EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NEMZETI KÉPESSÉGEK ÉRTÉKELÉSÉNEK KERETRENDSZERE

2020. DECEMBER

AZ EINSA-RÓL

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) az Unió azon ügynöksége, amelynek célja az Európa-szerte egységesen magas szintű kiberbiztonság megvalósítása. A 2004-ben létrehozott és az uniós kiberbiztonsági jogszabály által megerősített Európai Uniós Kiberbiztonsági Ügynökség hozzájárul az uniós kiberpolitikához, kiberbiztonsági tanúsítási rendszerek alkalmazásával javítja az IKT-termékek, -szolgáltatások és -folyamatok megbízhatóságát, együttműködik a tagállamokkal és az uniós szervekkel és segíti Európát abban, hogy felkészüljön a jövő kiberbiztonsággal kapcsolatos kihívásaira. A tudásmegosztás, a kapacitásépítés és a figyelemfelkeltés révén az Ügynökség a legfontosabb érdekelt felekkel együtt arra törekszik, hogy megerősítse az összekapcsolt gazdaságba vetett bizalmat, fokozza az uniós infrastruktúra ellenálló-képességét és végső soron megőrizze Európa társadalmának és polgárainak digitális biztonságát. Bővebb információért lásd: www.enisa.europa.eu.

KAPCSOLAT

Ha kapcsolatba szeretne lépni a szerzőkkel, írjon a következő e-mail-címre: team@enisa.europa.eu.
A dokumentummal kapcsolatos sajtómegkereséseket, kérjük, az alábbi címre küldjék: press@enisa.europa.eu.

SZERZŐK

Anna Sarri, Pinelopi Kyranoudi – Európai Uniós Kiberbiztonsági Ügynökség (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique – Wavestone

KÖSZÖNETNYILVÁNÍTÁS

Az ENISA ezúton is szeretne köszönetet mondani minden szakértőnek, aki részt vett e jelentés megalkotásában és értékes információkkal szolgált, különös tekintettel az alábbiakra (ábécésorrendben):

CFCS – Center for Cybersikkerhed (Dánia), Thomas Wulff

Digitális Politikáért Felelős Minisztérium (Görögország), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali és Sotiris Vasilos

Digitális Társadalom Fejlesztéséért Felelős Központi Állami Hivatal (Magyarország), Marin Ante Pivcevic

Gazdasági és Hírközlési Minisztérium (Észtország), Anna-Liisa Pärnalaas

Igazságügyi és Közbiztonsági Minisztérium (Norvégia), Robin Bakke

Információbiztonsági hatóság (Szlovén Köztársaság), Marjan Kavčič

Kiberbiztonsági Központ (Belgium)

Kiberbiztonsági Politikai Osztály, Környezetvédelemért, Klímapolitikáért és Kommunikációért Felelős Minisztérium (Írország), James Caffrey

Kiberbűnözés Elleni Európai Központ – EC3, Adrian-Ionut Bobeica

Kiberbűnözés Elleni Európai Központ – EC3, Alzofra Martinez Alvaro

Máltai Információtechnológiai Ügynökség (Málta), Katia Bonello és Martin Camilleri

NCTV, Igazságügyi és Biztonsági Minisztérium (Hollandia)

Nemzeti Biztonsági Hatóság (Szlovákia)

Nemzeti Biztonsági Osztály (Spanyolország), Maria Mar Lopez Gil

Nemzeti Kiber- és Információbiztonsági Ügynökség (Cseh Köztársaság), Veronika Netolická
Olaszország kormánya (Olaszország)
Oxfordi Egyetem – Globális Kiberbiztonsági Kapacitásépítési Központ, Carolin Weisser Harris
Portugál Nemzeti Kiberbiztonsági Központ (Portugália), Alexandre Leite és Pedro Matos
Szövetségi Belügyminisztérium (Németország), Sascha-Alexander Lettgen

Az ENISA azoknak a szakértőknek is köszönetét fejezi ki, akik jelentősen hozzájárultak e tanulmány létrejöttéhez, de szeretnének névtelenek maradni.

JOGI NYILATKOZAT

Felhívjuk rá a figyelmet, hogy ez a kiadvány – ellenkező állítás hiányában – az ENISA nézeteit és értelmezéseit ismerteti. E kiadvány nem tekinthető az ENISA vagy az ENISA szervezetei által tett jogi lépésnek, hacsak az (EU) 2019/881 rendeletnek megfelelően el nem fogadják. E kiadvány nem feltétlenül tekinthető naprakésznek, és az ENISA időnként aktualizálhatja.

A harmadik féltől származó idézeteket a szövegben megfelelően jelöljük. Az ENISA nem vállal felelősséget a külső források, köztük a kiadványban hivatkozott külső weboldalak tartalmáért.

Ez a kiadvány kizárólag tájékoztatási célt szolgál. Ingyenesen elérhetővé kell tenni. Sem az ENISA, sem más, a nevében eljáró személy nem vállal felelősséget e kiadványban szereplő információk esetleges felhasználásáért.

SZERZŐI JOGI NYILATKOZAT

ISBN: 978-92-9204-484-8

DOI: 10.2824/335350

KATALÓGUS: TP-02-21-253-HU-N

1. TARTALOMJEGYZÉK

FOGALOMMEGHATÁROZÁSOK

RÖVIDÍTÉS	MEGHATÁROZÁS
C2M2	Kiberbiztonsági képességérettségi modell
CCRA	Közös kritériumok elismerésére vonatkozó megállapodás
CII	Kritikus információs infrastruktúra
CMM	Kiberbiztonsági kapacitás érettségi modellje a nemzetek számára
CMMC	Kiberbiztonsági érettségi modellre vonatkozó tanúsítás
CPI	Kibererőindex
CVD	Összehangolt sebezhetőség-feltárás
CCSMM	Közösségi kiberbiztonsági érettségi modell
CSIRT	Számítógép-biztonsági eseményekre reagáló csoport
DPA	Adatvédelmi törvény
DSM	Digitális egységes piac
ECCG	Európai kiberbiztonsági tanúsítási csoport
ECSM	Európai kiberbiztonsági hónap
ECSO	Európai Kiberbiztonsági Szervezet
EFTA	Európai Szabadkereskedelmi Társulás
EKKR	Európai képesítési keretrendszer
GCI	Globális kiberbiztonsági index
GDPR	Általános adatvédelmi rendelet
GDS	Kormányzati digitális szolgáltatás
IA-CM	A belső ellenőrzési képesség modellje a közszféra számára
IKT	Információs és kommunikációs technológiák
ISMM	Információbiztonsági érettségi modell a NIST kiberbiztonsági keretrendszer tekintetében
ITU	Nemzetközi Távközlési Egyesület
K+F	Kutatás és fejlesztés
kkv-k	Kis- és középvállalkozások
LEA	Bűnüldöző hatóság
MI	Mesterséges intelligencia

MT	Műveleti technológia
NIS	Hálózat- és információbiztonság
NIST	Nemzeti Szabványügyi és Technológiai Intézet
NKBS	Nemzeti kiberbiztonsági stratégiák
NLO	Nemzeti kapcsolattartó tisztviselők
OES	Alapvető szolgáltatásokat nyújtó szereplő
PET	A magánélet védelmét erősítő technológia
PIMS	Magánéleti információk kezelésére szolgáló rendszer
PPP	Köz- és magánszféra közötti partnerségek
Q-C2M2	Katari kiberbiztonsági képességérettségi modell
SOG-IS MRA	Informatikai rendszerek biztonságáért felelős rangidős tisztviselők csoportja, kölcsönös elismerési megállapodás
Tagállam	Európai uniós tagállam
Unió	Európai Unió

ÖSSZEFOGLALÓ

Mivel a kiberfenyegetés jelenlegi területe tovább bővül és a kibertámadások intenzitása és száma egyre nő, az uniós tagállamoknak nemzeti kiberbiztonsági stratégiák (NKBS) továbbfejlesztésével és igazításával kell hatékony választ adniuk. Az ENISA első, NKBS-re vonatkozó tanulmányainak 2012. évi közzététele óta az uniós tagállamok és az Európai Szabadkereskedelmi Társulás (EFTA) országai nagy előrelépést tettek stratégiáik kidolgozása és végrehajtása terén.

Ez a jelentés az ENISA által végzett, a Nemzeti képességek értékelésének keretrendszere (National Capabilities Assessment Framework, NCAF) kialakítására irányuló munkát mutatja be.

A keretrendszer célja, hogy a nemzeti kiberbiztonsági stratégiáik célkitűzéseinek értékelése révén saját érettségi szintjükre vonatkozó önértékelési lehetőséget nyújtson a tagállamoknak, amely mind stratégiai, mind működési szinten segítséget nyújt számukra a kiberbiztonsági képességeik megerősítésében és kiépítésében.

Ez egyszerű reprezentatív képet fest a tagállam kiberbiztonsági érettségi szintjéről. Az NCAF egy olyan eszköz, amely segíti a tagállamokat az alábbiakban:

- Hasznos információk biztosítása egy hosszú távú stratégia kidolgozásához (pl. bevált gyakorlatok, iránymutatások);
- Az NKBS hiányzó elemeinek azonosítása;
- Kiberbiztonsági képességek továbbépítése;
- Politikai intézkedések elszámoltathatóságának támogatása;
- Hitelesség biztosítása a polgároknak és nemzetközi partnereknek;
- Tájékoztatás támogatása és a nyilvánosság körében az átlátható szervezetről kialakult kép erősítése;
- A felmerülő kérdések és problémák előrejelzése;
- A levont tanulságok és bevált gyakorlatok azonosítása;
- Kiberbiztonsági kapacitásra vonatkozó alapforgatókönyv biztosítása uniószerte eszmecserék elősegítése érdekében; és
- A kiberbiztonságra vonatkozó nemzeti képességek értékelése.

Ez a keretrendszer az ENISA témaszakértői, valamint 19 tagállam és EFTA-ország képviselői támogatásával jött létre[1]. E jelentés célközönsége az NKBS, és tágabb értelemben a

[1] Az alábbi tagállamok és EFTA-országok képviselői voltak az interjúalanyok: Belgium, Cseh Köztársaság, Dánia, Észtország, Görögország, Hollandia, Horvátország, Írország, Liechtenstein, Magyarország, Málta, Németország, Norvégia, Olaszország, Portugália, Spanyolország, Svédország, Szlovákia, Szlovénia.

kiberbiztonsági képességek tervezéséért, megvalósításáért és értékeléséért felelős, illetve ezekben részt vevő politikai döntéshozók, szakértők és kormánytisztviselők.

A Nemzeti képességek értékelésének keretrendszere 17 stratégiai célkitűzést foglal magában és négy fő csoport köré épül:

- 1. csoport: Kiberbiztonsági irányítás és szabványok
  1. egy nemzeti kibervészhelyzeti terv megalkotása
  2. biztonsági alapintézkedések létrehozása
  3. digitális személyazonosság biztonságának garantálása és a digitális közszolgáltatásokba vetett bizalom felépítése

- 2. csoport: Kapacitásépítés és tudatosságnövelés
  4. kiberbiztonsági gyakorlatok szervezése
  5. biztonsági eseményekre való reagálás képességének kialakítása
  6. felhasználói tudatosság növelése
  7. képzési és oktatási programok megerősítése
  8. K+F támogatása
  9. a magánszektor ösztönzése a biztonsági intézkedésekbe való befektetésre
  10. az ellátási lánc kiberbiztonságának növelése

- 3. csoport: Jogi és szabályozási kérdések
  11. a kritikus információs infrastruktúra, az alapvető szolgáltatásokat nyújtó szereplő (OES) és a digitális szolgáltató védelme
  12. a kiberbűnözés kezelése
  13. biztonsági események bejelentésére vonatkozó mechanizmusok létrehozása
  14. magánélet- és adatvédelem megerősítése

- 4. csoport: Együttműködés
  15. köz- és magánszféra közötti partnerség létrehozása
  16. állami ügynökségek közötti együttműködés intézményesítése
  17. nemzetközi együttműködésben való részvétel

1. BEVEZETÉS

A 2016 júliusában közzétett, hálózati és információs rendszerek biztonságáról (NIS) szóló irányelv előírja az uniós tagállamok számára, hogy fogadjanak el egy, az 1. és 7. cikkben szereplő, hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát, más néven NKBS-t (nemzeti kiberbiztonsági stratégia). Ebben az összefüggésben az NKBS egy olyan keretrendszert jelent, amely stratégiai elveket, iránymutatásokat, stratégiai célkitűzéseket, prioritásokat, megfelelő politikákat és szabályozási intézkedéseket határoz meg. Az NKBS tervezett célja magas szintű hálózati és rendszerbiztonság elérése és fenntartása, amely révén lehetővé teszi a tagállamok számára a potenciális fenyegetések csökkentését. Az NKBS továbbá az ipari fejlődés, valamint gazdasági és társadalmi előrehaladás katalizátora is lehet.

Az uniós kiberbiztonsági jogszabály kimondja, hogy az ENISA-nak elő kell segítenie a bevált gyakorlatok terjesztését egy NKBS meghatározása és végrehajtása során azáltal, hogy támogatja a tagállamokat a hálózati és információs rendszerek biztonságáról szóló irányelv elfogadásában, valamint összegyűjti a tapasztalataikról szóló értékes visszajelzéseket. E célból az ENISA kifejlesztett számos olyan eszközt, amely segíti a tagállamokat saját kiberbiztonsági stratégiáik kidolgozásában, végrehajtásában és értékelésében.

Feladatai körében az ENISA célja egy olyan, nemzeti képességek önértékelésére szolgáló keretrendszer kidolgozása, amely révén mérhető a különböző nemzeti kiberbiztonsági stratégiáik érettségi szintje. E jelentés célja az önértékelési keretrendszer meghatározása során készített tanulmány bemutatása.

1.1 A TANULMÁNY HATÁLYA ÉS CÉLKITŰZÉSEI

Ennek a tanulmánynak a fő célkitűzése egy olyan nemzeti képességek önértékelésére szolgáló keretrendszer (a továbbiakban: NCAF) megalkotása, amely révén megmérhető a tagállamok kiberbiztonsági képességeinek érettségi szintje. Pontosabban, a keretrendszernek képessé kell tennie a tagállamokat az alábbiakra:

- Saját nemzeti kiberbiztonsági képességeik értékelésének elvégzése;
- Az ország érettségi szintjére vonatkozó tudatosság növelése;
- Fejlesztendő területek azonosítása; és
- Kiberbiztonsági képességek kialakítása.

Ez a keretrendszer segíti a tagállamokat, különösen pedig a politikai döntéshozókat abban, hogy a nemzeti kiberbiztonsági képességek javítását célzó önértékelési gyakorlatot végezhessenek.

1.2 MÓDSZERTANI MEGKÖZELÍTÉS

A nemzeti képességek önértékelésére szolgáló keretrendszer kidolgozásához használt módszertani megközelítés négy fő lépésre épül:

1. **Másodelemzés:** Az első lépés egy átfogó szakirodalmi áttekintést foglalt magában azoknak a bevált gyakorlatoknak az összegyűjtésére, amelyek a nemzeti kiberbiztonsági stratégiákkal kapcsolatos érettségértékelési keretrendszer kidolgozására vonatkoznak. A másodelemzés középpontjában a kiberbiztonsági kapacitásépítésről és stratégiameghatározásról szóló releváns dokumentumok szisztematikus elemzése, a tagállamok meglévő NKBS-ei és a kiberbiztonsággal foglalkozó meglévő érettségi modellek összehasonlítása áll. E tanulmány céljaira

kidolgozott elemzési keretrendszer elfogadásával sikerült elvégezni egy, a meglévő érettségi modellekre vonatkozó teljesítménymérő gyakorlatot. Az elemzési keretrendszer az érettségi modellek kidolgozása tekintetében a Becker[2] módszertant veszi alapul, amely általános és egységes eljárási modellt határoz meg az érettségi modellek tervezéséhez, továbbá egyértelmű követelményeket fogalmaz meg azok kidolgozásához. Az elemzési keretrendszer további testreszabáson esett át a tanulmány igényeinek kielégítése érdekében.

2. **Szakértők és érdekelt felek álláspontjának összegyűjtése:** A másodelemzés során összegyűjtött adatok és az elemzés kapcsolódó előzetes eredményei alapján ez a szakasz szolgált az NKBS kidolgozása és végrehajtása terén tapasztalattal rendelkező szakértők azonosítására és interjúra való meghívására. Az ENISA kapcsolatba lépett a nemzeti kiberbiztonsági stratégiákkal foglalkozó szakértői csoportjával és nemzeti kapcsolattartó tisztviselőivel (National Liaison Officers, NLO) annak érdekében, hogy minden tagállamban megtalálják a megfelelő szakértőket. Továbbá néhány, az érettségi modellek kidolgozásában részt vevő szakértő egy interjú keretében mondta el véleményét. Összesen 22 ilyen interjú készült, amelyből 19-et a különböző tagállamokban (és EFTA-országokban) jelen lévő kiberbiztonsági ügynökségek képviselőivel folytattak le.

3. **A felmérési észrevételek elemzése:** A másodelemzés és az interjúk során gyűjtött adatokat ezt követően elemezték, hogy azonosítani tudják az NKBS-ek érettségének mérésére szolgáló önértékelési keretrendszer tervezésének bevált gyakorlatait, hogy megérthessék a tagállamok igényeit, továbbá hogy megállapíthassák, milyen adatok gyűjtése megvalósítható a különböző európai országokban[3]. Ez az elemzés lehetővé tette az előző lépésekben kidolgozott előzetes modell finomhangolását, valamint a modellben található mutatók, az érettségi szintek és a modell dimenzióinak finomítását.

4. **A modell véglegesítése:** Ezt követően az ENISA témaszakértői felülvizsgálták a nemzeti képességek önértékelésére szolgáló keretrendszer aktualizált változatát, és az említett változatot a közzététel előtt, 2020 októberében szakértők egy munkaértekezlet keretein belül hitelesítették.

1.3 CÉLKÖZÖNSÉG

E jelentés célközönsége az NKBS, és tágabb értelemben a kiberbiztonsági képességek tervezéséért, megvalósításáért és értékeléséért felelős, illetve ezekben részt vevő politikai döntéshozók, szakértők és kormánytisztviselők. Továbbá az ebben a dokumentumban formalizált megállapítások nemzeti és európai szinten is értékesek lehetnek a kiberbiztonsági politikával foglalkozó szakértők és kutatók számára.

[2] Becker, J., Knackstedt, R., és Pöppelbuß, J.: Developing Maturity Models for IT Management: A Procedure Model and its Application, *Business & Information Systems Engineering*, 1. kiad.,3. sz., 2009. június, 213–222. o.
[3] E kutatás alkalmazásában a jelentésben említett „európai országok” a 27 uniós tagállamot foglalják magukban.

2. HÁTTÉR

2.1 AZ NKBS ÉLETCIKLUSÁVAL KAPCSOLATBAN VÉGZETT KORÁBBI MUNKA

Az uniós kiberbiztonsági jogszabály szerint az ENISA egyik fő célkitűzése, hogy támogassa a tagállamokat a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiák kidolgozásában, az említett stratégiák terjesztésének előmozdításában és azok végrehajtásának figyelemmel kísérésében. Feladatai körében az ENISA számos dokumentumot hozott létre e témakörben azért, hogy előmozdítsa a bevált gyakorlatokat és támogassa az NKBS-ek Unióban történő végrehajtását:

- „Practical guide on the development and execution phase of NCSS" (magyarul: „A nemzeti kiberbiztonsági stratégiák fejlesztési és végrehajtási fázisára vonatkozó gyakorlati útmutató")[4], amelyet 2012-ben tettek közzé;
- „Setting the course for national efforts to strengthen security in cyberspace" (magyarul: „A kibertér biztonságának megerősítésére irányuló nemzeti erőfeszítések irányának meghatározása")[5], amelyet 2012-ben tettek közzé;
- Az ENISA tagállamok nemzeti kiberbiztonsági stratégiáinak értékelésére vonatkozó első keretrendszere[6], amelyet 2014-ben tettek közzé;
- „Online NCSS Interactive Map" (magyarul: „NKBS-re vonatkozó online interaktív térkép")[7], amelyet 2014-ben tettek közzé;
- „NCSS Good Practice Guide" (magyarul: NKBS – útmutató a bevált gyakorlatokhoz")[8], amelyet 2016-ban tettek közzé;
- „National Cybersecurity Strategies Evaluation Tool" (magyarul: „A nemzeti kiberbiztonsági stratégiák értékelési eszköze")[9], amelyet 2018-ban tettek közzé;
- „Good practices in innovation on Cybersecurity under the NCSS" (magyarul: „Az NKBS keretében a kiberbiztonság terén végzett innováció bevált gyakorlatai")[10], amelyet 2019-ben tettek közzé.

[4] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] National Cybersecurity Strategies - Interactive Map (ENISA, 2014, frissítve 2019-ben)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Ez a dokumentum a 2012. évi útmutató frissített verziója: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Az A. MELLÉKLET tartalmaz egy rövid összefoglalót az ENISA e témakörben kiadott fő dokumentumairól.

Az említett útmutatókat és dokumentumokat a másodelemzés során tanulmányozták. Különösen a „National Cybersecurity Strategies Evaluation Tool”[11] című dokumentum az NCAF alapvető eleme. Az NCAF az NKBS online értékelési eszközében foglalt célkitűzésekre épül.

2.2 AZ EURÓPAI NKBS-EKBEN AZONOSÍTOTT KÖZÖS CÉLKITŰZÉSEK

Az egyes tagállamok közötti különbözőségek megnehezítik a közös cselekvések és cselekvési tervek azonosítását a különböző nemzeti környezetek, jogi keretek és politikai menetrendek között. Ugyanakkor a tagállamok NKBS-einek stratégiai célkitűzései gyakran csoportosulnak ugyanazon témák köré. Ezért az ENISA tagállamok NKBS-eire vonatkozó korábbi munkája és elemzése alapján 22 stratégiai célkitűzést azonosítottak. Ezek közül 15-öt már az ENISA korábbi munkája során azonosítottak, ebben a tanulmányban pedig 2 újat adtak hozzá, illetve 5 célkitűzést határoztak meg későbbi megfontolásra.

2.2.1 A tagállamok közös stratégiai célkitűzései

Az ENISA korábbi munkája, nevezetesen a nemzeti kiberbiztonsági stratégiák értékelési eszköze[12] alapján az alábbi táblázatban fel van tüntetve az a már említett 15 stratégiai célkitűzés, amely általánosan szerepel a tagállamok nemzeti kiberbiztonsági stratégiáiban. A célok felvázolják a témára vonatkozó általános „nemzeti filozófia” lényegét. Az alábbiakban ismertetett célkitűzésekre vonatkozó további információk az ENISA „NCSS Good Practice Guide” című jelentésében[13] találhatók.

1. táblázat: A tagállamok NKBS-ében található közös stratégiai célkitűzések

Azonosító	NKBS stratégiai célkitűzései	Célok
1	**Nemzeti kibervészhelyzeti tervek megalkotása**	▶ Azoknak a kritériumoknak a bemutatása és kifejtése, amelyek alapján egy helyzetet válságként kell meghatározni; ▶ A válság kezelésére szolgáló kulcsfontosságú eljárások és intézkedések meghatározása; és ▶ A különböző érdekelt felek kiberbiztonsági válság idején betöltött szerepkörének és felelősségi körének egyértelmű meghatározása. ▶ Azoknak a kritériumoknak a bemutatása és kifejtése, amelyek alapján egy válságot megszűntnek lehet nyilvánítani, és/vagy annak bemutatása és kifejtése, kinek van felhatalmazása a válság végének kihirdetésére.
2	**Biztonsági alapintézkedések létrehozása**	▶ A köz- és magánszektor szervezetei által alkalmazott különböző gyakorlatok összehangolása; ▶ Az illetékes állami hatóságok és a szervezetek között használatos közös nyelv megalkotása, továbbá biztonságos kommunikációs csatornák megnyitása; ▶ Annak lehetővé tétele, hogy a különböző érdekelt felek leellenőrizhessék és összehasonlítva értékeljék saját kiberbiztonsági képességeiket; ▶ A bevált kiberbiztonsági gyakorlatokkal kapcsolatos információk megosztása minden iparágban; és

[11] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[12] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Ez a dokumentum a 2012. évi útmutató frissített verziója: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Azonosító	NKBS stratégiai célkitűzései	Célok
		▶ Az érdekelt felek támogatása abban, hogy befektetéseik terén elsőbbséget biztosítsanak a biztonságnak.
3	Kiberbiztonsági gyakorlatok szervezése	▶ Annak meghatározása, miket kell tesztelni (tervek és eljárások, emberek, infrastruktúra, reakcióképességek, együttműködési képességek, kommunikáció stb.); ▶ Egy nemzeti kibervédelmi gyakorlatot megtervező csapat felállítása, egyértelmű feladatok meghatározásával; és ▶ A kibervédelmi gyakorlatok beépítése a nemzeti kiberbiztonsági stratégia életciklusába vagy a nemzeti kibervészhelyzeti tervbe.
4	Biztonsági eseményekre való reagálás képességének kialakítása	▶ Megbízatás – azokra a hatáskörökre, szerepkörökre és felelősségi körökre vonatkozik, amelyekkel az érintett kormánynak fel kell ruháznia a csapatot; ▶ Szolgáltatási portfólió – olyan szolgáltatásokat foglal magában, amelyet egy csapat biztosít választócsoportja számára, illetve amelyeket saját belső működéséhez használ; ▶ Operatív képességek – olyan technikai és operatív követelményekre vonatkozik, amelyeknek egy csapatnak meg kell felelnie; és ▶ Együttműködési képességek – ezek magukban foglalják az olyan más csapatokkal való információcserére vonatkozó követelményeket, amelyek nem tartoznak az előző három kategóriába, pl. politikai döntéshozók, hadsereg, szabályozó szervek, (kritikus információs infrastruktúrával foglalkozó) üzemeltetők, bűnüldöző hatóságok.
5	Felhasználói tudatosság növelése	▶ Kiberbiztonsági vagy információbiztonsági kérdésekre vonatkozó ismeretbeli hiányosságok azonosítása; és ▶ A hiányosságok megszüntetése tudatosságnövelés vagy a tudásalapok fejlesztése/megerősítése révén.
6	Képzési és oktatási programok megerősítése	▶ A meglévő információbiztonsági munkaerő operatív képességeinek növelése; ▶ Tanulók ösztönzése, hogy csatlakozzanak a kiberbiztonsági területhez, majd arra való felkészítésük, hogy bejussanak; ▶ Az információbiztonsággal foglalkozó tudományos környezet és az információbiztonsági iparág közötti kapcsolatok előmozdítása és ösztönzése; és ▶ A kiberbiztonsági képzés összehangolása az üzleti igényekkel.
7	K+F támogatása	▶ A sebezhetőségek mögött meghúzódó valódi okok azonosítása a hatásuk helyrehozása helyett; ▶ Különböző tudományágak tudósainak összefogása annak érdekében, hogy megoldást találjanak az olyan többdimenziós és összetett problémákra, mint a fizikai-kiberbiztonsági fenyegetések; ▶ Az ipar igényeinek és a kutatások eredményeinek egybegyűjtése, ezáltal elősegítve az elméletről gyakorlatra váltást; és ▶ A meglévő kiberinfrastruktúrákat támogató termékek és szolgáltatások kiberbiztonsági szintjének fenntartása mellet olyan lehetőségek keresése, amelyek révén növelhető az említett biztonsági szint.
8	A magánszektor ösztönzése a biztonsági intézkedésekbe való befektetésre	▶ Olyan lehetséges ösztönző programok meghatározása, amelyek a magánvállalatokat biztonsági intézkedésekbe történő befektetésre buzdítják; és ▶ Ösztönző programok biztosítása a vállalatok számára a biztonsági befektetések serkentésére.
9	A kritikus információs infrastruktúra, az alapvető szolgáltatásokat nyújtó szereplő (OES) és a digitális szolgáltató (CII) védelme	▶ A kritikus információs infrastruktúra (critical information infrastructure, CII) meghatározása; és ▶ A CII-t érintő releváns kockázatok azonosítása és csökkentése.
10	A kiberbűnözés kezelése	▶ Jogszabályok alkotása a kiberbűnözés területén; és ▶ A bűnüldöző hatóságok eredményességének növelése.

Azonosító	NKBS stratégiai célkitűzései	Célok
11	Biztonsági események bejelentésére vonatkozó mechanizmusok létrehozása	▶ Az általános fenyegetettségi környezet megismerése; ▶ A biztonsági események (pl. biztonsági szabályok megsértése, hálózati hibák, szolgáltatásmegszakítások) hatásainak kiértékelése ; ▶ A meglévő és új sebezhetőségekre és támadástípusokra vonatkozó ismeretek szerzése; ▶ A biztonsági intézkedések megfelelő aktualizálása; és ▶ A hálózati és információs rendszerek biztonságáról szóló irányelvben foglalt, biztonsági események bejelentésére vonatkozó rendelkezések végrehajtása.
12	Magánélet- és adatvédelem megerősítése	▶ A magánéletet érintő alapvető jogok és adatvédelem megerősítésében való közreműködés.
13	Köz- és magánszféra közötti partnerség létrehozása	▶ Elrettentés (támadók elrettentése); ▶ Védelem (biztonsági fenyegetésekkel kapcsolatos kutatás használatával); ▶ Észlelés (új fenyegetések kezelésére vonatkozó információmegosztás alkalmazásával); ▶ Reagálás (egy biztonsági esemény kezdeti hatásának kezelésére való képesség biztosításához); és ▶ Helyreállítás (egy biztonsági esemény végső hatásának helyreállítására való képesség biztosításához).
14	Állami ügynökségek közötti együttműködés intézményesítése	▶ Az állami ügynökségek közötti együttműködés kiberbiztonsággal kapcsolatos felelősségi körökkel és kompetenciákkal való növelése; ▶ A kompetenciák és erőforrások állami ügynökségek közötti átfedésének elkerülése; és ▶ Az állami ügynökségek közötti együttműködés javítása és intézményesítése különböző kiberbiztonsági területeken.
15	Nemzetközi együttműködésben való részvétel (nem csupán uniós tagállamokkal)	▶ Az uniós tagállamok közös tudásbázisának létrehozásából származó előnyök kiaknázása; ▶ Szinergikus hatások létrehozása a nemzeti kiberbiztonsági hatóságok között; és ▶ Nemzetközi bűncselekmények elleni harc lehetővé tétele és fokozása.

2.2.2 További stratégiai célkitűzések

Az ENISA által elvégzett másodelemzés és lefolytatott interjúk alapján további stratégiai célkitűzések kerültek meghatározásra. A tagállamok egyre inkább foglalkoznak ezekkel a témákkal saját NKBS-ükben, illetve cselekvési terveket határoznak meg ebben a témában. A tagállamok által végrehajtott intézkedések példái is rendelkezésre állnak. Amennyiben egy példa egy nyilvánosan elérhető forrásból származik, a hivatkozás szerepel a szövegben. Azokban az esetekben, amikor a példák uniós tagállamok tisztviselőivel készített bizalmas interjúkon alapulnak, nincs hivatkozás megjelölve.

A meghatározott további stratégiai célkitűzések a következők:

- Az ellátási lánc kiberbiztonságának növelése; és
- Digitális személyazonosság biztonságának garantálása és a digitális közszolgáltatásokba vetett bizalom felépítése.

Az ellátási lánc kiberbiztonságának növelése

A kis- és középvállalkozások (kkv-k) az európai gazdaság gerincét képezik. Az Unióban található összes vállalkozás 99 %-át teszik ki[14], valamint a 2015. évi becslések szerint a kkv-k hozták létre az új munkahelyek körülbelül 85 %-át és a teljes uniós magánszektorbeli foglalkoztatás kétharmadáért is ők felelnek. Továbbá mivel a kkv-k nagyvállalatoknak nyújtanak szolgáltatásokat és egyre inkább együttműködnek a közigazgatási szervekkel[15], meg kell jegyezni, hogy a jelenlegi összekapcsolt kontextusban a kkv-k a kibertámadások gyenge láncszemének számítanak. Valóban a kkv-k vannak leginkább kitéve a kibertámadásoknak, mégis gyakran nem engedhetik meg maguknak, hogy kellő mértékben befektessenek a kiberbiztonságba[16]. Az ellátási lánc kiberbiztonságának növelését ezért a kkv-kra összpontosítva kell megvalósítani.

E rendszerszintű megközelítés mellett a tagállamok összpontosíthatják erőfeszítéseiket az alábbi konkrét IKT-szolgáltatások és alapvetőnek számító termékek kiberbiztonságára is: a kritikus információs infrastruktúrában használt IKT-technológiák, a távközlési ágazatban végrehajtott biztonsági mechanizmusok (ellenőrzések internetszolgáltatói szinten stb.), bizalmi szolgáltatások az eIDAS-rendeletben meghatározottak szerint, valamint felhőszolgáltatók. Például Lengyelország a 2019–2024. évi nemzeti kiberbiztonsági stratégiájában[17] elköteleződött egy olyan nemzeti kiberbiztonsági értékelési és tanúsítási rendszer kidolgozása mellett, amely az ellátási lánc minőségbiztosításának mechanizmusaként szolgál. Az említett tanúsítási rendszer igazodni fog az Unió kiberbiztonsági jogszabályában (2019/881) megállapított digitális IKT-termékek, -szolgáltatások és -folyamatok tanúsítási keretrendszeréhez.

Az ellátási lánc kiberbiztonságának növelése ezért kiemelkedő fontosságú. Ez többek között a kkv-k támogatására szolgáló erős szakpolitikák létrehozásával, a közigazgatási közbeszerzési eljárások kiberbiztonsági követelményeire vonatkozó iránymutatások biztosításával, a magánszektoron belüli együttműködés elősegítésével, a köz- és magánszféra közötti partnerségek (PPP) kialakítása révén, összehangolt sebezhetőség-feltárási (CVD) mechanizmusok támogatásával[18], terméktanúsítási rendszerek – beleértve a kkv-kra vonatkozó digitális kezdeményezésekben foglalt kiberbiztonsági alkotóelemek – megalkotásával, valamint képességfejlesztés finanszírozásával érhető el.

Digitális személyazonosság biztonságának garantálása és a digitális közszolgáltatásokba vetett bizalom felépítése

2020 februárjában az „Shaping Europe's digital future" (magyarul: „Európa digitális jövőjének alakítása")[19] című közleményében az Európai Bizottság ismertette az Unió digitális átalakulásával kapcsolatos jövőképét azzal a céllal, hogy olyan inkluzív technológiákat biztosítson, amelyek az emberek számára működnek és tiszteletben tartják az Unió alapvető értékeit. A közlemény különösen azt állítja, hogy a közigazgatási szervek digitális átalakulásának Európa-szerte történő előmozdítása alapvető fontosságú. Éppen ezért a digitális személyazonossággal kapcsolatban a kormányzatba, valamint a közszolgáltatásokba vetett bizalom felépítése rendkívül fontos. Ez még fontosabb abban az esetben, ha figyelembe vesszük a tényt, miszerint a közszféra tranzakciói és az adatátvitelek gyakran érzékeny természetűek.

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16] https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Shaping Europe's digital future, COM(2020) 67 final
https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

Számos ország, nevezetesen az alábbiak szándékukat fejezték ki arra vonatkozóan, hogy az említett témával foglalkozzanak saját nemzeti kiberbiztonsági stratégiájukban: Dánia, Egyesült Királyság, Észtország, Franciaország, Hollandia, Luxemburg, Málta és Spanyolország. Az említett országok közül néhányan azt is elmondták, hogy ezzel a stratégiai célkitűzéssel egy átfogóbb terv részeként is lehetne foglalkozni:

- Észtország saját „Az elektronikus személyazonosság és elektronikus hitelesítési képesség biztonsága” című kapcsolódó cselekvési tervét összeköti átfogó, 2020. évi digitális menetrendjével.
- A francia NKBS kifejti, hogy a digitális technológiáért felelős államtitkár felügyeli az ütemterv kidolgozását a „francia emberek digitális életének, magánéletének és személyes adatainak védelme érdekében”.
- Hollandia NKBS-e ismerteti, hogy a közigazgatási szervek, valamint a polgároknak és vállalkozásoknak biztosított közszolgáltatások kiberbiztonságával részletesen foglalkozik a Digitális kormányzás átfogó menetrendje.
- Mivel az Egyesült Királyság kormánya egyre több szolgáltatását online térbe helyezi, kinevezte a Kormányzati Digitális Szolgálatot (Government Digital Service, GDS) annak biztosítására, hogy a Brit Nemzeti Kiberbiztonsági Központ (British National Cybersecurity Centre, NCSC) támogatásával a kormány által kidolgozott vagy létrehozott új digitális szolgáltatások „alapértelmezés szerint biztonságosak” legyenek.

2.2.3 Egyéb figyelembe vett stratégiai célkitűzések

Az ENISA által elvégzett másodelemzési fázis során és a lefolytatott interjúk részeként további stratégiai célkitűzéseket tanulmányoztak. Azonban az a döntés született, hogy ezek a célkitűzések nem képezik az önértékelési keretrendszer részét. C. MELLÉKLET – Egyéb tanulmányozott célkitűzések

meghatározza az összes olyan célkitűzést, amely felhasználható az NKBS lehetséges javításáról szóló jövőbeni eszmecserék előmozdítására.

Az alábbi stratégiai célkitűzéseket tanulmányozták jövőbeni megfontolásra:

- Ágazatspecifikus kiberbiztonsági stratégiák kidolgozása;
- Dezinformációs kampányok elleni küzdelem;
- Élvonalbeli technológiák (5G, MI, kvantuminformatika stb.) biztonságosságának garantálása;
- Adatszuverenitás biztosítása; és
- A kiberbiztosítási ágazat fejlesztésére vonatkozó ösztönző programok biztosítása.

2.3 A TELJESÍTMÉNYMÉRŐ GYAKORLAT FŐ TÉNYEZŐI

A kiberbiztonsággal kapcsolatos meglévő érettségi modellek másodelemzését azzal a céllal végezték el, hogy információt és bizonyítékokat gyűjtsenek az NKBS területére vonatkozó nemzeti képességek önértékelési keretrendszere megtervezésének támogatására. Ebben az összefüggésben a meglévő modellek átfogó szakirodalmi áttekintését azért végezték el, hogy kiegészítsék a 2.1. és a 2.2. szakaszban kialakított kezdeti, kiberbiztonsági érettségi modellekkel és meglévő NKBS-ekkel kapcsolatos megalapozó kutatás megállapításait. Ez a szisztematikus áttekintés segíti az értékelési keretrendszer érettségi szintjeinek kiválasztását és indoklását, valamint a különféle dimenziók és mutatók meghatározását.

Az érettségi modell szisztematikus áttekintése keretében 10 modellt vettek figyelembe és elemeztek fő jellemzőik alapján. Az e tanulmány keretében végzett szakirodalmi áttekintés

tárgyát képező modellek fő jellemzőinek átfogó helyzetképe a 2. táblázatban – Elemzett érettségi modellek helyzetképe, részletesebb leírása pedig az A. MELLÉKLETBEN található.

2. táblázat: Elemzett érettségi modellek helyzetképe

Modell neve	Érettségi szintek száma	Attribútumok száma	Értékelési módszer	Eredmények ábrázolása
Kiberbiztonsági kapacitás érettségi modellje a nemzetek számára (CMM)	5	5 fő dimenzió	Együttműködés egy helyi szervezettel a modell nemzeti környezetben történő alkalmazása előtti finomhangolása érdekében	ötrészes radar
Kiberbiztonsági képességérettségi modell (C2M2)	4	10 fő tartomány	Önértékelési módszertan és eszköztár	Eredménymutató kördiagramokkal
Kritikus infrastruktúra kiberbiztonságának javítására szolgáló keretrendszer	n.a. (4 lépcső)	5 alapvető funkció	Önértékelés	n.a.
Katari kiberbiztonsági képességérettségi modell (Q-C2M2)	5	5 fő tartomány	n.a.	n.a.
Kiberbiztonsági érettségi modellre vonatkozó tanúsítás (CMMC)	5	17 fő tartomány	Harmadik fél ellenőr által végzett értékelés	n.a.
Közösségi kiberbiztonsági érettségi modell (CCSMM)	5	6 fő dimenzió	Közösségeken belül végzett értékelés állami és szövetségi bűnüldöző hatóságok hozzájárulásával	n.a.
Információbiztonsági érettségi modell a NIST kiberbiztonsági keretrendszer tekintetében (ISMM)	5	23 értékelt terület	n.a.	n.a.
A belső ellenőrzési képesség modellje (IA-CM) a közszféra számára	5	6 elem	Önértékelés	n.a.
Globális kiberbiztonsági index (GCI)	n.a.	5 pillér	Önértékelés	Rangsortáblázat
Kibererőindex (CPI)	n.a.	4 kategória	A Gazdasági Hírszerző Egység által végzett teljesítménymérés	Rangsortáblázat

Ez a szisztematikus áttekintés lehetővé tette a meglévő modellekben alkalmazott bevált gyakorlatokra vonatkozó olyan következtetések levonását, amelyek segítik a jelenlegi érettségi modellel kapcsolatos koncepcionális modell kidolgozását. Főleg a teljesítménymérő gyakorlat segített az érettségi szintek meghatározásában, a dimenziócsoportok megalkotásában és a mutatók, valamint a modell eredményeire vonatkozó megfelelő megjelenítési módszertan kiválasztásában. Az egyes elemekre vonatkozó legfontosabb megállapítások részletei a 3. táblázatban találhatók.

3. táblázat: A teljesítménymérő gyakorlat fő tényezői

Jellemző	Fő tényező
Érettségi szintek	▶ A kiberbiztonsági képességek értékelési keretrendszereinek ötszintű érettségi skálája általánosan elfogadott és képes részletes értékelési eredményeket szolgáltatni (az egyes modellek érettségi szintjeinek részletes leírásáért lásd: 6. táblázat Érettségi szintek összehasonlítása; ▶ Minden modell biztosítja az egyes érettségi szintek magas szintű meghatározását, amelyet aztán a különböző dimenziókhoz vagy dimenziócsoportokhoz igazítanak; ▶ A kiberbiztonsági képességek érettségének mérésekor általában két fő szempontot értékelnek: a stratégiák érettségét és a stratégiák végrehajtására bevezetett folyamatok érettségét.
Attribútumok	▶ A meglévő érettségi modellek attribútumainak összehasonlító elemzése eltérő eredményeket mutat, modellenként átlagosan négy és öt közötti attribútumszámmal; ▶ A körülbelül négy vagy öt attribútumra épülő modell biztosítja az országok számára a megfelelő szintű adatrészletességet azáltal, hogy csoportosítja a megfelelő dimenziókat és garantálja az eredmények olvashatóságát (az egyes modellek attribútumainak leírásáért lásd: 7. táblázat – Attribútumok/**dimenziók** összehasonlítás); ▶ A csoportok meghatározásakor az összes modell által elfogadott legfőbb elv az egyes csoportokba besorolt elemek következetességén alapul.
Értékelési módszer	▶ A különböző elemzett modellekben alkalmazott értékelési módszerek eltérnek egymástól; ▶ A leggyakoribb értékelési módszer az önértékelésen alapul.
Eredmények ábrázolása	▶ Fontos az eredmények különféle részletességi szinteken történő bemutatása; ▶ A megjelenítési módszertannak magától értetődőnek és könnyen olvashatónak kell lennie.

A koncepcionális modellt a különböző érettségi modellek teljesítménymérő gyakorlata, valamint az ENISA korábbi munkája alapján dolgozták ki. Továbbá az a döntés született, hogy az *ENISA online interaktív eszközét* használják az egyes attribútumok érettségi mutatóinak kidolgozásához.

2.4 AZ NKBS ÉRTÉKELÉSÉRE VONATKOZÓ KIHÍVÁSOK

A tagállamok számos kihívással szembesülnek kiberbiztonsági képességeik kialakítása során, pontosabban akkor, amikor biztosítaniuk kell, hogy képességeik naprakészek legyenek a legújabb fejleményekhez viszonyítva. Az alábbiakban azoknak a kihívásoknak az összefoglalója olvasható, amelyeket e tanulmány keretében a tagállamok azonosítottak és megvitattak:

- **Nehézségek az összehangolásban és együttműködésben:** a kiberbiztonsági erőfeszítések nemzeti szintű összehangolása a kiberbiztonsági problémákra vonatkozó megfelelő válasz kidolgozása érdekében kihívás lehet az érdekelt felek nagy száma miatt.
- **Az értékelés elvégzéséhez szükséges erőforrások hiánya:** a helyi körülményektől és a kiberbiztonság nemzeti irányítási struktúrájától függően az NKBS és célkitűzéseinek értékelése akár 15 munkanapot is igénybe vehet.
- **Támogatás hiánya a kiberbiztonsági képességek kidolgozása során:** néhány tagállam kiemelte, hogy az erre irányuló költségvetés megvédéséhez és a kiberbiztonsági képességek kidolgozására irányuló támogatás megszerzéséhez először egy értékelési fázis során azonosítaniuk kell a hiányosságokat és korlátokat.
- **Nehézségek a stratégiának tulajdonított sikerek vagy változások terén:** a fenyegetések folyamatos jelenléte és a technológia fejlődése miatt szükségszerű, hogy

a cselekvési terveket ezekhez igazítsák. Azonban egy NKBS kiértékelése és a változások stratégiának tulajdonítása továbbra is fáradságos feladat. Ez viszont megnehezíti az NKBS korlátainak és hiányosságainak azonosítását.

- **Az NKBS eredményessége mérésének nehézségei:** mérőszámok gyűjthetők olyan különféle területek mérésére, mint az előrehaladás, végrehajtás, érettség és eredményesség. Míg a végrehajtás és előrehaladás mérése viszonylag egyszerű az eredményesség méréséhez képest, ez utóbbi jelentősebb szerepet játszik egy NKBS eredményeinek és hatásainak értékelésében. Az ENISA által végzett interjúk alapján sok tagállam úgy véli, hogy egy NKBS eredményességének kvantitatív mérése fontos, de nagyon nehéz feladat, néhány esetben pedig jóformán lehetetlen.
- **Közös keretrendszer elfogadásának nehézsége:** az Európai Unió tagállamai különböző környezetben működnek a politikát, szervezeteket, kultúrát, társadalomszerkezetet és NKBS-érettséget illetően. A tanulmány keretében megkérdezett egyes tagállamok hangot adtak véleményüknek, miszerint nehézségekbe ütközhet egy mindenki által egységesen alkalmazandó önértékelési keretrendszer megvédése és használata.

2.5 A NEMZETI KÉPESSÉGEK ÉRTÉKELÉSÉNEK ELŐNYEI

2017 óta minden uniós tagállam rendelkezik nemzeti kiberbiztonsági stratégiával[20]. Bár ez egy pozitív fejlemény, az is fontos, hogy a tagállamok képesek legyenek értékelni az NKBS-eket, így teremtve hozzáadott értéket a stratégiai tervezésükhöz és végrehajtásukhoz.

A Nemzeti képességek értékelésének keretrendszere egyik fő célja, hogy a különféle NKBS-ekben meghatározott prioritások alapján értékelje a kiberbiztonsági képességeket. A keretrendszer alapvetően a tagállamok kiberbiztonsági képességeinek érettségi szintjét értékeli az NKBS célkitűzései által meghatározott tartományokon belül. Így a keretrendszer eredményei támogatják a tagállamok politikai döntéshozóit a kiberbiztonságra vonatkozó nemzeti stratégia meghatározásában azáltal, hogy országos információkat szolgáltatnak az aktuális helyzetről[21]. Az NCAF végső soron arra szolgál, hogy segítse a tagállamokat a javítási területek azonosításában és a képességek kiépítésében.

A keretrendszer célja, hogy a nemzeti kiberbiztonsági stratégiáik célkitűzéseinek értékelése révén saját érettségi szintjükre vonatkozó önértékelési lehetőséget nyújtson a tagállamoknak, amely mind stratégiai, mind működési szinten segítséget nyújt számukra a kiberbiztonsági képességeik megerősítésében és kiépítésében.

Egy gyakorlatiasabb megközelítés szerint, az ENISA által az egyes tagállamokban a kiberbiztonság területéért felelős ügynökségekkel készített interjúk alapján a Nemzeti képességek értékelésének keretrendszerére vonatkozóan az alábbi előnyöket azonosították és emelték ki:

- Hasznos információk biztosítása egy hosszú távú stratégia kidolgozásához (pl. bevált gyakorlatok, iránymutatások);
- Az NKBS hiányzó elemeinek azonosítása;
- Kiberbiztonsági képességek továbbépítése;
- Politikai intézkedések elszámoltathatóságának támogatása;
- Hitelesség biztosítása a polgároknak és nemzetközi partnereknek;

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999): *The interface between evaluation and public policy*. Értékelés, 5(4), 468–486.

- Tájékoztatás támogatása és a nyilvánosság körében az átlátható szervezetről kialakult kép erősítése;
- A felmerülő kérdések és problémák előrejelzése;
- A levont tanulságok és bevált gyakorlatok azonosítása;
- Kiberbiztonsági kapacitásra vonatkozó alapforgatókönyv biztosítása uniószerte eszmecserék elősegítése érdekében; és
- A kiberbiztonságra vonatkozó nemzeti képességek értékelése.

3. A NEMZETI KÉPESSÉGEK ÉRTÉKELÉSÉNEK KERETRENDSZERÉRE VONATKOZÓ MÓDSZERTAN

3.1 ÁLTALÁNOS CÉL

Az NCAF **fő célkitűzése** a **tagállamok** kiberbiztonsági képességei érettségi szintjének mérése annak érdekében, hogy támogassa őket saját nemzeti kiberbiztonsági képességük értékelésének elvégzésében, az ország érettségi szintjére vonatkozó tudatosság növelésében, a fejlődési területek azonosításában és a kiberbiztonsági képességek kialakításában.

3.2 ÉRETTSÉGI SZINTEK

A keretrendszer **öt érettségi szintre** épül, amelyek meghatározzák azokat a szakaszokat, amelyeken egy tagállam keresztülmegy az NKBS egyes célkitűzései által lefedett területek kiberbiztonsági képességeinek kialakítása során. A szintek az érettség növekvő szintjeit jelölik az **1. szintről** kiindulva, amelyben a tagállamok nem rendelkeznek az NKBS célkitűzései által lefedett területeken a kiberbiztonsági kapacitásépítésre vonatkozó, világosan meghatározott megközelítéssel, és az **5. szinttel** befejezve, amelyben a kiberbiztonsági kapacitásépítési stratégia dinamikus és alkalmazkodik a környezeti változásokhoz. A 4. táblázat bemutatja az érettségi szintek skáláját és megmagyarázza az egyes érettségi szinteket.

4. táblázat: Az ENISA Nemzeti képességek értékelésének keretrendszerére vonatkozó ötszintű érettségi skálája

1. SZINT – KEZDETI / *AD HOC*	2. SZINT – KORAI MEGHATÁROZÁS	3. SZINT – LÉTREHOZÁS	4. SZINT – OPTIMALIZÁLÁS	5. SZINT – ALKALMAZKODÓKÉPESSÉG
A tagállam nem rendelkezik az NKBS célkitűzései által lefedett területeken a kiberbiztonsági kapacitásépítésre vonatkozó, világosan meghatározott megközelítéssel. Ugyanakkor az országnak lehetnek általános céljai, és már elvégezhetett néhány, a nemzeti képességek javítását szolgáló (technikai, politikai, szakpolitikai) tanulmányt.	Az NKBS célkitűzései által lefedett területen történő kapacitásépítés nemzeti megközelítését már meghatározták. A cselekvési terveket, illetve az eredmények eléréséhez szükséges tevékenységeket már kidolgozták, de ezek még csak korai szakaszban vannak. Továbbá lehetséges, hogy az aktív érdekelt feleket már azonosították és/vagy bevonták a munkába.	Az NKBS célkitűzései által lefedett területen történő kapacitásépítés cselekvési tervét már világosan meghatározták, valamint azt az érintett érdekelt felek támogatják. A gyakorlatokat és tevékenységeket nemzeti szinten egységesen hajtják végre és juttatják érvényre. A tevékenységeket világos forráselosztással és irányítással, valamint meghatározott határidőkkel állapítják meg és dokumentálják.	A cselekvési tervet rendszeres értékelésnek vetik alá: fontossági sorrendbe állítják, optimalizálják és fenntarthatóvá teszik. A kiberbiztonsági kapacitásépítő tevékenységek teljesítményét rendszeresen mérik. Azonosítják a sikertényezőket, valamint a tevékenységek végrehajtására vonatkozó kihívásokat és az abban rejlő hiányosságokat.	A kiberbiztonsági kapacitásépítési stratégia dinamikus és alkalmazkodó. A környezeti változásokra (műszaki haladásra, globális konfliktusra, új fenyegetésekre stb.) való állandó figyelem elősegíti a gyors döntés, valamint a fejlődés érdekét szolgáló gyors cselekvés képességét.

3.3 AZ ÖNÉRTÉKELÉSI KERETRENDSZER CSOPORTJAI ÉS ÁTFOGÓ STRUKTÚRÁJA

Az önértékelési keretrendszert **négy csoport** jellemzi: a (I) Kiberbiztonsági irányítás és szabványok, a (II) Kapacitásépítés és tudatosságnövelés, a (III) Jogi és szabályozási kérdések, valamint az (IV) Együttműködés. Az említett csoportok mindegyike a kiberbiztonsági kapacitásépítés egyik kulcsfontosságú tematikus területét fedi le egy országban, továbbá olyan különféle célkitűzéseket tartalmaz, amelyeket a tagállamok beépíthetnek saját NKBS-ükbe. Ideértendők különösen az alábbiak:

- **(I) Kiberbiztonsági irányítás és szabványok**: ez a csoport méri, hogy a tagállamok képesek-e megfelelő irányítást megvalósítani, szabványokat és bevált gyakorlatokat létrehozni a kiberbiztonság területén. Ez a dimenzió a kibervédelem és a kibertámadásokkal szembeni ellenálló képesség különböző vonatkozásait veszi figyelembe, miközben támogatja a nemzeti kiberbiztonsági ipar fejlődését és növeli a kormányokba vetett bizalmat;
- **(II) Kapacitásépítés és tudatosságnövelés**: ez a csoport kiértékeli, hogy a tagállamok képesek-e növelni a tudatosságot a kiberbiztonsági kockázatok és fenyegetések tekintetében, valamint arra vonatkozóan, hogyan kell ezeket kezelni. Továbbá ez a dimenzió azt is felméri, hogy az ország képes-e folyamatosan építeni saját kiberbiztonsági képességeit, valamint növelni a tudás és szakértelem általános szintjét az említett tartományon belül. Foglalkozik a kiberbiztonság piacának fejlődésével és a kiberbiztonsági K+F előrehaladásával. Ez a csoport átrendezi az összes célkitűzést, amely megalapozza a kapacitásépítés előmozdítását;
- **(III) Jogi és szabályozási kérdések**: ez a csoport méri, hogy a tagállamok képesek-e bevezetni a szükséges jogi és szabályozási eszközöket a kiberbűnözés és kapcsolódó

kiberbiztonsági események elterjedésének kezelésére és leküzdésére, valamint a kritikus információs infrastruktúra védelmére. Emellett ez a dimenzió méri fel azt is, hogy a tagállamok képesek-e egy olyan jogi keret létrehozására, amely megóvja a polgárokat és vállalkozásokat – például – a magánélet védelme és a biztonság közötti egyensúly megteremtése során; és

- **(IV) Együttműködés:** ez a csoport fontos eszközként nemzeti és nemzetközi szinten kiértékeli a különböző érdekelt felek csoportjai közötti együttműködést és információmegosztást a folyamatosan változó fenyegetettségi környezet jobb megértése és a jobb válaszadás érdekében.

A modellben szereplő célkitűzések azok, amelyeket a tagállamok általánosan elfogadnak, és amelyeket a 2.2. szakaszban felsorolt célkitűzések közül választottak ki. A modell különösen az alábbi célkitűzéseket értékeli:

- 1. Nemzeti kibervészhelyzeti tervek megalkotása (I)
- 2. Biztonsági alapintézkedések létrehozása (I)
- 3. Digitális személyazonosság biztonságának garantálása és a digitális közszolgáltatásokba vetett bizalom felépítése (I)
- 4. Biztonsági eseményekre való reagálás képességének kialakítása (II)
- 5. Felhasználói tudatosság növelése (II)
- 6. Kiberbiztonsági gyakorlatok szervezése (II)
- 7. Képzési és oktatási programok megerősítése (II)
- 8. K+F támogatása (II)
- 9. A magánszektor ösztönzése a biztonsági intézkedésekbe való befektetésre (II)
- 10. Az ellátási lánc kiberbiztonságának növelése (II)
- 11. A kritikus információs infrastruktúra, az alapvető szolgáltatásokat nyújtó szereplő (OES) és a digitális szolgáltató védelme (III)
- 12. A kiberbűnözés kezelése (III)
- 13. Biztonsági események bejelentésére vonatkozó mechanizmusok létrehozása (III)
- 14. Magánélet- és adatvédelem megerősítése (III)
- 15. Állami ügynökségek közötti együttműködés intézményesítése (IV)
- 16. Nemzetközi együttműködésben való részvétel (IV)
- 17. Köz- és magánszféra közötti partnerség létrehozása (IV)

A négy csoport és az alapvető célkitűzések egyesülnek a modellben, hogy holisztikus képet alkossanak a tagállamok kiberbiztonsági képességeinek érettségéről. Az 1. ábra bemutatja az önértékelési keretrendszer átfogó struktúráját és azt, hogyan kapcsolódnak ezek az elemek, nevezetesen a célkitűzések, csoportok és az önértékelési keretrendszer egy ország teljesítményének értékeléséhez.

1. ábra: Az önértékelési keretrendszer struktúrája

Az önértékelési keretrendszerben szereplő mindegyik célkitűzéshez mutatók tartoznak, amelyek az öt érettségi szint között vannak elosztva. Minden mutató egy eldöntendő (igen/nem) kérdésen alapul. A mutató lehet kötelező vagy nem kötelező.

3.4 PONTOZÁSI MECHANIZMUS

Az önértékelési keretrendszer **pontozási mechanizmusa** a fent említett elemeket és a 3.5. szakaszban felsorolt elveket veszi figyelembe. Tulajdonképpen a modell két paraméter, az **érettségi szint** és a **lefedettségi arány** értéke alapján adja meg a pontokat. Mindegyik paraméter különböző szinteken számítható ki: (i) célkitűzés szerint, (ii) célkitűzések csoportja szerint vagy (iii) átfogó szinten.

Pontszámok a célkitűzés szintjén

Az **érettségi szint pontszáma** azáltal nyújt áttekintést az érettségi szintről, hogy bemutatja, milyen képességeket és gyakorlatokat alakítottak ki. Az érettségi szint pontszámát úgy számolják, mint a legmagasabb szintet, amelyen a válaszadó teljesítette az összes követelményt (tehát valamennyi kötelező kérdésre „Igen”-nel válaszolt), továbbá teljesítette a korábbi érettségi szint valamennyi követelményét.

A **lefedettségi arány** azoknak a mutatóknak a lefedettségét mutatja meg, amelyek esetében a válasz pozitív volt, szintjüktől függetlenül. Ez egy kiegészítő érték, amely figyelembe veszi a célkitűzést mérő valamennyi mutatót. A lefedettségi arányt a célkitűzésen belüli összes kérdés számának és a pozitív válasszal jelölt kérdések számának arányaként számolják ki.

Fontos tisztázni, hogy a dokumentum további részében a ***pontszám*** szó alatt mind az érettségi szint, mind pedig a lefedettségi arány értékeit értjük.

2. ábra – A célkitűzés szerinti pontozási mechanizmus megjeleníti a 3.1. szakaszban leírt értékelési mechanizmust, amelynek részletesebb leírása alább olvasható.

2. ábra: Célkitűzés szerinti pontozási mechanizmus

A 2. ábra példával mutatja be, hogyan lehet az érettségi szintet célkitűzés alapján kiszámítani. Érdemes megjegyezni, hogy a válaszadó az első három érettségi szint valamennyi követelményét teljesítette, a 4. szint követelményeit viszont csak részben teljesítette. Ezért jelzi azt a pontozás, hogy ***a válaszadó érettsége 3. szintű a „Kiberbiztonsági gyakorlat szervezése" célkitűzés tekintetében.***

Azonban a 2. ábrán bemutatott példában a célkitűzés érettségi szintje nem tudja rögzíteni a pozitív pontszámú és a 3. érettségi szintet meghaladó mutatók által biztosított információkat. Ebben az esetben a lefedettségi arány áttekintést nyújthat mindazokról az elemekről, amelyeket a válaszadó – tényleges érettségi szintje ellenére – végrehajtott a célkitűzés elérése érdekében. Ez esetben a célkitűzésen belüli összes kérdés számának és a pozitív válasszal jelölt kérdések számának aránya 19/27, azaz ***a lefedettségi arány értéke 70 %.***

Ezenkívül a tagállamok sajátosságaihoz való alkalmazkodás érdekében, illetve egy konzisztens áttekintést lehetővé téve, a pontszámot csoportszinten és átfogó szinten két mintából számolják ki:

- **Általános pontszámok:** egy teljes minta, amely magában foglalja a csoportban vagy a teljes keretrendszerben szereplő összes célkitűzést (egytől 17-ig);
- **Meghatározott pontszámok:** egy meghatározott minta, amely kizárólag azokat a célkitűzéseket foglalja magában, amelyeket a tagállam egy csoporton vagy a teljes keretrendszeren belül kiválasztott (ezek általában megegyeznek az adott ország NKBS-ében szereplő célkitűzésekkel).

Pontszámok a csoport szintjén

Az **egyes csoportok általános érettségi szintjét** a csoporton belüli összes célkitűzés érettségi szintjének számtani átlagaként számolják ki.

Az **egyes csoportok meghatározott érettségi szintjét** az adott csoporton belüli olyan célkitűzések érettségi szintjének számtani átlagaként számolják ki, amelyeket a tagállam

értékelésre kiválasztott (ezek általában megegyeznek az adott ország NKBS-ében szereplő célkitűzésekkel).

Például az 1. ábra azt mutatja be, hogy a (I) Kiberbiztonsági irányítás és szabványok csoport három célkitűzésből áll. Feltéve, hogy a válaszadó csak az első két célkitűzést választotta ki értékelésre, de a harmadikat nem, és hogy az első két célkitűzés 2. és 4. érettségi szintet mutat, akkor az összes célkitűzést figyelembe véve a csoport érettsége 2. szintű ([I] csoport általános érettségi szint = [2+4]/3]), míg kizárólag az értékelő által kiválasztott meghatározott célkitűzést figyelembe véve a csoport érettsége 3. szintű ([I] csoport meghatározott érettségi szint = [2+4]/2]).

Az **egyes csoportok általános lefedettségi arányát** a csoporton belüli összes kérdés számának és a pozitív válasszal jelölt kérdések számának arányaként számolják ki.

Az **egyes csoportok meghatározott lefedettségi arányát** a tagállam által értékelésre kiválasztott célkitűzésekkel (ezek általában megegyeznek az adott ország NKBS-ében szereplő célkitűzésekkel) kapcsolatos csoporton belüli összes kérdés számának és a pozitív válasszal jelölt kérdések számának arányaként számolják ki.

Pontszámok átfogó szinten

Egy **ország átfogó általános érettségi szintjét** a keretrendszeren belüli összes – egytől 17-ig terjedő – célkitűzés érettségi szintjének számtani átlagaként számolják ki.

Egy **ország átfogó meghatározott érettségi szintjét** a keretrendszeren belüli olyan célkitűzések érettségi szintjének számtani átlagaként számolják ki, amelyeket a tagállam értékelésre kiválasztott (ezek általában megegyeznek az adott ország NKBS-ében szereplő célkitűzésekkel).

Egy **ország átfogó általános lefedettségi arányát** a keretrendszerben szereplő valamennyi célkitűzésen (egytől 17-ig) belüli összes kérdés számának és a pozitív válasszal jelölt kérdések számának arányaként számolják ki.

Egy **ország átfogó meghatározott lefedettségi arányát** a keretrendszerben szereplő, a tagállam által értékelésre kiválasztott célkitűzéseken (ezek általában megegyeznek az adott ország NKBS-ében szereplő célkitűzésekkel) belüli összes kérdés számának és a pozitív válasszal jelölt kérdések számának arányaként számolják ki.

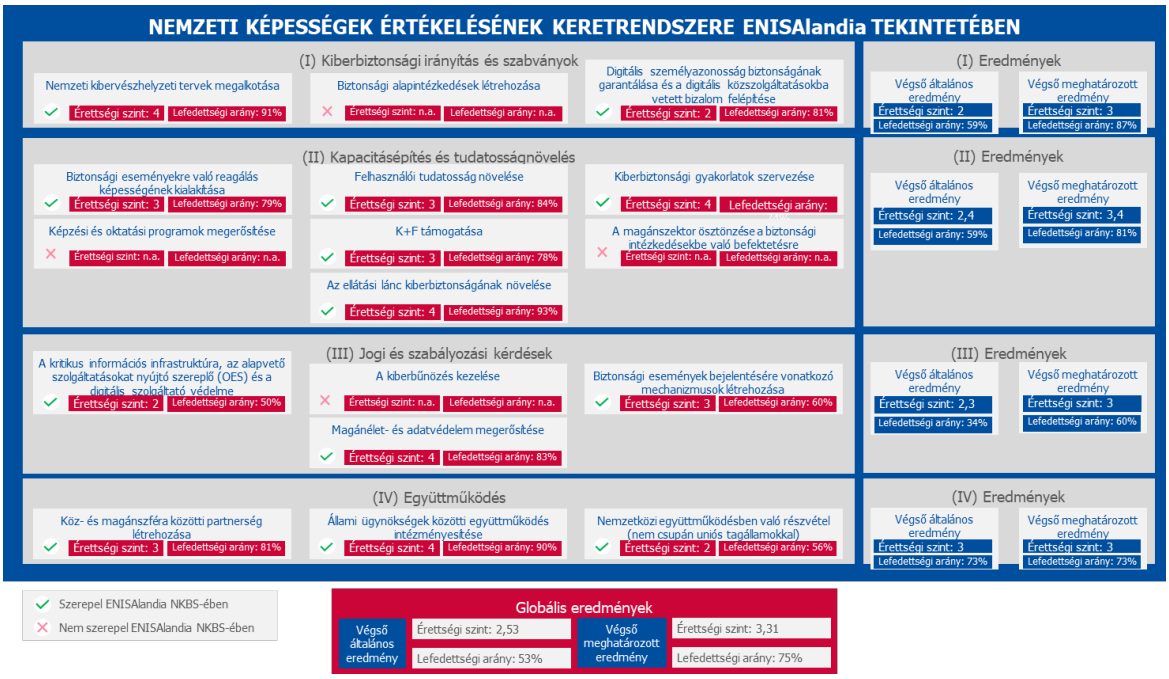
Mindegyik mutató esetében a válaszadók választhatják a harmadik, „nem tudom / nem alkalmazandó” válaszlehetőséget. Ebben az esetben a mutató egyáltalán nem szerepel az eredmények kiszámításában.

Az érettségi szinteket csoport- és átfogó szinten számtani átlaggal számolják, hogy megmutatkozzon a két értékelés közötti előrehaladás. Habár a csoportszint és átfogó szint mint a legkevésbé érett célkitűzés érettségi szintjének kiszámításában rejlő alternatíva – bár érettségi szempontból releváns – nem magyarázhatja a más célkitűzések által lefedett területeken elért előrehaladást.

Mivel a csoportszint és átfogó szint jelentéstételi célokból összevonásra került, döntés született a számtani átlag használata mellett. A pontosság érdekében, kérjük, jelentéstételi célból használják a célkitűzési szintű pontszámokat.

Az alábbi 3. ábra a pontozási mechanizmusokat foglalja össze a modell különböző szintjein (célkitűzés-, csoport-, átfogó).

3. ábra: Átfogó pontozási mechanizmus



3.5 AZ ÖNÉRTÉKELÉSI KERETRENDSZERRE VONATKOZÓ KÖVETELMÉNYEK

Az ebben a szakaszban bemutatott Nemzeti képességek értékelésének keretrendszere a tagállamok által kiemelt igényeken alapul és az alábbiakban felsorolt követelmények köré épül:

- A Nemzeti képességek értékelésének keretrendszerét (NCAF) a tagállam önértékelési keretrendszerként önkéntes alapon alkalmazza;
- Az NCAF célja, hogy mérje a tagállamok kiberbiztonsági képességeit a 17 célkitűzés vonatkozásában. Ugyanakkor a tagállam kiválaszthatja azokat a célkitűzéseket, amelyek alapján az értékelést el akarja végezni, és értékelheti a 17 célkitűzés egy meghatározott részét is;
- Az önértékelési keretrendszer célja, hogy mérje a tagállamok kiberbiztonsági képességeinek érettségi szintjét;
- Az értékelés eredményeit nem teszik közzé, kivéve ha a tagállam saját hatáskörében a közzététel mellett dönt;
- A tagállam bemutathatja az értékelés eredményeit azáltal, hogy ismerteti az ország kiberbiztonsági képességeinek, valamint célkitűzések egy csoportjának vagy akár egyetlen célkitűzés érettségi szintjét.
- Valamennyi értékelt célkitűzés egyformán releváns az értékelési keretrendszerben, ezért mindegyik ugyanolyan fontos. Ugyanez vonatkozik a benne alkalmazott mutatókra is; és
- A tagállam képes nyomon követni saját időbeli előrehaladását.

Az önértékelési keretrendszer célja, hogy támogassa a tagállamokat kiberbiztonsági képességeik kialakításában, ezért olyan ajánlásokat vagy iránymutatásokat is tartalmaz, amelyek utat mutatnak az európai országoknak abban, hogyan javíthatják érettségi szintjüket.

Megjegyzés: az említett ajánlások vagy iránymutatások általánosak, amelyek az ENISA kiadványain és más országok példáin alapulnak, továbbá az önértékelés eredményeire épülnek.

4. AZ NCAF MUTATÓI

4.1 A KERETRENDSZER MUTATÓI

Ez a szakasz bemutatja az ENISA Nemzeti képességek értékelésének keretrendszerére vonatkozó mutatókat. A következő szakaszok csoport szerint vannak elrendezve.

Mindegyik csoport vonatkozásában a mutatók átfogó rendszerét egy táblázat mutatja be az adott érettségi szintre jellemző kérdések formájában. A kérdőív az önértékelés legfőbb eszköze. Minden célkitűzés tekintetében a mutatók két csoportját kell megemlíteni:

- Az általános stratégiai érettséggel kapcsolatos kérdések csoportja (9 általános kérdés), amelyeket „a”-tól „c”-ig jelölnek minden érettségi szintre vonatkozóan, és ismétlődnek valamennyi célkitűzésnél; és
- A kiberbiztonsági kapacitással kapcsolatos kérdések csoportja (319 kiberbiztonsági kapacitással kapcsolatos kérdés), amelyeket „1”-től „10”-ig számoznak minden érettségi szintre vonatkozóan, valamint az adott célkitűzés által lefedett területre jellemzőek.

Minden kérdés egy címkével (0–1) van ellátva, amely azt jelzi, hogy a kérdés az adott érettségi szint kötelező (1) vagy nem kötelező (0) mutatója.

Mindegyik kérdés egy azonosító szám segítségével azonosítható, amely a következőkből áll:

- A célkitűzés száma;
- Az érettségi szint; és
- A kérdés száma.

Például az 1.2.4 kérdésazonosító esetében az (I) „Nemzeti kibervészhelyzeti tervek megalkotása” nevű stratégiai célkitűzés 2. érettségi szintjének 4. kérdéséről van szó.

Fontos megjegyezni, hogy a kérdőív egészében a kérdések köre a nemzeti szintre vonatkozik, kivéve ha ennek ellenkezője szerepel a szövegben. Valamennyi kérdésben az „Ön/Önök” névmás általánosan a tagállamra értendő, és nem az értékelést végző személyre vagy kormányzati szervre utal.

Az egyes célkitűzések meghatározása a 2.2 - Az európai NKBS-ekben azonosított közös célkitűzések fejezetben található.

4.1.1 1. csoport: Kiberbiztonsági irányítás és szabványok

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
1 – Nemzeti kibervészhelyzeti tervek megalkotása	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Elkezdték-e már kidolgozni a nemzeti kibervészhelyzeti terveket? *pl.* a vészhelyzeti tervek általános céljainak, hatályának és/vagy elveinek stb. meghatározása.	1	Van olyan alapelvük / nemzeti stratégiájuk, amely a kiberbiztonságot válságtényezőként foglalja magában (azaz egy tervezet, egy politika stb.)?	1	Rendelkeznek nemzeti szintű kiberbiztonsági válságkezelési tervvel?	1	Elégedettek a nemzeti kibervészhelyzeti tervben foglalt kritikus ágazatok számával vagy százalékával?	1	Rendelkeznek tanulságok levonására irányuló eljárással, amely nemzeti szinten a kibervédelmi gyakorlatokat vagy a tényleges válságokat követi?	1
	2	Általánosan ismert tény, hogy a kiberbiztonsági események olyan válságtényezőt rejtenek magukban, amely a nemzeti biztonságot fenyegetheti?	0	Rendelkeznek olyan platformmal, amelyet információgyűjtésre és a döntéshozók tájékoztatására használnak? *azaz* olyan módszerek, felületek vagy helyszínek, amelyek révén biztosítják, hogy a válságkezelésben részt vevő valamennyi fél valós időben hozzáfér a kiberbiztonsági válságra vonatkozó ugyanazon információkhoz.	1	Rendelkeznek nemzeti szintű válságspecifikus eljárásokkal?	1	Megfelelő gyakorisággal szerveznek olyan tevékenységeket (pl. gyakorlatokat), amelyek a nemzeti kibervészhelyzeti tervezéshez kapcsolódnak?	1	Rendelkeznek a nemzeti terv rendszeres tesztelésére kialakított eljárással?	1
	3	Végeztek (technikai, operatív, politikai) tanulmányokat a kibervészhelyzeti tervezés terén?	0	Megfelelő forrásokat fordítanak a nemzeti kibervészhelyzeti tervek kidolgozásának és végrehajtásának felügyeletére?	1	Van olyan kommunikációs csapatuk, amelyet kifejezetten a kiberbiztonsági válságok megválaszolására és a nyilvánosság tájékoztatására képeztek ki?	1	Rendelkeznek elegendő emberrel a válságtervezéshez, a levont tanulságok áttekintéséhez és a változtatások végrehajtásához?	1	Rendelkeznek a helyzetismeret kiépítéséhez szükséges megfelelő eszközökkel és platformokkal?	1
	4	-		Rendelkeznek egy nemzeti szintű kiberfenyegetés-értékelési módszertannal, amely hatásvizsgálatra vonatkozó eljárásokat tartalmaz?	0	Bevonják a munkába az összes érintett nemzeti érdekelt felet (nemzetbiztonság, -védelem, polgári védelem, bűnüldözés, minisztériumok, hatóságok stb.)?	1	Elegendő emberrel rendelkeznek, akik képzettek a kiberbiztonsági vészhelyzetek nemzeti szintű megválaszolása terén?	1	Egy meghatározott érettségi modellt követnek a kibervészhelyzeti terv nyomon követésére és javítására?	0

	5	-		-		Rendelkeznek megfelelő válságkezelési eszközökkel és válsághelyzetre kialakított helyiségekkel?	1	-		Rendelkeznek-e olyan erőforrásokkal, amelyeket kimondottan a fenyegetések előrejelzésére vagy a kiberbiztonsági helyzet előreláthatóságának kidolgozására fordítanak annak érdekében, hogy kezelni tudják a jövőbeni válságokat vagy kihívásokat?	0
	6	-		-		Szükség esetén felveszik-e a kapcsolatot nemzetközi érdekelt felekkel az Unióban?	0	-		-	
	7	-		-		Szükség esetén felveszik-e a kapcsolatot nemzetközi érdekelt felekkel a nem uniós országokban?	0	-		-	
NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**K**
2 – Biztonsági alapintézkedések létrehozása	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Végeztek-e tanulmányt az **állami** szervezetekre vonatkozó követelmények és hiányosságok azonosítására nemzetközileg elismert szabványok alapján? *pl.* ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS stb.	1	A bevezetett biztonsági intézkedések összhangban vannak a nemzetközi/nemzeti szabványokkal?	1	A biztonsági alapintézkedések kötelezőek?	1	Rendelkeznek a biztonsági alapintézkedések gyakori aktualizálására szolgáló eljárással?	1	Rendelkeznek olyan eljárással, amely arra szolgál, hogy megerősítse az IKT-t, ha az intézkedések nem tudják kezelni az eseményeket?	1

	2	Végeztek-e tanulmányt a **magánszektorbeli** szervezetekre vonatkozó követelmények és hiányosságok azonosítására nemzetközileg elismert szabványok alapján? pl. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS stb.	1	A biztonsági alapintézkedések meghatározása során egyeztetnek a magánszektorbeli és egyéb érdekelt felekkel?	1	Megvalósítanak horizontális biztonsági intézkedéseket a kritikus ágazatokban?	1	Rendelkeznek olyan nyomonkövetési mechanizmussal, amely a biztonsági alapintézkedések alkalmazásának vizsgálatára szolgál?	1	Kiértékelik-e az olyan új szabványok relevanciáját, amelyeket a fenyegetettségi helyzet legújabb fejleményeire adandó válaszként fejlesztettek ki?	1
	3	-		-		Megvalósítanak ágazatspecifikus biztonsági intézkedéseket a kritikus ágazatokban?	1	Van olyan nemzeti hatóságuk, amely azt ellenőrzi, hogy alkalmazzák-e a biztonsági alapintézkedéseket?	1	Rendelkeznek-e egy nemzeti összehangolt sebezhetőség-feltárási (CVD) eljárással vagy támogatnak-e ilyen eljárást?	1
	4	-				A biztonsági alapintézkedések megfelelnek a releváns tanúsítási rendszereknek?	1	Rendelkeznek olyan eljárással, amely egy meghatározott időtartamon belül azonosítja a meg nem felelő szervezeteket?	1	-	
	5	-		-		Rendelkeznek a biztonsági alapintézkedésekre vonatkozó kockázati önértékelési eljárással?	1	Rendelkeznek olyan ellenőrzési eljárással, amely biztosítja, hogy a biztonsági intézkedéseket megfelelően alkalmazzák?	1	-	
NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**R**
2 – Biztonsági alapintézkedések létrehozása	6	-		-		Felülvizsgálják a kötelező biztonsági alapintézkedéseket a kormányzati szervek beszerzési eljárásában?	0	Meghatározzák-e, illetve aktívan ösztönzik-e a biztonságos szabványok elfogadását a kritikus IT- / MT-termékek (orvosi eszközök, összekapcsolt és autonóm járművek, professzionális rádióegységek, nehézipari berendezések stb.) fejlesztése terén?	0	-	

NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**K**
3 – Digitális személyazonosság biztonságának garantálása és a digitális	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1

közszolgáltatásokba vetett bizalom felépítése	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Végeztek tanulmányokat vagy hiányelemzést annak érdekében, hogy azonosítsák a digitális közszolgáltatások polgároknak és vállalkozásoknak történő biztonságossá tételére vonatkozó igényeket?	1	Az eszközök vagy szolgáltatások kockázati profiljának meghatározása érdekében végeznek kockázatelemzést, mielőtt az említett eszközöket vagy szolgáltatásokat a felhőbe küldenék, illetve bármilyen digitális átalakítási projektbe kezdenének?	1	Támogatják a beépített adatvédelemmel kapcsolatos módszertanokat minden e-kormányzati projektben?	1	Olyan kiberbiztonsági eseményekre vonatkozó mutatókat is gyűjtenek, amelyek digitális közszolgáltatások megsértésével járnak?	1	Közreműködnek európai munkacsoportokban a bizalmi szolgáltatásokkal (elektronikus aláírás, elektronikus bélyegző, ajánlott elektronikus kézbesítési szolgáltatás, időbélyegző, weboldal-hitelesítés) kapcsolatos szabványok fenntartása és/vagy új követelmények megalkotása érdekében? *pl.* ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU stb.	1
	2	-		Rendelkeznek egy, a biztonságos nemzeti elektronikus azonosítási rendszerek (eIDs) polgároknak és vállalkozásoknak történő kiépítésére vagy népszerűsítésére szolgáló stratégiával?	1	Bevonják a magánszektorbeli érdekelt feleket a biztonságos digitális közszolgáltatások tervezésébe és megvalósításába?	1	Rendelkeznek-e olyan rendszerrel, amelyben más tagállamokkal kölcsönösen elismerik az elektronikus azonosító eszközöket?	1	Aktívan részt vesznek kölcsönös felülvizsgálatokban az Európai Bizottság eID-rendszerekre vonatkozó értesítése keretében?	1
	3	-		Rendelkeznek egy, a biztonságos nemzeti bizalmi szolgáltatások (elektronikus aláírás, elektronikus bélyegző, ajánlott elektronikus kézbesítési szolgáltatás, időbélyegző, weboldal-hitelesítés) polgároknak és vállalkozásoknak történő kiépítésére vagy népszerűsítésére szolgáló stratégiával?	1	Meghatároznak egy minimális biztonsági alapvonalat valamennyi digitális közszolgáltatás tekintetében?	1	-		-	

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
3 – Digitális személyazonosság biztonságának garantálása és a digitális közszolgáltatásokba vetett bizalom felépítése	4	-		Rendelkeznek egy, a kormányzati felhőre vonatkozó stratégiával (felhőalapú számítástechnikai stratégia, amely a kormányt és az olyan állami szerveket célozza meg, mint a minisztériumok, kormányzati ügynökségek és közigazgatási egységek stb.), amely figyelembe veszi a következményeket a biztonság szempontjából?	0	Elérhető-e a polgárok és vállalkozások számára bármely olyan elektronikus azonosítási rendszer, amely a 910/2014/EU eIDAS-rendelet mellékletében meghatározott jelentős vagy magas biztonsági szintű?	1	-		-	
	5	-		-		Rendelkeznek olyan elektronikus azonosítási rendszereket igénylő digitális közszolgáltatásokkal, amelyek a 910/2014/EU eIDAS-rendelet mellékletében meghatározott jelentős vagy magas biztonsági szintűek?	1	-		-	
	6	-		-		Rendelkeznek olyan bizalmi szolgáltatókkal, amelyek a polgároknak és vállalkozásoknak nyújtanak szolgáltatásokat (elektronikus aláírás, elektronikus bélyegző, ajánlott elektronikus kézbesítési szolgáltatás, időbélyegző, weboldal-hitelesítés)?	1	-		-	
	7	-		-		Támogatják a biztonsági alapintézkedések elfogadását valamennyi számításifelhő-alkalmazási modell (pl. magán, állami, hibrid, IaaS, PaaS, SaaS) esetében?	0	-		-	

4.1.2 2. csoport: Kapacitásépítés és tudatosságnövelés

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
4 – Biztonsági eseményekre való reagálás képességének kialakítása	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Rendelkeznek informális, biztonsági eseményekre való reagálási képességekkel, amelyeket a köz- és magánszektorok között és azokon belül kezelnek?	1	Rendelkeznek legalább egy hivatalos nemzeti CSIRT-tel?	1	Rendelkeznek biztonsági eseményekre való reagálási képességekkel a hálózati és információs rendszerek biztonságáról szóló irányelv II. mellékletében hivatkozott ágazatok terén?	1	Meghatároztak és támogatnak a biztonsági eseményekre való reagálás eljárásaira és biztonsági események osztályozásának rendszereire vonatkozó standard gyakorlatokat?	1	Rendelkeznek nulladik napi sebezhetőségek korai észlelésére, azonosítására, megelőzésére, csökkentésére és az említett sebezhetőségekre való reagálásra szolgáló mechanizmusokkal?	1
	2	-		Nemzeti CSIRT-jük/CSIRT-jeik világosan meghatározott beavatkozási hatállyal rendelkezik/rendelkeznek? *pl.* a célzott ágazattól, a biztonsági események típusától, a hatásoktól függően	1	Országuk rendelkezik a CSIRT-re vonatkozó együttműködési mechanizmussal, amely a biztonsági eseményekre való reagálásra szolgál?	1	Értékelésnek vetik alá saját, biztonsági eseményekre való reagálási képességüket annak érdekében, hogy biztosítsák, hogy megfelelő erőforrásokkal és szakértelemmel rendelkeznek a hálózati és információs rendszerek biztonságáról szóló irányelv I. mellékletének 2. pontjában meghatározott feladatok ellátásához?	1	-	

	3	-		Nemzeti CSIRT-jük/CSIRT-jeik világosan meghatározott kapcsolatot ápolnak más nemzeti érdekelt felekkel a nemzeti kiberbiztonsági helyzetet és a biztonsági eseményekre való reagálás gyakorlatát illetően (pl. LEA, hadsereg, internetszolgáltatók, NCSC)?	0	Nemzeti CSIRT-jük/CSIRT-jeik rendelkeznek a hálózati és információs rendszerek biztonságáról szóló irányelv I. mellékletének megfelelő, biztonsági eseményekre való reagálási képességgel? *azaz* hozzáférhetőség, fizikai biztonság, üzletmenet-folytonosság, nemzetközi együttműködés, biztonsági események nyomon követése, korai előrejelzési és riasztási kapacitás, biztonsági eseményekre való reagálás, kockázatelemzés és helyzetismeret, magánszektorral való együttműködés, standard gyakorlatok stb.	1	-		-	
	4	-				Rendelkeznek a más szomszédos országokkal való együttműködésre vonatkozó mechanizmussal a biztonsági eseményeket illetően?	1	-		-	
	5	-		-		Hivatalosan meghatároztak egyértelmű, biztonsági események kezelésével kapcsolatos politikákat és eljárásokat?	1	-		-	
NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**K**
4 – Biztonsági eseményekre való reagálás képességének kialakítása	6	-		-		Nemzeti CSIRT-jük/CSIRT-jeik részt vesz / részt vesznek mind nemzeti, mind nemzetközi szintű kiberbiztonsági gyakorlatokban?	1	-		-	
	7	-		-		Nemzeti CSIRT-jük/CSIRT-jeik kapcsolatban áll/állnak a FIRST-tel (Forum of Incident Response and Security Teams, azaz számítógép-biztonsági eseményekre reagáló és biztonsági csoportok fóruma)?	0	-		-	

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
5 – Felhasználói tudatosság növelése	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Történt-e minimális felismerés a kormányzati, magánszektorbeli vagy általános felhasználók részéről, hogy szükséges a kiberbiztonsági és adatvédelmi kérdésekre vonatkozó tudatosság növelése?	1	Meghatároztak konkrét célközönséget a felhasználói tudatosság tekintetében? *pl.* általános felhasználók, fiatalok, üzleti felhasználók (amely tovább bontható: kkv-k, alapvető szolgáltatásokat nyújtó szereplők, digitális szolgáltatók stb.)	1	Kidolgozták a kampányok kommunikációs terveit/stratégiáját?	1	Megállapítanak a kampányuk értékelésére szolgáló mérőszámokat a tervezési szakasz során?	1	Rendelkeznek olyan mechanizmusokkal, amelyek biztosítják, hogy a tudatosságnövelő kampányok folyamatosan relevánsak a műszaki haladás, a fenyegetettségi helyzet változásai, a jogi előírások és a nemzeti biztonsági irányelvek tekintetében?	1
	2	Az állami ügynökségek megvalósítanak *ad hoc* alapú, kiberbiztonsági tudatosságot növelő kampányokat saját szervezetükön belül? pl. egy kiberbiztonsági eseményt követően.	0	Készítenek-e az információbiztonsággal és adatvédelmi kérdésekkel kapcsolatos tudatosság növelését célzó projekttervet?	1	Rendelkeznek olyan eljárással, amely kormányzati szintű tartalomlétrehozásra szolgál?	1	Megvalósításuk után kiértékelik saját kampányaikat?	1	Végeznek időszakos értékelést vagy tanulmányt a kiberbiztonsági vagy adatvédelmi kérdésekkel kapcsolatos szemléletváltás vagy viselkedésbeli változások mérésére a köz- és magánszektorban?	1

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
5 – Felhasználói tudatosság növelése	3	Az állami ügynökségek folytatnak *ad hoc* alapú, kiberbiztonsági tudatosságot növelő kampányokat a nagyközönség számára? *Pl.* egy kiberbiztonsági eseményt követően.	0	Rendelkeznek bármely olyan felhasználó számára elérhető és könnyen azonosítható erőforrásokkal (*pl.* egy egységes internetes portál, tudatosságnövelő csomagok), aki szeretne tájékozódni a kiberbiztonsági és adatvédelmi kérdésekről?	1	Rendelkeznek tudatosságnövelésre vonatkozó célterületek azonosítására szolgáló mechanizmusokkal (azaz az ENISA fenyegetettségi helyzetjelentése, nemzeti helyzetjelentések, nemzetközi helyzetjelentések, nemzeti kiberbűnözés elleni központok stb.)?	1	Rendelkeznek olyan mechanizmusokkal, amelyek révén azonosítható a tájékoztatás és figyelemfelkeltés maximalizálására alkalmas, célközönségtől függő legrelevánsabb média vagy hírközlési csatorna? *pl.* digitális média különböző típusai, prospektusok, e-mailek, műszaki anyagok, plakátok a forgalmas területeken, televízió, rádió stb.	1	Egyeztetnek-e viselkedési szakértőkkel azért, hogy kampányaikat a célközönség igényeihez igazítsák?	1
	4	-		-		A tartalmak létrehozása érdekében biztosítanak együttműködési lehetőséget a szakértőkkel és kommunikációs csapatokkal rendelkező érintett felek számára?	1			-	
	5	-		-		Bevonják-e a magánszektort a tudatosság növelésére irányuló erőfeszítéseikbe annak érdekében, hogy az üzeneteket egy szélesebb közönség körében is népszerűsítsék és terjesszék?	1	-		-	
	6	-		-		Készítenek olyan konkrét tudatosságnövelő kezdeményezéseket, amelyek a köz-, illetve magánszektor, tudományos vagy civil társadalmi szektor vezetőinek szólnak?	1	-		-	
	7	-		-		Részt vesznek az ENISA európai kiberbiztonsági hónap (European Cybersecurity Month, ECSM) nevű kampányaiban?	0	-		-	

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
6 – Kiberbiztonsági gyakorlat szervezése	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1

6 – Kiberbiztonsági gyakorlat szervezése	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Végeznek válságkezelési gyakorlatokat más (nem kiberbiztonsági) ágazatokban nemzeti vagy páneurópai szinten?	1	Rendelkeznek nemzeti szintű, kiberbiztonsági gyakorlatra vonatkozó programmal?	1	Bevonják a közigazgatás valamennyi érintett hatóságát? (akkor is, ha a forgatókönyv ágazatspecifikus)	1	Készítenek cselekmény utáni jelentéseket / értékelő jelentéseket?	1	Rendelkeznek-e kiberbiztonságra vonatkozó tanulságlevonó elemzési kapacitással (jelentési eljárások, elemzés, csökkentés)?	1
	2	Elkülönítettek a válságkezelési gyakorlat tervezésére és megalkotására szolgáló forrásokat?	1	Végeznek vagy fontossági sorrendbe állítják a létfontosságú társadalmi feladatokra és kritikus infrastruktúrára vonatkozó kiberbiztonsági válságkezelési gyakorlatokat?	1	Bevonják a magánszektort a gyakorlatok tervezésébe és végrehajtásába?	1	Tesztelik a nemzeti szintű terveket és eljárásokat?	1	Rendelkeznek kidolgozott, tanulságok levonására irányuló eljárással?	1
	3	-		Meghatároztak olyan koordináló szervezetet, amely a kiberbiztonsági gyakorlatok kidolgozását és tervezését felügyeli (állami ügynökség, tanácsadói szolgálat stb.)?	0	Szerveznek ágazatspecifikus gyakorlatokat nemzeti és/vagy nemzetközi szinten?	1	Részt vesznek kiberbiztonsági gyakorlatokban páneurópai szinten?	1	Végeznek igazításokat a gyakorlati forgatókönyveken a legújabb fejlemények függvényében (műszaki haladás, globális konfliktusok, fenyegetettségi helyzet stb.)?	1
	4	-		-		A hálózati és információs rendszerek biztonságáról szóló irányelv II. mellékletében szereplő minden kritikus ágazatban szerveznek gyakorlatokat?	1	-		Összehangolják saját válságkezelési eljárásaikat más tagállamokéval a hatékony páneurópai válságkezelés biztosítása érdekében?	1
	5	-		-		Szerveznek ágazatközi és/vagy ágazatokon átívelő kiberbiztonsági gyakorlatokat?	1	-		Rendelkeznek olyan mechanizmussal, amely arra szolgál, hogy a gyakorlatok során levont tanulságok alapján gyorsan igazítson a stratégián, terveken és eljárásokon?	0
	6	-		-		Szerveznek kifejezetten az egyes szinteknek megfelelő kiberbiztonsági gyakorlatokat? (technikai és operatív szint, eljárási szint, döntéshozatali szint, politikai szint stb.)	0	-		-	

NKBS-célkitűzés	#	Level 1	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
7 – Képzési és oktatási programok megerősítése	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Gondolkodnak-e kiberbiztonsági képzési és oktatási programok kidolgozásán?	1	Létrehoznak a kiberbiztonság témájával foglalkozó tanfolyamokat?	1	Országuk beépíti a kiberbiztonsági kultúra oktatását a tanulók tanulmányainak korai szakaszába? Például támogatják a kiberbiztonság oktatását általános és középiskolában?	1	Ösztönzik-e a köz- és magánszektor munkatársait arra, hogy szerezzenek akkreditációt vagy képesítést?	1	Rendelkeznek olyan mechanizmusokkal, amelyek biztosítják, hogy a képzések és oktatási programok folyamatosan naprakészek maradnak az aktuális és leendő technológiai fejlesztések, a fenyegetettségi helyzet változásai, a jogi előírások és a nemzeti biztonsági irányelvek tekintetében?	1
	2	-		Országuk egyetemei kínálnak-e olyan doktori képzést, amely a kiberbiztonsággal mint önálló tudományággal foglalkozik, nem pedig a számítástechnika tárgya alá vonja azt?	1	Rendelkeznek a kiberbiztonságra szakosodott nemzeti kutatólaboratóriumokkal és oktatási intézményekkel?	1	Országukban elérhetők a nemzeti induló vállalkozások és kkv-k támogatására kidolgozott kiberbiztonsági képzési vagy mentorprogramok?	1	Létrehoznak a kutatás és oktatás gócpontjaként funkcionáló, kiberbiztonsággal foglalkozó tudományos kiválósági központokat?	1
	3	-		Tervezik-e, hogy szakterületüktől függetlenül az oktatóknak képzést biztosítanak az információbiztonsági és adatvédelmi kérdések terén? *pl.* az online biztonságról, személyes adatok védelméről, internetes megfélemlítésről.	1	Ösztönzik a tagállami munkaközvetítő ügynökségek alkalmazottainak szóló, kiberbiztonsági tanfolyam- és képzési tervek létrehozását, illetve finanszíroznak ilyen terveket?	1	Aktívan támogatják az információbiztonsági kurzusok felsőoktatásba való beépítését nem csupán a számítástechnikát tanulók, hanem bármely egyéb szakterületet választók számára is? *pl.* az adott szakterület igényeinek megfelelően alakított kurzusok	1	A felsőoktatási intézmények részt vesznek a kiberbiztonság oktatásáról és kutatásáról folytatott nemzetközi szintű eszmecserékben?	0
	4	-		-		Rendelkeznek az EKKR (európai képesítési keretrendszer) 5. és 8. szintjére vonatkozó kiberbiztonsági kurzusokkal és/vagy speciális tantervvel?	1	Rendszeresen felmérik a szakemberhiányt (kiberbiztonsággal foglalkozók hiánya) az információbiztonság területén?	1	-	

	5	-		-		Ösztönzik és/vagy támogatják az olyan kezdeményezéseket, amelyek szerint internetbiztonsági tanfolyamokat kell beépíteni az alap- és középfokú oktatásba?	1	Támogatják a felsőoktatási intézmények közötti nemzeti és nemzetközi szintű hálózatépítést és információmegosztást?	1		
NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**K**
7 - Képzési és oktatási programok megerősítése	6	-		-		Finanszíroznak, illetve ingyenesen kínálnak-e a polgároknak alapvető kiberbiztonsági képzéseket?	0	Bevonják a magánszektort bármilyen formában a kiberbiztonsági oktatási kezdeményezésekbe? *pl.* tanfolyamok kidolgozása és végrehajtása, gyakornoki programok, szakmai gyakorlatok stb.	1	-	
	7	-		-		Rendeznek éves információbiztonsági eseményeket (pl. hackerversenyek vagy hachathonok)?	0	Megvalósítanak olyan finanszírozási mechanizmusokat, amelyek révén ösztönzik a kiberbiztonsági képesítések megszerzését? *pl.* ösztöndíjak, garantált tanulószerződéses gyakorlati képzések / szakmai gyakorlatok, garantált munkalehetőségek az adott iparágban vagy pozíciók az állami szektorban	0	-	

NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**K**
8 – K+F támogatása	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						

	1	Végeztek a kiberbiztonsági K+F prioritásainak azonosítására szolgáló tanulmányokat vagy elemzéseket?	1	Rendelkeznek a K+F prioritásainak meghatározására szolgáló eljárással (pl. felmerülő új témák az újfajta kibertámadásoktól való elrettentésre, az azok elleni védelemre, azok észlelésére és a hozzájuk való alkalmazkodásra vonatkozóan)?	1	Rendelkeznek a K+F kezdeményezéseket a reálgazdasághoz kapcsoló tervvel?	1	A kiberbiztonsági K+F kezdeményezések összhangban vannak az olyan releváns stratégiai célkitűzésekkel, mint pl. a digitális egységes piac (DSM), a Horizont 2020, a Digitális Európa program, az Európai Unió kiberbiztonsági stratégiája?	1	Nemzeti szinten részt vesznek bármely, kiberbiztonsággal kapcsolatos nemzetközi K+F kezdeményezésben?	1
	2	-		Bevonják a magánszektort a K+F prioritásainak meghatározásába?	1	Jelenleg rendelkeznek kiberbiztonsággal kapcsolatos nemzeti projektekkel?	1	Rendelkeznek a K+F kezdeményezésekre vonatkozó értékelési rendszerrel?	1	A K+F prioritásai összhangban vannak a jelenlegi vagy készülő rendeletekkel (nemzeti szinten)?	1
NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**K**
8 – K+F támogatása	3	-		Bevonják a tudományos köröket a K+F prioritásainak meghatározásába?	1	Rendelkeznek az induló vállalkozásoknak szóló helyi/regionális ökoszisztémákkal és egyéb hálózatépítő csatornákkal (pl. technológiai parkok, innovációs klaszterek, hálózatépítő események/platformok), amelyek elősegítik az innovációt (pl. az induló kiberbiztonsági vállalkozások számára)?	1	Kötöttek együttműködési szerződéseket egyetemekkel és más kutatási létesítményekkel?	1	Részt vesznek egy vagy több korszerű K+F témával kapcsolatos nemzetközi szintű eszmecserében?	0
	4	-		Rendelkeznek kiberbiztonsággal kapcsolatos nemzeti K+F kezdeményezésekkel?	0	Történt a kiberbiztonsági K+F programokba való befektetés a tudományos körökben és a magánszektorban?	1	Rendelkeznek olyan elismert intézményi szervvel, amely felügyeli a kiberbiztonsági K+F tevékenységeket?	0	-	
	5	-		-		Az egyetemeken jelen vannak olyan, ipari kutatással foglalkozó professzorok, akik összekötik a kutatási tárgyakat a piaci igényekkel?	1	-		-	
	6	-		-		Rendelkeznek a kifejezetten kiberbiztonság témakörében létrehozott K+F finanszírozási programokkal?	0	-		-	

NKBS-célkitűzés	#	Level 1	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
9 – A magánszektor ösztönzése a biztonsági intézkedésekbe való befektetésre	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Van olyan ipari politika vagy politikai szándék, amely a kiberbiztonsági ipar fejlesztését ösztönzi?	1	Bevonják a magánszektort az ösztönző programok tervezésébe?	1	Vannak a kiberbiztonsági befektetések támogatására szolgáló gazdasági/szabályozási vagy egyéb típusú ösztönzők?	1	Van olyan magánfél, amely az ösztönző programokra úgy reagál, hogy befektet a biztonsági intézkedésekbe? *pl.* kiberbiztonságra szakosodott befektetők vagy nem szakosodott befektetők	1	A legújabb fenyegetettségi fejlemények alapján irányítják az ösztönző programokat a kiberbiztonsági témákra?	1

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
9 – A magánszektor ösztönzése a biztonsági intézkedésekbe való befektetésre	2	-		Meghatároztak-e konkrét fejlesztendő kiberbiztonsági témákat? *pl.* kriptográfia, adatvédelem, hitelesítés új formája, MI kiberbiztonságra vonatkozóan stb.	0	Segítik támogatásokkal (pl. adókedvezményekkel) a kiberbiztonsággal foglalkozó induló vállalkozásokat és kkv-kat?	1	Biztosítanak olyan ösztönzőket a magánszektor számára, amely az élvonalbeli technológiák, *pl.* 5G, mesterséges intelligencia, dolgok internete (IoT), kvantuminformatika stb. biztonságára való összpontosítást szorgalmazza?	1	-	
	3	-		-		Biztosítanak adókedvezményeket vagy egyéb pénzügyi motivációs eszközöket az induló kiberbiztonsági vállalkozásokba befektető magánszektorbeli szereplők számára?	1	-		-	
	4	-		-		Megkönnyítik a kiberbiztonsággal foglalkozó induló vállalkozások és kkv-k hozzáférését a közbeszerzési eljárásokhoz?	0	-		-	
	5	-		-		Rendelkeznek a magánszektor ösztönzésére fordítható költségvetési kerettel?	0	-		-	

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
10 – Az ellátási lánc kiberbiztonságának növelése	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						

	1	Végeztek-e tanulmányokat a különböző ágaztokban és/vagy az állami szektorban történő beszerzés során alkalmazott, ellátási lánc irányítására vonatkozó bevált biztonsági gyakorlatokról?	1	Végeznek kiberbiztonsági értékeléseket a kritikus ágazatok IKT-szolgáltatásainak és -termékeinek teljes ellátási láncán (a hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 irányelv II. mellékletében meghatározottak szerint)?	1	Alkalmaznak biztonsági tanúsítási rendszert az IKT-alapú termékek és szolgáltatások vonatkozásában? *pl.* SOG-IS MRA (Informatikai rendszerek biztonságáért felelős rangidős tisztviselők csoportja, kölcsönös elismerési megállapodás) Európában, közös kritériumok elismerésére vonatkozó megállapodás (CCRA), nemzeti kezdeményezések, ágazati kezdeményezések stb.	1	Rendelkeznek olyan eljárással, amely aktualizálja a kritikus ágazatok IKT-szolgáltatásai és -termékei ellátási láncának kiberbiztonsági értékeléseit (a hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 irányelv II. mellékletében meghatározottak szerint)?	1	Vannak az ellátási lánc kulcsfontosságú elemeiben olyan, észlelésre alkalmas eszközök, amelyek felismerik az adtok illetéktelen tudomására jutásának korai jeleit? *pl.* védelmi ellenőrzések internetszolgáltatói szinten, biztonsági vizsgálatok egy infrastruktúra fő elemeiben stb.	1

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
10 – Az ellátási lánc kiberbiztonságának növelése	2	-		Alkalmaznak szabványokat a közigazgatás beszerzési politikáiban annak biztosítására, hogy az IKT-termékeket és -szolgáltatásokat biztosító vállalkozások megfeleljenek az alapvető információbiztonsági követelményeknek? *pl.* ISO/IEC 27001 és 27002, ISO/IEC 27036 stb.	1	Aktívan támogatják a biztonság és beépített adatvédelem bevált gyakorlatait az IKT-termékek és -szolgáltatások fejlesztésében? *pl.* biztonságos szoftverfejlesztési életciklus, IoT életciklus	1	Rendelkeznek olyan eljárással, amely révén azonosítják a kritikus ágazatok ellátási láncában mutatkozó kiberbiztonsági gyengeségeket (a hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 irányelv II. mellékletében meghatározottak szerint)?	1	-	
	3	-		-		Fejlesztenek és rendelkezésre bocsátanak a kkv-khoz igazítható és általuk alkalmazható, meglévő információbiztonsági és adatvédelmi szabványok részletes információit tartalmazó központi katalógusokat?	1	Rendelkeznek olyan mechanizmusokkal, amelyek biztosítják, hogy az OES számára létfontosságú IKT-termékek és -szolgáltatások kibertámadásokkal szemben ellenállóak (*azaz* a kiberbiztonsági eseményekkel szembeni hozzáférhetőség és biztonság fenntartásának képessége)? *pl.* tesztelés, rendszeres értékelések, illetéktelen tudomására jutott elemek észlelése stb. révén	1	-	
	4	-				Aktívan részt vesznek az Unió kiberbiztonsági jogszabálya, azaz az (EU) 2019/881 rendelet szerint meghatározott, digitális IKT-termékekre, -szolgáltatásokra és -folyamatokra vonatkozó uniós tanúsítási keretrendszer kidolgozásában? *pl.* részvétel az európai kiberbiztonsági tanúsítási csoportban (ECCG), IKT-termékek/szolgáltatások biztonságára vonatkozó műszaki szabványok és eljárások támogatása	0	Támogatják a kkv-knak szóló tanúsítási rendszerek fejlesztését az információbiztonsági és adatvédelmi szabványok elfogadási hajlandóságának fokozása érdekében?	0	-	
	5	-		-		Biztosítanak a kkv-k számára bármely olyan ösztönző programot, amely a biztonsági és adatvédelmi szabványok elfogadására motiválja őket?	0	Elfogadtak-e olyan rendelkezéseket, amelyek arra ösztönzik a nagyvállalatokat, hogy saját ellátási láncukban növeljék a kisvállalkozások kiberbiztonságát? *pl.* kiberbiztonsági központ, képzés és tudatosságnövelő kampányok stb.	0	-	

	6	-		-		Ösztönzik arra a szoftverforgalmazókat, hogy támogassák a kkv-kat azáltal, hogy a kis szervezeteknek szóló termékekben biztonságos alapértelmezett konfigurációkat biztosítanak?	0	-		-	

4.1.3 3. csoport: Jogi és szabályozási kérdések

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
11 – A kritikus információs infrastruktúra, az alapvető szolgáltatásokat nyújtó szereplő (OES) és a digitális szolgáltató védelme	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Általános az egyetértés abban, hogy a CII-üzemeltetők hozzájárulnak a nemzetbiztonsághoz?	1	Rendelkeznek az alapvető szolgáltatások azonosítására szolgáló módszertannal?	1	Végrehajtották a hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 irányelvet?	1	Rendelkeznek a kockázatnyilvántartás aktualizálására szolgáló eljárással?	1	Létrehoznak fenyegetettségi helyzetjelentéseket és aktualizálják azokat?	1

2	-		Rendelkeznek a CII-k azonosítására szolgáló módszertannal?	1	Végrehajtották az európai kritikus infrastruktúrák (ECI) azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelvet?	1	Rendelkeznek olyan egyéb mechanizmusokkal, amelyek azt mérik, hogy az OES által végrehajtott technikai és szervezeti intézkedések megfelelőek-e a hálózati és információs rendszerek biztonságát érintő kockázatok kezelésére? pl. rendszeres kiberbiztonsági ellenőrzések, a standard intézkedések végrehajtására vonatkozó nemzeti keretrendszer, a kormány által biztosított technikai eszközök, pl. észlelésre alkalmas eszközök vagy rendszerspecifikus konfiguráció-felülvizsgálat stb.	1	A fenyegetettségi helyzet legújabb fejleményeitől függően fel tudnak venni új ágazatot a kritikus információs infrastruktúra védelméről (CIIP) szóló cselekvési tervükbe?	1
3	-		Rendelkeznek az OES azonosítására szolgáló módszertannal?	1	Rendelkeznek az azonosított OES-t kritikus ágazatonként tartalmazó nemzeti nyilvántartással?	1	Legalább kétévente felülvizsgálják és a felülvizsgálatnak megfelelően aktualizálják az azonosított OES-ek jegyzékét?	1	A fenyegetettségi helyzet legújabb fejleményeitől függően el tudnak fogadni új követelményeket a CIIP-ről szóló cselekvési tervükben?	1

NKBS-célkitűzés	#										
11 – A kritikus információs infrastruktúra, az alapvető szolgáltatásokat nyújtó szereplő (OES) és a digitális szolgáltató védelme	4	-		Rendelkeznek a digitális szolgáltatók azonosítására szolgáló módszertannal?	1	Rendelkeznek az azonosított digitális szolgáltatókat tartalmazó nemzeti nyilvántartással?	1	Rendelkeznek olyan egyéb mechanizmusokkal, amelyek azt mérik, hogy az digitális szolgáltató által végrehajtott technikai és szervezeti intézkedések megfelelőek-e a hálózati és információs rendszerek biztonságát érintő kockázatok kezelésére? pl. rendszeres kiberbiztonsági ellenőrzések, a standard intézkedések végrehajtására vonatkozó nemzeti keretrendszer, a kormány által biztosított technikai eszközök, pl. észlelésre alkalmas eszközök vagy rendszerspecifikus konfiguráció-felülvizsgálat stb.	1	-	
	5	-		Rendelkeznek egy vagy több olyan nemzeti hatósággal, amely felügyeli a kritikus információs infrastruktúra védelmét és a hálózati és információs rendszerek biztonságát? pl. a hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 irányelvben előírtak szerint	1	Rendelkeznek egy, az azonosított vagy ismert kockázatokat tartalmazó nemzeti kockázatnyilvántartással?	1	Legalább kétévente felülvizsgálják és a felülvizsgálatnak megfelelően aktualizálják az azonosított digitális szolgáltatók jegyzékét?	1	-	
	6	-		Kidolgoznak ágazatspecifikus védelmi terveket? pl. olyanokat, amelyek tartalmaznak kiberbiztonsági alapintézkedéseket (kötelező vagy iránymutatások)	0	Rendelkeznek a CII-függőségek feltérképezésére szolgáló módszertannal?	1	Rendelkeznek olyan biztonsági tanúsítási rendszerrel (nemzeti vagy nemzetközi), amely segíti az OES-eket vagy digitális szolgáltatókat a biztonságos IKT-termékek azonosításában? pl. SOG-IS MRA Európában, nemzeti kezdeményezések stb.	1	-	

	7	-		-		Alkalmaznak a CII-kkel kapcsolatos kockázatok azonosítására, számszerűsítésére és kezelésére szolgáló, nemzeti szintű kockázatkezelési gyakorlatokat?	1	Használnak az OES-ekkel együttműködő szolgáltatók értékelésére szolgáló biztonsági tanúsítási rendszert vagy minősítési eljárást? pl. a biztonsági események észlelése, azokra való reagálás, kiberbiztonsági ellenőrzések, felhőszolgáltatások, intelligens kártyák stb. terén működő szolgáltatók	1	-	
	8	-		-		Részt vesznek egy konzultációs folyamatban a határokon átnyúló kölcsönös függőségek azonosítása érdekében?	1	Rendelkeznek olyan mechanizmusokkal, amelyek az OES-ek és digitális szolgáltatók kiberbiztonsági alapintézkedésekre vonatkozó megfelelési szintjét mérik?	0	-	
NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**K**
11 – A kritikus információs infrastruktúra, az alapvető szolgáltatásokat nyújtó szereplő (OES) és a digitális szolgáltató védelme	9					Rendelkeznek olyan egyedüli kapcsolattartó ponttal, amely nemzeti szinten a hálózati és információs rendszerek biztonságával kapcsolatos kérdések koordinálásáért, uniós szinten pedig a határokon átnyúló együttműködésért felel?	1	Vannak olyan intézkedéseik, amelyek a kritikus információs infrastruktúrák által biztosított szolgáltatások folytonosságának garantálására szolgálnak? pl. válság-előrejelzés, a kritikus információs rendszerek újjáépítésére szolgáló eljárások, információtechnológia (IT) nélküli üzletmenet-folytonosság, „air gap” alapú biztonsági mentési eljárások stb.	0		
	10					Meghatároznak kiberbiztonsági alapintézkedéseket (kötelező vagy iránymutatások) a digitális szolgáltatók, illetve a hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 irányelv II. mellékletében meghatározott valamennyi ágazat számára?	1				
	11	-		-		Biztosítanak a kiberbiztonsági események észlelésére szolgáló eszközöket vagy módszertanokat?	1	-		-	

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
12 – Kiberbűnözés kezelése	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Végeztek olyan tanulmányt, amelyben azonosították a kiberbűnözés hatékony kezelésére szolgáló bűnüldözési követelményeket (jogi alap, erőforrások, szakértelem stb.)?	1	Nemzeti jogi keretük teljes mértékben megfelel a vonatkozó uniós jogi keretnek, beleértve az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelvet? pl. Információs rendszerekhez való jogellenes hozzáférés, Rendszert érintő jogellenes beavatkozás, Adatot érintő jogellenes beavatkozás, Jogellenes adatszerzés, A bűncselekmények elkövetéséhez használt eszközök stb.	1	Az ügyészségeken jelen vannak a kiberbűnözés kezelésére szakosodott egységek?	1	Gyűjtenek statisztikákat az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv 14. cikke (1) bekezdésének megfelelően?	1	Rendeznek intézményközi képzéseket vagy képzési munkaértekezleteket a bűnüldöző hatóságok (LEA), bírók, ügyészek és nemzeti/kormányzati CSIRT-ek számára nemzeti és/vagy többoldalú szinten?	1
	2	Végeztek olyan tanulmányt, amelyben azonosították a kiberbűnözés hatékony kezelésére szolgáló ügyészi és bírói követelményeket (jogi alap, erőforrások, szakértelem stb.)?	1	Rendelkeznek az online személyazonosság-lopással és személyes adatok lopásával foglalkozó bármely jogi rendelkezéssel?	1	Biztosítanak külön költségvetést a kiberbűnözéssel foglalkozó egységek számára?	1	Gyűjtenek külön statisztikákat a kiberbűnözésre vonatkozóan? pl. műveleti statisztikák, kiberbűnözési trendekre vonatkozó statisztikák, kiberbűncselekményekből származó javakra és az okozott károkra vonatkozó statisztikák stb.	1	Részt vesznek a bűncselekmények megzavarását célzó, nemzetközi szintű összehangolt fellépésekben? pl. beszivárgás a bűnözői hackerfórumokba, szervezett kiberbűnözői csoportokba, a „dark web” piacaira, valamint botnetek eltávolítása stb.	1
	3	Országuk aláírta az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményét?	1	Rendelkeznek a szellemi tulajdon és szerzői jogok online megsértésével foglalkozó bármely jogi rendelkezéssel?	1	Létrehoztak a kiberbűnözés elleni küzdelem területén végzett tevékenységek koordinálását végző központi szervet/egységet?	1	Végeznek értékelést a LEA-k, az igazságszolgáltatási rendszer és nemzeti CSIRT(ek) személyzetének kiberbűnözés kezelésével kapcsolatban biztosított képzés megfelelőségéről?	1	A CSIRT-ek, LEA-k és az igazságszolgáltatási rendszer (ügyészek és bírók) feladatai egyértelműen elkülönülnek, amikor együttműködnek a kiberbűnözés kezelésében?	1

	4			Rendelkeznek az online zaklatással vagy internetes megfélemlítéssel foglalkozó bármely jogi rendelkezéssel?	1	Létrehoztak együttműködési mechanizmusokat a kiberbűnözés elleni küzdelemben részt vevő érintett nemzeti intézmények, többek között a bűnüldöző nemzeti CSIRT-ek között?	1	Végeznek rendszeres értékeléseket annak biztosítására, hogy rendelkezzenek a LEA-kon belül kiberbűnözéssel foglalkozó egységeknek szánt elegendő (emberi, költségvetési és eszközbeli) erőforrásokkal?	1	Szabályozási keretük támogatja a CSIRT-ek/LEA-k és az igazságszolgáltatási rendszer (ügyészek és bírók) együttműködését?	1
NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**R**
12 – Kiberbűnözés kezelése	5			Rendelkeznek a számítógépes csalással foglalkozó bármely jogi rendelkezéssel? pl. az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményében foglalt rendelkezéseknek való megfelelés	1	Együttműködnek és osztanak meg információkat más tagállamokkal a kiberbűnözés elleni küzdelem területén?	1	Végeznek rendszeres értékeléseket annak biztosítására, hogy rendelkezzenek a bűnüldöző hatóságokon belül kiberbűnözéssel foglalkozó egységeknek szánt elegendő (emberi, költségvetési és eszközbeli) erőforrásokkal?	1	Részt vesznek az uniós érdekelt felekkel (LEA-k, CSIRT-ek, ENISA, az Europol Kiberbűnözés Elleni Európai Központja, azaz az EC3 stb.) megosztandó szabványosított eszközök és módszertanok, formanyomtatványok és eljárások kidolgozásában és fenntartásában?	1
	6	-		Rendelkeznek a gyermekek online védelmével foglalkozó bármely jogi rendelkezéssel? pl. az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményében foglalt rendelkezéseknek való megfelelés	1	Együttműködnek és osztanak meg információkat uniós ügynökségekkel (pl. EC3, Eurojust, ENISA) a kiberbűnözés elleni küzdelem területén?	1	Rendelkeznek olyan egységekkel, bíróságokkal vagy szakbírókkal, amelyek/akik kifejezetten kiberbűnügyekkel foglalkoznak?	1	Rendelkeznek olyan fejlett mechanizmusokkal, amelyek az egyéneket elrettentik attól, hogy részt akarjanak venni vagy részt vegyenek egy kiberbűncselekményben?	0
	7	-		Meghatároztak olyan működő nemzeti kapcsolattartó pontot, amely információk megosztására és az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelvben szereplő bűncselekményekkel kapcsolatos, más tagállamoktól érkező sürgős információkérésekre vonatkozó válaszadásra szolgál?	1	Rendelkeznek a kiberbűnözés kezelésére szolgáló megfelelő eszközökkel? pl. kiberbűnözés taxonómiája és osztályozása, elektronikus bizonyítékok gyűjtésére szolgáló eszközök, kiberkriminalisztikai eszközök, megbízható megosztóplatformok stb.	1	Vannak olyan intézkedéseik, amelyek arra szolgálnak, hogy támogatást és segítséget nyújtsanak a kiberbűnözés áldozatainak (általános felhasználók, kkv-k, nagyvállalatok)?	1	Országuk alkalmazza az Európai Unió nagyszabású kiberbiztonsági eseményekre való reagálásról szóló tervezetét és/vagy bűnüldözésre vonatkozó vészhelyzet-elhárítási jegyzőkönyvét (EU LE ERP)?	0
	8			Bűnüldöző ügynökségük rendelkezik kiberbűnözéssel foglalkozó egységgel?	1	Rendelkeznek az elektronikus bizonyítékok kezelésére szolgáló szabványműveleti előírásokkal?	1	Létrehoztak intézményközi keretet és együttműködési mechanizmusokat valamennyi releváns érdekelt fél (pl. LEA, nemzeti CSIRT, igazságszolgáltatási közösségek), köztük adott esetben a magánszektorbeli érdekeltek (alapvető szolgáltatásokat nyújtó szereplők, szolgáltatók) között a kibertámadásokra való válaszadás érdekében?	1	-	

	9			A budapesti egyezmény 35. cikke szerint kijelöltek egy, a hét minden napján, éjjel-nappal elérhető kapcsolattartó pontot?	1	Országuk részt vesz az uniós ügynökségek (pl. Europol, Eurojust, OLAF, CEPOL, ENISA) által kínált és/vagy támogatott képzési lehetőségekben?	0	Szabályozási keretük támogatja a CSIRT-ek és a bűnüldözés közötti együttműködését?	1	-	
NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**K**
12 – Kiberbűnözés kezelése	10	-		Kijelöltek egy, a nagyszabású kibertámadásokra való reagálás érdekében a hét minden napján, éjjel-nappal elérhető operatív kapcsolattartó pontot az Unió bűnüldözésre vonatkozó vészhelyzet-elhárítási jegyzőkönyve (EU LE ERP) tekintetében?	1	Országuk mérlegeli az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezménye 2. kiegészítő jegyzőkönyvének elfogadását?	0	Rendelkeznek olyan mechanizmusokkal (pl. eszközökkel, eljárásokkal), amelyek révén elősegítik az információmegosztást és az együttműködést a CSIRT/LEA és esetleg az igazságszolgáltatási rendszer (ügyészek és bírók) között a kiberbűnözés elleni küzdelem terén?	1	-	
	11			Biztosítanak rendszeres speciális képzést a kiberbűnözés kezelésében részt vevő érdekelt felek (LEA-k, igazságszolgáltatási szervek, CSIRT-ek) számára? pl. kiberbűnügyekkel kapcsolatos vádemelésre/eljárásokra vonatkozó tanfolyamok, elektronikus bizonyítékok gyűjtésére vonatkozó képzés, valamint többek között az őrizet digitális láncára és kiberkriminalisztikára vonatkozó integritás biztosításával kapcsolatos képzés	1						
	12			Országuk ratifikálta az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményét, illetve csatlakozott az említett egyezményhez?	1			-	-	-	
	13	-		Országuk aláírta és ratifikálta az Európa Tanács számítástechnikai bűnözésről szóló budapesti egyezményének kiegészítő jegyzőkönyvét (számítógépes rendszereken keresztül elkövetett rasszista és idegengyűlölő jellegű cselekmények bűncselekménnyé nyilvánítása)?	0	-	-	-		-	

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
13 – Biztonsági események bejelentésére vonatkozó mechanizmusok létrehozása	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Rendelkeznek informális, a kiberbiztonsági eseményekre vonatkozó, magánszervezetek és nemzeti hatóságok közötti információmegosztási mechanizmusokkal?	1	Rendelkeznek biztonsági események bejelentésére szolgáló rendszerrel a hálózati és információs rendszerek biztonságáról szóló irányelv II. mellékletében szereplő valamennyi ágazat terén?	1	Rendelkeznek olyan kötelező, biztonsági események bejelentésére szolgáló rendszerrel, amely már működik a gyakorlatban?	1	Rendelkeznek egy harmonizált eljárással az ágazati biztonsági események bejelentésére szolgáló rendszerek tekintetében?	1	Készítenek a biztonsági eseményekre vonatkozó éves jelentést?	1
	2	-		Eleget tettek a távközlési szolgáltatásokat nyújtó szolgáltatókra vonatkozó értesítési követelményeknek az (EU) 2018/1972 irányelv 40. cikkével összhangban? Az említett irányelv előírja a tagállamok számára, hogy a nyilvános elektronikus hírközlő hálózatokat üzemeltető és a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók indokolatlan késedelem nélkül értesítsék az illetékes hatóságot minden olyan biztonsági eseményről, amely jelentős hatással volt a hálózatok, illetve a szolgáltatások működésére.	1	Rendelkeznek az általános adatvédelmi rendeletre, a hálózati és információs rendszerek biztonságáról szóló irányelvre, a 40. cikkre (régi 13. cikk) és az eIDAS-rendeletre vonatkozó, biztonsági események bejelentési kötelezettségeivel kapcsolatos koordinációs/együttműködési mechanizmussal?	1	Rendelkeznek biztonsági események bejelentésére szolgáló rendszerrel a hálózati és információs rendszerek biztonságáról szóló irányelvben nem szereplő ágaztok tekintetében?	1	Készülnek kiberbiztonsági helyzetjelentések vagy más típusú elemzések, amelyeket a biztonsági eseményekről szóló jelentéseket megkapó szervezet készít?	1

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
13 – Biztonsági események bejelentésére vonatkozó mechanizmusok létrehozása	3	-		Eleget tettek a bizalmi szolgáltatókra vonatkozó bejelentési követelményeknek a 910/2014/EU rendelet (eIDAS-rendelet) 19. cikkével összhangban? A 19. cikk többek között előírja, hogy a bizalmi szolgáltatóknak be kell jelenteniük a felügyeleti hatóságoknak a jelentős biztonsági eseményeket / biztonság megsértésének eseteit.	1	Rendelkeznek a különféle bejelentési csatornákon keresztül megosztott információk titkosságát és sértetlenségét biztosító megfelelő eszközökkel?	1	Mérik a biztonsági események bejelentési eljárásainak hatékonyságát? *pl.* a megfelelő csatornákon keresztül bejelentett biztonsági eseményekre vonatkozó mutatók, a biztonsági esemény bejelentésének időzítése stb.	1	-	
	4	-		Eleget tettek a digitális szolgáltatókra vonatkozó bejelentési követelményeknek a hálózati és információs rendszerek biztonságáról szóló irányelv 16. cikkével összhangban? A 16. cikk előírja, hogy a digitális szolgáltatók indokolatlan késedelem nélkül bejelentenek az illetékes hatóságnak vagy a nemzeti CSIRT-nek minden olyan biztonsági eseményt, amely jelentős hatást gyakorol az általuk az Unión belül kínált, a III. mellékletben említett szolgáltatás nyújtására.	1	Rendelkeznek a bejelentési folyamatot megkönnyítő platformmal/eszközzel?	0	Rendelkeznek a biztonsági események osztályozására és a kiváltó okok kategóriáira vonatkozó, nemzeti szintű közös taxonómiával?	0	-	

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
14 – Magánélet- és adatvédelem megerősítése	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Végeztek olyan tanulmányokat vagy elemzéseket, amelyek révén azonosítják a polgárok magánélethez való jogainak jobb védelmére szolgáló, javítást igénylő területeket.	1	A nemzeti adatvédelmi hatóság részt vesz a kiberbiztonsággal kapcsolatos ügyekben (pl. új kiberbiztonsági jogszabályok és rendeletek, meghatározott minimális biztonsági intézkedések kidolgozása)?	1	Népszerűsítik a biztonsági intézkedésekre és beépített adatvédelemre vonatozó bevált gyakorlatokat a köz- és magánszektornak?	1	Végeznek rendszeres értékeléseket annak biztosítására, hogy rendelkezzenek az adatvédelmi hatóságnak szánt elegendő (emberi, költségvetési és eszközbeli) erőforrásokkal?	1	Rendelkeznek olyan mechanizmusokkal, amelyek révén nyomon követhetik a technológiai fejlődést a releváns iránymutatások és jogi rendelkezések/kötelezettségek hozzáigazítása érdekében?	1
	2	Nemzeti szinten kidolgoztak az (EU) 2016/679 rendelet, azaz az általános adatvédelmi rendelet érvényesítésére szolgáló jogalapot? pl. a rendelet szabályai konkrétabb rendelkezéseinek vagy korlátozásainak fenntartása vagy bevezetése	0	-		Indítanak az ezzel a témával foglalkozó tudatosságnövelő és képzési programokat?	1	Ösztönzik a szervezeteket és vállalkozásokat arra, h szerezzenek a magánélet védelmére vonatkozó információkezelési rendszerről (Privacy Information Management System, PIMS) szóló ISO/IEC 27701:2019 szabvány szerinti tanúsítást?	1	Aktívan részt vesznek a magánélet védelmét erősítő technológiákra (PET) vonatkozó K+F kezdeményezésekben, illetve támogatják azokat?	0
	3	-		-		A biztonsági események bejelentésének eljárását egyeztetik az adatvédelmi hatósággal?	1	-		-	
	4	-		-		Elősegítik és támogatják az információbiztonsággal és a magánélet védelmével kapcsolatos műszaki szabványok fejlesztését? Ezeket kifejezetten a kis- és középvállalkozásokra (kkv-k) szabják?	0	-		-	

	5	-		-		Biztosítanak gyakorlati és méretezhető iránymutatásokat, amelyek arra szolgálnak, hogy támogassák a különböző adatkezelőket az adatvédelemre vonatkozó jogi követelmények és kötelezettségek betartásában?	0	-		-	

4.1.4 4. csoport: Együttműködés

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
15 – Köz- és magánszféra közötti partnerség létrehozása	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Általánosan ismert tény, hogy a köz- és magánszféra közötti partnerségek (PPP-k) különböző eszközökkel hozzájárulnak az ország kiberbiztonsági szintjének növeléséhez? *pl.* a kiberbiztonsági ipar növekedéséhez fűződő közös érdekek, egy vonatkozó kiberbiztonsági szabályozási keret létrehozásában való együttműködés, K+F támogatása stb.	1	Rendelkeznek a PPP-k létrehozására szolgáló nemzeti cselekvési tervvel?	1	Létrehoztak nemzeti, köz- és magánszféra közötti partnerségeket?	1	Létrehoztak ágazatokon átívelő PPP-ket?	1	Képesek-e a legújabb technológiai és szabályozási fejleményekhez igazítani, illetve ezek függvényében létrehozni PPP-ket?	1
	2	-		Létrehoznak a PPP-k részletes kialakítására szolgáló jog- vagy szerződéses alapot (konkrét jogszabályok, titoktartási megállapodások, szellemi tulajdon)?	1	Létrehoztak ágazatspecifikus PPP-ket?	1	A létrehozott PPP-k keretében az állami szektorok közötti és a magánszektorok közötti együttműködésre is összpontosítanak?	1		
	3	-		-		Biztosítanak finanszírozási lehetőségeket a létrehozott PPP-k számára?	1	Népszerűsítik a PPP-ket a kis- és középvállalkozások (kkv-k) körében?	1	-	

	4	-		-		Általánosságban az állami intézmények vezetik a PPP-ket? *azaz* egy közszférabeli fél egyedüli kapcsolattartó pontként irányítja és koordinálja a PPP-t; az állami szervek előre megállapodnak abban, hogy mit akarnak elérni; a közigazgatás világos iránymutatásai a magánszektorra vonatkozó igényeikről és korlátozásaikról stb.	1	Mérik a PPP-k eredményeit?	1	-	
	5	-		-		Önök tagjai az Európai Kiberbiztonsági Szervezet (ECSO) szerződéses PPP-jének?	0	-		-	
NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**K**
15 – Köz- és magánszféra közötti partnerség létrehozása	6	-		-		Rendelkeznek egy vagy több, CSIRT-tevékenységekkel foglalkozó PPP-vel?	0	-		-	
	7					Rendelkeznek egy vagy több olyan PPP-vel, amely a kritikus információs infrastruktúra védelmére vonatkozó ügyekkel foglalkozik?	0				
	8	-		-		Rendelkeznek egy vagy több olyan PPP-vel, amely a kiberbiztonsági tudatosság növelésével és készségfejlesztéssel foglalkozik?	0	-		-	

NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**K**
16 – Állami ügynökségek közötti együttműködés intézményesítése	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1

	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Rendelkeznek nem hivatalos együttműködési csatornákkal az állami ügynökségek között?	1	Rendelkeznek egy, a kiberbiztonságra összpontosító nemzeti együttműködési rendszerrel? *pl.* tanácsadó testületek, irányítócsoportok, fórumok, testületek, kiberbiztonsági központok vagy ülésező szakértői csoportok	1	Az állami hatóságok részt vesznek az együttműködési rendszerben?	1	Biztosítják a kiberbiztonsággal foglalkozó együttműködési csatornák legalább az alábbi állami szervek közötti meglétét: hírszerző szolgálatok, belföldi bűnüldöző és igazságszolgáltatási hatóságok, kormányzati szereplők, nemzeti CSIRT és a hadsereg?	1	Az állami ügynökségek kapnak egységes minimális tájékoztatást a fenyegetettségi helyzet és a kiberbiztonsági helyzet legújabb fejleményeiről?	1
	2	-		-		Létrehoztak az információk megosztására szolgáló együttműködési platformokat?	1	Mérik-e a különböző együttműködési rendszerek hatékony együttműködés elősegítésében elért sikereit és korlátait?	1	-	
NKBS-célkitűzés	**#**	**1. szint**	**K**	**2. szint**	**K**	**3. szint**	**K**	**4. szint**	**K**	**5. szint**	**K**
16 – Állami ügynökségek közötti együttműködés intézményesítése	3	-		-		Meghatározták az együttműködési platformok alkalmazási körét? (pl. feladatok és felelősségi körök, kérdéskörök száma)	1	-		-	
	4	-		-		Szerveznek éves találkozókat?	1	-		-	
	5	-		-		Rendelkeznek együttműködési mechanizmusokkal a különböző földrajzi területeken található illetékes hatóságok között? *pl.* régiónkénti biztonsági kapcsolattartók hálózata, kiberbiztonsági tisztviselő a regionális gazdasági kamarákban stb.	1	-		-	

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
17 – Nemzetközi együttműködésben való részvétel (nem csak uniós tagállamokkal)	a	Foglalkoznak a célkitűzéssel a jelenlegi NKBS-ükben vagy tervezik azt belefoglalni a következő kiadásba?	1	Vannak olyan informális gyakorlatok vagy tevékenységek, amelyek nem koordinált módon működnek közre a célkitűzés elérésében?	1	Rendelkeznek egy hivatalosan meghatározott és dokumentált cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy teszteljék a teljesítményét?	1	Bevezettek olyan mechanizmusokat, amelyek biztosítják, hogy a cselekvési terv dinamikusan alkalmazkodik a környezeti változásokhoz?	1
	b			Meghatároztak kívánt eredményeket, irányadó alapelveket vagy kulcsfontosságú tevékenységeket a cselekvési tervükhöz?	1	Rendelkeznek egy világos forráselosztású és irányítású cselekvési tervvel?	1	Felülvizsgálják a cselekvési tervüket a célkitűzésre vonatkozóan azért, hogy biztosítsák benne a helyes fontossági sorrend felállítását és a cselekvési terv optimalizálását?	1		
	c			Amennyiben releváns: cselekvési tervük végrehajtás alatt áll-e, illetve korlátozott hatállyal életbe lépett-e már?	0						
	1	Rendelkeznek egy nemzetközi szerepvállalási stratégiával?	1	Kötöttek (kétoldalú, többoldalú) együttműködési megállapodásokat más országokkal vagy más országokban található partnerekkel? *pl.* információmegosztásról, kapacitásépítésről, támogatásról stb.	1	Cserélnek információkat stratégiai szinten? *pl.* magas szintű politikáról, kockázatok észleléséről stb.	1	Országuk nemzeti, kiberbiztonsággal foglalkozó állami ügynökségei részt vesznek nemzetközi együttműködési rendszerekben?	1	Folytatnak eszmecseréket egy vagy több témáról a többoldalú megállapodásokban?	1
	2	Van nem hivatalos együttműködési csatornájuk más országokkal?	1	Rendelkeznek olyan egyedüli kapcsolattartó ponttal, amely összekötő feladatot láthat el a tagállami hatóságokkal (együttműködési csoport, CSIRT-ek hálózata stb.) való határokon átnyúló együttműködés biztosítása érdekében?	1	Cserélnek információkat taktikai szinten? *pl.* fenyegető szereplőkről szóló közlemény, információmegosztó és -elemző központok (ISAC), taktikák, technikák és eljárások (Tactics, Techniques and Procedures, TTP) stb.	1	Végeznek rendszeres értékelést a nemzetközi együttműködési kezdeményezések eredményeiről?	1	Folytatnak eszmecseréket egy vagy több témáról nemzetközi szerződésekben és egyezményekben?	1

NKBS-célkitűzés	#	1. szint	K	2. szint	K	3. szint	K	4. szint	K	5. szint	K
17 – Nemzetközi együttműködésben való részvétel (nem csak uniós tagállamokkal)	3	Az állami vezetés kifejezte szándékát arra vonatkozóan, hogy részt kíván venni a kiberbiztonság területén folytatott nemzetközi együttműködésben?	1	Rendelkeznek nemzetközi együttműködésben való részvételre elkötelezett emberekkel?	1	Cserélnek információkat operatív szinten? *pl.* operatív koordinációs adatokról, folyamatban lévő biztonsági eseményekről, fertőzöttségi mutatókról stb.	1	-		Folytatnak eszmecseréket vagy tárgyalásokat egy vagy több témáról nemzetközi szakértői csoportokkal? *pl.* a kibertér stabilitásával foglalkozó globális bizottsággal (GCSC), az ENISA Kiberbiztonsági Együttműködési Csoportjával, az ENSZ kormányzati információbiztonsági szakértői csoportjával (GGE) stb.	1

	4	-		-		Részt vesznek nemzetközi kiberbiztonsági gyakorlatokban?	1	-		-	
	5	-		-		Részt vesznek nemzetközi kapacitásépítési kezdeményezésekben? *pl.* képzések, készségfejlesztés, standard eljárások kidolgozása stb.	0	-		-	
	6	-		-		Megvalósítottak kölcsönös segítségnyújtási megállapodásokat más országokkal? *pl.* LEA-k tevékenységeire, jogi eljárásokra, a biztonsági eseményekre való reagálási képességek kölcsönösségére, kiberbiztonsági eszközök megosztására stb. vonatkozóan	0	-		-	
	7	-		-		Aláírtak vagy ratifikáltak a kiberbiztonsággal kapcsolatos nemzetközi szerződéseket vagy egyezményeket? *pl.* az információbiztonságról szóló nemzetközi magatartási kódex, a számítástechnikai bűnözésről szóló budapesti egyezmény	0	-		-	

4.2 A KERETRENDSZER HASZNÁLATÁRA VONATKOZÓ IRÁNYMUTATÁSOK

E szakasz célja, hogy a tagállamoknak iránymutatásokat és ajánlásokat biztosítson a keretrendszer elindítására és a kérdőív kitöltésére vonatkozóan. Az alábbiakban felsorolt ajánlások főként a tagállamok képviselőivel folytatott interjúk során gyűjtött visszajelzésekből erednek:

- **Előre mérlegeljék az adatok gyűjtésére és egységes szerkezetbe foglalására szolgáló koordinációs tevékenységeket.** A tagállamok többsége elismeri, hogy egy ilyen önértékelési gyakorlat elvégzése körülbelül 15 munkanapot venne igénybe. Az önértékelés elvégzése érdekében számos különböző érdekelt felet kell együttműködésre kérni. Ezért ajánlott az előkészítési fázisra bizonyos időt meghatározni, hogy azonosítani tudják a kormányzati szervekben, az állami ügynökségekben és a magánszektorban az összes érintett érdekelt felet.
- **Határozzanak meg nemzeti szinten egy, az önértékelés elvégzéséért felelős központi szervet.** Mivel az NCAF valamennyi mutatójára vonatkozó anyaggyűjtés sok érdekelt fél bevonásával járhat, ajánlott egy központi szervet vagy ügynökséget megbízni azzal, hogy az önértékelést az érintett érdekelt felekkel való kapcsolatfelvétel és egyeztetés útján elvégezze.
- **Használják az értékelési gyakorlatot a kiberbiztonsági témák megosztásának és közlésének eszközeként.** A tagállamok által közölt levont tanulságok szemléltették, hogy az eszmecserék jó lehetőséget biztosítanak a kiberbiztonsági témákról folytatott párbeszédek előmozdítására (akár az egyes interjúk, akár közös munkaértekezletek formájában), valamint a közös nézetek és javítási területek megosztására. Amellett, hogy rávilágít a legfontosabb sikerekre, az eredmények megosztása elősegítheti a kiberbiztonsági témák népszerűsítését is.
- **Használják az NKBS-t az értékelés tárgyát képező célkitűzések kiválasztására.** Az NCAF-et alkotó 17 célkitűzés a tagállamok által saját NKBS-ükben általánosan lefedett célkitűzések alapján épült fel. Az NKBS részét képező célkitűzéseket az értékelés részletes megtervezésére szolgáló eszközként lehet felhasználni. Ugyanakkor az NKBS nem korlátozhatja az értékelést. Mivel az NKBS természeténél fogva a prioritásokra összpontosít, bizonyos területek szándékosan nem szerepelnek benne. Ez azonban nem jelenti azt, hogy egy adott kapacitás nincs jelen. Például ha egy meghatározott célkitűzés hiányzik az NKBS-ből, de az ország rendelkezik az említett célkitűzéssel kapcsolatos kiberbiztonsági képességekkel, megtörténhet a célkitűzés értékelése.
- **Amikor az NKBS alkalmazási köre megnő, biztosítsák, hogy a pontszám értelmezése összhangban maradjon az NKBS fejlődésével.** Az NKBS életciklusa egy sokéves folyamat. Egyes tagállamok NKBS-ét általában 3–5 éves ütemtervvel hajtják végre, és változtatnak az alkalmazási körön két egymást követő NKBS-kiadás között. Ebben a tekintetben különös gonddal kell eljárni, amikor bemutatják az önértékelés eredményeit a két NKBS-kiadás között: az alkalmazási kör változásai befolyásolhatják a végső érettségi pontszámot. Ajánlott összehasonlítani a pontszámokat évről évre a stratégiai célkitűzések teljes alkalmazási körén (*azaz* átfogó általános pontszám).

A pontozási mechanizmusra vonatkozó emlékeztető – példa a lefedettségi arányra
A pontozási mechanizmus két pontszámszintet foglal magában:
(i) egy **átfogó általános lefedettségi arányt**, amely az önértékelési keretrendszerben lévő stratégiai célkitűzések teljes listáján alapul; és
(ii) egy **átfogó meghatározott lefedettségi arányt**, amely a tagállam által kiválasztott stratégiai célkitűzéseken alapul (ezek általában megegyeznek az adott ország NKBS-ében szereplő célkitűzésekkel).

Kialakítása alapján (lásd a pontozási mechanizmusról szóló 3.1. szakaszt) az átfogó meghatározott lefedettségi arány ugyanannyi vagy magasabb lesz, mint az átfogó általános lefedettségi arány, mivel az utóbbi olyan célkitűzéseket is tartalmazhat, amelyekkel a tagállam nem foglalkozik, ezáltal csökken az átfogó általános lefedettségi arány. Amikor egy tagállam új célkitűzést vesz fel, az átfogó lefedettségi arány növekedni fog (azaz több lesz a lefedett érettségi mutató), míg az átfogó meghatározott érettség csökkenhet (abban az esetben, ha az újonnan felvett célkitűzés kezdeti szakaszban jár, így az érettségi szintje alacsony).

- **Az önértékelési kérdőív kitöltése során ne feledjék, hogy az elsődleges cél a tagállamok kiberbiztonsági kapacitásépítésének támogatása.** Ezért az önértékelés elvégzésekor, még ha bizonyos helyzetekben nehéz is határozott választ adni a kérdésekre, ajánlott a legáltalánosabban elfogadott választ megadni. Ha például egy kérdésre „Igen” a válasz egy bizonyos témakört illetően, de „Nem” a válasz egy másik témakörben, a tagállamoknak figyelembe kell venniük, hogy „Nem” esetén intézkedniük kell: vagy egy helyreállítási tervet vagy egy, a javítási területtel foglalkozó tervet kell készíteni, amelyre a jövőbeni fejlesztések során tekintettel kell lenni.

5. KÖVETKEZŐ LÉPESEK

5.1 JÖVŐBENI FEJLESZTÉSEK

A tagállamok képviselőivel folytatott interjúk és a másodelemzési fázis során az alábbi, nemzeti képességek értékelése aktuális keretrendszerének javítására vonatkozó ajánlásokat határozták meg mint potenciális jövőbeni fejlődési lehetőségeket:

- **A nagyobb pontosság elérése érdekében fejleszteni kell a pontozási rendszert.** Például a bináris Igen/Nem válasz helyett megadhatnák a lefedettségi százalékot, hogy jobban figyelembe lehessen venni nemzeti szinten a képességek megszilárdításának összetettségét. Első lépésként az Igen/Nem válaszú egyszerű megközelítést választották.
- **A tagállamok NKBS-e hatékonyságának mérésére kvantitatív mérési módszert kell bevezetni.** A Nemzeti képességek értékelésének keretrendszere középpontjában tulajdonképpen a tagállamok kiberbiztonsági képességei érettségi szintjének értékelése áll. Ezt ki lehet egészíteni a tagállamok által e képességek kiépítése érdekében végrehajtott tevékenységek és cselekvési tervek hatékonyságának mérésére szolgáló mérőszámokkal. Nem tűnt reálisnak az ilyen hatékonysági mérőszámok kidolgozása a jelenlegi szakaszban, tekintettel arra, hogy: kevés a területtől érkező visszajelzés; nehéz olyan értelmezhető mutatókat találni, amelyek az eredményt az NKBS végrehajtásához kapcsolják; és nehéz olyan reális mutatókat létrehozni, amelyeket a későbbiekben össze lehet gyűjteni. Ez azonban olyan téma, amellyel a jövőben foglalkozni kell.
- **Az önértékelési gyakorlatról egy értékelési megközelítésre kell váltani.** A keretrendszer jövőbeni lehetséges fejlődése lehet az értékelési megközelítés felé történő elmozdulás a tagállamok kiberbiztonsági képességei érettségének következetesebb értékelése érdekében. Amennyiben egy harmadik fél végzi el az értékelést, az tulajdonképpen lehetővé teszi a potenciális elfogultság minimalizálását.

A. MELLÉKLET – A MÁSODELEMZÉS EREDMÉNYEINEK ÁTTEKINTÉSE

Az A. melléklet összefoglalja az ENISA NKBS-sel kapcsolatos korábbi munkáját és ismerteti a kiberbiztonsági kapacitásra vonatkozó releváns, nyilvánosan elérhető érettségi modelleket. A modellek kiválasztása és felülvizsgálata során az alábbi feltételezéseket vesszük figyelembe:

- Nem minden modell épül szigorú kutatási módszertanra;
- A modellek struktúrájára és eredményeire vonatkozóan nem mindig kapunk részletes magyarázatot, amelyben megmutatkozik az egyes modelleket jellemző különböző elemek közötti egyértelmű kapcsolat;
- Egyes modellek nem részletezik a fejlesztési folyamatot, struktúrát és az értékelési módszertant;
- Más olyan modellek és eszközök, amelyeket találtunk, nem részletezik a struktúrát és tartalmat, ezért nem szerepelnek a felsorolásban; és
- A felülvizsgálandó modellek kiválasztása a földrajzi lefedettség alapján történik. Az elsődleges hangsúly az európai országok teljesítményének értékelésére kidolgozott, kiberbiztonsági kapacitásra vonatkozó érettségi modellen lesz. Fontos azonban a földrajzi lefedettség kiterjesztése az érettségi modellek világszerte történő kiépítésével kapcsolatos bevált gyakorlatok elemzése érdekében.

A kiberbiztonsági kapacitásra vonatkozó releváns, nyilvánosan elérhető érettségi modell szisztematikus áttekintését a Becker által az érettségi modellek kidolgozására meghatározott módszertanon alapuló egyedi kialakítású elemzési keretrendszer segítségével végezték el[22]. Mindegyik meglévő modell tekintetében az alábbi elemeket elemezték:

- **Az érettségi modell neve:** az érettségi modell neve és a fő referenciák;
- **Intézményi forrás:** a modell megalkotásáért felelős állami vagy magánintézmény;
- **Általános cél:** a modell általános alkalmazási köre és a tervezett cél(ok);
- **A szintek száma és meghatározása:** a modell érettségi szintjeinek száma, valamint azok általános leírása;
- **Attribútumok száma és neve:** az érettségi modell által használt attribútumok száma és neve. Az attribútumok elemzésének három célja van:
  - az érettségi modell könnyen érthető részekre bontása;
  - az attribútumok összesítése attribútumcsoportokba, amelyek ugyanazt a célt szolgálják; és
  - az érettségi szint tárgyára vonatkozó különböző nézőpontok biztosítása.
- **Értékelési módszer:** az érettségi modell értékelésének módszere;
- **Eredmények ábrázolása**: az érettségi modell eredményeire vonatkozó megjelenítési módszer meghatározása. Az e lépés mögött meghúzódó logika, hogy az érettségi

[22] Becker, J., Knackstedt, R., és Pöppelbuß, J.: Developing Maturity Models for IT Management: A Procedure Model and its Application, *Business & Information Systems Engineering*, 1. kiad.,3. sz., 2009. június, 213–222. o.

modellek általában kudarcot vallanak, ha túl összetettek, ezért az ábrázolás módjának meg kell felelnie a gyakorlati igényeknek.

Az NKBS-sel kapcsolatos korábbi munkák

Korai munkái keretében az ENISA két dokumentumot tett közzé 2012-ben az NKBS témakörében. Először is a „Practical guide on the development and execution phase of NCSS”[23] című dokumentum az NKBS hatékony végrehajtására vonatkozó konkrét intézkedéseket javasolt, illetve az NKBS életciklusát négy fázisban mutatta be: stratégiakidolgozás, stratégiavégrehajtás, stratégiaértékelés és stratégiafenntartás. Másodszor a „Setting the course for national efforts to strengthen security in cyberspace”[24] című dokumentum felvázolta a kiberbiztonsági stratégiák 2012. évi helyzetét az Unióban és azon kívül, valamint azt javasolta, hogy a tagállamok határozzák meg az NKBS-eik közötti közös témákat és különbségeket.

2014-ben megjelent az ENISA első, egy tagállam NKBS-ének értékelésére szolgáló keretrendszere[25]. Ez a keretrendszer az NKBS értékelésére vonatkozó ajánlásokat, bevált gyakorlatokat és kapacitásépítő eszközöket tartalmaz (*pl.* azonosított célkitűzéseket, hozzájárulásokat, eredményeket, kulcsfontosságú teljesítménymutatókat stb.). Ezek az eszközök igazodnak a stratégiai tervezésük szempontjából különböző érettségi szinten lévő országok eltérő igényeihez. Ugyanebben az évben az ENISA közzétette az „Online NCSS Interactive Map”[26] nevű interaktív térképet, amely lehetővé teszi a felhasználók számára, hogy gyorsan tanulmányozhassák valamennyi tagállam és EFTA-ország NKBS-ét, beleértve a stratégiai célkitűzéseket és a végrehajtásra vonatkozó jó példákat. Először egy NKBS-adattár funkcióját töltötte be (2014), majd 2018-ban végrehajtási példákkal egészítették ki, és 2019 óta a térkép *információs platformként* szolgál a tagállamok által nemzeti kiberbiztonságuk fokozására irányuló erőfeszítéseikkel kapcsolatban biztosított adatok centralizálására.

A 2016-ban közzétett „NCSS Good Practice Guide”[27] című dokumentum tizenöt stratégiai célkitűzést határoz meg. Ez az útmutató az egyes tagállamok NKBS-e végrehajtásának helyzetét is elemzi, továbbá azonosítja a végrehajtásra vonatkozó különböző hiányosságokat és kihívásokat.

2018-ban az ENISA közzétette a „National Cybersecurity Strategies Evaluation Tool”[28] nevű interaktív önértékelési eszközt, amely segíti a tagállamokat az NKBS-ükkel kapcsolatos prioritásaik és célkitűzéseik értékelésében. Ez az eszköz egyszerű kérdések révén az egyes célkitűzések megvalósítására vonatkozó konkrét ajánlásokkal látja el a tagállamokat. Végül a 2019-ben kiadott „Good practices in innovation on Cybersecurity under the NCSS”[29] című dokumentum az NKBS keretében végzett kiberbiztonsági innováció témáját mutatja be. A dokumentum a téma szakértői által felismert, a különböző innovációs dimenziókban rejlő

[23] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] National Cybersecurity Strategies - Interactive Map (ENISA, 2014, frissítve 2019-ben)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Ez a dokumentum a 2012. évi útmutató frissített verziója: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

kihívásokat és bevált gyakorlatokat határoz meg, ezzel segítve a jövőbeni innovatív stratégiai célkitűzések megalkotását.

A.1 Kiberbiztonsági kapacitás érettségi modellje a nemzetek számára (CMM)

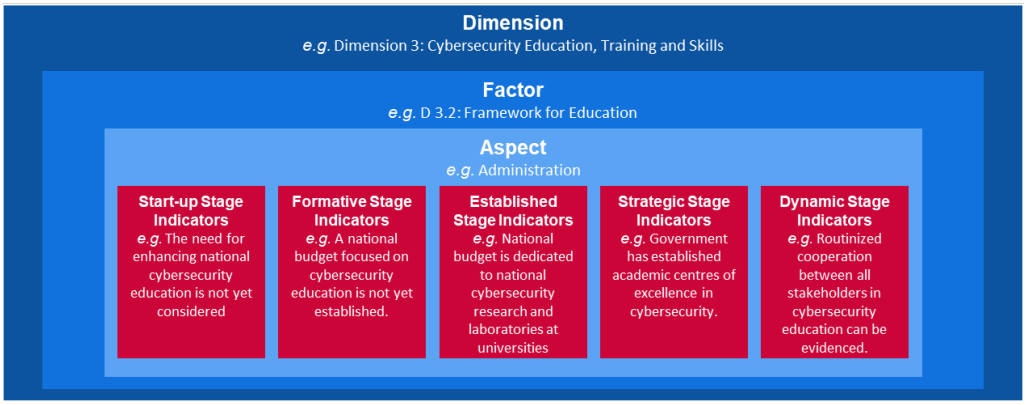
A Kiberbiztonsági kapacitás érettségi modellje a nemzetek számára (Cybersecurity Capacity Maturity Model for Nations, CMM) nevű modellt a Globális Kiberbiztonsági Kapacitásépítési Központ (Kapacitásépítési Központ) dolgozta ki, amely az Oxfordi Egyetem Oxford Martin School intézményének része. A Kapacitásépítési Központ célja, hogy mind az Egyesült Királyságban, mind nemzetközi szinten növelje a kiberbiztonsági kapacitásépítés terjedelmét és hatékonyságát a kiberbiztonsági kapacitás érettségi modelljének (CMM) alkalmazása révén. A CMM közvetlenül azoknak az országoknak szól, amelyek növelni szeretnék nemzeti kiberbiztonsági kapacitásukat. Az eredetileg 2014-ben bevezetett CMM-et 2016-ban átdolgozták, miután felhasználták 11 nemzeti kiberbiztonsági kapacitás felülvizsgálatában.

Attribútumok/Dimenziók

A CMM szerint a kiberbiztonsági kapacitás **öt dimenzióból** áll, amelyek a kiberbiztonsági kapacitás csoportjait képviselik. Mindegyik csoport különböző kutatási „lencséket” jelöl, amelyeken keresztül tanulmányozható és értelmezhető a kiberbiztonsági kapacitás. Az öt dimenzión belül **tényezők** írják le a kiberbiztonsági kapacitás birtoklására vonatkozó részleteket. Ezek a részletek olyan elemek, amelyek hozzájárulnak a kiberbiztonsági kapacitás érettségének javításához az egyes dimenziókban. Mindegyik tényező tekintetében különféle **szempontok** jelölik a tényező különböző alkotóelemeit. A szempontok egy olyan szervezési módszert jelölnek, amely a mutatókat kisebb, könnyebben felfogható csoportokra osztja. Ezután az egyes szempontokat **mutatók** segítségével értékelik, hogy leírhatók legyenek azok a lépések, műveletek vagy építőelemek, amelyek egy adott szemponton, tényezőn és dimenzión belül jelzik az érettség egy adott szakaszát (ennek meghatározása a következő szakaszban olvasható).

A fent említett kifejezések az alábbi ábrán bemutatott módon rétegezhetőek.

4. ábra: CMM-mutatókra vonatkozó példa



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Dimenzió pl. 3. dimenzió: Kiberbiztonsági oktatás, képzés és készségek
Factor e.g. D 3.2: Framework for Education	Tényező pl. D 3.2.: Oktatási keretrendszer
Aspect e.g. Administration	Szempont pl. Adminisztráció

Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Kezdeti szakasz mutatói pl. A nemzeti kiberbiztonsági oktatás erősítésének szükségességét még nem mérlegelik
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Alakító szakasz mutatói pl. Még nem hoztak létre a kiberbiztonsági oktatásra fordítandó nemzeti költségvetést
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Megalapozott szakasz mutatói pl. Rendelkeznek a nemzeti kiberbiztonsági kutatásra és egyetemi laboratóriumokra fordított nemzeti költségvetéssel
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Stratégiai szakasz mutatói pl. A kormány létrehozott egy, a kiberbiztonsággal foglalkozó tudományos kiválósági központot
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Dinamikus szakasz mutatói pl. A kiberbiztonsági oktatás valamennyi érdekelt fele közötti rutinszerű együttműködés bizonyítható

Az öt dimenzió részletes leírása alább olvasható:

i Kiberbiztonsági politika és stratégia kidolgozása (6 tényező);
ii Felelős kiberbiztonsági kultúra ösztönzése a társadalomban (5 tényező);
iii Kiberbiztonsági ismeretek fejlesztése (3 tényező);
iv Hatékony jogi és szabályozási keretek létrehozása (3 tényező);
v Kockázatok ellenőrzése szabványok, szervezetek és technológiák révén (7 tényező).

Érettségi szintek

A CMM **5 érettségi szintet** használ annak meghatározására, milyen mértékben fejlődött egy ország a kiberbiztonsági kapacitás egy adott tényezőjével/szempontjával kapcsolatban. Ezek a szintek a meglévő kiberbiztonsági kapacitásról készült pillanatfelvételek:

- **Kezdeti szakasz**: Ebben a szakaszban vagy még egyáltalán nem beszélhetünk kiberbiztonsági érettségről, vagy még nagyon kezdetleges. Lehetnek a kiberbiztonsági kapacitásépítéssel kapcsolatos kezdeti eszmecserék, de még nem történtek konkrét intézkedések. Ebben a szakaszban nincs megfigyelhető bizonyíték;
- **Alakító szakasz**: Megfigyelhető a szempontok egyes jellemvonásainak növekedése és kialakulása, de ez történhet *ad hoc* alapon, szervezetlen, rosszul meghatározott lehet, vagy egyszerűen csak „új”. Ennek a tevékenységnek a bizonyítéka azonban egyértelműen kimutatható;
- **Megalapozott szakasz**: A szempont elemei már meghatározottak és működnek. Ugyanakkor még nincs jól átgondolt stratégia a kapcsolódó erőforrások elosztására. Kevés kompromisszumos döntés született a szempont különböző elemeibe történő „relatív” befektetést illetően. A szempont azonban funkcionál és meg van határozva;
- **Stratégiai szakasz**: Döntés született arról, hogy a szempont mely részei fontosak, és melyek kevésbé fontosak az adott szervezet vagy nemzet számára. A stratégiai szakasz tükrözi azt a tényt, hogy ezeket a döntéseket a nemzet vagy szervezet sajátos körülményeitől függően meghozták; és
- **Dinamikus szakasz**: Ebben a szakaszban világos mechanizmusok vannak érvényben a stratégia az alapján történő megváltoztatására, hogy milyenek a fennálló körülmények, mint például a fenyegetettségi környezet, a globális konfliktus technológiája, illetve egy érintett terület (*pl.* kiberbűnözés vagy adatvédelem) jelentős változása. A dinamikus szervezetek módszereket fejlesztettek ki a stratégiák lépésről lépésre történő megváltoztatására. E szakasz jellemvonásai a gyors döntéshozatal, az erőforrások újraelosztása és állandó figyelem a változó környezetre.

Értékelési módszer

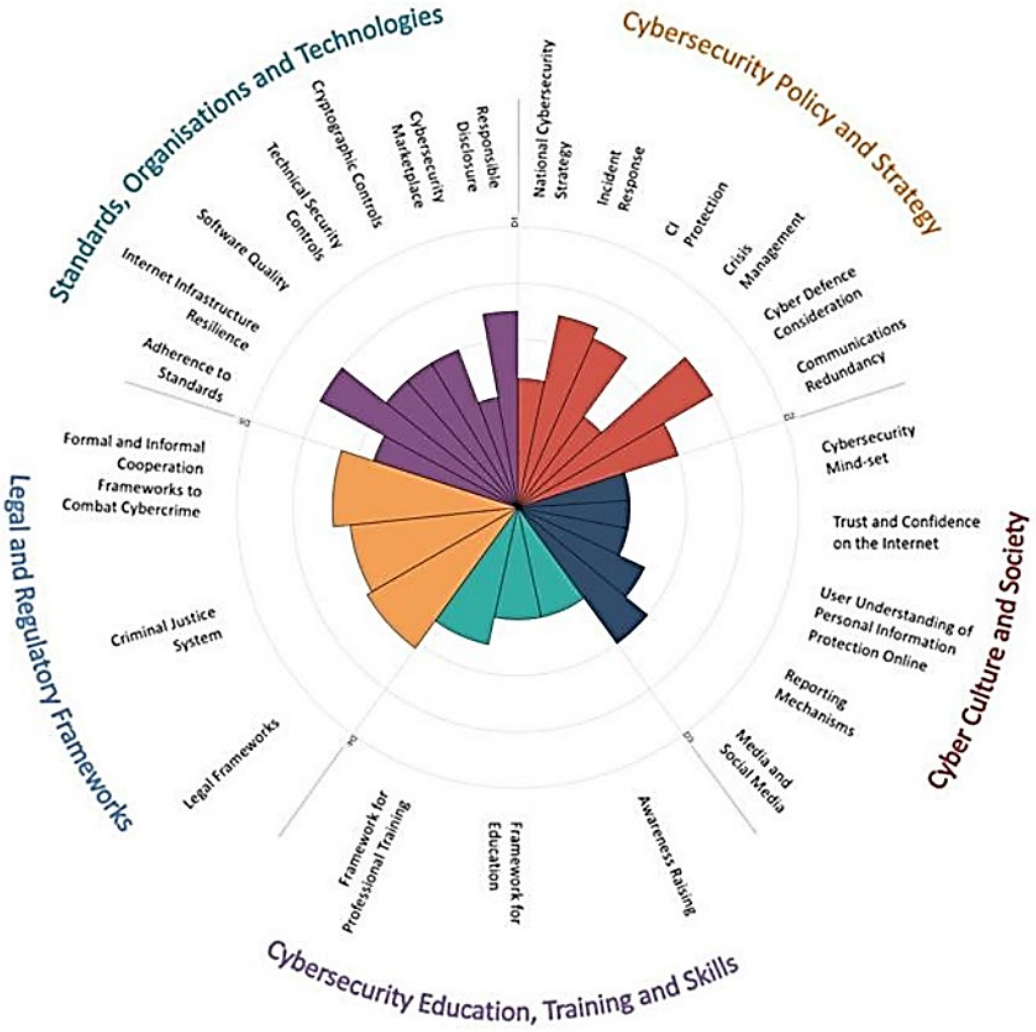
Mivel a Kapacitásépítési Központ nem rendelkezik alapos és mélyreható ismeretekkel azt a belföldi környezetet illetően, amelyben a modellt alkalmazzák, a kiberbiztonsági kapacitás érettségének felülvizsgálata érdekében együttműködik nemzeti szervezetekkel, az adott országban működő fogadó minisztériumokkal vagy szervezetekkel. A CMM-ben szereplő öt

dimenzió érettségi szintjének értékelése érdekében a Kapacitásépítési Központ és a fogadó szervezet 2 vagy 3 nap leforgása alatt találkozik a köz- és magánszektor érintett nemzeti érdekeltjeivel, hogy a CMM dimenzióival foglalkozó fókuszcsoportokat hozzanak létre. Minden dimenziót legalább kétszer megvitatnak az érintett felek különböző csoportjai. Ez képezi az előzetes adatkészletet a későbbi értékeléshez.

Az eredmények módusza vagy ábrázolása

A CMM egy öt részből álló radar segítségével nyújt áttekintést az egyes országok érettségi szintjéről, ahol minden dimenzióhoz tartozik egy ilyen rész. Minden dimenzió a grafikus ábra egyötödét foglalja el, az egyes tényezők öt érettségi szakasza a grafikus ábra középpontjától kifelé halad; az alább bemutatottak szerint a „kezdeti szakasz" van az ábra középpontjához legközelebb, míg a „dinamikus szakasz" a szélén helyezkedik el.

5. ábra CMM: Eredmények áttekintése



Standards, Organisations and Technologies	Szabványok, szervezetek és technológiák
Legal Regulatory Frameworks	Jogi szabályozási keretek
Cybersecurity Education, Training and Skills	Kiberbiztonsági oktatás, képzés és készségek
Cybersecurity Policy and Strategy	Kiberbiztonsági politika és stratégia
Cyber Culture and Society	Kiberkultúra és -társadalom
Responsible Disclosure	Felelős közzététel
Cybersecurity market place	Kiberbiztonsági piac

Cryptographic Controls	Kriptográfiai ellenőrzések
Technical Security Controls	Műszaki biztonsági ellenőrzések
Software Quality	Szoftverminőség
Internet Infrastructure Resilience	Internetes infrastruktúra rezilienciája
Adherence to Standards	Szabványok betartása
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Kiberbűnözés elleni küzdelemre kialakított formális és informális együttműködési keretek
Criminal Justice System	Igazságszolgáltatási rendszer
Legal Frameworks	Jogi keretrendszerek
Framework for Professional Training	Szakképzési keretrendszer
Framework for Education	Oktatási keretrendszer
Awareness Raising	Tudatosságnövelés
Media and Social Medai	Média és közösségi média
Reporting Mechanisms	Bejelentési mechanizmusok
User Understanding of Personal Information Protection Online	A személyes információk online védelmének felhasználók általi megértése
Trust and Confidence on the Internet	Bizalom az interneten
Cybersecurity Mind-set	Kiberbiztonsági mentalitás
Communications Redundancy	Kommunikációs felesleg
Cyber Defence Consideration	Kibervédelmi tanácskozás
Crisis Management	Válságkezelés
CI Protection	Kritikus infrastruktúra védelme
Incident Response	Biztonsági eseményekre való reagálás
National Cybersecurity Strategy	Nemzeti kiberbiztonsági stratégia

Globális Kiberbiztonsági Kapacitásépítési Központ, Oxford Martin School, Oxfordi Egyetem, 2017.

A.2 Kiberbiztonsági képességérettségi modell (C2M2)

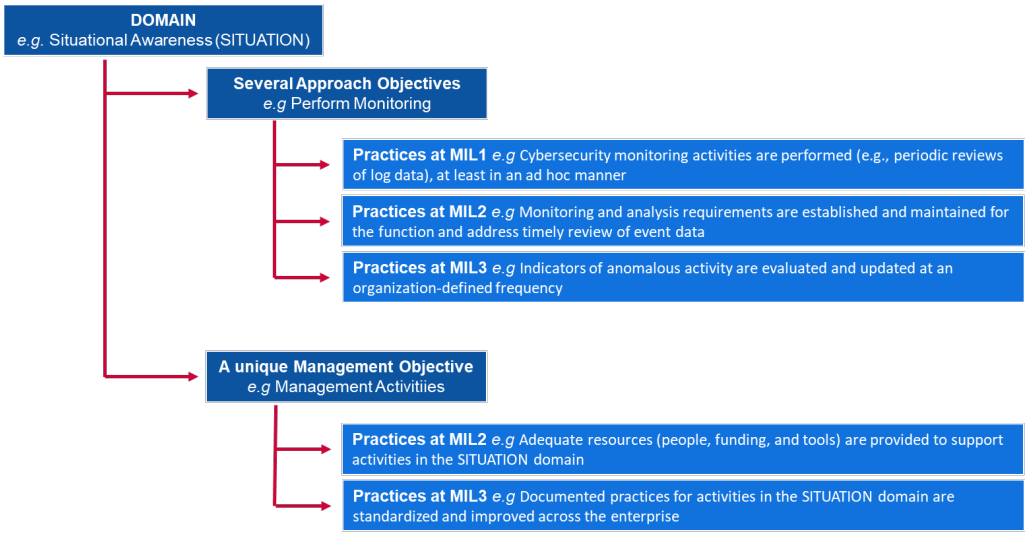
A Kiberbiztonsági képességérettségi modellt (C2M2) az Amerikai Egyesült Államok Energiaügyi Minisztériuma dolgozta ki a köz- és magánszektor szakértőivel együttműködve. A Kapacitásépítési Központ célja, hogy ágazattól, típustól és mérettől függetlenül segítse a szervezeteket saját kiberbiztonsági programjaik értékelésében és javításában, valamint működési rezilienciájuk megerősítésében. A C2M2 az információs, információtechnológiai (IT) és műveleti technológiai (MT) eszközökhöz kapcsolódó kiberbiztonsági gyakorlatok végrehajtására és kezelésére, illetve azokra a környezetekre összpontosít, amelyben működnek. A C2M2 szerint az érettségi modellek: „olyan jellemvonások, attribútumok, mutatók vagy minták összessége, amelyek képességet és előrehaladást jelölnek egy adott tudományágban”. Az eredetileg 2014-ben kiadott C2M2-t 2019-ben átdolgozták.

Attribútumok/Dimenziók

A C2M2 **tíz tartományt** jelöl ki a kiberbiztonsági gyakorlatok logikus csoportosítására. Az egyes gyakorlatcsoportok azokat a tevékenységeket jelölik, amelyeket egy szervezet elvégezhet a tartomány képességeinek kiépítésére és érlelésére. Ezután minden tartományhoz társítanak egy **egyedi kezelési célkitűzést** és **több megközelítési célkitűzést**. Mind a megközelítési, mind a kezelési célkitűzésekben megtalálható az intézményesített tevékenységeket ismertető **számos gyakorlat** részletes leírása.

Az alábbiakban olvasható az említett fogalmak közötti kapcsolat összefoglalása:

6. ábra: C2M2-mutatóra vonatkozó példa



Domain eg Situational Awareness (SITUATION)	**Tartomány** pl. helyzetismeret (HELYZET)
Several Approaches Objectives e.g. Perform Monitoring	**Több megközelítési célkitűzés** pl. nyomon követés
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Gyakorlatok MIL1 szinten** pl. végeznek nyomon követési tevékenységeket (pl. naplóadatok időszakos felülvizsgálata) legalább *ad hoc* módon
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Gyakorlatok MIL2 szinten** pl. meghatároztak és fenntartanak nyomon követési és elemzési követelményeket az eseményadatok működéséhez és időben történő felülvizsgálatához
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Gyakorlatok MIL3 szinten** pl. a rendellenes tevékenység mutatóit a szervezet által meghatározott gyakorisággal értékelik és aktualizálják
A unique Management Objectve e.g. Management Activities	Egy egyedi kezelési célkitűzés pl. kezelési tevékenységek
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Gyakorlatok MIL2 szinten** pl. megfelelő erőforrások (emberi, finanszírozási és eszközbeli) biztosítottak a HELYZET tartomány tevékenységeinek támogatására
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Gyakorlatok MIL3 szinten** pl. a HELYZET tartomány tevékenységeire vonatkozó dokumentált gyakorlatokat szabványosítják és javítják a vállalat egészében

A tíz tartomány részletes leírása az alábbiakban olvasható:

i Kockázatkezelés (KOCKÁZAT);
ii Eszköz-, változás- és konfigurációkezelés (ESZKÖZ);
iii Személyazonosság- és hozzáférés-kezelés (HOZZÁFÉRÉS);
iv Fenyegetés- és sebezhetőségkezelés (FENYEGETÉS);
v Helyzetismeret (HELYZET);
vi Eseményekre és biztonsági eseményekre való reagálás (REAGÁLÁS);
vii Ellátási lánc és külső függőségek kezelése (FÜGGŐSÉGEK);
viii Munkaerő-gazdálkodás (MUNKAERŐ)
ix Kiberbiztonsági architektúra (ARCHITEKTÚRA); és
x Kiberbiztonsági program kezelése (PROGRAM).

Érettségi szintek

A C2M2 **4 érettségi szintet** (a nevük érettségjelző szintek, azaz Maturity Indicator Levels – MIL) használ az érettség kettős előrehaladásának, mégpedig a megközelítési előrehaladás és a kezelési előrehaladás meghatározására. A MIL-ek MIL0 szinttől MIL3 szintig terjednek és mindegyik tartományban egymástól függetlenül alkalmazhatók.

- **MIL0**: Nem végeznek gyakorlatokat.
- **MIL1**: Kezdeti gyakorlatokat végeznek, de ez történhet *ad hoc* módon.
- **MIL2**: Kezelési jellemzők:
  - a gyakorlatokat dokumentálják;
  - a folyamat támogatására megfelelő erőforrásokat biztosítanak;
  - a gyakorlatokat elvégző személyzet megfelelő szakértelemmel és ismeretekkel rendelkezik; és

- ki vannak jelölve a gyakorlatok elvégzésére vonatkozó felelősségi és hatáskörök.

Megközelítési jellemző:

- a gyakorlatok teljesebbek vagy fejlettebbek, mint a MIL1 szinten.

- **MIL3**: Kezelési jellemzők:
  - a tevékenységek irányítása politikák (vagy egyéb szervezeti irányelvek) alapján történik;
  - a tartomány tevékenységeire vonatkozó teljesítési célkitűzéseket dolgoztak ki és monitoroznak a teljesítmény nyomon követése érdekében;
  - a tartomány tevékenységeire vonatkozó dokumentált gyakorlatokat szabványosítják és javítják a vállalat egészében.

Megközelítési jellemző:

- a gyakorlatok teljesebbek vagy fejlettebbek, mint a MIL1 szinten.

Értékelési módszer

A C2M2-t egy **önértékelési módszertannal** és eszköztárral (kérésre rendelkezésre áll) történő használatra tervezték azért, hogy a szervezetek megmérhessék és fejleszthessék saját kiberbiztonsági programjukat. Az eszköztár használatával az önértékelést egyetlen nap alatt el lehet végezni, de az eszköztárat szigorúbb értékelési munkához is lehet alkalmazni. Ezenkívül a C2M2 használható egy új kiberbiztonsági program kidolgozásának irányítására.

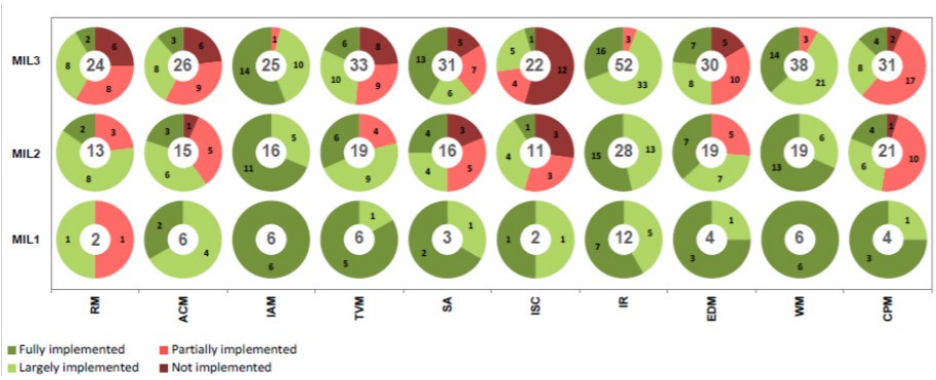
A modell tartalma magas szintű elvonatkoztatással jelenik meg, hogy a különböző típusú, felépítésű, méretű és ágazatbeli szervezetek értelmezni tudják. A modell széles körű használata egy ágazatban támogathatja az adott ágazat kiberbiztonsági képességeinek összehasonlító elemzését.

Az eredmények módusza vagy ábrázolása

A C2M2 rendelkezésre bocsát egy értékeléspontozási jelentést, amelyet a felmérés eredményeiből hoznak létre. A jelentés két nézet szerint mutatja be az eredményeket: a célkitűzés-alapú nézet, amely az egyes tartományok és célkitűzések szerint mutatja be a gyakorlati kérdésekre adott válaszokat, illetve a tartományalapú nézet, amely az összes tartomány és MIL szerint mutatja be a válaszokat. Mindkét nézet olyan ábrázolási rendszeren alapul, amelyet válaszonként egy kördiagram (vagy „fánkdiagram”) és egy jelzőlámpás rendszerre épülő pontozási mechanizmus jellemez. Amint az a 7. ábrán látható, a fánkdiagramokban szereplő piros körcikkek a felmérésben szereplő, „Nem végrehajtott” (sötétpiros) vagy „Részben végrehajtott” (világospiros) válaszokkal jelölt kérdések számát mutatja. A zöld körcikkek a „Nagyrészt végrehajtott” (világoszöld) vagy „Teljesen végrehajtott” (sötétzöld) válasszal jelölt kérdések számát mutatja.

Az alábbi 7. ábra az érettségértékelés végén kapott eredménytábla egyik példáját mutatja be. Az X tengelyen látható a C2M2 10 tartománya, az Y tengelyen pedig az érettségi szintek (MIL-ek). Ha megnézzük a grafikont, valamint tanulmányozzuk a kockázatkezelés (KK) tartományát, három kördiagramot vehetünk észre, amelyek mindegyike megfelel az ML1, ML2 és ML3 érettségi szinteknek. A KK tartomány tekintetében a grafikon kiemeli, hogy az ML1 szint eléréséhez két elemet kell értékelni. Ebben az esetben egy „Nagyrészt végrehajtott” és egy „Részben végrehajtott” pontszámot. Az ML2 érettségi szint vonatkozásában a modell 13 értékelendő elemet irányoz elő. A 13 elemből kettő az első, azaz az ML1 szinthez tartozik, 11 pedig az ML2 szinthez. Ugyanez vonatkozik a harmadik, azaz az ML3 szintre.

7. ábra: C2M2 – Példa a tartományalapú nézetre



Fully implemented	Teljesen végrehajtott
Largely implemented	Nagyrészt végrehajtott
Partially implemented	Részben végrehajtott
Not implemented	Nem végrehajtott
MIL1	MIL1
MIL2	MIL2
MIL3	MIL3
RM	KK
ACM	EVK
IAM	IAM
TVM	FSK
SA	SA
ISC	IMK
IR	ER
EDM	KFK
WM	MG
CPM	KPK

Forrás: Az Amerikai Egyesült Államok Energiaügyi Minisztériuma, Áramszolgáltatásért és Energiamegbízhatóságért felelős Hivatal, 2015.

A.3 Kritikus infrastruktúra kiberbiztonságának javítására szolgáló keretrendszer

A Kritikus infrastruktúra kiberbiztonságának javítására szolgáló keretrendszert a Nemzeti Szabványügyi és Technológiai Intézeten (NIST) belül dolgozták ki. Középpontjában a szervezeten belüli kiberbiztonsági tevékenységek irányítása és kockázatkezelés áll. Mérettől, a kiberbiztonsági kockázat mértékétől vagy a kiberbiztonsági kifinomultságtól függetlenül valamennyi szervezettípusnak szól. Mivel egy keretrendszerről, nem pedig egy modellről van szó, felépítése különbözik a korábban elemzett modellekétől.

A keretrendszer a következő három részből áll: a keretrendszer központi eleme, a végrehajtási lépcsők, valamint a keretrendszer profiljai:

- A **keretrendszer központi eleme** olyan kiberbiztonsági tevékenységeket, kívánt eredményeket és alkalmazandó referenciákat takar, amelyek gyakoriak a kritikus infrastruktúra ágazati között. Ezek hasonlóak a kiberbiztonsági kapacitás érettségi modelljeiben található attribútumokhoz vagy dimenziókhoz.
- A **keretrendszer végrehajtási lépcsői** („a lépcsők”) kontextusba helyezik azt, hogyan látja egy szervezet a kiberbiztonsági kockázatokat és az adott kockázatok kezelésére kidolgozott eljárásokat. A lépcsők, amelyek a „Részleges”-től (1. lépcső) az „Alkalmazkodó”-ig (4. lépcső) terjednek, a kiberbiztonsági kockázatok kezelésének gyakorlataira vonatkozó merevség és kifinomultság növekvő mértékét mutatják be. A lépcsők nem érettségi szintet jelölnek, inkább arra szolgálnak, hogy támogassák a szervezetet a kiberbiztonsági kockázatok kezelésének módjára vonatkozó döntések

meghozatalában, illetve annak eldöntésében, hogy a szervezet mely dimenziói magasabb prioritásúak és kaphatnak kiegészítő forrásokat.

- A **keretrendszer profilja** („a profil") jelöli az olyan, üzleti igényeken alapuló eredményeket, amelyeket a szervezet a keretrendszer kategóriáiból vagy alkategóriáiból választott ki. A profil jellemezhető egy adott végrehajtási forgatókönyvben a szabványok, iránymutatások és gyakorlatok a keretrendszer központi eleméhez való igazításával. A profilokat fel lehet használni a kiberbiztonsági helyzet javítására szolgáló lehetőségek azonosítására úgy, hogy egy „Jelenlegi" profilt (pillanatnyi állapot) összehasonlítanak egy „Cél" profillal (elérni kívánt állapot).

A keretrendszer központi eleme

A keretrendszer központi eleme öt **funkcióból** áll. Ha együtt vizsgálják őket, az említett funkciók magas szintű, stratégiai képet adnak egy szervezet kiberbiztonsági kockázatkezelésének életciklusáról. A keretrendszer központi eleme ezután azonosítja az egyes funkciók mögött álló kulcsfontosságú **kategóriákat** és **alkategóriákat**, valamint olyan informatív példareferenciákhoz igazítja őket, mint az egyes alkategóriákra vonatkozó meglévő szabványok, irányelvek és gyakorlatok.

A funkciók és kategóriák részletes leírása az alábbiakban olvasható:

i **Azonosítás**: szervezeti egyetértés kialakítása a rendszerekre, emberekre, eszközökre, adatokra és képességekre vonatkozó kiberbiztonsági kockázatok kezelésének módjáról.
   - Alkategóriák: eszközkezelés; üzleti környezet; irányítás; kockázatértékelés; és kockázatkezelési stratégia

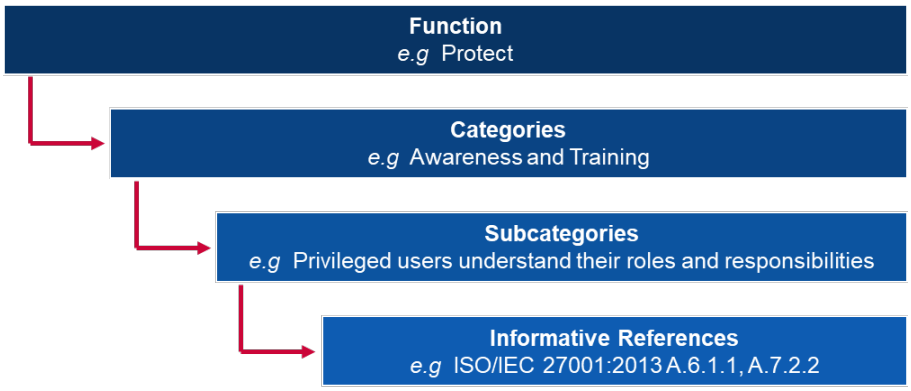
ii **Védelem**: a kritikus szolgáltatások biztosításának garantálására szolgáló megfelelő biztosítékok kidolgozása és megvalósítása.
   - Alkategóriák: személyazonosság-kezelés és hozzáférés-ellenőrzés; tudatosságnövelés és képzés; adatbiztonság; információvédelmi folyamatok és eljárások; fenntartás; és védelmi technológia

iii **Észlelés**: megfelelő tevékenységek kidolgozása és végrehajtása a kiberbiztonsági események előfordulásának azonosítására.
   - Alkategóriák: anomáliák és események; biztonsági folyamatos nyomon követés; és észlelési folyamatok.

iv **Reagálás**: megfelelő tevékenységek kidolgozása és végrehajtása az észlelt kiberbiztonsági eseményekre vonatkozó intézkedések megtételére.
   - Alkategóriák: reagálástervezés; kommunikáció; elemzés; csökkentés; és javítás.

v **Helyreállítás**: megfelelő tevékenységek kidolgozása és végrehajtása rezilienciatervek fenntartására, valamint minden olyan képesség vagy szolgáltatás helyreállítására, amely egy kiberbiztonsági esemény miatt károsodott.
   - Alkategóriák: helyreállítás-tervezés; javítás; és kommunikáció

8. ábra: Példa a Kritikus infrastruktúra kiberbiztonságának javítására szolgáló keretrendszerre



Function e.g Project	**Funkció** pl. projekt
Categories e.g Awarness and Training	**Kategóriák** pl. tudatosságnövelés és képzés

Subcategories e.g Privileged useres understand their roles and responsibilities	**Alkategóriák** pl. a kiváltságos felhasználók tisztában vannak szerepkörükkel és felelősségi körükkel
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Informatív referenciák** pl. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Lépcsők

A Kritikus infrastruktúra kiberbiztonságának javítására szolgáló keretrendszer **4 lépcsőre** támaszkodik, amelyek mindegyike három tengely mentén van meghatározva: kockázatkezelési folyamat, integrált kockázatkezelési program, valamint külső részvétel. A lépcsők nem érettségi szintek, hanem egy keretrendszer, amely biztosítja a szervezetek számára a kiberbiztonsági kockázatról alkotott nézeteik és a kockázat kezelésére szolgáló folyamatok kontextusba helyezését.

- **1. lépcső részlegesen**
  - **Kockázatkezelési folyamat**: a szervezeti kiberbiztonsági kockázatkezelési gyakorlatok nincsenek hivatalos formában rögzítve, a kockázatokat pedig *ad hoc*, néha reaktív módon kezelik;
  - **Integrált kockázatkezelési program**: korlátozott a kiberbiztonsági kockázatok szervezeti szintű ismerete. A szervezet a kiberbiztonsági kockázatkezelést nem rendszeres, eseti alapon hajtja végre, továbbá nem feltétlenül rendelkezik a kiberbiztonsági információk szervezeten belüli megosztását lehetővé tevő folyamatokkal.
  - **Külső részvétel**: a szervezet nem érti a nagyobb ökoszisztémában betöltött szerepét sem függőségei, sem eltartottjai tekintetében. A szervezet általában nincs tisztában az általa nyújtott és használt termékekben és szolgáltatásokban rejlő, számítógépes ellátási láncra vonatkozó kockázatokkal;
- **2. lépcső: Kockázattal kapcsolatos tájékozottság**
  - **Kockázatkezelési folyamat**: a vezetés elfogadott kockázatkezelési gyakorlatokat, de nem biztos, hogy ez az egész szervezetre kiterjedő politika;
  - **Integrált kockázatkezelési program**: szervezeti szinten ismerik a kiberbiztonsági kockázatot, de nincs az egész szervezetre kiterjedő kiberbiztonsági kockázatkezelési megközelítés. Előfordul a szervezeti és külső eszközök kiberbiztonsági kockázatértékelése, de ezt általában nem ismétlik meg, illetve nem történik meg újra;
  - **Külső részvétel**: általában a szervezet megérti a nagyobb ökoszisztémában betöltött szerepét vagy saját függőségei, vagy eltartottjai tekintetében, de nem mindkettőt illetően. Ezenkívül a szervezet tisztában van az általa kínált és használt termékekkel és szolgáltatásokkal kapcsolatos, számítógépes ellátási láncra vonatkozó kockázatokkal, de nem tesz következetes vagy hivatalos lépést az említett kockázatokat illetően.
- **3. lépcső: Megismételhető**
  - **Kockázatkezelési folyamat**: a szervezet kockázatkezelési gyakorlatait hivatalosan elfogadták és politikának nyilvánították. A szervezeti kiberbiztonsági gyakorlatokat rendszeresen aktualizálják a kockázatkezelési folyamatok üzleti/feladatbeli követelmények változásaira való alkalmazása, valamint a változó fenyegetettségi és technológiai helyzet alapján;
  - **Integrált kockázatkezelési program**: rendelkezésre áll egy, az egész szervezetre kiterjedő megközelítés a kiberbiztonsági kockázatok kezelésére. A kockázatokkal kapcsolatos tájékoztatásra épülő politikákat, folyamatokat és eljárásokat meghatározták, rendeltetésszerűen végrehajtották és felülvizsgálták. A vezető tisztviselők biztosítják a kiberbiztonság figyelembevételét a szervezet valamennyi működési területén.
  - **Külső részvétel**: a szervezet megérti a nagyobb ökoszisztémában betöltött szerepét, függőségeit, és ismeri eltartottjait, továbbá hozzájárulhat ahhoz, hogy a közösség szélesebb körben megismerje a kockázatokat. A szervezet tisztában van az általa nyújtott és használt termékekben és szolgáltatásokban rejlő, számítógépes ellátási láncra vonatkozó kockázatokkal;

- **4. lépcső: Alkalmazkodó**
  - **Kockázatkezelési folyamat**: a szervezet a korábbi és aktuális kiberbiztonsági tevékenységek, köztük a levont tanulságok és prediktív mutatók alapján igazít saját kiberbiztonsági gyakorlatain.
  - **Integrált kockázatkezelési program**: rendelkezésre áll egy olyan, az egész szervezetre kiterjedő megközelítés a kiberbiztonsági kockázatok kezelésére, amely a kockázatokkal kapcsolatos tájékoztatásra épülő politikákat, folyamatokat és eljárásokat használ a potenciális kiberbiztonsági események kezelése érdekében; és
  - **Külső részvétel**: a szervezet megérti a nagyobb ökoszisztémában betöltött szerepét, függőségeit, és ismeri eltartottjait, továbbá hozzájárul ahhoz, hogy a közösség szélesebb körben megismerje a kockázatokat.

Értékelési módszer

A Kritikus infrastruktúra kiberbiztonságának javítására szolgáló keretrendszer azért jött létre, hogy a szervezetek önmaguk értékeljék ki a kockázatokat saját kiberbiztonsági megközelítésük és befektetéseik észszerűbbé, hatékonyabbá és értékesebbé tétele érdekében. A befektetések eredményességének megvizsgálásához egy szervezetnek először is világosan értenie kell saját szervezeti célkitűzéseit, a célkitűzések közötti kapcsolatot, valamint a támogató kiberbiztonsági eredményeket. A keretrendszer központi elemének kiberbiztonsági eredményei támogatják a befektetési eredményesség és a kiberbiztonsági tevékenységek önértékelését.

A.4 Katari kiberbiztonsági képességérettségi modell (Q-C2M2)

A Katari kiberbiztonsági képességérettségi modellt (Q-C2M2) a Katari Egyetem College of Law intézménye dolgozta ki 2018-ban. A Q-C2M2 különféle meglévő modelleken alapul, hogy átfogó értékelési módszertant építsen ki Katar kiberbiztonsági keretrendszerének növelésére.

Attribútumok/Dimenziók

A Q-C2M2 elfogadja a Nemzeti Szabványügyi és Technológiai Intézet (NIST) keretrendszerének megközelítését, amely öt alapvető funkciót használt a modell fő tartományaiként. Az öt alapvető funkció alkalmazható a katari környezetben, mivel a funkciók általánosan jelen vannak a kritikus infrastruktúra ágazataiban, ez pedig fontos elem a katari kiberbiztonsági keretrendszerben. A Q-C2M2 **öt tartományra** épül, amelyek mindegyike több altartományra van osztva azért, hogy lefedjék a kiberbiztonsági képességérettség teljes egészét.

Az öt tartomány részletes leírása az alábbiakban olvasható:

i. A **Megértés tartománya** négy altartományra oszlik: kiberirányítás, eszközök, kockázatok és képzés;
ii. A **Biztonság tartományának** altartományaiba az adatbiztonság, a technológiai biztonság, a hozzáférés-ellenőrzési biztonság, a kommunikációs biztonság és a személyi biztonság tartozik.
iii. Az **Expozíció tartományában** a nyomon követés, a biztonsági események kezelése, az észlelés, az elemzés és az expozíció altartományok foglalnak helyet.
iv. A **Reagálás tartományában** olyan altartományok találhatóak, mint a reagálástervezés, csökkentés, valamint reakcióközlés; és
v. A **Fenntartás tartományába** a helyreállítás-tervezés, folytonosságirányítás, javítás és külső függőségek altartományai tartoznak.

Érettségi szintek

A Q-C2M2 **5 érettségi szintet** használ, amelyek az alapvető funkció szintjén mérik az állami szervek vagy nem állami szervezetek képességérettségét. Ezek a szintek az előző szakaszban kifejtett öt tartomány érettségének értékelésére irányulnak.

- **Elindító szakasz**: *ad hoc* kiberbiztonsági gyakorlatokat és folyamatokat alkalmaz egyes tartományokban;

- **Végrehajtó szakasz**: a tartományokban szereplő minden kiberbiztonsági tevékenység végrehajtására irányuló politikákat fogadott el azzal a céllal, hogy a végrehajtási szakasz egy bizonyos időpontban befejeződjön;
- **Fejlesztő szakasz**: a tartományokban szereplő kiberbiztonsági tevékenységek javítását és fejlesztését célzó politikákat és gyakorlatokat valósított meg azzal a céllal, hogy új végrehajtandó tevékenységeket indítványozzon;
- **Alkalmazkodó szakasz**: újból megvizsgálja és felülvizsgálja a kiberbiztonsági tevékenységeket, valamint a korábbi tapasztalatokból és intézkedésekből eredő prediktív mutatók alapján gyakorlatokat fogad el; és
- **Agilis szakasz**: folytatja az alkalmazkodó szakaszt, de nagyobb hangsúlyt fektet a tartományokban szereplő tevékenységek végrehajtásának agilitására és gyorsaságára.

Értékelési módszer

A Q-C2M2 a kutatás korai szakaszában jár és még nem kész a végrehajtásra. Ez egy olyan keretrendszer, amelyet a későbbiekben a katari szervezetek részletes értékelési modelljének kidolgozására használhatnak.

A.5 Kiberbiztonsági érettségi modellre vonatkozó tanúsítás (CMMC)

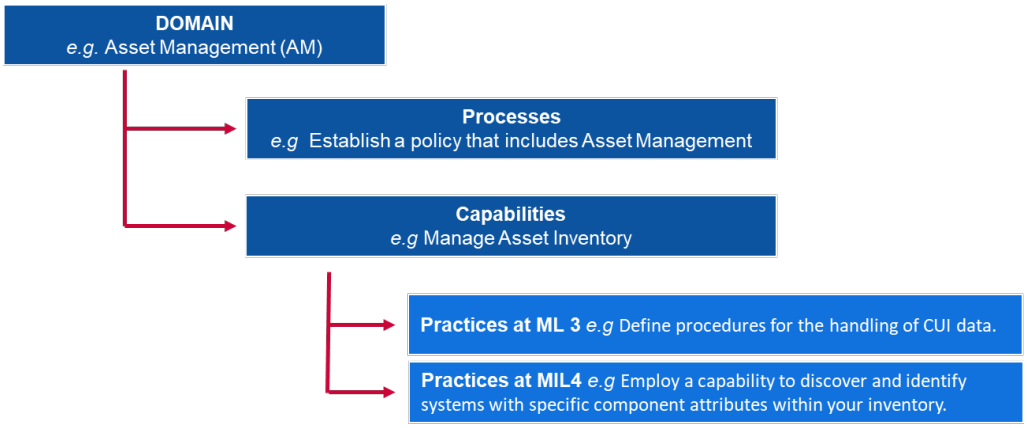
A Kiberbiztonsági érettségi modellre vonatkozó tanúsítást (CMMC) az Amerikai Egyesült Államok Védelmi Minisztériuma (Department of Defense, DoD) dolgozta ki a Carnegie Mellon Egyetemmel és a Johns Hopkins Egyetem Alkalmazott Fizikai Laboratóriumával együttműködve. A DoD fő célkitűzése e modell kidolgozásával az, hogy megóvja az információkat a védelmi iparágtól (DIB). A CMMC-vel érintett információk vagy „szövetségi szerződéses információknak” (Federal Contract Information, FCI) minősülnek, amelyek a kormány által vagy a kormány számára szerződésben biztosított, nem nyilvános közzétételre szánt információkat takarnak, avagy az „ellenőrzött, nem minősített információk” (Controlled Unclassified Information, CUI) kategóriába tartoznak, amelyek törvényeknek, rendeleteknek és az egész kormányra kiterjedő politikáknak megfelelő védelmet vagy közzétételi ellenőrzéseket igénylő információkat jelölnek. A CMMC méri a kiberbiztonsági érettséget és a bevált gyakorlatok mellett egy olyan tanúsítási elemet is biztosít, amely az egyes érettségi szintekhez kapcsolódó gyakorlatok végrehajtásának biztosítására szolgál. A CMMC legújabb verzióját 2020-ban adták ki.

Attribútumok/Dimenziók

A CMMC **tizenhét tartományban** mutatja be a kiberbiztonsági folyamatok és képességek csoportjait. Mindegyik tartomány több **folyamatra** bomlik, amelyek tartományonként hasonlóak; továbbá sok **képességre**, amelyek érettsége öt szinten határozható meg. Ezután a képességek (képesség) az egyes érettségi szintek tekintetében részletes **gyakorlatokra** oszlanak (oszlik).

Az alábbiakban olvasható az említett fogalmak közötti kapcsolat:

9. ábra: CMMC-mutatókra vonatkozó példa



DOMAIN e.g. Asset Management (AM)	**TARTOMÁNY** pl. eszközkezelés (EK)
Processes e.g Establish a policy that includes Asset Management	**Folyamatok** pl. egy, az eszközkezelést magában foglaló politika létrehozása
Capabilities e.g Manage Asset Inventory	**Képességek** pl. eszköznyilvántartás kezelése
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Gyakorlatok a 3. érettségi szinten** pl. CUI adatok kezelési eljárásainak meghatározása
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Gyakorlatok a 4. érettségi szinten** pl. olyan képesség alkalmazása, amely révén feltárhatók és azonosíthatók a nyilvántartásban szereplő konkrét alkotóelem-attribútumokkal rendelkező rendszerek

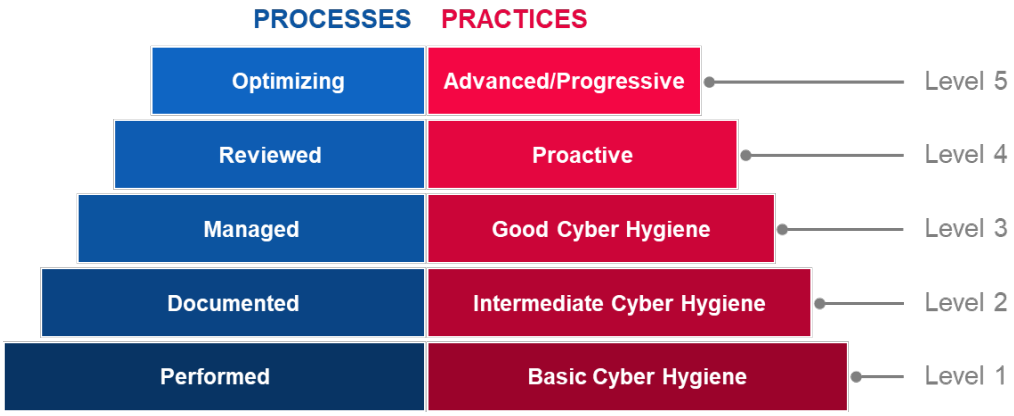
A tizenhét tartomány részletes leírása az alábbiakban olvasható:

i Hozzáférés-ellenőrzés (HE);
ii Eszközkezelés (EK);
iii Ellenőrzés és elszámoltathatóság (EE);
iv Tudatosságnövelés és képzés (TK);
v Konfigurációkezelés (KK);
vi Azonosítás és hitelesítés (AH);
vii Biztonsági eseményekre való reagálás (ER);
viii Fenntartás (FT);
ix Médiavédelem (MV);
x Személyi biztonság (SzB);
xi Fizikai védelem (FV);
xii Helyreállítás (HÁ);
xiii Kockázatkezelés (KK);
xiv Biztonsági értékelés (BÉ);
xv Helyzetismeret (HI);
xvi Rendszer- és kommunikációvédelem (RKV); és
xvii Rendszer- és információintegritás (RII).

Érettségi szintek

A CMMC folyamatok és gyakorlatok alapján meghatározott **5 érettségi szintet** alkalmaz. Ahhoz, hogy a CMMC-ben elérjen egy bizonyos érettségi szintet, a szervezetnek teljesítenie kell az adott szint folyamatainak és gyakorlatának előfeltételeit. Ez magában foglalja az említett szint alatti összes szint előfeltételeinek teljesítését is.

10. ábra: A CMMC érettségi szintjei



PROCESSES	FOLYAMATOK
Optimizing	Optimalizálás
Reviewed	Felülvizsgálva
Managed	Kezelve
Documented	Dokumentálva
Performed	Végrehajtva
PRACTICES	GYAKORLATOK
Advanced/Progressive	Fejlett/Progresszív
Proactive	Proaktív
Good Cyber Hygiene	Jó kiberhigiénia
Intermediate Cyber Hygiene	Közepes kiberhigiénia
Basic Cyber Hygiene	Alapvető kiberhigiénia
Level 5	5. szint
Level 4	4. szint
Level 3	3. szint
Level 2	2. szint
Level 1	1. szint

- **1. szint**
  - **Folyamatok – Végrehajtva**: mivel lehetséges, hogy a szervezet ezeket a gyakorlatokat csak *ad hoc* módon képes végrehajtani, továbbá nem biztos, hogy rendelkezésére áll bármilyen dokumentáció. A folyamatérettséget nem értékelik az 1. szintre vonatkozóan;
  - **Gyakorlatok – Alapvető kiberhigiénia**: az 1. szint az FCI védelmére összpontosít és csak olyan gyakorlatokat tartalmaz, amelyek megfelelnek az alapvető védelmi követelményeknek;
- **2. szint**
  - **Folyamatok – Dokumentálva**: a 2. szint előírja, hogy a szervezeteknek létre kell hozniuk és dokumentálniuk kell a CMMC-vel kapcsolatos erőfeszítéseik végrehajtását irányító gyakorlatokat és politikákat. A gyakorlatok dokumentálása lehetővé teszi az egyének számára, hogy a végrehajtás megismételhető legyen. A szervezetek érett képességeiket úgy dolgozzák ki, hogy dokumentálják, majd a dokumentált adatok szerint gyakorolják őket.
  - **Gyakorlatok – Közepes kiberhigiénia**: a 2. szint szerepe az 1. és 3. szint közötti előrehaladás bemutatása, továbbá a NIST 800-171. számú speciális kiadványában meghatározott biztonsági követelmények egy csoportját, valamint más szabványokból és referenciákból származó gyakorlatokat tartalmaz;

- **3. szint**
  - **Folyamatok – Kezelve**: a 3. szint előírja, hogy a szervezetek hozzanak létre, tartsanak fenn és finanszírozzanak egy, a gyakorlatvégrehajtás tevékenységeinek kezelését bemutató tervet. A tervben szerepelhetnek a feladatokra, célokra, projekttervekre, finanszírozására, szükséges képzésre, valamint az érintett érdekelt felek bevonására vonatkozó információk.
  - **Gyakorlatok – Jó kiberhigiénia**: a 3. szint a CUI védelmére összpontosít, valamint magában foglalja a NIST 800-171. számú speciális kiadványában szereplő valamennyi biztonsági követelményt és a fenyegetések csökkentésére szolgáló, más szabványokban és referenciákban szereplő további gyakorlatokat;
- **4. szint**
  - **Folyamatok – Felülvizsgálva**: a 4. szint előírja, hogy a szervezetek vizsgálják felül és mérjék a gyakorlatok eredményességét. A gyakorlatok eredményességének mérésén kívül a szervezetek ezen a szinten szükség esetén képesek korrekciós intézkedéseket hozni, továbbá rendszeresen tájékoztatni a felső vezetést a helyzetről vagy problémákról.
  - **Gyakorlatok – Proaktív**: a 4. szint a CUI védelmére összpontosít és magában foglalja a fokozott biztonsági követelmények egy csoportját. Ezek a gyakorlatok javítják a szervezet észlelési és reagálási képességeit a változó taktikák, technikák és eljárások kezelése és az azokhoz való alkalmazkodás érdekében;
- **5. szint**
  - **Folyamatok – Optimalizálás**: az 5. szint előírja, hogy a szervezetek az egész szervezetre kiterjedően szabványosítsák és optimalizálják a folyamatvégrehajtást; és
  - **Gyakorlatok – Fejlett/Proaktív**: az 5. szint a CUI védelmére összpontosít. A további gyakorlatok a kiberbiztonsági képességek intenzitását és kifinomultságát növelik.

Értékelési módszer

A CMMC egy viszonylag fiatal modell, amelyet 2020 első negyedévében véglegesítettek. Eddig még egyetlen szervezet sem alkalmazta. Azonban a DoD szerződő felei várhatóan hitelesített harmadik fél vizsgáztatókat kérnek fel az ellenőrzések elvégzésére. A DoD elvárja a szerződő feleitől, hogy a kiberbiztonság előmozdítására és az érzékeny információk védelmére irányuló bevált gyakorlatokat hajtsanak végre.

A.6 Közösségi kiberbiztonsági érettségi modell (CCSMM)

A Közösségi kiberbiztonsági érettségi modellt (CCSMM) a Texasi Egyetem Infrastruktúrabiztosítási és -biztonsági Központja fejlesztette ki. A CCSMM célja, hogy jobban meghatározza azokat a módszereket, amelyek a közösség aktuális kiberbiztonsági felkészültségi helyzetének meghatározására szolgálnak, továbbá hogy olyan ütemtervet biztosítson a közösségek számára, amelyet felkészülési munkájuk során követhetnek. A CCSMM által megcélzott közösségek elsősorban a helyi vagy állami kormányzati szervek. Ezt a modellt 2007-ben dolgozták ki.

Attribútumok/Dimenziók

Az érettségi szinteket **6 fő dimenzió** mentén határozzák meg, amelyek a kiberbiztonság különböző szempontjaival foglalkoznak a közösségeken és szervezeteken belül. Ezek a dimenziók egyértelműen meg vannak határozva mindegyik érettségi szint tekintetében (részletes leírásukat lásd a 31. ábrán: A CCSMM dimenzióinak szintenkénti összefoglalása). A 6 dimenzió nevezetesen:

i Kezelt fenyegetések;
ii Mérőszámok;
iii Információmegosztás;
iv Technológia;
v Képzés; és
vi Teszt.

Érettségi szintek

A CCSMM **5 érettségi szintre** épül az adott szinten kezelt fenyegetések és tevékenységek fő típusai alapján:

- **1. szint: Biztonságtudatosság**
  A tevékenységek fő témája ezen a szinten az egyének és szervezetek fenyegetésekkel, problémákkal, valamint kiberbiztonsági kérdésekkel kapcsolatos ismereteinek növelése;
- **2. szint: Folyamatfejlesztés**
  A kiberbiztonsági kérdések hatékony kezeléséhez szükséges biztonsági folyamatok létrehozásának és javításának segítésére kidolgozott szint;
- **3. szint: Információalapú**
  Arra tervezték, hogy javítsa a közösségen belüli információmegosztási mechanizmusokat, hogy a közösség hatékonyan vethesse össze a látszólag eltérő információkat;
- **4. szint: Taktikai fejlesztés**
  Ennek a szintnek az elemeit arra tervezték, hogy jobb és proaktívabb módszereket dolgozzanak ki a támadások észlelésére és a támadásokra való reagálásra. E szint elérése előtt a legtöbb megelőzési módszernek már érvényben kell lennie;
- **5. szint: Teljes biztonsági operatív képesség**
  Ez a szint azokat az elemeket jelöli, amelyekkel minden szervezetnek rendelkeznie kell ahhoz, hogy magát operatív értelemben teljesen készneknek mondhassa bármelyen kiberfenyegetés kezelésére.

31. ábra: A CCSMM dimenzióinak szintenkénti összefoglalása

	Level 1 Security Aware	**Level 2** Process Development	**Level 3** Information Enabled	**Level 4** Tactics Development	**Level 5** Full Security Operational Capability
Threats Addressed	Unstructured	Unstructured	Structured	Structured	Highly Structured
Metrics	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens
Information Sharing	Information Sharing Committee	Community Security Web Site	Information Correlation Center	State/Fed Correlation	Complete Info Vision
Technology	Rosters, GETS, Access Controls, Encryption	Secure Web Site Firewalls, Backups	Event Correlation SW IDS/IPS	24/7 manned operations	Automated Operations
Training	1-day Community Seminar	Conducting a CCSE	Vulnerability Assessments	Operational Security	Multi-Discipline Red Teaming
Test	Dark Screen - EOC	Community Dark Screen	Operational Dark Screen	Limited Black Demon	Black Demon

Level 1 Security Aware	1. szint Biztonságtudatosság
Level 2 Process Development	2. szint Folyamatfejlesztés

Level 3 Information Enabled	3. szint Információalapú
Level 4 Tactics Development	4. szint Taktikai fejlesztés
Level 5 Full Security Operational Capability	5. szint Teljes biztonsági operatív képesség
Threats Addressed	Kezelt fenyegetések
Metrics	Mérőszámok
Information sharing	Információmegosztás
Technology	Technológia
Training	Képzés
Test	Teszt
Unstructured	Strukturálatlan
Governement Industry Citizens	Kormány Ipar Polgárok
Information Sharing Committee	Információmegosztó bizottság
Rosters, GETS, Assess Controls, Encryption	Adatbázisok, GETS, hozzáférés-ellenőrzések, titkosítás
1-dat Community Seminar	Egynapos közösségi szeminárium
Dark Screen – EOC	Dark Screen gyakorlat – EOC
Unstructured	Strukturálatlan
Governement Industry Citizens	Kormány Ipar Polgárok
Community Security Web site	Közösségi biztonsági weboldal
Secure Web Site Firewalls, Backups	Biztonságos weboldali tűzfalak, biztonsági mentések
Conudcting a CCSE	Közösségi kiberbiztonsági gyakorlat elvégzése
Community Dark Screen	Közösségi Dark Screen gyakorlat
Structured	Strukturált
Governement Industry Citizens	Kormány Ipar Polgárok
Information Correlation Center	Információkorrelációs központ
Event Correlation SW IDS/IPS	Eseménykorrelációs IDS/IPS szoftver
Vulnerability Assessment	Sebezhetőségi értékelés
Operational Dark Screen	Operatív Dark Screen gyakorlat
Structured	Strukturált
Governement Industry Citizens	Kormány Ipar Polgárok
State/Fed Correlation	Állami/Szövetségi korreláció
24/7 manned operations	Ember irányította állandó, 24 órás műveletek
Operational Security	Üzembiztonság
Limited Black Demon	Korlátolt Black Demon gyakorlat
Highly Structured	Nagymértékben strukturált
Governement Industry Citizens	Kormány Ipar Polgárok
Complete Info Vision	Teljes adatlátás
Automated Operations	Automatizált műveletek
Multi-Discipline Red Teaming	Multidiszciplináris read teaming
Black Demon	Black Demon

Értékelési módszer

A közösségek a CCSMM-et értékelési módszertanként az állami és szövetségi bűnüldöző ügynökségek közreműködésével alkalmazhatják. Célja, hogy segítse a közösségeket annak meghatározásában, hogy mi a legfontosabb, melyek a legvalószínűbb célpontok, valamint mit kell megvédeni (és milyen mértékben). Ezeket a célkitűzéseket szem előtt tartva olyan terveket lehet kidolgozni, amelyek révén a közösség valamennyi aspektusát a szükséges kiberbiztonsági

érettségi szintre hozhatják. A CCSMM által megalkotott speciális információgyűjtés segít meghatározni a különféle tesztek és gyakorlatok céljait, amelyeket a létrehozott programok hatékonyságának mérésére használhatnak.

A.7 Információbiztonsági érettségi modell a NIST kiberbiztonsági keretrendszer tekintetében (ISMM)

Az Információbiztonsági érettségi modellt (ISMM) a szaúdi-arábiai King Fahd Kőolaj- és Ásványianyag-tudományi Egyetem Számítástechnikai és Mérnöki Intézményében dolgozták ki. Új képességérettségi modellt vet fel a kiberbiztonsági intézkedések végrehajtásának mérésére. Az ISMM célja, hogy lehetővé tegye a szervezetek számára végrehajtási folyamatuk fokozatos előrehaladásának mérését ugyanazon mérőeszköz rendszeres használatával, így biztosítva, hogy a kívánt kockázati helyzet fennmaradjon. Ezt a modellt 2017-ben dolgozták ki.

Attribútumok/Dimenziók

Az ISMM a NIST keretrendszer meglévő értékelt területeire épít, és hozzáad egy, a megfelelés értékelésére vonatkozó dimenziót. Így a modell **23 értékelt területet** foglal magában egy szervezet kockázati helyzete tekintetében. A 23 értékelt terület a következő:

i Eszközkezelés;
ii Üzleti környezet;
iii Irányítás;
iv Kockázatértékelés;
v Kockázatkezelési stratégia;
vi Megfelelésértékelés;
vii Hozzáférés-ellenőrzés;
viii Tudatosságnövelés és képzés;
ix Adatbiztonság;
x Információvédelmi folyamatok és eljárások;
xi Fenntartás;
xii Védelmi technológia;
xiii Anomáliák és események;
xiv Biztonsági folyamatos nyomon követés;
xv Észlelési folyamatok;
xvi Reagálástervezés;
xvii Reagálásra vonatkozó kommunikáció;
xviii Reagáláselemzés;
xix Reagálással kapcsolatos enyhítés;
xx Reagálással kapcsolatos javítások;
xxi Helyreállítástervezés;
xxii Helyreállítással kapcsolatos javítások; és
xxiii Helyreállításra vonatkozó kommunikáció.

Érettségi szintek

Az ISMM **5 érettségi szintre** hivatkozik, amelyeket sajnos nem részleteznek a rendelkezésre álló dokumentumok.

- **1. szint:** Elvégzett folyamat;
- **2. szint:** Kezelt folyamat;
- **3. szint:** Létrehozott folyamat;
- **4. szint:** Előrelátható folyamat; és
- **5. szint:** Optimalizáló folyamat.

Értékelési módszer

Az ISMM nem nevez meg konkrét módszertant arra vonatkozóan, hogy a szervezetek hogyan végezzék el az értékelést.

A.8 A belső ellenőrzési képesség modellje (IA-CM) a közszféra számára

A belső ellenőrzési képesség modelljét (IA-CM) a Belső Ellenőrök Intézete Kutatási Alapítvány dolgozta ki azzal a szándékkal, hogy a közszférában önértékelés útján építsen ki kapacitást és érdekérvényesítést. Az IA-CM célközönsége az ellenőrzési folyamatokban részt vevő szakemberek, és a modell áttekintésén kívül egy Alkalmazási útmutatót is biztosít, hogy segítse a modell önértékelési eszközként történő használatát.

Annak ellenére, hogy az IA-CM középpontjában a belső ellenőrzési képesség áll a kiberbiztonsági kapacitásépítés helyett, a modell egy érettségi önértékelési eszköz a közszférabeli szervezetek számára, amelyet globális szinten alkalmazhatnak a folyamatok és hatékonyság javítására. Mivel az alkalmazási kör nem a kiberbiztonságra összpontosít, nem történik meg az attribútumok elemzése. Az IA-CM modellt 2009-ben véglegesítették.

Érettségi szintek

A belső ellenőrzési képesség modellje (IA-CM) **5 érettségi szintet** foglal magában, amelyek mindegyike egy belső ellenőrzési tevékenység jellemvonásait és képességeit írja le az adott szinten. A modellben található képességi szintek folyamatos javításra vonatkozó ütemtervet biztosítanak.

- **1. szint: Kezdeti**
  Nincsenek fenntartható, megismételhető képességek – az egyéni erőfeszítések függvénye
  - *ad hoc* vagy strukturálatlan;
  - a dokumentumok és tranzakciók elkülönített egyszeri ellenőrzése vagy felülvizsgálata a pontosság és a megfelelés érdekében;
  - az eredmények a pozíciót betöltő konkrét személy szakértelmétől függnek;
  - a szakmai egyesületek által biztosítottakon túl nincsenek kialakított szakmai gyakorlatok;
  - a finanszírozást szükség szerint a vezetés hagyja jóvá;
  - infrastruktúra hiánya;
  - az ellenőrök valószínűleg egy nagyobb szervezeti egységbe tartoznak;
  - nincs kifejlődve az intézményi képesség.
- **2. szint: Infrastruktúra**
  Fenntartható és megismételhető gyakorlatok és eljárások
  - a 2. szint legfontosabb kérdése vagy kihívása, hogy hogyan alapozható meg és tartható fenn a folyamatok megismételhetősége, tehát egy megismételhető képesség;
  - a belső ellenőrzési jelentési kapcsolatok, a kezelési és adminisztratív infrastruktúra, valamint a szakmai gyakorlatok és folyamatok kialakítása folyamatban van (belső ellenőrzési iránymutatás, folyamatok és eljárások);
  - az ellenőrzés tervezése elsősorban a vezetői prioritásokon alapul;
  - folyamatos támaszkodás alapvetően konkrét személyek szakértelmére és kompetenciáira;
  - a szabványoknak való részleges megfelelés.
- **3. szint: Integrált**
  A vezetői és szakmai gyakorlatokat egységesen alkalmazzák
  - a belső ellenőrzési politikákat, folyamatokat és eljárásokat meghatározták, valamint integrálták egymásba és a szervezet infrastruktúrájába;
  - a belső ellenőrzésre vonatkozó vezetői és szakmai gyakorlatok jól megalapozottak és egységesen alkalmazzák őket valamennyi belső ellenőrzési tevékenység során;
  - a belső ellenőrzés kezd igazodni a szervezet üzleti tevékenységéhez és azokhoz a kockázatokhoz, amelyekkel a szervezet szembesül;
  - a belső ellenőrzés a csak hagyományos belső ellenőrzésből fejlődik a csapatjátékosként történő integrálásig, valamint a teljesítménnyel és kockázatkezeléssel kapcsolatos tanácsadásig;
  - a hangsúly a csapatépítésen és a belső ellenőrzési tevékenység képességén, valamint annak függetlenségén és objektivitásán van;

- a szabványoknak általában megfelel.

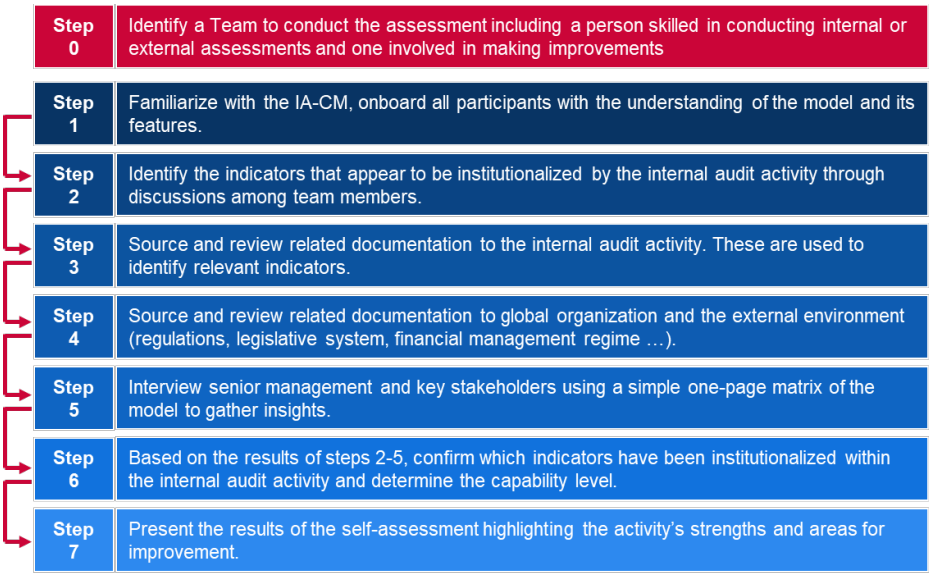
- **4. szint: Kezelt**
  Az irányítás és kockázatkezelés javítása érdekében integrálja az információkat a szervezet egészéből
  - a belső ellenőrzés és a kulcsfontosságú érdekelt felek elvárásai összhangban vannak;
  - teljesítményi mérőszámok vannak meghatározva a belső ellenőrzési folyamatok és eredmények mérésére és nyomon követésére;
  - elismerik, hogy a belső ellenőrzés jelentős mértékben hozzájárul a szervezet működéséhez;
  - a belső ellenőrzés a szervezet irányításának és kockázatkezelésének szerves részeként működik;
  - a belső ellenőrzés egy jól működtetett üzleti egység;
  - a kockázatok mérése és kezelése mennyiségi alapon történik;
  - olyan kötelező készségek és kompetenciák vannak meghatározva, amelyek megújulási és tudásmegosztási képességgel rendelkeznek (mind a belső ellenőrzésben, mind a szervezet egészében).

- **5. szint: Optimalizálás**
  Tanulás a szervezeten belül és kívül a folyamatos fejlődés érdekében
  - a belső ellenőrzés egy tanuló szervezet, folyamatos folyamatfejlesztéssel és innovációval;
  - a belső ellenőrzés a szervezetből és a szervezeten kívülről származó információkat is felhasznál a stratégiai célkitűzések elérésében való közreműködés érdekében;
  - világszínvonalú/ajánlott/bevált gyakorlatok végrehajtása;
  - a belső ellenőrzés a szervezet irányítási struktúrájának szerves részét képezi;
  - felső szintű szakmai és speciális készségek;
  - az egyéni, egységi és szervezeti teljesítményre vonatkozó mérések teljes mértékben integráltak
  - a teljesítmény javulásának elősegítése érdekében.

Értékelési módszer

A belső ellenőrzési képesség modelljét egyértelműen önértékelési célra dolgozták ki. Részletesen ismerteti azokat a lépéseket, amelyeket az IA-CM használatához követni kell, valamint biztosít egy prezentációs diasorozat-mintát, amely testreszabható. Az önértékelés elkezdése előtt meg kell határozni egy konkrét csapatot, amelybe fel kell venni legalább egy olyan személyt, aki jártas a belső ellenőrzések belső vagy külső értékelésének elvégzésében, továbbá egy olyan személyt, aki részt vesz az említett területen végzett fejlesztésekben.

12. ábra: Az IA-CM önértékelés lépései



Step 0	0. lépés
Step 1	1. lépés
Step 2	2. lépés
Step 3	3. lépés
Step 4	4. lépés
Step 5	5. lépés
Step 6	6. lépés
Step 7	7. lépés
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Határozzák meg az értékelést elvégző csapatot, amelybe fel kell venni legalább egy olyan személyt, aki jártas a belső vagy külső értékelések elvégzésében, továbbá egy olyan személyt, aki részt vesz a fejlesztésekben.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Ismerjék meg az IA-CM-et, valamint ismertessék meg a modellt és tulajdonságait valamennyi résztvevővel.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	A csapattagok közötti eszmecserék útján azonosítsák azokat a mutatókat, amelyeket a belső ellenőrzési tevékenység intézményesíteni látszik.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Szerezzék be a kapcsolódó dokumentumot és vizsgálják meg őket a belső ellenőrzési tevékenységgel összevetve. Ezeket a releváns mutatók azonosítására használják.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Szerezzék be a kapcsolódó dokumentumokat és vizsgálják meg őket a globális szervezeti és a külső környezethez viszonyítva (rendeletek, jogalkotási rendszer, pénzgazdálkodási rendszer stb.).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	A modell egyszerű, egyoldalas mátrixát felhasználva beszélgessenek el a felső vezetőkkel és a kulcsfontosságú érdekelt felekkel ismeretszerzés céljából.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	A 2–5. lépések eredményei alapján igazolják, hogy milyen mutatókat intézményesítettek a belső ellenőrzési tevékenység során, továbbá határozzák meg a kapacitási szintet.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Mutassák be az önértékelés eredményeit, kiemelve a tevékenység erősségeit és a fejlesztendő területeket.

A.9 Globális kiberbiztonsági index (GCI)

A Globális kiberbiztonsági index (GCI) a Nemzetközi Távközlési Egyesület (ITU) kezdeményezése, amelynek az a célja, hogy megvizsgálja a kiberbiztonsági elkötelezettséget és helyzetet valamennyi ITU-régióban, azaz Afrikában, Amerikában, az arab államokban, az ázsiai és csendes-óceáni térségben, a Független Államok Közösségében és Európában, illetve hogy a figyelem középpontjába helyezze az erősen elkötelezett és ajánlatos gyakorlatokkal rendelkező országokat. A GCI célja, hogy segítse az országokat a kiberbiztonság terén fejlesztendő területek azonosításában, valamint arra ösztönözze őket, hogy tegyenek lépéseket a rangsorban betöltött helyük javítására, így előmozdítva a teljes kiberbiztonsági szint emelkedését az egész világon.

Mivel a GCI egy mutató, nem pedig érettségi modell, nem érettségi szinteket alkalmaz, hanem pontozást, amellyel rangsorolja és összehasonlítja a nemzetek és régiók globális kiberbiztonsági elkötelezettségét.

Attribútumok/Dimenziók

A Globális kiberbiztonsági index (GCI) a globális kiberbiztonsági menetrend (Global Cybersecurity Agenda, GCA) 5 pillérén alapul. Ezek a pillérek alkotják a GCI öt részindexét, és mindegyik tartalmaz egy sor mutatót. Az öt pillér és mutató a következő:

i **Jogi**: a kiberbiztonsággal és kiberbűnözéssel foglalkozó jogi intézmények és keretrendszerek meglétén alapuló intézkedések.
- kiberbűnözéssel kapcsolatos jogszabályok;
- kiberbiztonsági rendelet; és
- kéretlen üzenetek megfékezésére/visszaszorítására vonatkozó jogszabályok.

ii **Műszaki**: a kiberbiztonsággal foglalkozó műszaki oktatási intézmények és keretrendszerek meglétén alapuló intézkedések.
- CSIRT/CIRT/CSRIT;
- szabványvégrehajtási keretrendszer;
- szabványügyi testület;
- a kéretlen üzenetek kezelésére alkalmazott műszaki mechanizmusok és képességek;
- számítási felhő kiberbiztonsági célú használata; és
- gyermekek online védelmére vonatkozó mechanizmusok.

iii **Szervezeti**: kiberbiztonsági fejlesztésre szolgáló nemzeti szintű szakpolitikai koordinációs intézmények és stratégiák meglétén alapuló intézkedések.
- nemzeti kiberbiztonsági stratégia;
- felelős ügynökség; és
- kiberbiztonság.

iv **Kapacitásépítési**: kapacitásépítést elősegítő kutatás-fejlesztési, oktatási és képzési programok, minősített szakemberek és magánszektorbeli ügynökségek meglétén alapuló intézkedések.
- nyilvánosságnak szóló tudatosságnövelő kampányok;
- a kiberbiztonsági szakemberek tanúsítására és akkreditálására szolgáló keretrendszer;
- kiberbiztonsági szakmai tanfolyamok;
- oktatási programok vagy egyetemi tantervek a kiberbiztonság területén;
- kiberbiztonsági K+F programok; és
- ösztönző mechanizmusok.

v **Együttműködési**: partnerségek, együttműködési keretrendszerek, valamint információmegosztó hálózatok meglétén alapuló intézkedések.
- kétoldalú megállapodások;
- többoldalú megállapodások;
- nemzetközi fórumokon/szövetségekben való részvétel;
- köz- és magánszféra közötti partnerségek;
- ügynökségek közötti / ügynökségeken belüli partnerségek; és
- bevált gyakorlatok.

Értékelési módszer

A GCI egy olyan önértékelési eszköz, amely egy bináris, előre kódolt és nyitott kérdésű felmérés[30] alapján épül fel. A bináris válaszok kiküszöbölik a véleményalapú értékelést és az esetleges elfogultságot bizonyos típusú válaszok irányában. Az előre kódolt válaszok időt takarítanak meg és pontosabb adatelemzést tesznek lehetővé. Továbbá egy egyszerű kétkimenetű skála gyorsabb és összetettebb értékelést tesz lehetővé, mivel nem igényel hosszú válaszokat, amely felgyorsítja és leegyszerűsíti a válaszadás és további értékelés folyamatát. A válaszadónak csak bizonyos előre meghatározott kiberbiztonsági megoldások meglétét vagy hiányát kell megerősítenie. A válaszok összegyűjtésére és a releváns anyagok feltöltésére

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf

használt online felmérési mechanizmus lehetővé teszi a bevált gyakorlatok kimásolását és a szakrétői testületek által végzett tematikus minőségi értékeléseket.

A teljes GCI-folyamatot az alábbiak szerint hajtják végre:

- Minden résztvevőnek meghívólevelet küldenek, amelyben tájékoztatják őket a kezdeményezésről, és elkérik annak a kapcsolattartó pontnak az adatait, amely a releváns adatok összegyűjtéséért, valamint az online GCI-kérdőív kitöltéséért felel. Az online felmérés során a jóváhagyott kapcsolattartó pontot az ITU hivatalosan felkéri a kérdőív kitöltésére;
- Elsődleges adatgyűjtés (a kérdőívre nem válaszoló országok számára):
  - az ITU a nyilvánosan elérhető adatokat és online kutatást felhasználva kidolgoz egy kezdeti választervezetet a kérdőívhez;
  - a kérdőívtervezetet áttekintésre elküldik a kapcsolattartó pontoknak;
  - a kapcsolattartó pontok javítják a pontosságot, majd visszaküldik a kérdőívtervezetet;
  - a kijavított kérdőívtervezetet végső jóváhagyásra elküldik minden kapcsolattartó pontnak; és
  - az érvényesített kérdőívet használják fel az elemzéshez, pontozáshoz és rangsoroláshoz.
- Másodlagos adatgyűjtés (a kérdőívre válaszoló országok számára):
  - az ITU azonosít minden hiányzó választ, alátámasztó dokumentumot, linket stb.;
  - a kapcsolattartó pont javítja a válaszok pontosságát, amennyiben szükséges;
  - a kijavított kérdőívtervezetet végső jóváhagyásra elküldik minden kapcsolattartó pontnak; és
  - az érvényesített kérdőívet használják fel az elemzéshez, pontozáshoz és rangsoroláshoz.

A.10 Kibererőindex (CPI)

A Kibererőindexet (CPI) a Gazdasági Hírszerző Egység kutatási program hozta létre 2001-ben, amelyet a Booz Allen Hamilton vállalat szponzorált. A CPI „egy dinamikus mennyiségi és minőségi modell, […] amely a kiberkörnyezet sajátos attribútumait méri a kibererő négy mozgatórugója mentén: a jogi és szabályozási keretben, a gazdasági és társadalmi környezetben, a technológiai infrastruktúrában, valamint az ipari alkalmazásban, amely a digitális előrehaladást vizsgálja a kulcsfontosságú iparágak között”[31]. A CPI célkitűzése, hogy összehasonlítva értékelje a G20-csoport országainak kibertámadásokkal szembeni ellenálló képességét, továbbá hogy bevezesse a virágzó és biztonságos gazdasághoz szükséges digitális infrastruktúrát. A CPI által biztosított összehasonlító értékelés a G20 19 országára összpontosít (az Európai Unió kivételével). Ezután az index minden mutatóra vonatkozóan rangsorolja az országokat.

Attribútumok/Dimenziók

A Kibererőindex (CPI) a kibererő négy mozgatórugóján alapul. Ezután az egyes kategóriákat több mutató segítségével megmérik, hogy az egyes országok konkrét pontszámot kapjanak. A kategóriák és pillérek a következők:

i **Jogi és szabályozási keret**
- a kormány kiberbiztonsági fejlesztés iránti elkötelezettsége
- kibervédelmi szakpolitikák
- kibercenzúra (vagy annak hiánya)
- politikai hatékonyság
- szellemi tulajdon védelme

[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

ii **Gazdasági és társadalmi környezet**
- oktatási szintek
- műszaki készségek
- kereskedelem nyitottsága
- innováció szintje az üzleti környezetben

iii **Technológiai infrastruktúra**
- az információs és kommunikációs technológiához való hozzáférés
- az információs és kommunikációs technológia minősége
- az információs és kommunikációs technológia megfizethetősége
- információtechnológiai kiadások
- biztonságos szerverek száma

iv **Ipari alkalmazás**
- intelligens energiahálózatok
- e-egészségügy
- e-kereskedelem
- intelligens közlekedés
- e-kormányzat

Értékelési módszer

A CPI egy mennyiségi és minőségi pontozási modell. Az értékelést a Gazdasági Hírszerző Egység végezte a rendelkezésre álló statisztikai forrásokból származó kvantitatív mutatók felhasználásával, valamint becslések készítésével, ha az adatok hiányosak voltak. A felhasznált fő források a következők: a Gazdasági Hírszerző Egység, az ENSZ Nevelésügyi, Tudományos és Kulturális Szervezete (UNESCO), a Nemzetközi Távközlési Egyesület (ITU), valamint a Világbank.

A.11 Kibererőindex (CPI)

Ez a szakasz a meglévő érettségi modellek elemzésének legfőbb megállapításait foglalja össze. Az 5. táblázat – Elemzett érettségi modellek helyzetképe az egyes modellek fő jellemvonásairól ad áttekintést a módosított Becker modell szerint. A 6. táblázat – Érettségi szintek összehasonlítása az elemzett modellek érettségi szintjeinek magas szintű meghatározását tartalmazza. A 7. táblázat áttekintést nyújt az egyes modellekben használt dimenziókról vagy attribútumokról.

5. táblázat: Elemzett érettségi modellek helyzetképe

Modell neve	Intézményi forrás:	Cél	Célcsoport	Szintek száma	Attribútumok száma	Értékelési módszer	Eredmények ábrázolása
Kiberbiztonsági kapacitás érettségi modellje a nemzetek számára (CMM)	Globális Kiberbiztonsági Kapacitásépítési Központ Oxfordi Egyetem	A kiberbiztonsági kapacitásépítés mértékének és hatékonyságának növelése nemzetközi szinten	Ország	5	5 fő dimenzió	Együttműködés egy helyi szervezettel a modell nemzeti összefüggésben történő alkalmazás előtti finomhangolása érdekében	Ötrészes radar
Kiberbiztonsági képességérettségi modell (C2M2)	Az Amerikai Egyesült Államok Energiaügyi Minisztériuma (DOE)	A szervezetek segítése kiberbiztonsági programjaik értékelése és javítása, valamint működési rezilienciájuk megerősítése terén	Bármely ágazatban működő, bármilyen típusú és méretű szervezet	4	10 fő tartomány	Önértékelési módszertan és eszköztár	Eredménytábla kördiagramokkal
Kritikus infrastruktúra kiberbiztonságának javítására szolgáló keretrendszer	Nemzeti Szabványügyi és Technológiai Intézet (NIST)	A szervezeteken belüli kiberbiztonsági tevékenységek irányítására és kockázatkezelésre irányuló keretrendszer	Szervezetek	N.a. (4 lépcső)	5 alapvető funkció	Önértékelés	-
Katari kiberbiztonsági képességérettségi modell (Q-C2M2)	Katari Egyetem College of Law intézménye	Egy olyan működőképes modell biztosítása, amelyet Katar kiberbiztonsági keretrendszerének teljesítménymérésére, mérésére és fejlesztésére lehet használni	Katari szervezetek	5	5 fő tartomány	-	-
Kiberbiztonsági érettségi modellre vonatkozó tanúsítás (CMMC)	Az Amerikai Egyesült Államok Védelmi Minisztériuma (DOD)	Bevált kiberbiztonsági gyakorlatok elősegítése az információk védelmének biztosítására	Védelmi iparág (DIB) szervezetei	5	17 fő tartomány	Harmadik fél ellenőr által végzett értékelés	-
Közösségi kiberbiztonsági érettségi modell (CCSMM)	Texasi Egyetem Infrastruktúrabiztosítási és -biztonsági Központja	A közösség aktuális kiberbiztonsági felkészültségi helyzetének meghatározása, továbbá olyan ütemterv biztosítása a közösségek számára, amelyet felkészülési erőfeszítéseik során követhetnek	Közösségek (helyi vagy állami kormányzati szervek)	5	6 fő dimenzió	Közösségeken belül végzett értékelés állami és szövetségi bűnüldöző hatóságok hozzájárulásával	-
Információbiztonsági érettségi modell a NIST kiberbiztonsági keretrendszer tekintetében (ISMM)	Számítástechnikai és Mérnöki Intézmény King Fahd Kőolaj- és Ásványianyag-tudományi Egyetem, Dhahran, Szaúd-Arábia	A szervezetek fokozatos végrehajtási előrehaladása mérésének lehetővé tétele azért, hogy biztosítani tudják a kívánt kockázati helyzet fennmaradását	Szervezetek	5	23 értékelt terület	-	-
A belső ellenőrzési képesség modellje (IA-CM) a közszféra számára	Belső Ellenőrök Intézete Kutatási Alapítvány	Belső ellenőrzési képesség és érdekérvényesítés kiépítése a közszférában végzett önértékelés útján	Közszférába tartozó szervezetek	5	6 elem	Önértékelés	-

Globális kiberbiztonsági index (GCI)	Nemzetközi Távközlési Egyesület (ITU)	A kiberbiztonsági elkötelezettség és helyzet vizsgálata, valamint az országok támogatása abban, hogy azonosítani tudják a kiberbiztonság terén fejlesztendő területeket	Ország	N.a.	5 pillér	Önértékelés	Rangsortáblázat
Kibererőindex (CPI)	A Gazdasági Hírszerző Egység és a Booz Allen Hamilton	A G20-csoport országai kibertámadásokkal szembeni ellenálló képességének összehasonlító értékelése, továbbá a virágzó és biztonságos gazdasághoz szükséges digitális infrastruktúra bevezetése	A G20-csoport országai	N.a.	4 kategória	A Gazdasági Hírszerző Egység által végzett teljesítménymérés	Rangsortáblázat

6. táblázat Érettségi szintek összehasonlítása

Modell	1. szint	2. szint	3. szint	4. szint	5. szint
Kiberbiztonsági kapacitás érettségi modellje a nemzetek számára (CMM)	**Kezdeti** Vagy még egyáltalán nem beszélhetünk kiberbiztonsági érettségről, vagy még nagyon kezdetleges. Lehetnek a kiberbiztonsági kapacitásépítéssel kapcsolatos kezdeti eszmecserék, de még nem történtek konkrét intézkedések. Ebben a szakaszban nincs megfigyelhető bizonyíték.	**Alakító** Megfigyelhető a szempontok egyes jellemvonásainak növekedése és kialakulása, de ez történhet *ad hoc* alapon, szervezetlen, rosszul meghatározott lehet, vagy egyszerűen csak „új”. Ennek a tevékenységnek a bizonyítéka azonban egyértelműen kimutatható.	**Megalapozott** A szempont elemei már meghatározottak és működnek. Ugyanakkor még nincs jól átgondolt stratégia a kapcsolódó erőforrások elosztására. Kevés kompromisszumos döntés született a szempont különböző elemeibe történő „relatív” befektetést illetően. A szempont azonban funkcionál és meg van határozva.	**Stratégiai** Döntés született arról, hogy a szempont mely részei fontosak, és melyek kevésbé fontosak az adott szervezet vagy nemzet számára. A stratégiai szakasz tükrözi azt a tényt, hogy ezeket a döntéseket a nemzet vagy szervezet körülményeitől függően meghozták.	**Dinamikus** Világos mechanizmusok vannak érvényben a stratégia az alapján történő megváltoztatására, hogy milyenek a fennálló körülmények, mint például a fenyegetettségi környezet, a globális konfliktus technológiája, illetve egy érintett terület (pl. kiberbűnözés vagy adatvédelem) jelentős változása. A dinamikus szervezetek módszereket fejlesztettek ki a stratégiák lépésről lépésre történő megváltoztatására. E szakasz jellemvonásai a gyors döntéshozatal, az erőforrások újraelosztása és állandó figyelem a változó környezetre.
Kiberbiztonsági képességérettségi modell (C2M2)	**MIL0** Nem végeznek gyakorlatokat.	**MIL1** Kezdeti gyakorlatokat végeznek, de ez történhet *ad hoc* módon.	**MIL2** Kezelési jellemzők: a gyakorlatokat dokumentálják; a folyamat támogatására megfelelő erőforrásokat biztosítanak; a gyakorlatokat elvégző személyzet megfelelő szakértelemmel és ismeretekkel rendelkezik; és ki vannak jelölve a gyakorlatok elvégzésére vonatkozó felelősségi és hatáskörök.	**MIL3** Kezelési jellemzők: a tevékenységek irányítása politikák (vagy egyéb szervezeti irányelvek) alapján történik; a tartomány tevékenységeire vonatkozó teljesítési célkitűzéseket dolgoztak ki és monitoroznak a teljesítmény nyomon követése érdekében; a tartomány tevékenységeire vonatkozó dokumentált	-

			Megközelítési jellemző: a gyakorlatok teljesebbek vagy fejlettebbek, mint a MIL1 szinten.	gyakorlatokat szabványosítják és javítják a vállalat egészében. Megközelítési jellemző: a gyakorlatok teljesebbek vagy fejlettebbek, mint a MIL1 szinten.	
Információbiztonsági érettségi modell a NIST kiberbiztonsági keretrendszer tekintetében (ISMM)	**Elvégzett folyamat**	**Kezelt folyamat**	**Létrehozott folyamat**	**Előrelátható folyamat**	**Optimalizáló folyamat**
Katari kiberbiztonsági képességérettségi modell (Q-C2M2)	**Elindító** *Ad hoc* kiberbiztonsági gyakorlatokat és folyamatokat alkalmaz egyes tartományokban.	**Fejlesztő** A tartományokban szereplő kiberbiztonsági tevékenységek javítását és fejlesztését célzó politikákat és gyakorlatokat valósított meg azzal a céllal, hogy új végrehajtandó tevékenységeket indítványozzon.	**Végrehajtó** A tartományokban szereplő minden kiberbiztonsági tevékenység végrehajtására irányuló politikákat fogadott el azzal a céllal, hogy a végrehajtási szakasz egy bizonyos időpontban befejeződjön.	**Alkalmazkodó** Újból megvizsgálja és felülvizsgálja a kiberbiztonsági tevékenységeket, valamint a korábbi tapasztalatokból és intézkedésekből eredő prediktív mutatók alapján gyakorlatokat fogad el.	**Agilis** Folytatja az alkalmazkodó szakaszt, de nagyobb hangsúlyt fektet a tartományokban szereplő tevékenységek végrehajtásának agilitására és gyorsaságára.
Kiberbiztonsági érettségi modellre vonatkozó tanúsítás (CMMC)	**Folyamatok Végrehajtva** Mivel lehetséges, hogy a szervezet ezeket a gyakorlatokat csak *ad hoc* módon képes végrehajtani, továbbá nem biztos, hogy rendelkezésére áll bármilyen dokumentáció, a folyamatérettséget nem értékelik az 1. szintre vonatkozóan. **Gyakorlatok: Alapvető kiberhigiénia** Az 1. szint az FCI (szövetségi szerződéses információk) védelmére összpontosít és csak olyan gyakorlatokat tartalmaz, amelyek megfelelnek az alapvető védelmi követelményeknek.	**Folyamatok: Dokumentálva** A 2. szint előírja, hogy a szervezeteknek létre kell hozniuk és dokumentálniuk kell a CMMC-vel kapcsolatos erőfeszítéseik végrehajtását irányító gyakorlatokat és politikákat. A gyakorlatok dokumentálása lehetővé teszi az egyének számára, hogy a végrehajtás megismételhető legyen. A szervezetek érett képességeiket úgy dolgozzák ki, hogy dokumentálják, majd a dokumentált adatok szerint gyakorolják őket. **Gyakorlatok: Közepes kiberhigiénia** A 2. szint szerepe az 1. és 3. szint közötti előrehaladás bemutatása, továbbá a NIST 800-171. számú speciális kiadványában meghatározott biztonsági követelmények egy csoportját, valamint más szabványokból és referenciákból származó gyakorlatokat tartalmaz.	**Folyamatok: Kezelve** A 3. szint előírja, hogy a szervezetek hozzanak létre, tartsanak fenn és finanszírozzanak egy, a gyakorlatvégrehajtás tevékenységeinek kezelését bemutató tervet. A tervben szerepelhetnek a feladatokra, célokra, projekttervekre, finanszírozására, szükséges képzésre, valamint az érintett érdekelt felek bevonására vonatkozó információk. **Gyakorlatok: Jó kiberhigiénia**. A 3. szint a CUI (ellenőrzött, nem minősített információk) védelmére összpontosít, valamint magában foglalja a NIST 800-171. számú speciális kiadványában szereplő valamennyi biztonsági követelményt és a fenyegetések csökkentésére szolgáló, más szabványokban és referenciákban szereplő további gyakorlatokat.	**Folyamatok: Felülvizsgálva.** A 4. szint előírja, hogy a szervezetek vizsgálják felül és mérjék a gyakorlatok eredményességét. A gyakorlatok eredményességének mérésén kívül a szervezetek ezen a szinten szükség esetén képesek korrekciós intézkedéseket hozni, továbbá rendszeresen tájékoztatni a felső vezetést a helyzetről vagy problémákról. **Gyakorlatok: Proaktív** A 4. szint a CUI védelmére összpontosít és magában foglalja a fokozott biztonsági követelmények egy csoportját. Ezek a gyakorlatok javítják a szervezet észlelési és reagálási képességeit a változó taktikák, technikák és eljárások kezelése és az azokhoz való alkalmazkodás érdekében.	**Folyamatok: Optimalizálás** Az 5. szint előírja, hogy a szervezetek az egész szervezetre kiterjedően szabványosítsák és optimalizálják a folyamatvégrehajtást. **Gyakorlatok: Fejlett/Proaktív** Az 5. szint a CUI védelmére összpontosít. A további gyakorlatok a kiberbiztonsági képességek intenzitását és kifinomultságát növelik.

Közösségi kiberbiztonsági érettségi modell (CCSMM)	**Biztonságtudatosság** A tevékenységek fő témája ezen a szinten az egyének és szervezetek fenyegetésekkel, problémákkal, valamint kiberbiztonsági kérdésekkel kapcsolatos ismereteinek növelése	**Folyamatfejlesztés** A kiberbiztonsági kérdések hatékony kezeléséhez szükséges biztonsági folyamatok létrehozásának és javításának segítésére kidolgozott szint.	**Információalapú** Arra tervezték, hogy javítsa a közösségen belüli információmegosztási mechanizmusokat, hogy a közösség hatékonyan vethesse össze a látszólag eltérő információkat.	**Taktikai fejlesztés** Ennek a szintnek az elemeit arra tervezték, hogy jobb és proaktívabb módszereket dolgozzanak ki a támadások észlelésére és a támadásokra való reagálásra. E szint elérése előtt a legtöbb megelőzési módszernek már érvényben kell lennie;	**Teljes biztonsági operatív képesség** Ez a szint azokat az elemeket jelöli, amelyekkel minden szervezetnek rendelkeznie kell ahhoz, hogy magát operatív értelemben teljesen késznek mondhassa bármelyen kiberfenyegetés kezelésére.
A belső ellenőrzési képesség modellje (IA-CM) a közszféra számára	**Kezdeti** Nincsenek fenntartható, megismételhető képességek – az egyéni erőfeszítések függvénye	**Infrastruktúra** Fenntartható és megismételhető gyakorlatok és eljárások	**Integrált** A vezetői és szakmai gyakorlatokat egységesen alkalmazzák	**Kezelt** Az irányítás és kockázatkezelés javítása érdekében integrálja az információkat a szervezet egészéből	**Optimalizálás** Tanulás a szervezeten belül és kívül a folyamatos fejlődés érdekében

7. táblázat: Attribútumok/dimenziók összehasonlítás

	Kiberbiztonsági kapacitás érettségi modellje a nemzetek számára (CMM)	Kiberbiztonsági képességérettségi modell (C2M2)	Katari kiberbiztonsági képességérettségi modell (Q-C2M2)	Kiberbiztonsági érettségi modellre vonatkozó tanúsítás (CMMC)	Kiberbiztonsági érettségi modellre vonatkozó tanúsítás (CMMC)	Információbiztonsági érettségi modell a NIST kiberbiztonsági keretrendszer tekintetében (ISMM)	Kritikus infrastruktúra kiberbiztonságának javítására szolgáló keretrendszer	Globális kiberbiztonsági index (GCI)	Kibererőindex (CPI)
Szintek	Több tényezőre bontott öt dimenzió, amely tényezők maguk is több szempontot és mutatót foglalnak magukban (4. ábra)	Tíz tartomány, amely tartalmaz egy egyedi kezelési célkitűzést és számos megközelítési célkitűzést (6. ábra)	Altartományokra osztott öt tartomány	Tizenhét tartományt folyamatokra osztanak, egyet pedig több képességre, amelyek ezután gyakorlatokra vannak bontva (9. ábra).	Hat fő dimenzió	Huszonhárom értékelt terület	Öt funkció, amely mögött kulcsfontosságú kategóriák és alkategóriák állnak (ábra).	Öt pillér, amely mutatókat tartalmaz	Mutatókból álló négy kategória
Attribútumok/Dimenziók	i Kiberbiztonsági politika és stratégia kidolgozása; ii Felelős kiberbiztonsági kultúra ösztönzése a társadalomban; iii Kiberbiztonsági ismeretek fejlesztése; iv Hatékony jogi és szabályozási keretek létrehozása; v Kockázatok ellenőrzése szabványok, szervezetek és technológiák révén.	i Kockázatkezelés; ii Eszköz-, változás- és konfigurációkezelés; iii Személyazonosság- és hozzáférés-kezelés; iv Fenyegetés- és sebezhetőségkezelés; v Helyzetismeret; vi Eseményekre és biztonsági eseményekre való reagálás; vii Ellátási lánc és külső függőségek kezelése; viii Munkaerő-gazdálkodás; ix Kiberbiztonsági architektúra; x Kiberbiztonsági program kezelése.	i Megértés (kiberirányítás, eszközök, kockázatok és képzés); ii Biztonság (adatbiztonság, technológiai biztonság, hozzáférés-ellenőrzési biztonság, kommunikációs biztonság és személyi biztonság); iii Expozíció (nyomon követés, biztonsági események kezelése, észlelés, elemzés és expozíció); iv Reagálás (reagálástervezés, csökkentés, valamint reakcióközlés); v Fenntartás (helyreállítás-tervezés, folytonosságirányítás, javítás és külső függőségek).	i Hozzáférés-ellenőrzés; ii Eszközkezelés; iii Ellenőrzés és elszámoltathatóság; iv Tudatosságnövelés és képzés; v Konfigurációkezelés; vi Azonosítás és hitelesítés; vii Biztonsági eseményekre való reagálás; viii Fenntartás; ix Médiavédelem; x Személyi biztonság; xi Fizikai védelem; xii Helyreállítás; xiii Kockázatkezelés; xiv Biztonsági értékelés; xv Helyzetismeret; xvi Rendszer- és kommunikációvédelem; xvii Rendszer- és információintegritás.	i Kezelt fenyegetések; ii Mérőszámok; iii Információmegosztás; iv Technológia; v Képzés; vi Teszt.	i Eszközkezelés; ii Üzleti környezet; iii Irányítás; iv Kockázatértékelés; v Kockázatkezelési stratégia; vi Megfelelésértékelés; vii Hozzáférés-ellenőrzés; viii Tudatosságnövelés és képzés; ix Adatbiztonság; x Információvédelmi folyamatok és eljárások; xi Fenntartás; xii Védelmi technológia; xiii Anomáliák és események; xiv Biztonsági folyamatos nyomon követés; xv Észlelési folyamatok; xvi Reagálástervezés; xvii Reagálásra vonatkozó kommunikáció; xviii Reagáláselemzés; xix Reagálással kapcsolatos enyhítés; xx Reagálással kapcsolatos javítások; xxi Helyreállítástervezés; xxii Helyreállítással kapcsolatos javítások; xxiii Helyreállításra vonatkozó kommunikáció.	i Azonosítás; ii Védelem; iii Észlelés; iv Reagálás; v Helyreállítás.	i Jogi; ii Műszaki; iii Szervezeti; iv Kapacitásépítési; v Együttműködési.	i Jogi és szabályozási keret; ii Gazdasági és társadalmi környezet; iii Technológiai infrastruktúra; iv Ipari alkalmazás.

B. MELLÉKLET – A MÁSODELEMZÉS SZAKIRODALMI JEGYZÉKE

A Biztonsági Bizottság Titkársága: *Finland's Cyber Security Strategy 2019*, 2019. Elérhető az alábbi címen: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

A Francia Miniszterelnök Hivatala: *French National Digital Security Strategy*, 2014. Elérhető az alábbi címen: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

A Miniszterek Tanácsának 92/2019 rendelete, *Portugál Hivatalos Lap*, 1. sor., 108. sz., 2019. Elérhető az alábbi címen: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

A Miniszterek Tanácsának elnöksége: *The Italian Cybersecurity Action Plan*, 2017. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről, *az Európai Unió Hivatalos Lapja*, 2008. Elérhető az alábbi címen: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Almuhammadi, S. és Alsaleh, M.: Information Security Maturity Model for Nist Cyber Security Framework, *Computer Science & Information Technology (CS & IT)*, 2017. Hatodik nemzetközi konferencia az információtechnológiai konvergenciáról és szolgáltatásokról, Felsőoktatási és Ipari Együttműködési Központ (AIRCC), 2017.

Almuhammadi, S. és Alsaleh, M.: Information Security Maturity Model for Nist Cyber Security Framework, *Computer Science & Information Technology (CS & IT)*, 2017. Elérhető az alábbi címen: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. és mtsai: *Stocktaking, analysis and recommendations on the protection of CIIs*, 2016. Elérhető az alábbi címen: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Az Amerikai Egyesült Államok Fehér Háza: *National Cyber Strategy of the United States of America*, 2018. Elérhető az alábbi címen: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Az Egyesült Államok Elnökének Végrehajtó Hivatala: *Memorandum for Heads of Executive Departments and Agencies*, 2015. Elérhető az alábbi címen: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Az Elektronikus Hírközlés és Postaügyi Rendelkezések Biztosának Hivatala: *Cybersecurity Strategy of the Republic of Cyprus*, 2012.

Az Észt Köztársaság Gazdasági és Hírközlési Minisztériuma: *Cybersecurity Strategy – Republic of Estonia*, 2019. Elérhető az alábbi címen: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Az Európa Tanács és az Európai Unió CyberCrime@IPA projektje, az Európa Tanács számítógépes bűnözésről szóló globális projektje, valamint az Európai Unió számítástechnikai bűnözéssel foglalkozó munkacsoportja: *Specialised cybercrime units - Good practice study*, 2011. Elérhető az alábbi címen: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Az Osztrák Köztársaság Szövetségi Kancelláriája: *Austrian Cyber Security Strategy*, 2013. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Becker, J., Knackstedt, R. és mtsai: *Developing Maturity Models for IT Management – A Procedure Model and its Application*, 2009. Elérhető az alábbi címen: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Belgium kormánya: *Cyber Security Strategy*, 2012. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. és mtsai: *Developing Cybersecurity Capacity: A proof-of-concept implementation guide*, RAND Corporation, 2018. Elérhető az alábbi címen: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Belső Ellenőrök Intézete (szerk.): *Internal audit capability model (IA-CM) for the public sector: overview and application guide*, Altamonte Springs, Fla: Belső Ellenőrök Intézete Kutatási Alapítvány, 2009.

Biztonsági Tanulmányok Központja (CSS), ETH Zürich: *National Cybersecurity Strategies in Comparison – Challenges for Switzerland*, 2019. Elérhető az alábbi címen: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Bourgue, R.: *Introduction to Return on Security Investment*, 2012.

Bulgária kormánya: *National Cyber Security Strategy - Cyber-resistant Bulgaria 2020*, 2015.

Carnegie Mellon Egyetem Szoftvertechnikai Intézete: *Cybersecurity Capability Maturity Model (C2M2)*, 2.0. változat, Amerikai Egyesült Államok, Pittsburgh, 2019. Elérhető az alábbi címen: https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Creese, S.: *Cybersecurity Capacity Maturity Model for Nations (CMM)*, Oxfordi Egyetem, 2016.

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (nincs dátum). Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

CSIRT Maturity - Self-assessment Tool (nincs dátum). Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Dánia kormánya – Pénzügyminisztérium: *Danish Cyber and Information Security Strategy*, 2018. Elérhető az alábbi címen: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Darra, E.: *Public Private Partnerships (PPP)*, 2017.

Darra, E.: *Welcome to the NCSS Training Tool* (nincs dátum).

Dekker, M. A. C.: *Guideline on Threats and Assets*, 2015. Elérhető az alábbi címen: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Dekker, M. A. C.: *Technical Guideline on Incident Reporting*, 2014. Elérhető az alábbi címen: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C.: *Technical Guideline on Security Measures*, 2014. Elérhető az alábbi címen: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Digital Slovenia Cybersecurity Strategy, 2016. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. és mtsai: *Privacy and data protection by design - from policy to engineering, 2014.* Elérhető az alábbi címen: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Európai Bizottság: *Az Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és megbízható szolgáltatásokról*, 2012. Elérhető az alábbi címen: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0238&from=EN

Európai Unió és Hálózat- és Információbiztonsági Ügynökség: *ENISA–CERT Inventory, Inventory of CERT teams and activities in Europe*, 2014. Elérhető az alábbi címen: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Európai Unió és Hálózat- és Információbiztonsági Ügynökség: *Handbook on security of personal data processing*, 2017. Elérhető az alábbi címen: http://dx.publications.europa.eu/10.2824/569768

Európai Uniós Hálózat- és Információbiztonsági Ügynökség: *Guidelines for SMEs on the security of personal data processing*, 2016.

Európai Uniós Hálózat- és Információbiztonsági Ügynökség: *NCSS good practice guide: designing and implementing national cyber security strategies*, Heraklion: ENISA, 2016.

Európai Uniós Hálózat- és Információbiztonsági Ügynökség: *NCSS: Practical Guide on Development and Execution*, Heraklion: ENISA, 2012.

Európai Uniós Hálózat- és Információbiztonsági Ügynökség: *NCSS: Setting the course for national efforts to strengthen security in cyberspace*, Heraklion: ENISA, 2012.

Ferette, L. és Európai Uniós Hálózat- és Információbiztonsági Ügynökség: *The 2015 report on national and international cyber security exercises: survey, analysis and recommendations*, 2015. Elérhető az alábbi címen: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Ferette, L.: *NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises*, 2016. Elérhető az alábbi címen: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Galan Manso, C. és mtsai: *Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises*, 2015. Elérhető az alábbi címen: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Gazdasági Együttműködési és Fejlesztési Szervezet (OECD): *Cybersecurity policy making at a turning point*, 2012. Elérhető az alábbi címen: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Genti Egyetem és mtsai: Evaluating Business Process Maturity Models, *Journal of the Association for Information Systems*, 2017. Elérhető az alábbi címen: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Görögország kormánya: *National Cyber Security Strategy*, 2017. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Hollandia kormánya: *National Cyber Security Agenda*, 2018. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

Horvátország kormánya: *The National Cyber Security Strategy of The Republic of Croatia*, 2015. Elérhető az alábbi címen: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Innsbrucki Egyetem és mtsai: *Understanding Maturity Models*, 2009.

Írország kormánya: *National Cyber Security Strategy*, 2019. Elérhető az alábbi címen: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

J.D., R. D. B.: Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework, *International Review of Law*, 2019.

Lettország kormánya: *Cyber Security Strategy of Latvia*, 2014. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Litvánia Honvédelmi Minisztériuma: *National Cyber Security Strategy*, 2018.

Liveri, D. és mtsai: *An evaluation framework for national cyber security strategies*, Heraklion: ENISA, 2014. Elérhető az alábbi címen: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Luxemburgi Kormánytanács: *National Cybersecurity Strategy*, 2018. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Magyarország kormánya: *A hálózati és információs rendszerek biztonságára vonatkozó stratégia*, 2018. Elérhető az alábbi címen: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Málta Versenyképességi, Digitális, Tengerészeti és Szolgáltatásgazdaságért Felelős Minisztériuma: *Malta Cyber Security Strategy*, 2016. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Mattioli, R. és mtsai: *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks*, 2014. Elérhető az alábbi címen: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

National Cyber Security Strategies - Interactive Map (nincs dátum). Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

National Cybersecurity Strategies Evaluation Tool, 2018. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Nemzeti Kiberbiztonsági Központ: *National Cyber Security Strategy of the Czech Republic*, 2015. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Nemzeti Szabványügyi és Technológiai Intézet: *Framework for Improving Critical Infrastructure Cybersecurity*, 1.1. változat, Gaithersburg, MD: Nemzeti Szabványügyi és Technológiai Intézet,

2018. Elérhető az alábbi címen: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Nemzetközi Távközlési Egyesület (ITU): *The Global Cybersecurity Index*, 2018. Elérhető az alábbi címen: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Nemzetközi Távközlési Egyesület (ITU): *The Global Cybersecurity Index*, 2018. Elérhető az alábbi címen: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Object Management Group: *Business Process Maturity Model*, 2008. Elérhető az alábbi címen: https://www.omg.org/spec/BPMM/1.0/PDF

OECD, az Európai Uniós és a Közös Kutatóközpont – az Európai Bizottság: *Handbook on Constructing Composite Indicators: Methodology and User Guide*, OECD, 2008. Elérhető az alábbi címen: https://www.oecd.org/sdd/42495745.pdf.

Ouzounis, E.: *Good Practice Guide on National Exercises*, 2012.

Ouzounis, E.: *National Cyber Security Strategies - Practical Guide on Development and Execution*, 2012.

Portesi, S.: *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects*, 2017.

Rady Ministrów: *Dziennik Urzędowy Rzeczypospolitej Polskiej*, 2019. Elérhető az alábbi címen: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Románia kormánya: *Cyber security strategy of Romania*, 2013. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. és az Európai Uniós Kiberbiztonsági Ügynökség: *Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies*, 2019. Elérhető az alábbi címen: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Smith, R.: *Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010*, 2015

Smith, R.: Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010, in: *Smith, R., Core EU Legislation*, London: Macmillan Education, 2016. Elérhető az alábbi címen: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Spanyolország kormánya: *National Cyber Security Strategy*, 2019. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Stavropoulos, V.: *European Cyber Security Month 2017*, 2017.

Svéd kormány: *Nationell strategi för samhällets informations- och cybersäkerhet*, 2017. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Szlovákia kormánya: *Cyber Security Concept of the Slovak Republic*, 2015. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Szövetségi Belügyminisztérium: *Cyber Security Strategy for Germany*, 2011. Elérhető az alábbi címen: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Szövetségi Tanács: *National strategy for the protection of Switzerland against cyber risks*, 2018.

Trimintzios, P. és mtsai: *Cyber Europe Report*, 2011. Elérhető az alábbi címen: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. és az Európai Uniós Hálózat- és Információbiztonsági Ügynökség: *National-level risk assessments: an analysis report*, 2013. Elérhető az alábbi címen: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R. és mtsai: *Report on cyber-crisis cooperation and management*, 2015. Elérhető az alábbi címen: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A. és mtsai: *Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises*, 2015. Elérhető az alábbi címen: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

UK National Cyber Security Strategy 2016-2021, 2016. Elérhető az alábbi címen: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Wamala, D. F.: *ITU National Cybersecurity Strategy Guide*, 2011. Elérhető az alábbi címen: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G.: The Community Cyber Security Maturity Model, in: *a 40. Éves Hawaii Rendszertudományi Nemzetközi Konferencia (HICSS'07)*, 2007.

C. MELLÉKLET – EGYÉB TANULMÁNYOZOTT CÉLKITŰZÉSEK

Az alább részletezett célkitűzések tanulmányozása a másodelemzési fázis, valamint az ENISA által lefolytatott interjúk részeként történt meg. A következő célkitűzések nem képezik a nemzeti képességek értékelése keretrendszerének részét, de olyan témákra világítanak rá, amelyeket érdemes megvitatni. Az alábbi alfejezetek mindegyikében magyarázatot találunk arra, miért vetették el az adott célkitűzést.

- Ágazatspecifikus kiberbiztonsági stratégiák kidolgozása;
- Dezinformációs kampányok elleni küzdelem;
- Élvonalbeli technológiák (5G, MI, kvantuminformatika stb.) biztonságosságának garantálása;
- Adatszuverenitás biztosítása; és
- A kiberbiztosítási ágazat fejlesztésére vonatkozó ösztönző programok biztosítása.

Ágazatspecifikus kiberbiztonsági stratégiák kidolgozása

Az ágazati beavatkozásokat és ösztönzőket megcélzó ágazatspecifikus stratégiák elfogadása kétség kívül erősebb decentralizált képességet vezet be. Ez különösen azoknak a tagállamoknak jó, amelyek OES-einek különböző keretrendszerekkel és rendeletekkel kell megbirkózniuk, valamint ahol a kiberbiztonság transzverzális jellege miatt sok a függőség. Valóban, több tagállam rendelkezik több tucat olyan nemzeti hatósággal és szabályozó szervvel, amelyek ismerik az egyes ágazatok sajátosságait, és amelyeknek felhatalmazása van az egyes ágazatokra vonatkozó specifikus rendelet érvényesítésére.

Dánia például hat olyan célzott stratégiát indított el, amelyek a legkritikusabb ágazatok kiber- és információbiztonsági erőfeszítéseivel foglalkoznak, azért, hogy egy erősebb decentralizált képességet hozzanak létre a kiber- és információbiztonság terén. Minden „ágazati egység” hozzájárul többek között a fenyegetések ágazati szintű értékeléséhez, a nyomon követéshez, a felkészültségi gyakorlatokhoz, a biztonsági rendszerek létrehozásához, az ismeretek megosztásához és az oktatáshoz. Az ágazatspecifikus stratégiák az alábbi ágazatokra terjednek ki:

- Energiaügy;
- Egészségügy;
- Közlekedés;
- Távközlés;
- Pénzügy; és
- Tengeri ágazat.

Más tagállamok érdeklődésüket fejezték ki olyan ágazatspecifikus kiberbiztonsági stratégiák megfontolása iránt, amelyek valamennyi szabályozási követelményre kiterjednek. Azonban meg kell jegyezni, hogy egy ilyen célkitűzés méretük, nemzeti politikáik és érettségük függvényében nem biztos, hogy minden tagállamnak megfelel. Nagyon nehéz biztosítani, hogy a

keretrendszer az összes sajátosságra magyarázatot tudjon adni, ez pedig arra késztette az ENISA-t, hogy ne foglalja bele ezt a célkitűzést a keretrendszerbe.

Dezinformációs kampányok elleni küzdelem

A tagállamok saját nemzeti kiberbiztonsági stratégiáikba beépítik az olyan alapelvek védelmét, mint az emberi jogok, az átláthatóság és a közbizalom. Ez különösen fontos, amikor olyan dezinformációról van szó, amelyet a hagyományos hírközlő médiákon vagy a közösségi médiaplatformokon keresztül terjesztenek. Ráadásul a kiberbiztonság jelenti jelenleg az egyik legnagyobb választási kihívást. Fontos választások előtt különböző országokban megfigyelhetők voltak olyan tevékenységek, mint a hamis információk terjesztése vagy a negatív propaganda. Ez a fenyegetés alááshatja az Európai Unió demokratikus folyamatát. Európai szinten a Bizottság elkészítette egy cselekvési terv[32] vázlatát, amely erőfeszítéseket tesz arra, hogy erősítse Európában a dezinformáció elleni küzdelmet: ez a terv 4 kulcsfontosságú területre összpontosít (észlelés, együttműködés, online platformokkal való együttműködés és tudatosságnövelés) és arra szolgál, hogy kiépítse az Unió képességeit és megerősítse a tagállamok közötti együttműködést.

A 19 megkérdezett ország közül 4 kifejezte szándékát, miszerint foglalkozni kíván a dezinformáció és propaganda problémájával saját NKBS-ében.

A francia NKBS[33] például megjegyzi a következőket: „az állam felelőssége tájékoztatni a polgárokat a rosszindulatú szereplők által az interneten alkalmazott manipulációs és propagandatechnikák kockázatairól. Például a 2015 januárjában történt franciaországi terrortámadások után a kormány létrehozott egy, az elektronikus kommunikációs hálózatokon keresztül történő iszlám radikalizálódással kapcsolatos kockázatokról szóló információs platformot: »Stop-djihadisme.gouv.fr«.” Ez a megközelítés kiterjeszthető a propaganda vagy a destabilizáció egyéb jelenségeire.

Egy másik példában Lengyelország 2019–2024. évi NKBS-e[34] szerint: „a manipulatív tevékenységek, például a dezinformációs kampányok ellen rendszerszintű fellépésre van szükség a polgárok tudatosságának növelése érdekében az információk hitelességének ellenőrzése és az információk eltorzítására tett kísérletekre adott reakció kontextusában.”

Azonban az ENISA által lefolytatott interjúk során számos tagállam elmondta, hogy ezzel a kérdéssel mint kiberfenyegetéssel nem az NKBS-ük keretében foglalkoznak, hanem szélesebb körű társadalmi szinten, például politikai kezdeményezésekkel.

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Élvonalbeli technológiák (5G, MI, kvantuminformatika stb.) biztonságosságának garantálása

Mivel a kiberfenyegetés jelenlegi területe tovább bővül, az új technológiák fejlődése valószínűleg a kibertámadások intenzitásának és számának növekedését, valamint a fenyegető szereplők által alkalmazott módszerek, eszközök és célok diverzifikációját fogja eredményezni. Mindeközben az említett új technológiai megoldások élvonalbeli technológiák formájában potenciálisan az európai digitális piac alkotóelemeivé válhatnak. A tagállamok növekvő digitális függőségének és az új technológiák megjelenésének védelme érdekében ösztönző programokat és teljes értékű szakpolitikákat kell létrehozni az említett technológiák Unión belüli biztonságos és megbízható kidolgozásának és alkalmazásának támogatására.

A tagállamok NKBS-ein végzett másodelemzés fázisában az alábbi élvonalbeli technológiák kerültek a tagállamok érdeklődésének középpontjába: 5G, MI, kvantuminformatika, kriptográfia, pereminformatika, összekapcsolt és autonóm járművek, „big data” és „smart data” technológia, blokklánc, robotika és dolgok internete (IoT).

Konkrétabban 2020 elején az Európai Bizottság egy közleményt adott ki, amelyben felszólította a tagállamokat, hogy tegyenek lépéseket az 5G hálózatok biztonságával kapcsolatos uniós eszköztár következtetéseiben ajánlott intézkedések végrehajtása érdekében[35]. Ez az 5G eszköztár a Bizottság által 2019-ben elfogadott 5G hálózatok kiberbiztonságáról szóló (EU) 2019/534 ajánlás nyomán jött létre, amely egységes európai megközelítést szorgalmazott az 5G hálózatok biztonsága tekintetében[36].

Az ENISA által készített interjúk során kiemelték, hogy ez inkább egy transzverzális jellegű téma, amellyel az NKBS-ben általánosan foglalkoznak, nem pedig önmagában, meghatározott célkitűzésként.

Adatszuverenitás biztosítása

A kibertér egyrészt tekinthető félelmetes globális közös térnek, amely könnyen hozzáférhető, magas szintű összekapcsoltságot biztosít, valamint nagyszerű lehetőségeket kínál a társadalmi-gazdasági növekedésre. Másrészt a kibertérre jellemző a gyenge joghatóság, az intézkedések nehézségei, a határok hiánya, valamint az összekapcsolt rendszerek, amelyek porózusak lehetnek és adataikat ellophatják, illetve amelyek adataihoz akár külföldi kormányok is hozzáférhetnek. E két nézőpont mellett a digitális ökoszisztémára az is jellemző, hogy az online szolgáltató platformok és infrastruktúra az érdekelt felek nagyon szűk körének kezében összpontosul. Minden említett szempont arra készteti a tagállamokat, hogy támogassák a digitális szuverenitást. A digitális szuverenitás elérése azt jelenti, hogy a polgárok és vállalkozások képesek teljesen kibontakozni a megbízható digitális szolgáltatások és IKT-termékek használatával anélkül, hogy félteniük kellene személyes adataikat, digitális eszközeiket, illetve gazdasági autonómiájukat vagy politikai befolyásukat.

Az adatszuverenitást vagy digitális szuverenitást a tagállamok nemzeti és európai szinten is támogatják. Úgy tűnik, hogy a tagállamok NKBS-eikben nem közvetlenül, meghatározott célkitűzésként kezelik ezt a kérdést, hanem vagy transzverzális elvként foglalkoznak vele, vagy pedig *ad hoc* kiadványokban vázolják fel a digitális szuverenitás nemzeti szintű biztosításának

[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission

[36] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

szándékát, a legfontosabb technológiákra összpontosítva. Például a kibervédelem 2018. évi francia stratégiai felülvizsgálatában az szerepel, hogy „a következő technológiák ellenőrzése kiemelt fontosságú a digitális szuverenitás biztosítása érdekében: kommunikáció titkosítása, kibertámadás észlelése, professzionális mobilrádió, felhőalapú számítástechnika és mesterséges intelligencia”[37].

Európai szinten a tagállamok aktívan részt vesznek az európai adatstratégia (COM/2020/66 final) meghatározásában, valamint az Unió kiberbiztonsági jogszabálya, azaz az (EU) 2019/881 rendelet szerint meghatározott digitális IKT-termékekre, -szolgáltatásokra és -folyamatokra vonatkozó uniós tanúsítási keretrendszer kidolgozásában, mindezt azért, hogy stratégiai digitális autonómiát biztosítsanak európai szinten.

A tagállamokkal folytatott interjúk fázisában megmutatkozott, hogy a digitális szuverenitás témáját gyakran tágabb kérdésnek tekintik, amely nem csupán a kiberbiztonságra korlátozódik. A tagállamok ezért ezzel a témával nem foglalkoznak saját NKBS-ükben, illetve azok, amelyek mégis, nem egy meghatározott célkitűzésként kezelik azt.

A kiberbiztosítási ágazat fejlesztésére vonatkozó ösztönző programok biztosítása

A kiberbiztosítási ágazat aktuális helyzete a globális piac vitathatatlan növekedését mutatja. Azonban ez még mindig korai szakaszban van, mivel adatokat kell gyűjteni és számos precedenst kell teremteni (*pl.* „silent” kiberbiztosítási lefedettség, rendszerszintű kiberkockázat stb.). Ezenkívül a világszerte elkövetett kibertámadásokból összesített becsült veszteségek több nagyságrenddel magasabbak, mint a kiberbiztosítási ágazat aktuális lefedettségi kapacitása (az IMF munkadokumentuma – Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143). A kiberbiztosítási ágazat fejlesztése azonban mindenképp előnyekkel járhat és megalapozhatja a mintaszerű mechanizmusokat. A kiberbiztosítási mechanizmusok bizonyosan segíthetnek a következőkben:

- Kiberbiztonsági kockázatokra vonatkozó tudatosságnövelés a vállalatoknál;
- A kiberkockázati kitettség mennyiségi értékelése;
- Kiberbiztonsági kockázatok kezelésének javítása;
- Kibertámadások áldozatává váló szervezetek támogatása; és
- Egy kibertámadás által okozott (anyagi vagy nem anyagi) károk fedezése.

Egyes tagállamok elkezdtek dolgozni ezen a témán. Például:

- Észtország egy „várjunk, és majd meglátjuk” megközelítést alkalmazott az NKBS-ében: „A magánszektorban rejlő kiberkockázatok általános csökkentése érdekében elemezni kell a kiberbiztosítási szolgáltatásra vonatkozó keresletet és kínálatot Észtországban és az alapján történik megállapodás a kapcsolt felek együttműködési elveiről, köztük az információmegosztásról, a kockázatértékelés előkészítéséről stb. Jelenleg kevés kiberbiztosító van jelen az észt piacon és először fel kell térképezni, hogy ki mit kínál. A biztosítási védelem összetettségét gyakran akadályozó tényezőnek tekintik a kiberbiztosítási piac fejlődésében.”
- Luxemburg saját NKBS-ében kifejezetten támogatja a kiberbiztosítási ágazat fejlesztését: „1. célkitűzés: Új termékek és szolgáltatások létrehozása. A kockázatok összegyűjtése érdekében és azért, hogy arra ösztönözzük a digitális kiberbiztonsági események áldozatait, hogy szakértőktől kérjenek segítséget az esemény

[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

kezeléséhez, valamint egy rosszindulatú cselekménnyel érintett rendszer helyreállításához, a biztosítótársaságokat arra kell biztatni, hogy hozzanak létre speciális termékeket a kiberbiztosítás területére vonatkozóan.”

Az interjúalanyok visszajelzései meglehetősen eltérőek voltak ebben a témában: míg néhány tagállam kifejtette, hogy a kiberbiztosítás témaköre a közelmúltban az eszmecserék részévé vált, addig mások úgy vélték, hogy bár a téma ígéretes, az iparág még nem elég érett. Ugyanakkor az interjúalanyok nagy hányada azt állította, hogy ezzel a témával nem foglalkoznak az NKBS keretében, vagy azért, mert túl specifikusnak gondolják, vagy pedig azért, mert nem tartozik az NKBS hatálya alá.

TP-02-21-253-HU-N

Az Európai Uniós Kiberbiztonsági Ügynökség

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) az Unió azon ügynöksége, amelynek célja az Európa-szerte egységesen magas szintű kiberbiztonság megvalósítása. A 2004-ben létrehozott és az uniós kiberbiztonsági jogszabály által megerősített Európai Uniós Kiberbiztonsági Ügynökség hozzájárul az uniós kiberpolitikához, kiberbiztonsági tanúsítási rendszerek alkalmazásával javítja az IKT-termékek, -szolgáltatások és -folyamatok megbízhatóságát, együttműködik a tagállamokkal és az uniós szervekkel és segíti Európát abban, hogy felkészüljön a jövő kiberbiztonsággal kapcsolatos kihívásaira. A tudásmegosztás, a kapacitásépítés és a figyelemfelkeltés révén az Ügynökség a legfontosabb érdekelt felekkel együtt arra törekszik, hogy megerősítse az összekapcsolt gazdaságba vetett bizalmat, fokozza az uniós infrastruktúra ellenálló-képességét és végső soron megőrizze Európa társadalmának és polgárainak digitális biztonságát. Bővebb információért lásd: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-484-8
DOI: 10.2824/335350