolás új kontroll célja a szoftver biztonságos megírása, a szoftverben lévő potenciális információbiztonsági sebezhetőségek számának csökkentése. Részletes követelményeket határoz meg a tervezés és kódolás előtti folyamatra, magára a kódolásra, tesztelésre és üzembe helyezésre is. Szintén szabályozásra kerül a felülvizsgálat és karbantartás, de jelentős súllyal szerepelnek a külső eszközök/könyvtárak használata esetén alkalmazandó kontrollok.

4.7. Alkalmazásbiztonság

- Kapcsolódó kontrollok:
  - 5.37. Dokumentált működési eljárások
  - 8.4. Hozzáférés a forráskódhoz
  - 8.18. A kiváltságos segédprogramok használata
  - 8.19. Szoftverek telepítése az operációs rendszerre
  - 8.25. Biztonságos fejlesztési életciklus
  - 8.26. Az alkalmazások biztonsági követelményei
  - 8.27. Biztonságos rendszerarchitektúra és műszaki elvek
  - 8.28. Biztonságos kódolás
  - 8.29. Biztonsági tesztelés a fejlesztés és elfogadás után
  - 8.30. Kiszervezett fejlesztés
  - 8.31. A fejlesztési, tesztelési és termelési környezetek elkülönítése
  - 8.32. Változáskezelés
- Szabályozandó területek, témakörök:
  - Az Alkalmazásbiztonság alkalmazási terület az informatikai rendszeren futó programok, alkalmazások biztonságos üzemeltetésének és használatának követelményeiről szól.
  - Ezen belül két nagy területet ölel fel: a programok (alkalmazások) telepítésének és üzemeltetésének biztonsági kérdéseit, valamint a fejlesztési tevékenységek és az előállított szoftvertermékek biztonsági szempontjait, amennyiben a szervezetben szoftverfejlesztés (alkalmazásfejlesztés) is működik.
  - Általános követelmény, hogy a szervezet összes folyamata dokumentált és szabályozott legyen (5.37.), valamint elő kell írni, hogy minden változás végrehajtása csak a dokumentált változáskezelési eljárás keretében történhessen (8.32.).
  - A programok (alkalmazások) telepítésének, üzemeltetésének biztonsági szempontjait tartalmazza a 8.19. kontroll. Az informatikai rendszerhez hozzáférést biztosító segédprogramok használatához kapcsolódó biztonsági megszorítások szempontjaira pedig a 8.18. kontroll tér ki. Különleges esetnek számít a forráskódok védelme, az ahhoz való hozzáférések szempontjait a 8.4. kontroll foglalja össze.
  - Szoftverfejlesztés esetén külön kontrollcsoport foglalkozik annak információbiztonsági kérdéseivel, amiből kitűnik a téma kiemelt jelentősége. Egy alkalmazás feltörése nemcsak a nem kellően biztonságos üzemeltetési környezeten múlhat, hanem magának a szoftvernek a saját belső sérülékenységén is. Emiatt szükséges a szoftverfejlesztési tevékenység során a teljes folyamatba az információbiztonság szempontjait figyelembe venni, amelyek kiterjednek a szoftverfejlesztési életciklus minden egyes lépéseinek biztonságára, a fejlesztés során alkalmazott eszközök információbiztonsági szempontjaira, valamint magának az elkészített szoftverterméknek az információbiztonsági követelményeire, sérülékenységeinek felmérése és kezelése módszereire is. Ezeket a szempontokat foglalják össze a 8.25. – 8.31. kontrollok. A 8.28. kivételével, amely új kontroll ebben a szabványban, megtalálhatóak mind a megelőző verziójú ISO/IEC 27002-ben, de a jelen szabványban kiegészültek újabb szempontokkal.

4.8. Biztonságos konfiguráció

- Kapcsolódó kontrollok:
  - 5.37. Dokumentált működési eljárások
  - 8.4. Hozzáférés a forráskódhoz
  - 8.9. Konfigurációkezelés
  - 8.18. A kiváltságos segédprogramok használata
  - 8.19. Szoftverek telepítése az operációs rendszerre
  - 8.24. A kriptográfia használata
- Szabályozandó területek, témakörök:
  - A Biztonságos konfiguráció alkalmazási terület – noha a régi, az ISO/IEC 27002:2013 szab-

vány 12.1.1. fejezetében említésre került – önálló területként és azon belül önálló, új kontrollként (8.9.) jelenik meg ebben a szabványban.
  - Az alkalmazási területnek, és magának a 8.9. Konfigurációkezelés c. kontrollnak a célja annak biztosítása, hogy a hardver, a szoftver, a szolgáltatások és a hálózatok megfelelően működjenek a szükséges biztonsági beállításokkal, és a konfiguráció ne módosuljon jogosulatlan vagy helytelen módosításokkal.
  - Ehhez szükséges egyrészt az összes meglévő elem konfigurációjának kellően részletes és egységes felépítésű dokumentációja és annak folyamatos karbantartása. A konfigurációk változása is csak külön változáskezelési eljárás keretében valósítható meg, ezért ajánlott itt még a 8.32. Változáskezelés c. kontroll szempontjait is figyelembe venni.
  - A témacsoport további kontrolljai olyan területek szempontjait mutatja be, amely területek tartalmuknál fogva kapcsolódnak bizonyos elemek konfigurációinak megváltoztatásához, vagy a konfigurációváltozások végrehajtásának egyes biztonsági technikáihoz.

4.9. Identitás- és hozzáférés-kezelés

- Kapcsolódó kontrollok:
  - 5.3. A feladatok elkülönítése
  - 5.15. Hozzáférés-ellenőrzés;
  - 5.16. Személyazonosság-kezelés
  - 5.17. Hitelesítési információk
  - 5.18. Hozzáférési jogok
  - 5.37. Dokumentált működési eljárások
  - 7.2. Fizikai belépés
  - 7.3. Irodák, helyiségek és létesítmények biztosítása
  - 8.2. Privilegizált hozzáférési jogok
  - 8.3. Az információhoz való hozzáférés korlátozása
  - 8.4. Hozzáférés a forráskódhoz
  - 8.5. Biztonságos hitelesítés
- Szabályozandó területek, témakörök
  - Az Identitás- és hozzáférés-kezelés alkalmazási terület az egyik legösszetettebb és legsokrétűbb alkalmazási területe az információbiztonság működésének. Célja annak biztosítása, hogy az egyes információkhoz csakis és kizárólag az arra jogosultak férhessenek hozzá. (Tulajdonképpen ez valósítja meg a „szükséges és elégséges információkhoz való hozzáférés" alapelvét.)
  - Az információkhoz való hozzáférések biztosítása kiterjed magukon az információkon túlmenően minden információs vagyonelemre, azaz az információt tartalmazó, feldolgozó, illetve kezelő infrastruktúra-elemekre, adathordozókra, folyamatokra és eszközökre, az azokhoz való minden fizikai és logikai hozzáférés tekintetében.
  - Ezek a kontrollok kiterjednek a szükséges hozzáférések meghatározására, azok szabályrendszerének kialakítására és dokumentálására, valamint a megvalósítások különböző területeken történő technikai kivitelezésére, beleértve az egyes hozzáférések biztosítása során a megfelelő azonosítási és feljogosítási (authentikációs és authorizációs) módszerek alkalmazását is. Az egyes kontrollok ennek a folyamatnak az egyes részeinek megvalósításához adnak támogatást, a betartandó szempontok bemutatásával, beleértve a lehetséges speciális esetek kezelését is (pl. 8.2., 8.4).
  - A folyamat kialakításának egyik első lépése tulajdonképpen annak meghatározása, hogy melyik adatunk mennyire érzékeny, azaz milyen szinten kell védeni. Ehhez magát az adatvagyont kell felmérni, és megfelelő információbiztonsági osztályba sorolni, majd azok alapján meghatározni a biztonsági intézkedések szükséges szintjét, szigorát. (Ezek a lépések részletesen megtalálhatók az 'Információvédelem' és a 'Vagyonelemek kezelése' c. területek kontrolljaiban.) A másik kiindulási lépés annak meghatározása, hogy a szervezet melyik működési folyamata alapján kinek (és milyen jogosultsággal) szükséges hozzáférni az egyes adatokhoz, adattípusokhoz. Ebből a 2 információhalmazból kell összeállítani, hogy a vállalat mely adatá-

hoz ki férhet hozzá, és ezeknek a hozzáféréseknek milyen szigorú biztonsági követelményeket kell teljesíteni
  - Az egyes vagyonelemek biztonságos működését, és az azokhoz való biztonságos hozzáféréseket technikailag úgy kell kialakítani, hogy az az előzőekben meghatározott szempontoknak az adott vagyonelem vonatkozásában megvalósítható legyen. Ezek kiterjednek mind a feljogosított személyek kellő biztonsági szintnek megfelelő azonosítására, mind utána a feljogosításnak pontosan megfelelő jogosultságok engedélyezésére. A követelmények kiterjednek ezek folyamatos felügyeletére és naplózására, valamint a változások karbantartására is. Az egyes kontrollok tulajdonképpen a különböző vagyonelem-típusok esetén az ezen alapelvek megvalósításához szükséges szempontokat és tanácsokat írják le.
  - Ez a tématerület minden témaköre megtalálható volt már a régi szabványban is, így noha nem tartalmaz új kontrollt, de a meglévő kontrollokhoz tartozó magyarázatok részletesebbek és érthetőbbek lettek.

4.10. Fenyegetések és sebezhetőség kezelése

- Kapcsolódó kontrollok:
  - 5.7. Fenyegetettségi információk
  - 5.37. Dokumentált működési eljárások
  - 8.8. A műszaki sebezhetőség kezelése
- Szabályozandó területek, témakörök:
  - A Fenyegetések és sebezhetőségek kezelése alkalmazási terület az információs rendszerek fenyegetettségi környezetének tudatosításáról, és a technikai sebezhetőségek kihasználásának megakadályozásáról szól.
  - A műszaki sebezhetőség kezelése c. kontroll (8.8.) a folyamat a teljes életciklusán keresztüli szabályozott működését írja elő, a műszaki sebezhetőségek azonosításától kezdve azok értékelésén át egészen a megfelelő intézkedések meghatározásáig és azok alkalmazásáig. A műszaki sebezhetőség kezelése már a megelőző verziójú, az ISO/IEC 27002:2013 szabványban is szerepelt a 12.6.1 fejezetben, és itt kibővült az előző szabvány a 18.2.3. Műszaki megfelelés felülvizsgálata c. kontroll szempontjaival és néhány további magyarázattal.
  - Új kontrollként jelent meg ebben a szabványban az 5.7. Fenyegetettségi információk. Ez elsősorban a lehetséges fenyegetések előzetes feltárásáról, továbbá az elhárításuk megtervezéséről és előkészítéséről szól. A fenyegetésekről szóló információk előállíthatók saját szervezeten belül is, de gyakori a külső, független szolgáltatók vagy ügynökségek (pl. CERT-szervezetek) szolgáltatásai által nyújtott fenyegetettségi információk használata.
  - A fenyegetések felderítése 3 szintre osztható (stratégiai, taktikai és operatív fenyegetésfelderítés). A kontroll ehhez kapcsolódóan szabályozza a felderítési és elhárítási folyamatokat, valamint elvárást fogalmaz meg az elhárítás során keletkezett információk elemzésére, későbbi hasznosítására, és ezek alapján a megelőző intézkedések módosítására. Ezek alkalmazhatók megelőző, felderítő, valamint javító intézkedésként is.

4.11. Folyamatosság (működési vagy üzletmenet folytonosság)

- Kapcsolódó kontrollok:
  - 5.29. Információbiztonság zavarok során
  - 5.30. Az IKT készenléte az üzletmenet-folytonossághoz
  - 5.37. Dokumentált működési eljárások
  - 8.6. Kapacitáskezelés
  - 8.13. Információbiztonsági mentés
  - 8.14. Az információfeldolgozó létesítmények redundanciája
- Szabályozandó területek, témakörök:
  - A Folyamatosság alkalmazási területnek a célja a vállalat üzletmenet-folytonosságának biztosítása a rendkívüli helyzetekben is (pl. természeti katasztrófák, fizikai támadások,

kibertámadások, társadalmi vészhelyzetek, balesetek vagy jelentős hatású infrastrukturális hibák).

- Az üzletmenet-folytonosság kérdése alapvetően a vállalat felső vezetői szintű feladata, de a megvalósításban sokszor az informatikai infrastruktúra üzemeltetés területére komoly szerep jut. Ennek oka egyrészt az adott folyamatok informatikai támogatottságának a jelentős szerepe, másrészt pedig az, hogy az üzletmenet-folytonosságot veszélyeztető zavarok sokszor épp az informatikai infrastruktúrát érintik.
- Ennek a területnek az elvárása, hogy üzleti hatáselemzéssel kell meghatározni azokat a kritikus folyamatokat, amelyeknél nagyobb zavarok bekövetkezése esetén üzletmenet-folytonossági terv kidolgozása szükséges. Továbbá azok informatikai támogatásához szükséges feltételeket kell meghatározni és biztosítani. Ezek meghatározásáról szólnak az 5.29. és 5.30. kontrollok.
- A szükséges folyamatokat és eljárásokat dokumentáltan kell szabályozni és azokat karban kell tartani (5.37.). Az üzletmenet-folytonossági tervekhez szükséges IKT (infokommunikációs technológiai) feltételek biztosítása érdekében a szükséges elvárásokat a kapacitáskezelés (8.6.), a mentési rendszer kialakítása (8.13.) valamint az IKT eszközök redundanciájának biztosítása (8.14.) során kell fontos szempontként figyelembe venni.

4.12. Beszállítói kapcsolatok biztonsága

- Kapcsolódó kontrollok:
  - 5.19. Információbiztonság a beszállítói kapcsolatokban
  - 5.20. Az információbiztonság kezelése a beszállítói megállapodásokban
  - 5.21. Az információbiztonság kezelése az IKT ellátási láncban
  - 5.22. A beszállítói szolgáltatások nyomon követése, felülvizsgálata és változásmenedzsmentje
  - 5.23. Információbiztonság a felhőszolgáltatások használatakor
  - 6.6. Bizalmassági vagy titoktartási megállapodások
  - 8.30. Kiszervezett fejlesztés
- Szabályozandó területek, témakörök:
  - A Beszállítói kapcsolatok biztonsága alkalmazási területnek a célja, hogy az alvállalkozókkal és beszállítókkal való együttműködés során az információbiztonság megfelelő szintje megmaradjon. Ehhez természetesen az szükséges, hogy az alvállalkozók és beszállítók által hozzáfért, kezelt adatok biztonsága, illetve amennyiben ők hozzáférnek rendszereinkhez, akkor azon hozzáférések által is a rendszereink biztonsága ugyanolyan szinten maradjon.
  - A követelmények elvárják, hogy először legyenek felmérve az alvállalkozói és beszállítói együttműködések során a megosztott adatok érzékenysége és az adathozzáférések módjából következő információbiztonsági kockázatok. Ezeken keresztül kell meghatározni az alvállalkozók és beszállítók által teljesítendő információbiztonsági elvárásokat, amiket természetesen csak akkor lehet betartatni, ha azok a szerződéseken keresztül is rögzítettek.
  - Külön kiemelt alvállalkozói témakör az informatikai infrastruktúra-szolgáltatás kiszervezése, ahol annak megbízható üzemeltetése és biztonsága külön jelentőséggel bír a szervezet működésére és információinak biztonságára. Emiatt az ezekre vonatkozó követelményeket kiemelt jelentőséggel kell kezelni. Gyakran előfordul, hogy nagyobb infrastruktúraszolgáltatók esetén nincs lehetőség a saját biztonsági elvárások beépítése céljából a szerződéseket egyénileg megtárgyalni, hanem az adott szolgáltató Általános Szerződéses Feltételeiben meghatározottak az adottak. Ilyen esetben mérlegelni kell, hogy az abban foglalt garanciák elegendőek-e a vállalat számára, vagy a kockázatok felmérése alapján a kockázatok vállalhatók-e vagy sem.
  - Ezen informatikai szolgáltatások egy kiemelt és az utóbbi években egyre elterjedtebb speciális esete a felhő alapú szolgáltatások, amelyek követelményeire egy új, önálló kontroll (5.32.) is megfogalmazásra került. További speciális terület a szoftverfejlesztést végző szervezeteknél a szoftverfejlesztés kiszervezése (8.30.), ahol a szoftverfejlesztés és -termék biztonságára vonatkozó követelményeket a kiszervezett alvállalkozón keresztül is kell tudni biztosítani.

4.13. Jog és megfelelőség

- Kapcsolódó kontrollok:
  - 5.31. Jogi, jogszabályi, szabályozási és szerződéses követelmények
  - 5.32. Szellemi tulajdonjogok
  - 5.33. A feljegyzések védelme
  - 5.34. Adatvédelem és PII (személyes adatok) védelme
  - 5.36. Az információbiztonságra vonatkozó irányelveknek, szabályoknak és szabványoknak való megfelelés
  - 8.10. Információk törlése
- Szabályozandó területek, témakörök:
  - A Jog és megfelelőség alkalmazási területnek a célja az információbiztonság működése során a jogi és egyéb külső követelményeknek való megfelelés biztosítása.
  - Ide tartoznak külső követelményként a jogi, szerződéses, illetve egyéb vállalt szabványok által megfogalmazott követelmények azonosítása és teljesítése (5.31.), illetve belső követelményként a saját szervezet által megfogalmazott irányelveknek és szabályozásoknak való megfelelések biztosítása (5.36.) is.
  - Külön kiemelt témaként jelenik meg a személyes adatok megfelelő védelmének biztosítása (5.34.), valamint a feljegyzések kezelése c. kontroll (5.33.) keretein belül a különböző szerződések, bizonylatok és egyéb igazoló dokumentumok jogszabályoknak megfelelő biztonságos kezelése. A szellemi tulajdonjogok megfelelő kezelése kontroll (5.32.) magába foglalja mind a munkahelyi találmányok, szabadalmi jogok megfelelő kezelését, mind a jogszerű szoftverlicensz-gazdálkodást.
  - Új technológiai kontrollként jelent meg az Információk törlése (8.10.), amelynek célja az adatszivárgás megelőzése érdekében a már nem megőrzendő dokumentumok és információk biztonságos törlési módszereinek alkalmazása, amely során fontos szempont a kapcsolódó jogi követelmények ismerete és betartása is.

4.14. Információbiztonsági események kezelése

- Kapcsolódó kontrollok:
  - 5.24. Információbiztonsági incidensek kezelésének tervezése és előkészítése
  - 5.25. Értékelés és döntés az információbiztonsági eseményekről
  - 5.26. Az információbiztonsági eseményekre való reagálás
  - 5.27. Tanulás az információbiztonsági incidensekből
  - 5.28. Bizonyítékok gyűjtése
  - 5.37. Dokumentált működési eljárások
  - 6.8. Információbiztonsági események jelentése
  - 8.15. Naplózás
  - 8.16. Monitoring tevékenységek
  - 8.17. Óraszinkronizálás
- Szabályozandó területek, témakörök
  - Az Információbiztonsági események kezelése alkalmazási terület az információbiztonsági események és incidensek kezelése folyamatának követelményeit foglalja össze.
  - A kontrollok nagy része a folyamat teljes életciklusának szabályozására vonatkozó szabályozási és technikai lépéseket írja elő, beleértve a felkészülést támogató, az utólagos értékelő és a tanulást biztosító adminisztratív tevékenységeket is.
  - Az adminisztratív kontrollok gyakorlatilag előírják a folyamat életciklusának mindegyik lépésére vonatkozó követelményeket, összehangban a kapcsolódó ISO/IEC 27036-os szabványcsoporttal, amely részletesen tárgyalja az információbiztonsági esemény- és incidenskezelés követelményeit.
  - Megjelennek továbbá az események és incidensek elemzéséhez szükséges naplózási (loggolási) követelmények, valamint az incidensek előrejelzésében és kiértékelésében fontos szerepet kapó monitoring tevékenységek is.

- A Monitoring tevékenységek című kontroll (8.16.) új követelményként jelenik meg ebben a szabványban, elsődleges célja a potenciális információbiztonsági incidensek felderítése a hálózatok, rendszerek és alkalmazások monitorozásával. A kontroll hasznos célokat és szempontokat mutat be az alkalmazandó rendszerek automatizmusainak beállítására.

4.15. Információbiztonság biztosítása

- Kapcsolódó kontrollok:
  - 5.22. A beszállítói szolgáltatások nyomon követése, felülvizsgálata és változásmenedzsmentje
  - 5.35. Az információbiztonság független felülvizsgálata
  - 5.36. Az információbiztonságra vonatkozó irányelveknek, szabályoknak és szabványoknak való megfelelés
  - 8.29. Biztonsági tesztelés a fejlesztés és elfogadás után;
- Szabályozandó területek, témakörök:
  - Az Információbiztonság biztosítása alkalmazási területnek a célja az információbiztonsági irányítási rendszer működtetésének független és megbízható ellenőrzése. Alapvető elvárás, hogy a kialakított információbiztonsági rendszer kontrolljainak működése, hatékonysága elérje a kitűzött célokat, és ezek megfelelő ellenőrzésekkel igazolhatók legyenek.
  - Ehhez a területhez tartoznak elvárásként magának a teljes információbiztonsági rendszernek és kontrolloknak a független felülvizsgálata a hatékonyság és a kialakított szabályoknak való megfelelés szempontjából (5.35., 5.36.), a beszállítói szolgáltatások ellenőrzése (5.22.) és szoftverfejlesztések esetén a fejlesztés elfogadása utáni külön biztonsági tesztelések elvégzése (8.29.).
  - Tulajdonképpen a szabvány nem említi, de úgy vélem, hogy az informatikai rendszerek IT biztonsági auditjai során az informatikai rendszerek védelmének (8.34. kontroll) is van ilyen aspektusa. Hiszen az audit során nemcsak arra kell odafigyelni, hogy az IT audit az auditált informatikai rendszerben (vagy egyéb környezetben) ne okozhasson kárt, hanem magának az ellenőrzések elvégzésének és eredményének megfelelőségére és naplózására is.

5. Összefoglalás

Az ISO/IEC 27001:2022 szabvány legnagyobb változásának, az 'A mellékletben' megújult információbiztonsági kontrolloknak a magyarázata és értelmezése teljes egészben az ISO/IEC 27002:2022 szabványban található. Az új szabványkövetelményeknek való megfeleléshez szükséges az egyes kontrollok követelményeinek a megismerése és megértése. Ezért nagyon ajánlott minden vállalatnak az új ISO/IEC 27002 szabvány megismerése és használata is.

A jelen publikációban az ISO/IEC 27002:2022 szabvány kontrolljainak megújult struktúráját és annak használati lehetőségeit tekintettem át, az ezzel foglalkozni kívánó vállalatok és szakemberek segítése céljából.

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

DR. HORVÁTH ZSOLT, CSc. szilikátipari mérnök, matematikai modellezési szakmérnök, a műszaki tudomány kandidátusa. EOQ MNB Minőségirányítási és Információbiztonsági Rendszermenedzser és Auditor személytanúsítvánnyal rendelkezik. 10 évi ipari majd 3 évi IT vezetői gyakorlat után 10 éven keresztül a Siemens magyarországi szoftverházának, a Sysdata Kft-nek (amiből közben a Siemens PSE Kft. lett) a minőségügyi vezetőjeként dolgozott. Négy évet az Óbudai Egyetemen információbiztonságot oktatott. 2000-től folyamatosan több tanúsító szervezetnél minőségügyi és információbiztonsági vezető auditor. 2006-tól az INFOBIZ Kft. vezetőjeként és vezető tanácsadójaként minőségügyi és információbiztonsági tanácsadó.