Dr. Muha Lajos

Információbiztonsági szabványok

NEMZETI KÖZSZOLGÁLATI EGYETEM,
BUDAPEST

Információbiztonsági szabványok

Szerző:
Dr. Muha Lajos

Szakmai lektor:
Dr. Magyar Sándor

A kézirat lezárásának dátuma:
2026. február 8.

Kiadó:
Nemzeti Közszolgálati Egyetem
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős kiadó:
Dr. Deli Gergely rektor
Címe: 1083 Budapest, Üllői út 82.

TARTALOMJEGYZÉK

BEVEZETÉS

A kiberbiztonság az elmúlt évtizedben kilépett a tisztán technikai „IT-biztonság” keretei közül, és a szervezetek stratégiai, jogi és irányítási kérdéseinek egyik központi elemévé vált. A digitális működés, a felhőszolgáltatások, az ipari vezérlőrendszerek, az IoT-eszközök és a globális beszállítói láncok olyan összefüggő ökoszisztémát alkotnak, amelyben egyetlen súlyosabb kiberincidens is komoly gazdasági, társadalmi vagy akár fizikai következményekkel járhat. Ezért a szabályozók és felügyeleti hatóságok, valamint a piaci partnerek egyre inkább elvárják, hogy a szervezetek kockázatarányosan és ezt igazolhatóan kezeljék az információbiztonságot és a kiberbiztonságot. [1]

Ebben a környezetben különös jelentőséget kapnak a nemzetközi szabványok és keretrendszerek. A jogszabályok – így az Európai Unió NIS2 irányelve és a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény – jellemzően nem tételes technikai előírásokat, hanem elvárt eredményeket fogalmaznak meg: folyamatos kockázatértékelést, kockázattal arányos védelmi intézkedéseket, incidenskezelő és üzletmenet-folytonossági képességeket, auditálhatóságot. [1] Ezek megfogható, mérhető és tanúsítható megvalósításához adnak eszközt az olyan szabványcsaládokkal, mint az ISO/IEC 27000-es sorozat és az ISO/IEC 15408 (Common Criteria). [2][3]

A kézikönyv ennek megfelelően megpróbálja bemutatni a szervezeti szintű szabványok és keretek mellett a termék- és eszközszintű szabványokat. Ezek közül az ISO/IEC 27000-es család és a Common Criteria kiemelt jelentőségűek, mert ezekre épül többek között a NIS2 értelmezése, a nemzetközileg elfogadott tanúsítási rendszerek működése, az IT-szolgáltatásmenedzsmenttel és OT-biztonsággal való integráció, valamint az eszközszintű biztonsági szabványok szerepe.

1. A KIBERBIZTONSÁGI SZABVÁNYOK SZEREPE

1.1 A szabvány

„A szabvány *elismert szervezet által alkotott vagy jóváhagyott, közmegegyezéssel elfogadott olyan műszaki (technikai) dokumentum, amely tevékenységre vagy azok eredményére vonatkozik, és olyan általános és ismételten alkalmazható szabályokat, útmutatókat vagy jellemzőket tartalmaz, amelyek alkalmazásával a rendező hatás az adott feltételek között a legkedvezőbb."* [4] A szabványok készítését, használatát a nemzeti szabványosításról szóló 1995. évi XXVIII. törvény szabályozza.

A szabvány alkalmazása a nemzeti szabványosításról szóló törvény alapján önkéntes. Az önkéntesség választási lehetőséget biztosít a szabvány alkalmazása vagy mellőzése tekintetében. A szabvány közmegegyezéssel elfogadott műszaki dokumentum, amelynek révén általánosan elismert megoldás érhető el. [4]

A szabványnak való megfelelőség akkor valósul meg, ha változtatás nélkül érvényesülnek az előírásai. Ezt a szabványra hivatkozva kell igazolni. [4]

Szabványügyi szervezetek és az általuk kibocsátott szabványok jelölése:

- **ISO** International Standards Organization – ISO
- **IEC** International Electrotechnical Commission – IEC
- **IEEE** Institute of Electrical and Electronics Engineers – IEEE
- **ITU** International Telecommunication Union – ITU
- **CEN** Comité Européen de Normalisation – EN
- **ETSI** European Telecommunications Standards Institute – ETSI
- **MSZT** Magyar Szabványügyi Testület – MSZ
- **DIN** Deutsches Institut für Normung – DIN
- **BSI** British Standards Institute – BS
- **NIST** National Institute of Standards and Technology – NIST
- **ANSI** American National Standards Institute – ANSI

A szabványok jelölésében először a kibocsátói jelet vagy jeleket kell feltüntetni a kibocsátás sorrendjében. Ezt követi a szabvány azonosítószáma, más néven a szabványszám, amelyhez, ha az többkötetes, akkor egy kötőjellel elválasztva a kötet számát is csatolják A teljes hivatkozási szám megadásához egy kettőspont után feltüntetik az első helyen szereplő kibocsátó általi közzététel évszámát.

1. ábra A szabványok jelölése

1.2 Az európai és a magyar szabályozások

Hazánkban az informatikai rendszerek biztonságának szakmai támogatása a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) „Informatikai biztonsági módszertani kézikönyv" címet viselő, 1994-ben kiadott MeH ITB 8. számú ajánlásával [5] kezdődött. Ez a brit kormány Központi Számítógép és Távközlési Ügynökség (Central Computer and Telecommunications Agency) *„CCTA Risk Analysis and Management Method"* és az északrajna–vesztfáliai kormány *„Informationtechnik Sicherheitshandbuch"* felhasználásával, valamint az EU informatikai ajánlásai és az akkori hazai jogszabályok alapján készült. A MeH ITB 8. számú ajánlását mint az informatikai biztonság – CRAMM-alapú – kockázatelemzési módszertanát a közigazgatás területén kívül is sokáig használták.

A MeH ITB kezdeményezésére 1995-ben kezdődött meg a következő hazai ajánlás kidolgozása, amelyet 1996 decemberére véglegesítettek *Informatikai Rendszerek Biztonsági Követelményei* címmel, és a MeH ITB 12. számú ajánlásként vált *de facto* szabványnyá. [6] Az Informatikai Rendszerek Biztonsági Követelményeiben logikai védelem esetében az EU Information Technology Security Evaluation Criteria (ITSEC) [7] ajánlása lett adaptálva, ugyanakkor részletes követelményeket és védelmi intézkedéseket tartalmaz az informatikai biztonság adminisztratív és a fizikai védelem területeire, a szervezeti, szabályozási, személyi és fizikai biztonság kérdéseire is. A gazdasági élet számos szereplője a saját biztonsági politikája kialakításakor figyelembe vette a 12. sz. ajánlást. [8] Belső szabályzóként, követelményrendszerként használták a biztonsági követelmények meghatározására, például a Belügyminisztérium Informatikai Biztonsági Stratégiájáról szóló 23/2011. (IX. 2.) BM utasításban még hivatkoznak ezekre az ajánlásokra. A MeH ITB 12. számú ajánlásban megalkotott biztonsági osztályba sorolást alkalmazza többek között *a 7/2024. (VI. 24.) MK rendelet* [9] a *Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény* [10] hatálya alá tartozó elektronikus információs rendszerei biztonsági osztályba sorolására.

A mai magyar kiberbiztonsági jogi környezet közvetlenül az Európai Unió szabályozására épül, különösen a NIS2-ként közismert (EU) 2022/2555 számú irányelvre, amely az unió egész területén egységesen magas szintű kiberbiztonságot célzó intézkedéseket ír elő. A NIS2 nem konkrét technikai megoldásokat követel, hanem olyan irányítási és kocká-

zatkezelési keretet, amely biztosítja a kockázatarányos védelmi intézkedések kialakítását, az incidenskezelés és -jelentés folyamatainak működtetését, az ellátási lánc kiberbiztonsági követelményeinek kezelését és a vezetői felelősség megerősítését. [1]

Az irányelv mögöttes logikája kifejezetten kedvez az olyan szabványcsaládok alkalmazásának, mint az ISO/IEC 27000, mivel a „megfelelő technikai és szervezési intézkedések" tartalmát a tagállamok többsége ezekhez a szabványokhoz viszonyítja. Az ENISA szakmai anyagai [11] is rendszeresen utalnak arra, hogy az ISO/IEC 27001-re [12] épülő információbiztonsági irányítási rendszer jól illeszkedik a NIS2 elvárásaihoz.

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: *kiberbiztonsági törvény*) a NIS2 hazai átültetésére alkotott jogszabály. A törvény hatálya kiterjed az államigazgatás meghatározott szereplőire, a kritikus és fontos ágazatokban működő szervezetekre (például energetika, közlekedés, egészségügy, digitális infrastruktúra, banki-pénzügyi szolgáltatások), valamint más olyan szervezetekre, amelyek szolgáltatásainak zavara rendszerszintű hatással bírhat. [10]

A törvény alapelvei között kiemelt szerepet játszik a folyamatos kockázatértékelés és kockázatkezelés, a kockázattal arányos védelmi intézkedések előírása, valamint a rendszerszintű kiberbiztonsági irányítási megoldások bevezetésének kötelezettsége. [10] Ezek az elvek közvetlenül rámutatnak az ISO/IEC 27001-re épülő Információbiztonsági Irányítási Rendszer jelentőségére, amely a PDCA-ciklus, a vezetői felelősség, a szabályozási rendszer, a dokumentált kockázatkezelés és a biztonságtudatosítás, valamint a tanúsítási rendszere révén gyakorlati keretet adhatna a törvényben megfogalmazott elvárásoknak. [12]

A magyar jogalkotók nem ezt választották ki a kiberbiztonsági törvény végrehajtásának megoldásához iránymutatóul, hanem az USA szövetségi információs rendszereire vonatkozó NIST SP800-53-at, és egy az európai gyakorlatban egyedülálló auditálási rendszert [13] [14] alkottak hozzá.

A kiberbiztonsági törvény alapján a Nemzeti Kiberbiztonsági Intézet (NKI) kiemelt felügyeleti és módszertani szerepkörrel rendelkezik. Feladatai közé tartozik a jogszabályban meghatározott szervezetek ellenőrzése (audit, helyszíni vizsgálat, dokumentum-ellenőrzés), módszertani útmutatók, ajánlások és mintadokumentumok kidolgozása, az incidensjelentések fogadása és elemzése, valamint a nemzetközi kiberbiztonsági együttműködésben való részvétel. [10]

1.3 A kiberbiztonsági szabványok szerepe és feladata

A kiberbiztonsági szabványok egyik legfontosabb funkciója, hogy közös fogalmi és követelményrendszert biztosítanak a szervezetek, beszállítók, felügyeleti hatóságok és auditorok számára. Egy ISO/IEC 27001 szerint tanúsított információbiztonsági irányítási rendszer, vagy egy Common Criteria szerinti terméktanúsítás esetében egyértelmű, hogy mely követelményrendszernek igyekezett a szervezet megfelelni, milyen auditálási elvárások és eljárások mellett.

Ez a közös nyelv három szinten nyújt előnyt:

- **Összehasonlíthatóság**: két, eltérő országban működő, de ugyanazon szabvány szerint tanúsított szervezet kiberbiztonsági érettsége, illetve különböző gyártók termékeinek biztonsági jellemzői viszonylag objektíven összevethetők.
- **Bizonyítékalap a megfeleléshez**: a „megfelelő technikai és szervezési intézkedések" teljesítése nem szubjektív állításokra, hanem tanúsítványokra, auditjelentésekre, intézkedéslistákra támaszkodik.

- **Átjárhatóság több joghatóság között**: egy multinacionális szervezet egyetlen, szabványalapú irányítási rendszert építhet ki, amelyet több ország különböző hatóságai is elfogadnak.

A NIS2 tudatosan nem ír elő konkrét szabványokat, hogy elkerülje a jogi szabályozás elavulását a technológia gyors változása mellett. [1] Ugyanakkor a gyakorlatban az auditorok a „megfelelő technikai és szervezési intézkedéseket" a nemzetközi szabványokhoz mérik, különösen az ISO/IEC 27001-hez és a Common Criteriához.

Incidensek vagy megfelelési vizsgálatok során gyakori kérdés, hogy a szervezet:
- kialakított-e és működtet-e az ISO/IEC 27001 [12] követelményeinek megfelelő információbiztonsági irányítási rendszert;
- végzett-e az ISO/IEC 27005 [15] logikája szerinti dokumentált kockázatértékelést;
- alkalmaz-e elismert termékszabványokon alapuló komponenseket például ISO/IEC 15408 szerint-tanúsított tűzfalakat [3] vagy ETSI EN 303 645-öt követő IoT-eszközöket (IoT: Internet of Things) [16] vagy IEC 62443-kompatibilis vezérlők [17].

A szabványok tehát egyfajta alkalmazói feladatot látnak el a jogi elvárások és a műszaki-szervezeti gyakorlat között: segítenek abban, hogy a magas szintű, elvárt kimenetek konkrét, ellenőrizhető intézkedésekké és követelményekké váljanak.

A kiberbiztonsági szabványok két fő csoportra bonthatók:
- **Szervezeti szintű irányítási és keretszabványok** – például ISO/IEC 27001 (Információbiztonsági Irányítási Rendszer), ISO/IEC 20000-1 [18] (IT-szolgáltatásmenedzsment), NIST Cybersecurity Framework [19], COBIT (Control Objectives for Information and Related Technologies) [20]. Ezek a szabványok a folyamatok, a felelősségek, a kockázatkezelés, az audit és a folyamatos fejlesztés logikáját adják meg.
- **Termék- vagy eszközszintű szabványok** – például ISO/IEC 15408 (Common Criteria), IEC 62443 komponensszabványok, ETSI EN 303 645 a fogyasztói IoT-re. Ezek konkrét IT-eszközökre, rendszerekre vonatkozó biztonsági követelményeket és értékelési módszereket határoznak meg.

A két szint egymást kiegészítve működik: egy ISO/IEC 27001 szerinti *Információbiztonsági Irányítási Rendszer* (IBIR, angolul Information Security Management System: ISMS) keretében egy ISO/IEC 270015 alapján végzett kockázatértékelés azonosítja azokat a területeket, ahol különösen nagy a technológiai kockázat (például tűzfalak, kriptográfiai modulok, ipari vezérlő eszközök). Ezeken a területeken a szervezet termékszintű szabványokra és tanúsításokra támaszkodhat, hogy megalapozza a beszállítói követelményeket és a beszerzési döntéseket.

2. KIBERBIZTONSÁGI KERETRENDSZEREK

A kiberbiztonsági keretrendszerek (frameworkök) nem mindig tanúsítható szabványok, de fontos szerepet játszanak abban, hogy az ISO/IEC 27001 szabvány szerinti Információbiztonsági Irányítási Rendszer és a Common Criteria-alapú termékbiztonság a gyakorlatban koherens egésszé álljon össze. Ezek a keretek magas szinten írják le, milyen funkciókat, képességeket és bizalmi szinteket kell elérnie egy szervezetnek vagy terméknek ahhoz, hogy adott kockázati környezetben megbízhatónak tekinthető legyen.

A NIST Kiberbiztonsági Keretrendszer (CSF: Cybersecurity Framework) a kiberbiztonsági életciklust öt alapvető funkció, az **Azonosítás (Identify)**, a **Védelem (Protect)**, az **Észlelés (Detect)**, a **Válasz (Respond)** és a **Helyreállítás (Recover)** mentén strukturálja. Ezek a funkciók képzik a keretrendszer magját, és a kockázatkezelési tevékenységek, a kívánt eredmények és a hivatkozott szabványok, irányelvek és gyakorlatok összességét foglalják össze. Az alapvető funkciók alá kategóriák és alkategóriák tartoznak. A keretrendszer kategóriáihoz hivatkozások tartoznak, többek között az ISO/IEC 27001, a PCI DSS (Payment Card Industry Data Security Standard), a HIPAA és a CIS Controls (Center for Internet Security Critical Security Controls) szabványokhoz, valamint a NIST 800-53, a GDPR (General Data Protection Regulation – az Európai Unió általános adatvédelmi rendelete) és más iparági szabványokhoz, így a keret segít az egyes szabványok közötti „térkép” megrajzolásában. A CSF 2.0 verzió egy kereshető hivatkozási katalógust is tartalmaz, amely lehetővé teszi a szervezetek számára, hogy több mint 50 másik releváns kiberbiztonsági dokumentumhoz férjenek hozzá.

A CSF gyakorlati előnye, hogy:

- átlátható, könnyen kommunikálható a felső vezetés felé;
- támogatja a kiberbiztonsági érettség önértékelését és fejlesztési útvonalak kijelölését;
- rugalmasan kombinálható az ISO/IEC 27001-alapú Információbiztonsági Irányítási Rendszerrel: a CSF funkciói jól megfeleltethetők az ISO/IEC 27001 követelményeinek és az ISO/IEC 27002 [21] szabványban részletezett védelmi intézkedéseinek.

Ez a kombináció különösen hasznos olyan szervezeteknél, amelyek egyszerre szeretnének megfelelni amerikai és európai elvárásoknak, vagy többféle auditrendszer (például ISO-tanúsítás és NIST-alapú ellenőrzés) szerint értékelik őket.

Az EU Cybersecurity Act [22] egységes európai kiberbiztonsági tanúsítási keretrendszert hozott létre az IKT-termékekre, -szolgáltatásokra és -folyamatokra. A rendelet különböző bizalomszinteket (alap, jelentős, magas) határoz meg, és előírja, hogy az egyes tanúsítási rendszerek világosan jelöljék a vonatkozó szabványokat, értékelési módszereket és tanúsítási követelményeket.

A gyakorlat szempontjából ez azt jelenti, hogy az ISO/IEC 27001-re épülő szervezeti irányítási és az IEC 62443 szerinti terméktanúsítási rendszer ugyanannak az európai tanúsítási logikának a részei. Egy jól felépített vállalati kiberbiztonsági stratégia ezért egyszerre törekszik:

- szervezeti szinten egy érett, tanúsítható információbiztonsági irányítási rendszer kialakítására;
- technológiai szinten pedig a kulcstermékek (tűzfalak, kriptográfiai modulok, OT-eszközök, IoT-komponensek stb.) esetében a Common Criteria, az IEC 62443 vagy az ETSI EN 303 645 szabvány szerint tanúsított termékek beszerzésére.

3. AZ ISO/IEC 27000

3.1 A szabványcsalád

Az ISO/IEC 27000 szabványcsalád alapját a Brit Szabványügyi Hivatal (BSI) által kiadott brit szabvány, a BS 7799 képezi. A BS 7799 szabvány első revíziója 1999-ben történt, és az első részét nemzetközi szabványként történő elfogadásra javasolta a BSI. A Nemzetközi Szabványügyi Szervezet (ISO) 2000 augusztusában a BS 7799 1:1999 szabványt változatlan szerkezetben és gyakorlatilag változatlan tartalommal nemzetközi szabványnak fogadta el ISO/IEC 17799 néven.

A brit szabvány második része, a BS 7799-2:1999 már a megjelenése után *de facto* nemzetközi szabvánnyá vált, de több ország (például Japán, Svédország) nemzeti szabványként is bevezette. 2002-ben kiadták a BS 7799-2:2002 szabványt, amely már az ISO 9001:2000 szabvány figyelembevételével készült. 2005-ben a BS 7799-2:1999 szabványt ISO/IEC 27001:2005 számon Informatika – Biztonsági technikák – Informatikai biztonsági irányítási rendszer – Követelmények címmel nemzetközi szabványnak fogadták el. Ezzel egyidejűleg átnevezték az ISO/IEC 17799:2005 szabványt, és ez lett az ISO/IEC 27002:2005 szabvány, azaz az informatikai rendszerek biztonságával foglalkozó ISO/IEC 27000 szabványcsalád első két eleme. Ez azért is jelentős esemény a szabvány történetében, mert létrehoztak egy egész szabványcsaládot, amelyben további, a kérdéskörhöz tartozó szabványok jelentek és jelennek meg. A sorozat számozása az ISO Informatikai Munkabizottsága (JTC1) illetékes albizottságának (IT Security techniques), az SC27-nek a számából eredt.

A szabvány 2013-as kiadása óta a kiberbűnözés egyre súlyosabbá és kifinomultabbá vált, nőtt a kibertámadások száma. A globális kiberbiztonsági kihívások kezelése érdekében 2022. februárban megjelent az új ISO/IEC 27002, majd 2022. október 25-én az új ISO/IEC 27001 szabvány is.

Amíg korábban az ISO/IEC 27xxx szabványsorozat az informatikai biztonság (Information technology – Security techniques) területén támogatta a felhasználókat, addig 2022-től már új megközelítésben és ehhez igazított új címmel jelennek meg a sorozat szabványai. Az új cím: *Információbiztonság, kiberbiztonság és a magánélet védelme* (*Information security, cybersecurity and privacy protection*). Ezzel együtt az ISO/IEC nemzetközi szabványügyi szervezetek JTC1 munkabizottságának SC27 albizottsága 2022-ben az *Information security, cybersecurity and privacy protection* nevet kapta. [23]

Az ISO/IEC 27000 szabványsorozat kifejezetten a felhasználók számára nyújt segítséget egy, a teljes szervezetet és minden rendszerelemet átfogó információbiztonság-menedzsment rendszer megvalósításához és ellenőrzéséhez az erre vonatkozó követelményrendszer kidolgozásával. [2]

Az ISO/IEC 27000 szabványcsalád a nemzetközileg legelterjedtebb, szervezeti szintű információbiztonsági, kiberbiztonsági és adatvédelmi keret, amelyre világszerte több tízezer tanúsított információbiztonsági irányítási rendszer és még több, tanúsítás nélkül bevezetett

rendszer épül. A sorozat célja nem csupán az, hogy „szabályokat” írjon elő, hanem hogy egységes fogalmi keretet, irányításimodell-logikát és a gyakorlatban is alkalmazható intézkedéskatalógust adjon azoknak a szervezeteknek, amelyek kockázatalapú módon szeretnék kezelni információbiztonsági kockázataikat.

AZ ISO/IEC 27000-es sorozat logikája jól illeszkedik a modern szabályozási környezethez: az EU NIS2 irányelve „kockázatokkal arányos”, dokumentált és folyamatosan felülvizsgált védelmi intézkedéseket követel meg anélkül, hogy tételes műszaki listát írna elő. [11] Az ISO/IEC 27001-re épülő Információbiztonsági Irányítási Rendszer ehhez ad olyan keretet, amelyet a hatóságok, auditorok és iparági partnerek világszerte értenek és elismernek.

Az ISO és az IEC közös JTC 1 Information Technology bizottságának **SC 27 Information security, cybersecurity and privacy protection** albizottsága kifejezetten az információbiztonság, kiberbiztonság és adatvédelem szabványosításáért felel. Feladatai közé tartozik az ISO/IEC 27000-es sorozat karbantartása és fejlesztése, a kriptográfiai szabványok, az identitás- és hozzáférés-kezelés, valamint az adatvédelmi szabványok kidolgozása. [2]

Az SC 27 több munkacsoportba (Working Group) szervezi tevékenységét. A munkacsoportok külön-külön is foglalkoznak, például:

- az információbiztonsági irányítási rendszerekkel (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005);
- a technológiaspecifikus szabványokkal (felhő, IoT, ellátási lánc);
- az adatvédelmi és magánszféra-védelmi követelményekkel (ISO/IEC 27701). [2]

A szabványtervezetek többlépcsős folyamatban haladnak a véglegesítés felé (working draft, committee draft, draft international standard, final draft international standard), amelyben a tagországok szakértői szavazással és kommentekkel vesznek részt. [2]

Bár az SC 27 formálisan szabványügyi testület, nem légüres térben működik: szoros, kétirányú kapcsolatban áll olyan szervezetekkel, mint az ENISA, a NIST és a tagállami kiberbiztonsági hatóságok. Az ENISA sok jelentésében az ISO/IEC 27001-re és kapcsolódó szabványokra hivatkozik mint a kiberbiztonság-irányítás *de facto* európai keretére. [11] A NIST több dokumentumában pedig összeveti saját keretrendszereit (például CSF, SP 800-53) az ISO/IEC 27001-gyel és ISO/IEC 27002-vel, jelölve az intézkedések és folyamatok közötti megfeleltetéseket.

A nemzeti intézmények – így a Magyar Szabványügyi Testület (MSZT) és a Nemzeti Kiberbiztonsági Intézet – részt vesznek az SC 27 munkájában, és a nemzetközi szabványok egy részét magyar nemzeti szabványként adják ki. Ez biztosítja, hogy a hazai jogszabályi környezetben hivatkozott elvárások és a gyakorlatban alkalmazott szabványok között ne legyen ellentmondás.

Az SC 27 által gondozott ISO/IEC 27000-es sorozat szorosan kapcsolódik más nemzetközi szabványcsaládokhoz is:

- az ISO/IEC 20000 sorozathoz az IT-szolgáltatásmenedzsment területén (incidenskezelés, változáskezelés, szolgáltatásfolytonosság);
- az IEC 62443-hoz az ipari és OT-környezetek kiberbiztonsága terén;
- az ISO/IEC 27701-hez és más adatvédelmi szabványokhoz a személyes adatok védelme szempontjából. [24]

A szabványcsaládban több tucat szabvány található, ezek közül néhány „gerinc” jellegű, mások speciális területekre koncentrálnak.

- **ISO/IEC 27000** – fogalmi és áttekintő szabvány – definiálja az alapfogalmakat (eszköz, kockázat, intézkedés, incidens stb.), tisztázza a sorozat elemei közötti kapcsolatot.
- **ISO/IEC 27001** – az Információbiztonsági Irányítási Rendszer kialakításának, működtetésének és folyamatos fejlesztésének követelményszabványa – ez a tanúsítás közvetlen tárgya.
- **ISO/IEC 27002** – részletes intézkedéskatalógus, amely irányelveket ad az ISO/IEC 27001 mellékletében szereplő intézkedések kialakításához és működtetéséhez.
- **ISO/IEC 27005** – információbiztonsági kockázatkezelési módszertan – támogatja az ISO/IEC 27001 kockázatalapú megközelítését.
- **ISO/IEC 27011** – információbiztonsági intézkedések az ISO/IEC 27002 szabvány alapul alapján kézikönyv a telekommunikációs szervezetek. [25]
- **ISO/IEC 27032** – iránymutatásokat ad a kiberbiztonság javítására, különös tekintettel a kibertérben (internetes rendszerekben) található adatok és infrastruktúra védelmére. [26]
- **ISO/IEC 27035** – strukturált keretrendszer az információbiztonsági incidensek, sebezhetőségek és események kezeléséhez. [27]
- **ISO/IEC 27701** – a Személyes Adatok Kezelésének Információbiztonsági Rendszere (Privacy Information Management System, PIMS). Útmutatást nyújt a személyazonosításra alkalmas adatok (PII) kezelésére és védelmére szolgáló rendszer létrehozásához, működtetéséhez és fejlesztéséhez. Ez a szabvány az ISO/IEC 27001 és az ISO/IEC 27002 szabványok kiterjesztése, célja a szervezetek segítése az adatvédelmi törvényeknek, például a GDPR-nak való megfelelésben.
- **ISO/IEC 27799** – információbiztonsági menedzsment az egészségügyben az ISO/IEC 27002 szabvány alkalmazásával. [28]
- **Speciális kiterjesztések** – például a felhőszolgáltatásokra, ellátási láncra, OT-környezetre, adatvédelemre vagy IoT-re vonatkozó szabványok, amelyek ugyanarra az alaplogikára épülnek, de egy adott szektorra, technológiára vonatkozó részleteket adnak.

A gyakorlatban a legtöbb szervezet számára az ISO/IEC 27001–27002–27005 hármasa jelenti az alapot. Ezekre épülhetnek rá a speciális szabványok ott, ahol a szervezet tevékenysége (például energiatermelés, felhőszolgáltatás, egészségügy) indokolja a részletek mélyebb kidolgozását.

3.2 Az ISO/IEC 27001:2022

Az ISO/IEC 27001 bevezetésével és ennek tanúsításával a szervezet bizonyítja az érdekelt feleknek és az ügyfeleknek, hogy elkötelezett az információk biztonságos kezelése iránt.

AZ ISO/IEC 27001:2022 szabvány alapvető célja bevezetni és fenntartani az Információbiztonsági Irányítási Rendszert, amelynek alapvető célja az információk *bizalmasság*ának, *sértetlenség*ének és *rendelkezésre állás*ának fenntartása. Az IBIR egy általános irányítási rendszer, amely az üzleti kockázatelemzésen alapul, megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot. A szabvány felhasználóinak a biztonsági követelményeket, intézkedéseket a szervezet üzleti céljaiból és stratégiájából kell levezetniük. A szabvány a megfelelőségi és ellenőrzési követelményei alapján elvégezhető az informatikai (információs) rendszer tanúsítása. [29]

Az ISO/IEC 27002 szabvány teljes szervezetre vonatkozó, az összes rendszerelemcsoportot átölelő információbiztonsági követelményeket és védelmi intézkedéseket tartalmaz a teljes körű információbiztonság megteremtéséhez.

Az ISO/IEC 27001:2022 szabvány kimondja, hogy a gyorsan változó környezetben a kiberbiztonsági kihívások kezelése érdekében a szervezeteknek fokozniuk kell ellenálló képességüket, és erőfeszítéseket kell tenniük a kiberfenyegetések mérséklésére, és a vezetőknek stratégiai megközelítést kell alkalmazniuk a kiberkockázatokkal kapcsolatban. A szabvány holisztikus megközelítése azt jelenti, hogy az egész szervezetet, a személyeket, a technológiát és a folyamatokat is lefedi, nem csak az informatikát. Olyan alapelvek, mint a bizalmasság, sértetlenség és rendelkezésre állás kockázatarányos védelme változatlanul megmaradtak, de ezt a 2022-es új szabvány kiterjesztette a papíralapú és felhőalapú adatkezelésre is. A fő célkitűzések közé tartozik a **kibertámadásokkal szembeni ellenálló képesség**, a **kiberreziliencia** növelése. A szabvány szerint a kiberrezilienciát alkalmazó szervezetek gyorsan vezető szerepet töltenek be iparágukban. [30]

Az Információbiztonsági Irányítási Rendszer akkor hatékony, ha hasznos a szervezet számára. Az információs rendszereket érintő biztonsági intézkedések megvalósítása nemcsak költséget jelent a szervezet számára, hanem segít a károk megelőzésében, csökkentésében, a kárfelszámolás meggyorsításában, és sikeressé teheti a szervezetet. [12]

Az ISO/IEC 27001 szabványban meghatározott Információbiztonsági Irányítási Rendszer egy általános irányítási rendszer, amely az üzleti kockázat elemzésén alapul, megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot. Az IBIR magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési tevékenységeket, a felelősségeket, a gyakorlatokat, az eljárásokat, a folyamatokat és az erőforrásokat. Az IBIR akkor hatékony, ha hasznos a szervezet számára.

„Az IBIR létrehozása és működtetése ugyanolyan megközelítést igényel, mint sok más irányítási rendszer. Az ISO 27001-es szabvány erre a célra az OECD (Organisation for Economic Co-Operation and Development: Gazdasági Együttműködési és Fejlesztési Szervezet) által is támogatott PDCA (Plan-Do-Check-Act: Tervezés-Végrehajtás-Ellenőrzés-Beavatkozás, TVEB) folyamatmodell használatát vezette be az Információbiztonsági Irányítási Rendszere fejlesztésének, megvalósításának és hatékonyságának biztosítására. Ezek a folyamatok lefedik a teljes tevékenységi ciklust, az effektív információbiztonság irányítását célozzák meg egy folytonos fejlesztési programon keresztül.

A PDCA bármilyen műveletre, tevékenységre, folyamatra, rendszerre, működtetésre, koncepcióra, elgondolásra vonatkoztatható, zárt hatásláncú, folytonosan ismétlődő körfolyamat-elv. A nemzetközi szakirodalomban elterjesztőjéről, W. Edwards Demingről elnevezve Deming-ciklusnak (Deming's Cycle) is nevezik." [31]

A PDCA-modell négy szakaszból áll [32]:

1. **Tervezés (Plan)** (Az Információbiztonsági Irányítási Rendszer létrehozása): A szervezet általános szabályainak megfelelő biztonságpolitika, célok, módszerek, folyamatok és eljárások meghatározása, amelyek relevánsak a kockázatkezelés és az információbiztonság fejlesztése szempontjából.
2. **Végrehajtás (Do)** (Az Információbiztonsági Irányítási Rendszer bevezetése és működtetése): A biztonsági szabályzat, intézkedések, módszerek és eljárások megvalósítása és üzemeltetése.
3. **Ellenőrzés (Check)** (Az Információbiztonsági Irányítási Rendszer ellenőrzése és felülvizsgálata): Fel kell becsülni és – ahol alkalmazható – fel kell mérni a biztonságpolitika végrehajtásának folyamatát, a célok és a gyakorlati tapasztalatok alapján az eredményeket a vezetés számára jelenteni kell.

4. **Beavatkozás (Act)** (Az Információbiztonsági Irányítási Rendszer továbbfejlesztése és karbantartása): A vezetői felülvizsgálat eredményén alapuló korrigáló és megelőző intézkedéseket kell hozni, illetve folyamatosan tovább kell fejleszteni az Információbiztonsági Irányítási Rendszert.

A fokozódó kiberbiztonsági kihívások kezelése érdekében a szervezeteknek fokozniuk kell ellenálló képességüket, és erőfeszítéseket kell tenniük a kiberfenyegetések mérséklésére. Az ISO/IEC 27001 a következőképpen hoz hasznot szervezetének:

- Biztonságos információ minden formában, beleértve a papíralapú, felhőalapú és digitális adatokat is.
- Növeli a kibertámadásokkal szembeni ellenálló képességet.
- Olyan központilag kezelt keretrendszert biztosít, amely minden információt egy helyen biztosít.
- Biztosítja az egész szervezetre kiterjedő védelmet, beleértve a technológiai kockázatokat és más fenyegetéseket is.
- Reagál a fejlődő biztonsági fenyegetésekre.
- Csökkenti a nem hatékony védelmi technológia költségeit és kiadásait.
- Védi az adatok bizalmasságát, sértetlenségét és rendelkezésre állását.

Az ISO/IEC 27001:2022 verzió szerkezete a közös „High Level Structure” (Annex SL) mintát követi, amelyet más irányítási rendszerszabványok, például a minőségirányítás (ISO 9001), az IT-szolgáltatásmenedzsment (ISO/IEC 20000), üzletmenet-folytonosság (ISO 22301) is alkalmaznak. Ez megkönnyíti az integrált irányítási rendszerek kialakítását, amikor a szervezet egyszerre kíván minőségirányítási, információbiztonsági és esetleg szolgáltatásirányítási tanúsítással rendelkezni. [33]

A szabvány fő fejezetei (a bevezető és fogalmi részek után) a következők:

- A szervezet kontextusa (érdekelt felek, hatókör, külső-belső tényezők).
- Vezetői szerepvállalás, politika és felelősségek (az információs rendszerek védelme elsődlegesen vezetői probléma).
- Tervezés: kockázatok és lehetőségek kezelése, információbiztonsági célok.
- Támogató folyamatok: erőforrások, kompetencia, tudatosság, kommunikáció, dokumentált információk kezelése.
- Működés: kockázatkezelési folyamat, intézkedések bevezetése és működtetése.
- Teljesítményértékelés: monitorozás, mérés, belső audit, vezetőségi átvizsgálás.
- Fejlesztés: eltérések, helyesbítő tevékenységek, folyamatos fejlesztés.

A szabvány *A melléklet*e tartalmazza a lehetséges információbiztonsági intézkedések listáját, hogy a felhasználók ne hagyják figyelmen kívül a szükséges információbiztonsági intézkedéseket. A 2022-es kiadásban az intézkedések 4 fő csoportba lettek szervezve:

5. Adminisztratív védelem (Organizational controls);
6. Személyi védelem (People controls);
7. Fizikai védelem (Physical controls);
8. Logikai védelem (Technological controls).

Az *A melléklet* intézkedései megegyeznek az ISO/IEC 27002:2022 szabvány 5–8. szakaszában felsoroltakkal – ezért is kezdődik 5-tel a számozás. Ezeket az intézkedéseket a kockázatkezeléssel összefüggésben kell felhasználni. Az *A melléklet*ben felsorolt információbiztonsági intézkedéseket a szabvány nem tekinti teljes körűnek, és szükség esetén további információbiztonsági intézkedések is beépíthetők. Ez a gyakorlatban nagyobb rugalmassá-

got ad a kockázatalapú védelmi intézkedések kiválasztásához, ugyanakkor azt is jelenti, hogy a szervezeteknek át kell tekinteniük, hogyan illeszkednek a meglévő intézkedéseik az új struktúrába.

3.3 A 27001 bevezetése

Noha a szabvány tudatosan nem ír elő „projektmodellt", a gyakorlatban a legtöbb bevezetés ilyen fázisokból áll:

1. **Helyzetfelmérés és gap-analízis** – a meglévő szabályozás, folyamatok, technikai intézkedések, szerződések és dokumentáció összevetése az ISO/IEC 27001 követelményeivel, az eltérések (hiányosságok, gyenge pontok) azonosítása.
2. **Kontextus és hatókör meghatározása** – mely szervezeti egységek, folyamatok, rendszerek tartoznak az IBIR körébe, milyen külső és belső tényezők befolyásolják az információbiztonságot, kik az érdekelt felek, és milyen elvárásaik vannak.
3. **Kockázatkezelési módszertan kialakítása** – az ISO/IEC 27005 elveire építve: kockázati kritériumok (valószínűség, hatás, kockázati szintek), értékelési módszer (kvalitatív, kvantitatív vagy hibrid), döntési szabályok. A szervezetnek meg kell határoznia és alkalmaznia kell egy információbiztonsági kockázatkezelési folyamatot. Ennek során:
   - kiválasztja a megfelelő információbiztonsági kockázatkezelési lehetőségeket, figyelembe véve a kockázatértékelés eredményeit;
   - meghatározza az összes intézkedést, amely a választott információbiztonsági kockázatkezelési lehetőség(ek) megvalósításához szükséges;
   - Alkalmazhatósági nyilatkozatot kell készíteni, amely tartalmazza:
     - ⇨ a szükséges védelmi intézkedéseket;
     - ⇨ a felvételük indoklását;
     - ⇨ a szükséges intézkedéseket végrehajtották-e vagy sem, és
     - ⇨ az A mellékletben szereplő intézkedések esetleges kizárásának indoklását.
   - információbiztonsági kockázatkezelési tervet készít, és
   - beszerzi a kockázattulajdonosok jóváhagyását az információbiztonsági kockázatkezelési tervhez és a fennmaradó információbiztonsági kockázatok elfogadását. A szervezetnek meg kell őriznie a dokumentált információkat az információbiztonsági kockázatkezelési folyamatról.
4. **Kockázatelemzés és -értékelés** – eszközök, fenyegetések, sebezhetőségek és hatások azonosítása, kockázatok felmérése és prioritássorrend meghatározása.
5. **Intézkedések kiválasztása és az Alkalmazhatósági Nyilatkozat elkészítése** – annak rögzítése, hogy mely intézkedéseket alkalmazza a szervezet, melyeket nem, és mi ennek az indoka, az intézkedések kapcsolása a kockázatokhoz.
6. **Szabályozás és eljárások kidolgozása** – biztonságpolitika, információbiztonsági szabályzat, részszabályzatok (hozzáférés-kezelés, eszközkezelés, incidenskezelés stb.), eljárások, irányelvek, formanyomtatványok.
7. **Megvalósítás és tudatosítás** – technikai megoldások bevezetése vagy finomhangolása, szerepkörök kijelölése, képzések, kommunikáció.
8. **Belső auditok és vezetőségi átvizsgálás** – az IBIR működésének értékelése, hiányosságok feltárása, fejlesztési döntések.
9. **Tanúsító audit** – független tanúsító szervezet általi vizsgálat, megfelelőség esetén tanúsítvány kiadása, majd rendszeres felügyeleti auditok.

Az Információbiztonsági Irányítási Rendszer jól megtervezett bevezetése nemcsak „papíron” működő IBIR-t eredményez, hanem beépíti az információbiztonsági szempontokat a napi működésbe: a változáskezelés, beszállítói menedzsment, incidenskezelés, üzletmenet-folytonosság és humán erőforrás-folyamatok is ennek részei lesznek. [3]

3.4 ISO/IEC 27002

Az ISO/IEC 27002 nem egy tanúsítható szabvány, hanem részletes útmutató az ISO/IEC 27001 A mellékletében felsorolt védelmi intézkedések megvalósításához. A 2022-es kiadás az intézkedéseket tematikus csoportokba rendezve tárgyalja, mindegyikhez megadva:

- az intézkedés célját;
- az intézkedés megvalósításának lehetséges módjait;
- példákat, kiegészítő megfontolásokat;
- kapcsolódási pontokat más intézkedésekhez és szabványokhoz.

A szabvány részletesen leírást ad az ISO/IEC 27001 A mellékletében megadott védelmi intézkedésekhez. AZ ISO/IEC 27002 külön értéke, hogy támogatja **a védelmi intézkedések testreszabását**: ugyanaz az intézkedés másként fog kinézni egy kis szolgáltató cégnél és egy kritikus infrastruktúra-üzemeltetőnél, mégis mindkét esetben ugyanarra a magas szintű célra (például hozzáférés-korlátozás, naplózás, adatvédelmi követelmények) reagál. Sok szervezet az ISO/IEC 27002-t használja belső „checklistaként” a technikai és szervezési intézkedések tervezéséhez, auditjához.

Az ISO/IEC 27002:2022 A melléklete egy táblázatot tartalmaz, amely bemutatja az attribútumok használatát a vezérlőelemek különböző nézeteinek létrehozására. A táblázat oszlopai:

1. ISO/IEC 27002 alfejezet azonosító;
2. az alfejezet címe;
3. szabályozási típus;
4. információbiztonsági követelmények;
5. kiberbiztonsági feladatok;
6. működési képességek;
7. biztonsági tartományok.

Szabályozási típusok:
Ezzel az attribútummal a vezérlőelemek abból a szempontból tekinthetők át, hogy a vezérlőelem mikor és hogyan módosítja a kockázatot az információbiztonsági incidens előfordulása tekintetében.
#Preventive – megelőző (az információbiztonsági incidens bekövetkezésének megakadályozására szolgál);
#Detective – észlelő (az irányítás információbiztonsági incidens bekövetkezésekor működik);
#Corrective – javító (az információbiztonsági incidens bekövetkezte után lép fel).

Információbiztonsági követelmények:
Ezzel az attribútummal a vezérlőelemek abból a szempontból tekinthetők át, hogy a vezérlőelem az információ mely jellemzőinek megőrzéséhez járul hozzá.
#Confidentiality – bizalmasság;
#Integrity – sértetlenség;
#Availability – rendelkezésre állás.

Kiberbiztonsági feladatok:
Ezzel az attribútummal a vezérlőelemek az ISO/IEC TS 27110 szabványban leírt kiberbiztonsági keretrendszerben meghatározott kiberbiztonsági koncepciókhoz való társítás szempontjából tekinthetők át.
#Identify – azonosítás;
#Protect – védelem;
#Detect – észlelés;
#Respond – válasz;
#Recover – visszaállítás.

Működési képességek:
Ezzel az attribútummal a vezérlőelemek az információbiztonsági követelmények gyakorlata szempontjából tekinthetők át.
#Governance – irányítás;
#Asset_management – eszközkezelés;
#Information_protection – információvédelem;
#Human_resource_security – humanerőforrás-biztonság;
#Physical_security – rendszer- és hálózatbiztonság;
#System_and_network_security – rendszer- és hálózatbiztonság;
#Application_security – alkalmazás biztonság;
#Secure_configuration – biztonságos konfiguráció;
#Identity_and_access_management– azonosítás- és hozzáféréskezelés;
#Threat_and_vulnerability_ management – fenyegetés- és sérülékenységkezelés;
#Continuity – folytonosság;
#Supplier_relationships_security – szállítói kapcsolatok biztonsága;
#Legal_and_compliance – jog és megfelelőség;
#Information_security_event_management – információbiztonsági eseménykezelés;
#Information_security_assurance – információbiztonság biztosítása.

Biztonsági tartományok:
Ezzel az attribútummal négy információbiztonsági tartomány szempontjából vizsgálhatók a vezérlőelemek.
#Governance_and_Ecosystem – az információs rendszer biztonságának irányítása és kockázatkezelése és az ökoszisztéma kiberbiztonsági menedzsmentje;
#Protection – IT-biztonsági architektúra, IT-biztonsági adminisztráció, azonosítókezelés és hozzáférés-vezérlés, IT-biztonsági karbantartás és fizikai és környezeti biztonság;
#Defence – észlelés, biztonsági esemény kezelése;
#Resilience – műveletek folytonossága és válságkezelés.

A szabvány B melléklete *Az ISO/IEC 27002:2022 megfeleltetése az ISO/IEC 27002:2013 szabványnak* és *Az ISO/IEC 27002:2013 megfeleltetése az ISO/IEC 27002:2022 szabványnak* táblázatokkal tájékoztató jellegű információkat tartalmaz a szabvány korábbi verziója alapján bevezetett IBIR-hez.

3.5 ISO/IEC 27005

Az ISO/IEC 27005 részletes módszertani keretet ad a kockázatkezeléshez:

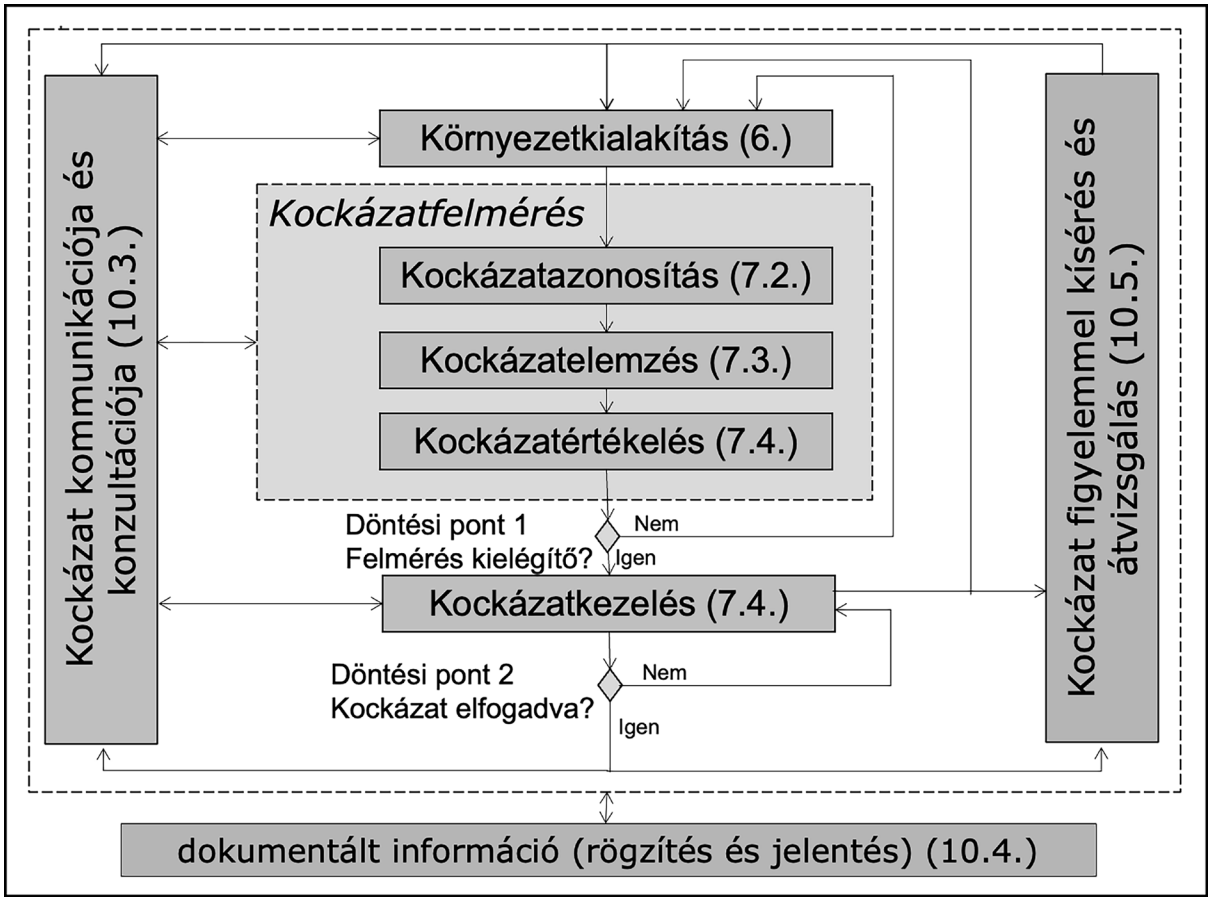
- olyan szervezeteknek, amelyek az ISO/IEC 27001 szabványnak megfelelő információbiztonsági irányítási rendszert (IBIR) kívánnak létrehozni és bevezetni;

- az információbiztonsági kockázatkezelést végző vagy abban részt vevő személyeknek (például IBIR-szakemberek, kockázattulajdonosok és más érdekelt felek);
- az információbiztonsági kockázatkezelési folyamatukat javítani szándékozó szervezeteknek.

A szabvány felépítése a következő:

- **Kontextus meghatározása** – szervezeti célok, hatókör, környezet, érdekelt felek, kockázati kritériumok.
- **Kockázatazonosítás** – eszközök, értékek, fenyegetések, sebezhetőségek, következmények.
- **Kockázatelemzés** – valószínűség és hatás becslése.
- **Kockázatértékelés** – kockázatok összevetése a kritériumokkal.
- **Kockázatkezelés** – opciók választása (csökkentés, elfogadás, átvállalás, elkerülés), kezelési tervek.
- **Kommunikáció és konzultáció – érintettek bevonása.**
- **Figyelemmel kísérés és felülvizsgálat** – a kockázati környezet és intézkedéskörnyezet változásainak követése.

A szabvány támogatja a kvalitatív (például skálás értékelés) és kvantitatív (például pénzben kifejezett kár, valószínűségi modellek) kockázatelemzési megközelítéseket is, a lényeg a következetesség és az átláthatóság. A NIS2 követelményrendszeréhez és a magyar kiberbiztonsági törvényhez jól illeszthető, mert elég részletes, továbbá segít dokumentáltan bemutatni, hogy a szervezet hogyan jutott el bizonyos védelmi intézkedések kiválasztásáig.



2. ábra A kockázatkezelés folyamata. ISO/IEC27005:2022 alapján készítette a szerző

Ha a kockázatfelmérés elegendő információt nyújt a kockázatok elfogadható szintre történő módosításához szükséges intézkedések hatékony meghatározásához, akkor a feladat befejeződött, és következik a kockázatkezelés. Ha az információ nem elegendő, a kockázatfelmérés újabb iterációját kell elvégezni. Ez magában foglalhatja a kockázatértékelés kontextusának megváltoztatását (például felülvizsgált hatókört), az adott területen szerzett szakértelem bevonását vagy a kockázat elfogadható szintre történő módosításához szükséges információk összegyűjtésének egyéb módjait.

A kockázatkezelés egy iteratív folyamatot foglal magában:
- kockázatkezelési lehetőségek megfogalmazása és kiválasztása;
- kockázatkezelés tervezése és végrehajtása;
- e kezelés hatékonyságának értékelése;
- annak eldöntése, hogy a fennmaradó kockázat elfogadható-e;
- további kezelésre, ha az nem elfogadható.

Lehetséges, hogy a kockázatkezelés nem vezet azonnal a fennmaradó kockázatok elfogadható szintjéhez. Ebben a helyzetben újabb kísérletet lehet végezni a további kockázatkezelés megtalálására, vagy a kockázatértékelés újabb iterációjára kerülhet sor, akár egészben, akár részben. Ez magában foglalhatja a kockázatértékelés kontextusának megváltoztatását (például egy átdolgozott hatókör) és a megfelelő területre vonatkozó szakértelem bevonását. A releváns fenyegetések vagy sebezhetőségek ismerete jobb döntéseket hozhat a megfelelő kockázatkezelési tevékenységekről a kockázatértékelés következő iterációjában.

A kockázatfelmérést és a kockázatkezelést a változások alapján rendszeresen frissíteni kell. A teljes kockázatértékelés és a frissítések két kockázatkezelési ciklusra oszthatók. A stratégiai ciklust hosszabb időre vagy jelentősebb változások bekövetkeztekor kell lefolytatni, míg a működési ciklusnak rövidebbnek kell lennie az azonosított és értékelt részletes kockázatoktól, valamint a kapcsolódó kockázatkezeléstől függően.

4. COMMON CRITERIA (ISO/IEC 15408 ÉS ISO/IEC 18045)

A Common Criteria for Information Technology Security Evaluation (Az információs technológia biztonságának értékelésére vonatkozó közös kritériumok, röviden CC) az informatikai termékek és rendszerek biztonsági értékelésére szolgáló nemzetközi keretrendszer, amelyet ma már az ISO/IEC 15408 szabványsorozat és az ISO/IEC 18045 értékelési módszertani szabvány ír le. [3] A CC célja, hogy egységes, összehasonlítható és auditálható módon tegye lehetővé a biztonsági funkciók és a hozzájuk kapcsolódó garanciális követelmények megfogalmazását, megvalósítását és független értékelését. Ez különösen fontos olyan környezetekben, ahol a termékek megbízhatósága kritikus (pénzügyi, közigazgatási, katonai, kritikus infrastruktúra), és a beszerzők nem tudnak minden egyes megoldást saját erőforrásból mélyen megvizsgálni.

A Common Criteria a bizalmasság, a sértetlenség, a hitelesség és a rendelkezésre állás védelmét jelöli meg az információbiztonsági követelmények és mechanizmusok értékelése alapjaként, továbbá ez alapján történik a rendszerek biztonsági szintjének meghatározása, valamint a biztonsági funkciók tervezése és validálása. Ez a megközelítés biztosítja, hogy az informatikai rendszerek és eszközök megvédhetők legyenek a jogosulatlan hozzáféréssel, módosítással, hamisítással és működésük megakadályozásával szemben.

A CC nem egy konkrét terméktípusra (például tűzfalra vagy intelligens kártyára) ír elő részletes követelményeket, hanem egy olyan „nyelvet” és modellkészletet ad, amelyben a különféle termékek biztonsági tulajdonságai és az azokra vonatkozó elvárások szabványos szerkezetben leírhatók. A részleteket védelmi profilok (Protection Profile, PP) és biztonsági célok (Security Target, ST) tartalmazzák, amelyek a gyártók, szabályozók vagy iparági konzorciumok által egy-egy termékkategóriára, vagy konkrét termékre megfogalmazott dokumentumok.

A CC kialakításának egyik legfontosabb motivációja az volt, hogy a korábbi, országonként eltérő termékértékelési rendszereket (például az amerikai TCSEC, az európai ITSEC) nehezen lehetett összehasonlítani, és a tanúsítások kölcsönös elismerése korlátozott volt. A Common Criteria egyrészt egységesítette a fogalomkészletet, másrészt olyan modellt vezetett be, amelyben:

- a biztonsági követelmények jól strukturált módon, újrahasznosítható „építőkockákból” állnak össze;
- a vizsgálati mélység és ráfordítás szintje (EAL1–EAL7) külön jelölhető;
- az értékelési eredmények nemzeti szinten tanúsítványként jelennek meg, de a CCRA (Common Criteria Recognition Arrangement, Megállapodás a Közös Kritériumokról) keretében kölcsönösen elismerhetők.

„A CCRA megállapodás résztvevői a következő célokat tűzték ki maguk elé:

1. biztosítani, hogy az információs technológiai (IT) termékek és védelmi profilok értékelése magas színvonalú és következetes szabványok szerint történjen, és hogy az értékelés jelentősen hozzájáruljon az említett termékek és profilok biztonságába vetett bizalom erősítéséhez;
2. javítani az értékelésen átesett, biztonságosabb IT-termékek és védelmi profilok elérhetőségét;
3. az informatikai termékek és védelmi profilok értékelésének megkettőzéséből adódó terhek kiküszöbölése;
4. az informatikai termékek és védelmi profilok értékelési és tanúsítási/érvényesítési folyamatának hatékonyságának és költséghatékonyságának folyamatos javítása.” [34]

„A megállapodás célja, hogy elősegítse e célok elérését oly módon, hogy olyan helyzetet teremt, amelyben a közös kritériumok szerinti tanúsítvánnyal rendelkező IT-termékek és védelmi profilok további értékelés nélkül beszerezhetők vagy használhatók. A megállapodás arra törekszik, hogy megalapozza a bizalmat az eredeti tanúsítvány alapjául szolgáló értékelések megbízhatóságában azáltal, hogy előírja, hogy a közös kritériumok szerinti tanúsítványokat kiadó tanúsító/érvényesítő szerveknek (CB) magas és következetes szabványoknak kell megfelelniük.” [34]

„A szabványban a funkcionális követelmények, bizonyossági követelmények és értékelési bizonyossági szintek (EAL) mátrixaként határozhatóak meg az alkalmazandó biztonsági követelmények. A követelmények konkretizálása céljából az általános, eszköz fajtájára jellemző védelmi profilok (Protection Profile, PP) alapján biztonsági célkitűzést (Security Target, ST) kell készíteni, amely már az eszköztípusra vonatkozó követelményeket tartalmazza, és ez alapján kerül megvalósításra maga a termék, a vizsgálat tárgya (Target of Evaluation, TOE).” [35]

A CC nem azt állítja, hogy egy EAL3-as tűzfal „biztonságosabb”, mint egy másik termék, hanem azt rögzíti, hogy az adott termék milyen követelmények mentén, milyen mélységben lett vizsgálva és dokumentálva. A biztonság „jó” vagy „elég” voltát továbbra is a kockázatkezelés és a felhasználási körülmények határozzák meg.

Az ISO/IEC 15408:2022 szabvány öt részből áll, amelyek együtt adják ki a Common Criteria „szabványosított nyelvét”:

1. rész: Bevezetés és általános modell – fogalmak, alapelvek, a CC alkalmazási területe, a TOE (Target of Evaluation) fogalma, a védelmi profil és biztonsági cél szerepe. [36]
2. rész: Biztonsági funkcionális követelmények (Security Functional Requirements, SFR) – osztályokba, családokba és komponensekbe rendezett funkcionális követelménykészlet. [37]
3. rész: Biztonsági garanciális követelmények (Security Assurance Requirements, SAR) – azokra a bizonyítékokra és tevékenységekre vonatkozó elvárások, amelyek igazolják, hogy a TOE valóban megvalósítja a megfogalmazott funkciókat. [38]
4. rész: Az értékelési módszerek és tevékenységek specifikációja (Framework for the specification of evaluation methods and activities) – objektív, megismételhető és reprodukálható értékelési módszereket és tevékenységeket tesz lehetővé, de nem mondja meg, hogyan kell értékelni, elfogadni vagy fenntartani magukat az értékelési módszereket. [39]
5. rész: A biztonsági követelmények előre definiált csomagjainak meghatározása (Pre-defined packages of security requirements) – segítenek az értékeléshez szükséges biztonsági követelmények meghatározásában. [40]

Az ISO/IEC 18045:2022 az értékelési módszertant (CEM – Common Evaluation Methodology) írja le, vagyis azt, hogyan kell a 15408 szabványokban megfogalmazott követelményeket a gyakorlatban vizsgálni és dokumentálni. A módszertan részletes útmutatást ad az értékelőknek a dokumentumelemzéstől a funkcionális teszteken át a sebezhetőségelemzésig. [41]

A CC-ben a vizsgálat tárgyát **TOE-ként** (Target of Evaluation) jelöljük. A TOE lehet szoftver (például operációs rendszer, alkalmazás), hardver (például kriptográfiai modul, intelligens kártya), vagy hardver-szoftver kombináció (például hálózati biztonsági átjáró). Fontos, hogy a TOE pontosan körülhatárolt legyen: a vizsgálat csak arra vonatkozik, ami a TOE definíciójában szerepel (verzió, konfiguráció, környezeti feltételek).

A CC fő jellemzői: [42]

- egységes követelményeket határoz meg, függetlenül a megvalósítás módjától;
- egységes kiértékelési módszert ad az informatikai rendszerek, termékek informatikai biztonsági értékeléséhez, tanúsításához;
- meghatározza az informatikai rendszerek biztonsági követelményeinek katalógusát, mely többszintű kategóriákból áll: osztály, család, komponens és elem;
- egyaránt felhasználható szoftver- és a hardverelemek vizsgálatához is;
- a termékek rugalmasan megválaszthatók, mert a követelmények nem hardver- vagy szoftverspecifikusak;
- a CC alapján kiértékelt informatikai rendszerek kiértékelésének eredménye egy dokumentum, amely kijelenti:
  - a rendszer egy adott védelmi profilnak való megfelelőségét;
  - adott biztonsági cél követelményeinek való megfelelést;
  - a definiált 7 biztonsági osztály (EAL1-7) valamelyikének való megfelelést;
- definiálható a biztonsági funkcionalitás, azaz a CC terminológiája szerint a védelmi profil (Protection Profiles: PP), amely függetlenül besorolható a meghatározott 7 biztonsági szint (Evaluation Assurance Level: EAL) valamelyikébe.

A CC dokumentumok két alapvető típusát különböztetjük meg: [43]

- **Protection Profile (PP)** – védelmi profil: egy termékfüggetlen, tipikus felhasználási esetet vagy termékkategóriát leíró dokumentum, amely egységes lehetőséget ad hasonló megoldások összehasonlítására (például tűzfalakra, intelligens kártyákra vagy e-aláíró eszközökre vonatkozó PP).
- **Security Target (ST)** – biztonsági cél: egy konkrét TOE biztonsági céljait és követelményeit leíró dokumentum, amely hivatkozhat egy vagy több PP-re, de akár önállóan is megfogalmazható.

A védelmi profil általában olyan elvárt tulajdonságokat rögzít, amelyek egy adott termékkategórián belül „elvárt minimumként” jelennek meg. A gyártó biztonsági célja megmutatja, hogy a konkrét termék hogyan elégíti ki ezeket a követelményeket, illetve milyen többletfunkciókat valósít meg.

A védelmi profil egy implementációfüggetlen funkcionális biztonsági követelményrendszert és objektumhalmazt határoz meg egy-egy terméktípusra vagy kategóriára, kielégítve a felhasználók informatikai biztonsági követelményeit. A **PP** újra felhasználható, a kifejlesztése során cél volt a funkcionális szabványok támogatása és a megvalósítás, kifejlesztés támogatása a fejlesztési specifikációkkal. A CC tartalmaz néhány védelmi profilt (nagyrészt a tűzfalakra), de korántsem minden területre, vagyis a **védelmi profilok még nem teljesek!** A hiányzó területekre vonatkozó védelmi profilok elkészítése még várat magára. A védelmi profilokat meghatározhatják a fejlesztők, amikor a biztonsági specifikációt

létrehozzák, illetve a nagyobb felhasználói szervezetek is definiálhatnak a számukra fontos területre vonatkozó védelmi profilt a CC-ben meghatározott követelményeket betartva. Példák védelmi profilokra: [35]

- Üzleti rendszerek biztonsága 1.: Kisebb termelői rendszerek alapszintű, ellenőrzött hozzáférés-védelme.
- Üzleti rendszerek biztonsága 3.: Adatbázis-kezelő rendszerek, többfelhasználós operációs rendszer környezetben. A felhasználóazonosítás egyedi, a hozzáférésjogosultságrendszer szerepkörökön alapul.
- Különböző tűzfalak védelmi profiljai:
  - Hálózati/szállítási szinten működtetett csomagszűrő tűzfal.
  - Application Gateway tűzfal.
  - USA Kormányzati tűzfal.

A CC funkcionális követelményrendszere gyakorlatilag egy funkcionális komponens-katalógus, amelyből összeállítható a vizsgált rendszerre (*Target of Evaluation, TO*E) vonatkozó funkcionális biztonsági követelményrendszer. A követelmények *osztályok*ra, azon belül *család*okra oszlanak. A családokon belül a komponensek már egyedi, konkrét követelményeket fogalmaznak meg. A gyakorlati megvalósításban egyes komponensek egy-egy csoportját, amelyek akár különböző osztályokból származhatnak, „összecsomagolják". A biztonsági követelmények **biztonsági osztályokba (*security assurance*)** vannak sorolva, elsősorban a forrásként használt követelményrendszerekkel való kompatibilitás, összehasonlíthatóság miatt. [35]

A Common Criteria egyik sajátossága, hogy a követelményeket két nagy csoportra osztja: funkcionális (SFR) és garanciális (SAR) követelményekre.

- A **funkcionális követelmények** a TOE-tól elvárt biztonsági viselkedést írják le: például hozzáférés-ellenőrzés, azonosítás és hitelesítés, auditálás, kriptográfiai funkciók, adatintegritás, megbízható csatornák. Ezeket osztályokba (például „Access Control"), azon belül családokba és komponensekbe rendezve adja meg a szabvány.
- A **garanciális követelmények** a TOE fejlesztési, dokumentációs, tesztelési és életciklus-folyamataira vonatkoznak. Ide tartozik például a fejlesztési dokumentáció részletezettsége, a konfigurációmenedzsment, a tesztelések mélysége, a sebezhetőségelemzés módszere, a gyártói minőségbiztosítás és a szállítási folyamatok védelmi intézkedései.

A gyakorlati CC-projektekben nagy munka a biztonsági célokhoz illeszkedő SFR/SAR-készlet kiválasztása, majd a megfelelő bizonyítékok előállítása. Egy magasabb EAL-szint eléréséhez nemcsak több funkcionális követelményt kell teljesíteni, hanem lényegesen szigorúbb dokumentációs és tesztelési elvárásoknak is meg kell felelni.

Az ISO/IEC 15408-2:2022 (CC Part 2) szabványban van leírva a 11 fő funkcionális osztály (Security Functional Classes), amelyek a TOE (Target of Evaluation) biztonsági funkcióit szervezik családokba és komponensekbe. Ezek hierarchikusan épülnek fel, függőségekkel, és alkotják a Security Functional Requirements (SFR) katalógusát. Ezek a következők:

- FAU: Security audit – Biztonsági átvilágítás. Auditálási funkciók, beleértve események rögzítését, elemzését és védelmét.
- FCO: Communication – Kommunikáció. A kommunikáció biztosítása, különösen letagadhatatlansági mechanizmusokkal.
- FCS: Cryptographic support – Kriptográfiai támogatás. Kulcskezelés, algoritmusok és random generálás.

- FDP: User data protection – Felhasználói adatok védelme. Hozzáférés- és információáramlás-vezérléssel.
- FIA: Identification and authentication – Azonosítás és hitelesítés. Felhasználók kezelése és hibakezelés.
- FMT: Security management – Biztonságirányítás. Biztonsági politika és funkciók kezelése, statikus/dinamikus döntéshozatal.
- FPR: Privacy – Adatvédelem. Adatvédelmi funkciók, személyes adatok anonimizálása és pszeudonimizálása.
- FPT: Protection of the TSF – A TSF védelme. TOE önvédelmi funkciói, belső integritás és szolgáltatásbiztonság.
- FRU: Resource utilisation – Erőforrás-felhasználás. Erőforrás-felhasználás priorizálása és korlátozása prioritási szinteken.
- FTA: TOE access – TOE-hozzáférés. TOE-hozzáférés korlátozása, felhasználói és adminisztrátori limitálással.
- FTP: Trusted path/channels – Bizalmi útvonal/csatornák. Megbízható kommunikációs csatornák és utak biztosítása.

Ezek az osztályok EAL (Evaluation Assurance Level) tanúsítványok alapját képezik, kiterjeszthetők.

Minden osztályban több család van, és családonként több komponens, amelyeket a következő módon jelölünk: FAU_ARP.1 Minden komponens egy adott követelményt fejt ki. „A garancia az alapja annak a bizalomnak, hogy egy IT-termék vagy -rendszer kielégíti biztonsági céljait. A garancia származtatható az olyan forrásokra hivatkozásból, mint a meg nem erősített állítások, az idevágó korábbi vagy speciális tapasztalatok. Azonban e szabvány az aktív vizsgálatok révén nyújt garanciát. Az aktív vizsgálat az IT-termék vagy -rendszer olyan értékelését jelenti, amely meghatározza annak biztonsági tulajdonságait.” [36]

A CC Part 3 (Security assurance components) 9 fő garanciaosztályt (assurance classes) tartalmaz, amelyek hierarchikusan szerveződnek családokba és komponensekbe, így alkotják a SAR (Security Assurance Requirements) katalógust:

- ACE: Automated component evaluation – Automatizált értékelési komponensek.
- ACO: Automated component observability – Automatizált megfigyelhetőségi komponensek.
- ADV: Development – Fejlesztési bizonyítékok (ADV_ARC, ADV_FSP, ADV_INT, ADV_IMP, ADV_TDS).
- AGD: Guidance documents – Útmutató dokumentumok (AGD_OPE, AGD_PRE).
- ALC: Life-cycle support – Életciklus-támogatás (ALC_CMC, ALC_CMS, ALC_DEL, ALC_DVS, ALC_FLR, ALC_LCD).
- ASE: Security Target evaluation – Biztonsági célok értékelése (ASE_CCL, ASE_ECD, ASE_INT, ASE_OBJ, ASE_REQ, ASE_SPD, ASE_TSS).
- ATE: Tests – Tesztelés (ATE_COV, ATE_DPT, ATE_FUN, ATE_IND).
- AVA: Vulnerability assessment – Sebezhetőség-értékelés (AVA_VAN).
- ACS: Automation on security – Biztonsági automatizálás komponensek.

Ezekből épülnek fel az EAL csomagok (EAL1–EAL7), PP/ST-k alapján válogatva.

Az EAL (Evaluation Assurance Level) szint azt jelöli, hogy a TOE milyen mélységű értékelésen esett át, illetve mennyi erőforrást és mennyi időt fordítottak a vizsgálatra.

- **EAL1 – Functionally Tested/**Funkcionálisan tesztelt:
  Minimális – gazdaságossági megfontolásokkal indokolható – védelmi szint, kisebb koc-

kázatú környezetre. Csak a legnyilvánvalóbb hibákat detektálja a lehető legkisebb költséggel. Kicsi az esélye annak, hogy a rejtett gyengeségek kiderüljenek.

- **EAL2 – Structurally Tested**/Strukturálisan tesztelt:
  A létező szabványok megfelelő alkalmazásával, kellő odafigyeléssel minimálisan növelt fejlesztői ráfordítási költséggel megvalósítható védelmi szint, mérsékelt biztonsági igényekhez. Olyan esetben használható, ha a TOE (védett objektum) alacsony vagy közepes védelmi szintet igényel, ugyanakkor a fejlesztés teljes folyamata nem elérhető, nem befolyásolható.
- **EAL3 – Methodically Tested and Checked**/Módszertanilag tesztelt és ellenőrzött:
  Közepes szintű, de alaposan ellenőrzött védelmi igények esetén megkövetelt védelmi szint. Jellemzője a „szürke doboz" tesztelés, jelentős dokumentációs és fejlesztési követelményekkel.
- **EAL4 – Methodically Designed, Tested and Reviewed**/Módszertanilag tervezett, tesztelt és auditált:
  Gazdaságossági szempontból valószínűleg ez a még elérhető legmagasabb védelmi szint. Gyakorlati maximum sok kereskedelmi termék számára. Átfogó dokumentáció, szigorú, biztonsági szempontokat figyelembe vevő, tervszerű, de nem túlságosan specializált tervezési folyamat és tesztelés jellemzi.
- **EAL5 – Semi-formally designed and tested**/Félformális módszerrel tervezett és tesztelt:
  Már a rendszer tervezése is az EAL5 szintű biztonsági követelmények kielégítése céljából történik. Magas biztonsági igényű fogyasztási cikkek, például a hardveres kriptopénztárcák esetén alkalmazzák.
- **EAL6 – Semi-formally verified design and tested**/Félformális módon ellenőrzött tervezés és tesztelés:
  Csak speciális biztonsági tervezési, fejlesztési technikákkal megvalósítható biztonsági szint, ami célszerűen biztonsági termékek tervezésénél és magas kockázatú rendszereknél alkalmazható. Magas kockázatú helyzetekre tartják fenn.
- **EAL7 – Formally verified design and tested**/Formálisan ellenőrzött tervezés és tesztelés:
  Az elméletileg még megvalósítható lehető legmagasabb védelmi szint. Gyakorlatilag csak kísérleti jellegű, jól definiálható funkcionalitással rendelkező, magasabb, részben speciális (például katonai) biztonsági igényű rendszerek esetén, különösen érzékeny környezetekben valósítható meg, ahol a biztonsági incidensek költsége rendkívül magas. Formális módszerekkel, rendkívül részletes dokumentációval kell rendelkezni.

A „**+**" kiterjesztés (EALn+) azt jelzi, hogy a termék a szabványos EAL-on túl további, speciális biztonsági követelményeknek is megfelel, például a fokozott sebezhetőségi elemzésnek.

A tanúsítási költségek több komponensből állnak: fejlesztési költségek, értékelési díjak és tanúsítási díjak, melyek a TOE összetettségétől, bonyolultságától, az értékelés hosszától és az EAL szintjétől függenek. Az értékelés általában 6–18 hónapig tart, különösen az EAL4-es vagy magasabb szintek esetén. Az értékelési és tanúsítási díj tipikusan **több százezer dollár**, különösen az EAL4+ vagy EAL5 szinteken, ahol részletes kódellenőrzések és átfogó sérülékenységvizsgálatok szükségesek. [44]

Fontos hangsúlyozni, hogy az EAL-szint **nem a biztonság „értékét" méri**, hanem az értékelés mélységét. Egy rosszul definiált követelménykészlettel rendelkező EAL4-es termék valós kockázati szempontból gyengébb lehet, mint egy jól célzott, kisebb hatókörű EAL2-es megoldás, ha az adott felhasználási környezetben az utóbbi jobban illeszkedik az igényekhez.

A CC-alapú tanúsítás folyamatában három fő szereplő vesz részt:

- **Fejlesztő/gyártó** – elkészíti a TOE-t és a hozzá tartozó dokumentációt (ST, design dokumentumok, tesztleírások, felhasználói és adminisztrátori dokumentáció).
- **Értékelő laboratórium** – akkreditált, független szervezet, amely a CC és az ISO/IEC 18045 alapján végzi az értékelést.
- **Tanúsító hatóság** – nemzeti szintű szervezet, amely jóváhagyja az értékelési jelentést, és kiadja a tanúsítványt.

A folyamat általános lépései:

1. A termék behatárolása, TOE-definíció és a Security Target kialakítása.
2. Az ST jóváhagyása (labor és tanúsító hatóság részéről) – ez lesz az értékelés „szerződése”.
3. A fejlesztő átadja a szükséges dokumentációt és tesztelési információkat.
4. Az értékelők dokumentációelemzést végeznek, majd funkcionális teszteket és sebezhetőségelemzést hajtanak végre.
5. Az eredmények alapján megállapítják, hogy a TOE megfelel-e az ST-ben megfogalmazott követelményeknek a választott EAL-szinten.
6. Pozitív eredmény esetén a tanúsító hatóság tanúsítványt ad ki, amelyet a CCRA tagjai meghatározott feltételekkel elismernek.

A tanúsítvány általában tartalmazza a TOE megnevezését, a vizsgált konfigurációt, az EAL-szintet, a védelmi profilokra való hivatkozásokat, az értékelés korlátait és a felhasználási feltételeket. Ezeket a tanúsítványokat a Common Criteria Portal nyilvánosan közzéteszi, ami átláthatóságot biztosít a beszerzők és auditorok számára. [3]

A CC-tanúsítás tipikusan olyan területeken jelenik meg, ahol a termékek biztonsági tulajdonságai közvetlenül kapcsolódnak jogszabályi vagy iparági követelményekhez:

- operációs rendszerek biztonsági funkciói;
- hálózati biztonsági eszközök (tűzfalak, VPN-átjárók, behatolásmegelőző rendszerek);
- kriptográfiai modulok, biztonságos kulcstárolók;
- intelligens kártyák, biztonságos elemek (például e-ID, bankkártyák, hozzáférési kártyák);
- speciális közigazgatási vagy védelmi célú alkalmazások.

Számos országban a közbeszerzési szabályok, ágazati rendeletek vagy belső irányelvek előírják, hogy bizonyos termékkategóriák esetében – különösen kritikus infrastruktúra vagy államigazgatási környezetben – csak meghatározott EAL-szinten tanúsított termékek szerezhetők be. Magyarországon is megjelentek már olyan gyakorlatok, ahol a CC-tanúsítás az ajánlatok elbírálásának egyik minőségi szempontja, különösen hitelesítésszolgáltatások, biztonságos eszközök és hálózati védelmi komponensek területén.

A Common Criteria nem helyettesíti az olyan irányítási rendszerszabványokat, mint az ISO/IEC 27001, hanem kiegészíti azokat a **termékszintű bizonyítottság** oldaláról. Egy ISO/IEC 27001 szerint tanúsított szervezet meg tudja mutatni, hogy folyamatai, szabályozása és kockázatkezelése megfelel bizonyos követelményeknek. A CC-tanúsított termék azt igazolja, hogy egy konkrét komponens biztonsági funkcióit függetlenül megvizsgálták. A kettő együtt erős bizalmi alapot adhat a partnereknek és a felügyeleti hatóságoknak.

Az IEC 62443 ipari, OT-környezetben hasonló logikát követ: rendszerszintű és komponensszintű követelményeket fogalmaz meg, amelyekből később CC-kompatibilis védelmi profilok is levezethetők. Emellett a NIST SP 800-53 és más intézkedéskatalógusok is gyakran szolgálnak inspirációként a védelmi profilok kidolgozásához, mert részletesen leírják, milyen intézkedések várhatók el például egy tűzfal vagy egy adminisztrációs felület esetén.

A Common Criteria előnyei közé tartozik:

- egységes, nemzetközileg elfogadott keretet ad az IT-termékek biztonsági értékelésére;
- lehetővé teszi a különböző gyártók termékeinek összehasonlítását;
- támogatja a „security by design” és „security by documentation” megközelítést, mert a tanúsításhoz részletes tervek és vizsgálatok szükségesek;
- testreszabható, és szükség esetén a felhasználó is képes védelmi profilt létrehozni;
- kiterjeszthető, bővíthető, a jelenleg még benne nem szereplő funkcionalitásokat be lehet építeni a kiterjesztési kritériumok betartásával;
- erősíti a beszállítói lánc és a kritikus infrastruktúrák biztonságát, mert a beszerzők tanúsítványokra támaszkodhatnak a kockázatértékelésben.

Ugyanakkor vannak korlátai is:

- kevés a létező, felhasználható védelmi profil;
- a precízebben megfogalmazott követelmények ellenére nagy szaktudást igényel;
- a magasabb EAL-szintek elérése idő- és költségigényes, ezért ritkán reális általános kereskedelmi termékek számára;
- a tanúsítás a vizsgálat időpontjában adott termékverzióra vonatkozik – gyorsan változó szoftverkörnyezetben a tanúsítvány gyorsan „elavulhat”, ha a terméket gyakran frissítik;
- a CC önmagában nem garantálja, hogy a terméket a gyakorlatban is biztonságosan konfigurálják és üzemeltetik – ehhez szervezeti szintű irányítási rendszerekre és szaktudásra is szükség van.

A gyakorlatban ezért sok szervezet olyan kompromisszumot választ, hogy kritikus funkciókhoz CC-tanúsított komponenseket használ, miközben az egész rendszerre ISO/IEC 27001-re épülő IBIR-t működtet, és OT-környezetben IEC 62443-at, illetve NIST-ajánlásokat is figyelembe vesz. Ez a „többrétegű” megközelítés képes egyszerre kezelni a szervezeti, a rendszer- és a termékszintű kockázatokat.

5. A NIST SP 800-53 ÉS NIST SP 800-82

Az Amerikai Egyesült Államokban 2002-ben fogadták a FISMA 2002-t (Federal Information Security Management Act of 2002, 2002. évi szövetségi információbiztonsági törvény), amelyet 2014-ben módosítottak. A FISMA szerint az *információbiztonság* kifejezés az információk és információs rendszerek védelmét jelenti a jogosulatlan hozzáférés, felhasználás, nyilvánosságra hozatal, megzavarás, módosítás vagy megsemmisítés ellen, a sértetlenség, a bizalmasság és a rendelkezésre állás biztosítása érdekében. A FISMA meghatározza az információbiztonság kezelésének keretrendszerét, amelyet minden olyan információs rendszer esetében be kell tartani, amelyet az Egyesült Államok szövetségi kormányzati szervezetei használnak vagy üzemeltetnek a végrehajtó vagy a törvényhozó hatalomban, vagy amelyeket szerződéses partnerek vagy más szervezetek használnak vagy üzemeltetnek a szövetségi kormányzati szervek nevében ezekben a hatalmakban. Ezt a keretrendszert a NIST (National Institute of Standards and Technology, Nemzeti Szabványügyi és Technológiai Intézet) által kidolgozott szabványok és irányelvek határozzák meg. A FISMA szerint a NIST felelős a szabványok, irányelvek és kapcsolódó módszerek és technikák kidolgozásáért, amelyek megfelelő információbiztonságot nyújtanak az összes ügynökségi művelet és eszköz számára, a nemzetbiztonsági rendszerek kivételével. [45]

Közvetlenül a FISMA-hoz kapcsolódik a FIPS 199 (Federal Information Processing Standard 199) amerikai szabvány, amely – az évekkel korábban, a MeH ITB 12. számú ajánlásban megalkotott magyar biztonsági osztályba soroláshoz hasonlóan – kategóriákba sorolja a szövetségi információs rendszereket a biztonsági követelmények szempontjából. A besorolás a bizalmasság, integritás, rendelkezésre állás követelményeit figyelembe véve alacsony, közepes vagy magas kategóriába sorolja az adott rendszert, amelynek védelmére ezután például a NIST SP 800-53 szerinti védelmi intézkedéseket kell alkalmazni. [46]

Az amerikai National Institute of Standards and Technology (NIST) Special Publication (SP) 800-as sorozata [47] az egyik legátfogóbb, világszerte használt biztonsági és adatvédelmi útmutatócsalád, amely eredetileg az amerikai szövetségi információs rendszerekre készült, de ma már számos országban *de facto* szabványként funkcionál. A NIST (Nemzeti Szabványügyi és Technológiai Intézet) az Amerikai Egyesült Államok Kereskedelmi Minisztériumához tartozik. A NIST SP (Special Publication) 800 sorozata 1990-ben jött létre mint olyan közérdekű dokumentumok gyűjteménye, amelyek az Amerikai Egyesült Államok szövetségi kormánya számítógépes biztonsági politikáit, eljárásait és irányelveit írják le. Új sorozatként az SP 1800-as kiadványok a kiberbiztonsági gyakorlatokat mutatják be 39 részben. [48] A dokumentumok ingyenesen elérhetők, és nagyon hasznosak úgy a kormányzati szervek, mind a vállalkozások és az oktatási intézmények számára.

NIST SP 800 sorozat kiadványai között megtalálhatók a fenyegetések és sérülékenységek, a nemkívánatos események értékelésére és dokumentálására, a biztonsági intézkedések meghozatalához ajánlott eljárások. A sorozatnak jelenleg 215 tagja van.

A NIST SP 800 sorozat leggyakrabban hivatkozott és legkritikusabb dokumentumai a kiberbiztonsági intézkedések, a kockázatkezelés és incidenskezelés területén találhatók, **az USA kormányzati rendszereinek védelmére készültek**, de globálisan alkalmazhatók.

Kiemelhető az információs rendszerekhez:

- NIST SP 800-53 (Rev. 5): Biztonsági és adatvédelmi intézkedéskatalógus információs rendszerekhez, 20 intézkedéscsaláddal (például hozzáférés-vezérlés, incidenskezelés, ellátási lánc kockázatkezelése). Alapja számos szabályozásnak, beleértve a magyar kiberbiztonsági jogszabályoknak is. [49]
- NIST SP 800-61 (Rev. 2): Számítógépes biztonsági incidensek kezelése, irányelvekkel a detektálásra, az elemzésre és a válaszadási folyamatokra. [50]
- NIST SP 800-63 (sorozat): Digitális identitás irányelvek (A: Beiratkozás és személyazonosság-ellenőrzés, B: Hitelesítés és életciklus-menedzsment, C: Összevonások és állítások), kulcsfontosságú IAM-rendszerekhez. [51]

OT- és Speciális Rendszerekhez (Ipari és speciális rendszerekhez) dedikált fontosabb dokumentumok:

- NIST SP 800-82 (Rev. 3): OT (operatív technológia) biztonsági útmutató, ICS rendszerek fenyegetéseire fókuszálva. [52]
- NIST SP 800-123: Szerverbiztonság alapelvek üzemeltetőknek. [53]
- NIST SP 800-144: Felhőbiztonsági ajánlások. [54]

Ezek a dokumentumok dinamikusan frissülnek, és a NIST CSRC oldalán elérhetők.

A sorozat két kiemelten fontos tagja a NIST SP 800-53, amely részletes biztonsági és adatvédelmi intézkedéskatalógust tartalmaz, valamint a NIST SP 800-82, amely az ipari vezérlőrendszerek (ICS/OT) kiberbiztonsági kérdéseit tárgyalja.

A NIST SP 800-53 Rev4. (Security and Privacy Controls for Federal Information Systems and Organizations) volt *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló a 41/2015. (VII. 15.) BM rendelet* alapja.

A magyar kiberbiztonsági törvényhez kapcsolódó 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről a NIST SP 800-53 Rev. 5. („Security and Privacy Controls for Information Systems and Organizations”) felhasználásával készült.

A NIST SP 800-53 Rev. 5. 20 intézkedéscsaládban 1189 védelmi intézkedést tartalmaz. Minden intézkedéshez tartozik célleírás, megvalósítási útmutató, gyakran példaimplementáció és javasolt ellenőrzési pont.

A NIST SP 800-53 a FIPS 199 alapján a bizalmasság, sértetlenség, rendelkezésre állás követelmények esetleges sérülésének hatása alapján három kategóriára (alacsony, közepes és magas) bontja az információs rendszereket, és mindegyikhez javasol egy alapszintű (baseline) intézkedéskészletet. Ezek alapszínű intézkedéskészletek a gyakorlatban kiindulópontként szolgálnak: egy szervezet a saját kockázatértékelése eredményei alapján növelheti vagy csökkentheti az intézkedések számát és szigorát, de alapvetően a NIST által ajánlott keretrendszeren belül marad. Az ENISA a NIS2 irányelv technikai megvalósítási javasolja, hogy az ISO/IEC 27002 intézkedéseinek megvalósításakor érdemes a NIST SP 800-53 részletes előírásait is figyelembe venni, különösen a magas kockázatú környezetekben. [55]

A NIST SP 800-82 („Guide to Industrial Control Systems (ICS) Security”) kifejezetten az ipari vezérlőrendszerek – SCADA, DCS, PLC-k, távoli terminál egységek – kiberbiz-

tonságának sajátosságaival foglalkozik. Részletesen bemutatja az ICS-architektúrákat, a tipikus kommunikációs protokollokat, a működési prioritásokat (ahol a rendelkezésre állás és a folyamatbiztonság gyakran megelőzi a bizalmasságot), valamint az ezekből fakadó sebezhetőségeket és fenyegetéseket. A dokumentum gyakorlati ajánlásokat ad a hálózat-szegmentációra, a távoli hozzáférések biztonságára, a konfiguráció- és változáskezelésre, a sebezhetőségkezelésre, a naplózásra és incidenskezelésre OT-környezetben. Ezek a javaslatok jól összehangolhatók az IEC 62443 rendszerszintű és komponensszabványaival: míg az IEC 62443 inkább a szabványos követelményeket rögzíti, a NIST SP 800-82 részletes, példákkal is illusztrált gyakorlati útmutatót nyújt a megvalósításhoz.

A NIST 800-as dokumentumokat és az z ISO/IEC 27000-es sorozatot nem kizárásos, vagy-vagy alapon érdemes használni, hanem az átfedéseket kihasználva egymást kiegészítve. Az ISO/IEC 27001 az ISO/IEC 27002-val egy irányítási rendszer- és intézkedéskatalógus-szintű keretet ad, míg ehhez a NIST SP 800-53 sok területen technikailag részletesebb előírásokat tartalmaz. Az OT-rendszerek esetében is hasonló a helyzet: például az ISO/IEC 27001 és az ISO/IEC 27019 az irányítási logikát és az energiaszektor adottságait rögzíti, addig az IEC 62443 és a NIST SP 800-82 együtt adják a rendszer- és termékszintű technikai követelményeket.

Amikor egy szervezetnél magas szintű biztonságot szeretnénk megvalósítani, akkor a következő megoldást érdemes használni:

- irányítási szinten az ISO/IEC 27001-re épülő IBIR;
- a védelmi intézkedésekben az ISO/IEC 27002 alkalmazása a NIST SP 800-53 „támogatásával”;
- az OT-környezetben IEC 62443 és a NIST SP 800-82 együttes alkalmazása;
- kulcseszközöknél a Common Criteria szerinti terméktanúsítás.

6. ISO/IEC 20000, ITIL

Az informatikai szolgáltásmenedzsmentre vonatkozó szabványcsalád az ISO/IEC 20000. Jelenleg három kötetből áll.

Az ISO/IEC 20000-1:2018 *Információtechnológia – Szolgáltatásmenedzsment – 1. rész: Szolgáltatásirányítási rendszer követelményei* szabvány egy tanúsítható szabvány, amely meghatározza az IT Szolgáltatásmenedzsment Rendszer (IT Service Management System, IT SMS) követelményeit. Azokat a követelményeket írja le, amelyek a szervezetekkel szemben támasztják alá a szolgáltatásirányításimenedzsment-rendszer (SMS) létrehozását, bevezetését, karbantartását és folyamatos fejlesztését. A meghatározott követelmények magukban foglalják a szolgáltatások tervezését, átállását, szállítását és fejlesztését, hogy egy szervezet megfeleljen a szolgáltatási követelményeknek, és értéket nyújtson. [18]

Jól felhasználhatják azok ügyfelek, akik a szolgáltatási életciklus következetes megközelítését követelik meg valamennyi szolgáltatójuktól, beleértve az ellátási láncban lévőket is, illetve IT-szolgáltatást keresnek, és e szolgáltatások minőségére vonatkozóan biztosítékot igényelnek.

Az ISO/IEC 20000-2:2019 *Információtechnológia – Szolgáltatásmenedzsment – 2. rész: Útmutató a szolgáltatásmenedzsment-rendszerek alkalmazásához* szabvány útmutatást ad az ISO/IEC 20000-1 szabványon alapuló szolgáltatásmenedzsment-rendszer (SMS) alkalmazásához. Példákat és ajánlásokat tartalmaz, amelyek lehetővé teszik a szervezetek számára az ISO/IEC 20000-1 értelmezését és alkalmazását, beleértve az ISO/IEC 20000 és más vonatkozó szabványok más részeire való hivatkozásokat is. [56]

Az ISO/IEC 20000-3:2019 *Információtechnológia – Szolgáltatásmenedzsment – 3. rész: Útmutató az ISO/IEC 20000-1 hatókör meghatározásához és alkalmazhatóságához* szabvány útmutatást tartalmaz a hatókör meghatározására és az ISO/IEC 20000-1 szabványban meghatározott követelményekre való alkalmazhatóságára vonatkozóan. Segíthet annak megállapításában, hogy az ISO/IEC 20000-1 alkalmazható-e egy szervezet körülményeire. Bemutatja, hogyan határozható meg egy SMS hatóköre. A szabvány segítséget nyújthat a szervezetnek az ISO/IEC 20000-1 szerinti megfelelőségértékelés tervezésében és elkészítésében. [57]

Az ISO/IEC 20000-3 szabvány A melléklete példákat tartalmaz az SMS-ek lehetséges hatókör-utasításaira. A megadott példák egy sor forgatókönyvet használnak szervezetek számára, a nagyon egyszerűtől az összetett szolgáltatási láncig.

A ISO/IEC 20000-3 szabvány az SMS megvalósításának tervezéséért felelős személyzetnek, valamint az értékelőknek és a tanácsadóknak szól. Kiegészíti 2. részben megadott, az SMS alkalmazására vonatkozó útmutatót.

Az ISO/IEC 20000 és az ISO/IEC 27001 struktúrája kompatibilis, ezért sok szervezet integrált irányítási rendszert alakít ki, ahol az IT-szolgáltatásmenedzsment és az információbiztonság együtt jelenik meg a vezetői szinten. Ehhez az ISO/IEC 27000 szabványsorozatban

az ISO/IEC 27013:2021 *Information security, cybersecurity and privacy protection – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1* szabvány [58] nyújt útmutatást az az ISO/IEC 27001 szabvány szerinti Információbiztonsági Irányítási Rendszer és az ISO/IEC 20000-1 szabvány szerinti IT Szolgáltatásirányítási Rendszer (ITSM) integrált bevezetéséhez. Célja, hogy a két rendszert hatékonyan, párhuzamosan vagy egymást követően vezessék be, csökkentve az ismétlődést, és javítva a folyamatokat. Azoknak a szervezeteknek szól, amelyek:

a. az ISO/IEC 20000-1 már bevezetett állapotában kívánják bevezetni az ISO/IEC 27001-et, vagy fordítva;
b. az ISO/IEC 27001-et és az ISO/IEC 20000-1-et együtt kívánják bevezetni; vagy
c. az ISO/IEC 27001 és az ISO/IEC 20000-1 szabványokon alapuló meglévő irányítási rendszereket kívánják integrálni. [59]

Az integrált bevezetéssel ISO/IEC 20000 egyfajta „operatív hordozófelületet" biztosít az ISO/IEC 27001-es IBIR és ezen keresztül a termékszintű biztonsági követelményeket megfogalmazó szabványok, például a Common Criteria számára.

Míg az ISO/IEC 20000 inkább „mit" típusú követelményeket fogalmaz meg, az ITIL, az *Information Technology Infrastructure Library* részletes „hogyan" jellegű jó gyakorlatokat tartalmaz. Az eredeti, 1989-es kiadás óta többször is frissítették, legújabb verzió az ITIL 4, mely 2019-ben jelent meg, és 2023-ban vezették be teljeskörűen. Ez a legújabb fejlesztés a digitális átalakulás elősegítésére összpontosít a felhőalapú számítástechnika, a hibrid felhő, a mesterséges intelligencia (AI) és más technológiák által dominált digitális korszakban. Az ITII 4 egy holisztikus megközelítést is kínál, amely az értékre összpontosít, és összhangban áll az agilis DevOps-filozófiákkal.

„Az ITIL egy 34 legjobb gyakorlatból álló keretrendszer az IT-támogatás és szolgáltatásnyújtás kezelésére és fejlesztésére. Az ITIL fő célja, hogy segítse a vállalkozásokat az IT-szolgáltatásaikból a lehető legnagyobb értéket kihozni azáltal, hogy azokat az üzleti célokkal összhangba hozza.

Az ITIL jelentősen fejlődött a 20. század végén történt bevezetése óta, amikor több mint 30 kötetes könyvsorozatként jelent meg. 2000-ben a második verzió egyszerűsítette ezeket a kiadványokat azáltal, hogy különböző IT-menedzsmentszempontok, -szolgáltatások és -alkalmazások szerint csoportosította őket. Ekkoriban a Microsoft az ITIL-t szabványosította a Microsoft Operations Framework fejlesztésének elősegítése érdekében. Azóta az ITIL újabb verziói jelentek meg, amelyek a jelenlegi IT-környezettel kapcsolatos kihívásokra reagálnak, és a változó üzleti igényeknek felelnek meg." [60]

„Az ITIL 4 hét alapelvet tartalmaz:

1. Összpontosítson az értékre.
2. Kezdje ott, ahol van.
3. Haladjon iteratív módon, visszajelzésekkel.
4. Működjön együtt és támogassa a láthatóságot.
5. Gondolkodjon és dolgozzon holisztikusan.
6. Tartsa egyszerűnek és praktikusnak.
7. Optimalizáljon és automatizáljon." [61]

Az ITIL 4 34 gyakorlatból áll, amelyek 3 fő kategóriába vannak csoportosítva:

1. Általános menedzsmentgyakorlatok.
2. Szolgáltatásmenedzsment-gyakorlatok.
3. Műszakimenedzsment-gyakorlatok. [61]

7. COBIT

A COBIT (Control Objectives for Information and Related Technologies) az ISACA (Information Systems Audit and Control Association) által kidolgozott IT-irányítási és -menedzsment-keretrendszer, amely a vállalati célokat, az IT-célokat, a folyamatokat és az intézkedéseket köti össze. A korábbi verziók a COBIT 5 (2012), a COBIT 4.1 (2007) és az auditfókuszú COBIT 3 voltak. A legújabb verzió, a COBIT 2019 [20] már nemcsak audit- és intézkedéskeretként, hanem átfogó irányítási modellként értelmezhető: különbséget tesz az irányítási (governance) és menedzsment (management) célok között.

„Mivel a COBIT szerint nincsen lehetőség tanúsításra, ezért elterjedtségének mértékére nincsen hiteles adat. Tény viszont az, hogy a COBIT-ra épülő Certified Information Systems Auditor (CISA) és Certified Information Security Manager (CISM) szakvizsgák világszerte széles körben, valamint az Amerikai Egyesült Államok Védelmi Minisztériuma (DoD) által is elismert informatikai biztonsági szakvizsgák." [35]

Az irányítási governance a felső vezetés felelősségeivel foglalkozik (stratégiaalkotás, kockázati étvágy meghatározása, teljesítmény és megfelelés monitorozása), míg a management a tervezés, megvalósítás, üzemeltetés és támogatás folyamatainak menedzselésére koncentrál (projektek, szolgáltatásmenedzsment, biztonság, kockázat, megfelelés). A COBIT folyamatmodelljében több folyamat kifejezetten információbiztonsággal és kiberbiztonsággal foglalkozik, például a kockázatkezelés, a biztonság- és adatvédelem-menedzsment, a megfelelőség biztosítása.

A COBIT 2019 képességi szintekkel (0–5) méri a folyamatok érettségét, és széles körben használatos vállalati IT-irányításhoz. A COBIT 2019 rugalmassága miatt vált dominánssá. Kiegészítve COBIT Core modelllel biztosítja, hogy az informatikai irányítás nem csupán technikai kérdés, hanem szerves része az üzleti stratégiának és a kockázatkezelésnek.

A COBIT egyik legfontosabb üzenete, hogy az információbiztonság és kiberbiztonság a vállalati irányítás szerves része. A keretrendszer a kiberbiztonsági feladatokat olyan üzleti célokhoz köti, mint az értékteremtés, kockázatcsökkentés, megfelelés és erőforrás-hatékonyság, és ehhez kapcsolódó ellenőrzési célokat (control objectives) fogalmaz meg. Ennek eredményeként a biztonsági intézkedések nem elszigetelt mechanizmusok, hanem a vállalati célrendszerhez kötött, mérhető hozzájárulások. [62]

A kiberbiztonsági kockázatok a COBIT logikájában az információs és technológiai kockázatok részét képezik, amelyeket ugyanabban a vállalati kockázatkezelési keretben kell kezelni, mint a pénzügyi, jogi vagy működési kockázatokat. Ez kedvez az ISO/IEC 27001-re épülő IBIR-eknek és a Common Criteria-szerű termékbiztonsági megközelítéseknek, mert a COBIT szintjén „helyet" kapnak az irányítási struktúrában: a felső vezetés számára is világossá válik, hogy például egy IBIR-tanúsítás vagy egy CC-tanúsított termékcsalád milyen kockázatokat csökkent, és milyen üzleti értéket teremt.

8. IT-ESZKÖZÖKRE VONATKOZÓ TERMÉKSZABVÁNYOK

A termékszabványok és a Common Criteria között szoros kapcsolat van. Sok termékszabványt úgy dolgoznak ki, hogy követelményei könnyen felhasználhatók legyenek a CC-ben, másrészt a CC nyújtja azt az értékelési keretet, amelybe az IEC 62443-hoz hasonló szabványok integrálhatók. A védelmi profilok (PP-k) gyakran épülnek termékszabványokra, például egy intelligens kártyára vonatkozó PP konkrétan hivatkozhat fizikai és logikai biztonsági szabványokra.

Ezen túlmenően egyre több ágazatspecifikus minősítési rendszer létezik (például fizetési terminálok, orvostechnikai eszközök, járművek fedélzeti rendszerei), amelyek részben a Common Criteria-ra, részben saját, termékspecifikus szabványrendszerre épülnek. A szervezetek számára ezek a minősítések kulcsfontosságúak lehetnek a beszállítói rizikó csökkentése, a megfelelés igazolása és a piacra jutás szempontjából.

8.1 ETSI EN 303 645 – fogyasztói IoT-eszközök

A fogyasztói IoT-eszközök (okos otthoni eszközök, háztartási gépek, kamerák, okos zárak, fitnesz- és egészségügyi trackerek stb.) kiberbiztonsági kockázataira válaszul dolgozta ki az ETSI az EN 303 645 szabványt, amely minimális biztonsági alapvonalat határoz meg a gyártók számára. [16] A szabvány olyan követelményeket fogalmaz meg, mint:

- tilos az univerzális gyári jelszavak alkalmazása;
- kötelező biztonságos frissítési mechanizmust biztosítani;
- biztosítani kell a sérülékenység-bejelentési csatornákat és folyamatokat;
- megfelelő titkosítást kell alkalmazni az érzékeny adatok tárolására és továbbítására;
- minimalizálni kell a támadási felületet (például felesleges szolgáltatások és portok kikapcsolása).

Az EN 303 645 a GDPR adatvédelmi elvárásaival is összhangban áll: előírja többek között az adatminimalizálást, a transzparens adatkezelési gyakorlatot és a felhasználói intézkedést az adatok felett. Az EU kiberbiztonsági tanúsítási keretrendszerében várhatóan kulcsszerepet játszik a fogyasztói IoT-eszközökre vonatkozó tanúsítási sémák alapjaként.

8.2 IEC 62443 termékszabványok – ipari és OT-eszközök

Az IEC 62443 szabványsorozat az ipari automatizálási és irányítórendszerek (IACS) kiberbiztonságának átfogó kerete, amely rendszerszintű, folyamat- és komponensszintű követelményeket tartalmaz. A komponensszintű részek azt írják le, hogy egy ipari vezérlő, ipari switch, távoli terminál egység vagy biztonsági átjáró milyen biztonsági funkciókat (autentikáció, hozzáférés-intézkedés, naplózás, kommunikációvédelem, frissítés, konfigurációvédelem) kell hogy támogasson, és milyen Security Level szinteknek (SL1–SL4) kell megfelelnie. [17]

Az IEC 62443 termékszintű követelményei szorosan kapcsolódnak az OT-kockázati környezet sajátosságaihoz: kiemelt hangsúlyt kap a rendelkezésre állás, a folyamatbiztonság, a fizikai következmények kezelése és a hosszú életciklusú eszközök frissíthetősége. Az ipari szektorban egyre gyakoribb, hogy a beszállítói szerződésekben előírják: bizonyos komponenseknek IEC 62443-kompatibilisnek kell lenniük, vagy adott biztonsági szintre vonatkozó tanúsítvánnyal kell rendelkezniük.

IRODALOMJEGYZÉK

[1] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS 2 irányelv)

[2] ISO/IEC 27000 family https://www.iso.org/standard/iso-iec-27000-family

[3] Common Criteria: Certified Products https://www.commoncriteriaportal.org/products/index.cfm

[4] 1995. évi XXVIII. törvény a szabványosításról

[5] Informatikai Biztonsági Módszertani Kézikönyv. Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság ajánlásai (8). Miniszterelnöki Hivatal, Budapest https://dsd.sztaki.hu/mockups/itb/ajanlasok/a8/index.html

[6] *Bodlaki Ákos, Csernay Andor, Mátyás Péter, Muha Lajos, Papp György, Vadász Dezső*. Informatikai Rendszerek Biztonsági Követelményei. Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság ajánlásai (12). Miniszterelnöki Hivatal, Budapest. 1996, ISBN 963-03-4264-2, https://dsd.sztaki.hu/mockups/itb/ajanlasok/a12/index.html

[7] Information Technology Security Evaluation Criteria (ITSEC) https://web.archive.org/web/20060523094527/ http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf

[8] *Muha Lajos* Informatikai biztonsági szabványok és irányelvek. In: IX. Országos Neumann Kongresszus, 2006.06.26-2006.06.29, Győr https://real.mtak.hu/11149/1/1228885.pdf

[9] 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

[10] Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény

[11] ENISA – Cybersecurity in the EU: threat landscape and strategic priorities https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[12] ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protections – Information security management systems – Requirements

[13] 7/2024. (VI. 24.) SZTFH rendelet a kiberbiztonsági audit végrehajtására jogosult auditorok nyilvántartásáról és az auditorral szemben támasztott követelményekről

[14] 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról

[15] ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks

[16] ETSI EN 303 645 – Cyber Security for Consumer Internet of Things

[17] IEC 62443 – Industrial automation and control systems security

[18] ISO/IEC 20000-1:2018 Információtechnológia – Szolgáltatásmenedzsment – 1. rész: Szolgáltatásirányítási rendszer követelményei

[19] NIST Cybersecurity Framework 2.0
https://www.nist.gov/cyberframework

[20] Control Objectives for Information and Related Technologies, ISACA, 2019.
https://www.isaca.org/resources/cobit#2

[21] ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls

[22] EU Cybersecurity Act – Az Európai Uniós Kiberbiztonsági Ügynökségről és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló (EU) 2019/881 rendelet

[23] ISO/IEC JTC 1/SC Information security, cybersecurity and privacy protection
https://www.iso.org/committee/45306.html

[24] ISO/IEC 27701:2025 Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

[25] ISO/IEC 27011:2024Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations

[26] ISO/IEC 27032:2023 – Cybersecurity — Guidelines for Internet security

[27] ISO/IEC 27035-1 … -4 – Information technology — Information security incident management

[28] ISO 27799:2016 Health informatics — Information security management in health using ISO/IEC 27002

[29] *Muha Lajos* Hazai és nemzetközi szabványok és ajánlások, In: Az információbiztonság alapjai, NKE RTK, Budapest, 2023. https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/az_informaciobiztonsag_alapjai_konyv_kesz_2.pdf

[30] *Muha Lajos* Egy szabvány változásai
https://www.ludovika.hu/blogok/cyberblog/2022/11/29/egy-szabvany-valtozasai/

[31] Muha Lajos: Az Informatikai Biztonsági Irányítási Rendszer, In: Az Informatika Korszerű Technikái Konferencia, Dunaújváros, 2010.03.05-2010.03.06., pp. 156-164., ISBN:978 963 9915 38 1

[32] Muha Lajos: Az informatikai biztonság mérése, In: Kadocsa László (szerk.): A Dunaújvárosi Főiskola Közleményei XXXI.: A Magyar Tudomány Napja és a Kreativitás és Innováció Európai Év 2009. tiszteletére rendezett interdiszciplináris tudományos Konferenciasorozat előadásai. Dunaújváros, Magyarország, 2009.11.09-2009.11.13. https://drive.google.com/file/d/0B-BNqgK1oZQEaGRJZUNMd3R1ZzA/edit?resourcekey=0-HTwXfTeBTQS4vf3VTOaU9g

[33] ISO: Directives and Policies
https://www.iso.org/directives-and-policies.html

[34] Common Criteria: A Common Criteriaról
https://www.commoncriteriaportal.org/ccra/index.cfm

[35] Szádeczky Tamás: Információbiztonsági szabványok, egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, Budapest, 2014., 50 p.
https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/Inform%C3%A1ci%C3%B3biztons%C3%A1gi%20szabv%C3%A1nyok.pdf

[36] ISO/IEC 15408-1:2022Information security, cybersecurity and privacy protection — Evaluation criteria for IT securityPart 1: Introduction and general model

[37] ISO/IEC 15408-2:2022Information security, cybersecurity and privacy protection — Evaluation criteria for IT securityPart 2: Security functional components

[38] ISO/IEC 15408-3:2022Information security, cybersecurity and privacy protection — Evaluation criteria for IT securityPart 3: Security assurance components

[39] ISO/IEC 15408-4:2022Information security, cybersecurity and privacy protection — Evaluation criteria for IT securityPart 4: Framework for the specification of evaluation methods and activities

[40] ISO/IEC 15408-5:2022Information security, cybersecurity and privacy protection — Evaluation criteria for IT securityPart 5: Pre-defined packages of security requirements

[41] ISO/IEC 18045:2022Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation

[42] *Krasznay Csaba* Common Criteria alapok https://www.slideserve.com/cisco/common-criteria-alapok-powerpoint-ppt-presentation

[43] Common Criteria
https://www.commoncriteriaportal.org/index.cfm

[44] Common Criteria Evaluation Assurance Levels - From EAL 1 To EAL 4
https://www.cclab.com/news/common-criteria-evaluation-assurance-levels-from-eal-1-to-eal-4

[45] Federal Information Security Management Act (FISMA) of 2014
https://csrc.nist.gov/topics/laws-and-regulations/laws/FISMA

[46] FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, National Institute of Standards and Technology, 2004.
https://csrc.nist.gov/pubs/fips/199/final

[47] Computer Security Resource Center, NIST SP 800 sorozat
https://csrc.nist.gov/publications/sp800

[48] Computer Security Resource Center, NIST SP 1800 sorozat
https://csrc.nist.gov/publications/sp1800

[49] NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations, 2020. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[50] NIST SP 800-61 Rev. 3 Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, 2025.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[51] NIST SP 800-63-4 Digital Identity Guidelines sorozat
https://csrc.nist.gov/pubs/sp/800/63/4/final

[52] NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security, 2023
https://csrc.nist.gov/pubs/sp/800/82/r3/final

[53] NIST SP 800-123 Guide to General Server Security, 2008
https://csrc.nist.gov/pubs/sp/800/123/final

[54] NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing, 2011
https://csrc.nist.gov/pubs/sp/800/144/final

[55] Technical Implementation Guidance on the NIS2 Directive,
https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

[56] ISO/IEC 20000-2:2019 Információtechnológia – Szolgáltatásmenedzsment – 2. rész: Útmutató a szolgáltatásmenedzsment-rendszerek alkalmazásához

[57] ISO/IEC 20000-3:2019 Információtechnológia – Szolgáltatásmenedzsment – 3. rész: Útmutató az ISO/IEC 20000-1 hatókör meghatározásához és alkalmazhatóságához

[58] ISO/IEC 27013:2021Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

[59] ISO/IEC 27013:2021Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

[60] What is the IT Infrastructure Library (ITIL)?
https://www.ibm.com/think/topics/it-infrastructure-library

[61] ITIL®-folyamatok és -gyakorlatok
https://otrs.com/hu/felhasznalasi-terueletek/itsm/itil-folyamatok/

[62] „Informatika az üzlet szolgálatában”
https://hopet.hu/index-en.php?menu=cobit&almenu=2_al

A Nemzeti Közszolgálati Egyetem kiadványa.

Nemzeti Közszolgálati Egyetem;
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős kiadó:
Dr. Deli Gergely rektor
Címe: 1083 Budapest, Üllői út 82.

Olvasószerkesztő:
Dorogi Katalin

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-749-9