**Kockázatértékelési és biztonsági osztályba sorolási útmutató DIMOP pályázat keretében fejlesztendő informatikai rendszerek előzetes besorolásához**

**A Dokumentum Adatai**

|  |  |
| --- | --- |
| **Cím** | Biztonsági osztályba sorolási útmutató DIMOP pályázat keretében fejlesztendő informatikai rendszerek előzetes besorolásához |
| **Leírás** | Jelen dokumentum támogatást kíván adni az elektronikus információs rendszer bevezetési projektek során szállítandó rendszerek előzetes, azaz a követelmények specifikálási fázisában történő biztonsági osztályba sorolásához. |
| **Biztonsági besorolás** | Nyilvános |

**Változatok**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kiadás dátuma** | **Szerző** | **Cégnév** | **Verzió** | **Leírás** |
|  |  |  |  |  |

**Tartalom jegyzék**

Használt fogalmak 3

Bevezetés 4

A dokumentum célja 4

Az előzetes biztonsági osztályba sorolás folyamata 4

Az adatok azonosítása, adatvagyon felmérése 5

Fenyegetettségek meghatározása 6

Kockázatok értékelése 7

Bizalmasság sérüléséből adódó kárérték megállapítása 7

Sértetlenség sérüléséből adódó kárérték megállapítása 8

Rendelkezésre állás sérüléséből adódó kárérték megállapítása 10

EIR előzetes biztonsági osztályba sorolása 11

Az előzetes biztonsági osztályba sorolás jóváhagyása és felülvizsgálata 12

# Használt fogalmak

|  |  |
| --- | --- |
| **Bizalmasság** | az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról – *Ibtv. 1. § (1) bekezdés 8. pont.* |
| **Biztonsági osztály** | az elektronikus információs rendszer védelmének elvárt erőssége *Ibtv. 1. § (1) bekezdés 11. pont* |
| **EIR** | elektronikus információs rendszer |
| **Fenyegetettség** | olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá́ olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát - *Ibtv. 1. § (1) bekezdés 19. pont* |
| **Ibtv.** | Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény |
| **Elektronikus információs rendszer** | Elektronikus információs rendszernek kell tekinteni adott adatkezelő vagy adatfeldolgozó által, adott cél érdekében az adatok, információk kezelésére használt eszközök – így különösen környezeti infrastruktúra, hardver, hálózat és adathordozók –, eljárások – így különösen szabályozás, szoftver és kapcsolódó folyamatok –, valamint az ezeket kezelő személyek együttesét. - *Ibtv. 1. § (3) bekezdés* |
| **Kockázat** | Az adott EIR-ek, valamint a bennük tárolt adatok bizalmasságát, sértetlenségét vagy rendelkezésre állását veszélyeztető fenyegetés bekövetkezési valószínűségét, valamint a lehetséges kár nagyságát is figyelembe vevő tényező. |
| **Különleges adat** | a személyes adatok különleges kategóriaiba tartozó́ minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló́ személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó́ biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó́ személyes adatok |
| **Rendelkezésre állás** | annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek – *Ibtv. 1. § (1) bekezdés 38. pont.* |
| **Sértetlenség** | az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség), és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható – *Ibtv. 1. § (1) bekezdés 39. pont.* |
| **Személyes adat** | azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy, vagy több tényező alapján azonosítható |

# Bevezetés

Az Ibtv. hatálya alá tartozó szervezeteknek biztosítaniuk kell az általuk használt elektronikus információs rendszer (EIR) zártságát, teljeskörű, folytonos és kockázatokkal arányos védelmét. Az információs rendszereknek és azok elemeinek már a használatba vételük pillanatában rendelkezniük kell azokkal a képességekkel, amelyekkel biztosítani tudják a bennük tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzését. Ez a jogszabály szerinti elvárás olyan követelményeket támaszt az információs rendszerekkel szemben, amelyeknek be kell épülniük a rendszer funkcionalitását meghatározó elvárások közé, ellenkező esetben az információs rendszer nem, vagy csak utólagos többletráfordítások árán lesz képes megfelelni az előírt megfelelési kötelezettségnek.

# A dokumentum célja

Jelen dokumentum elsődleges célja, hogy útmutatót adjon a beszerzendő/fejlesztendő elektronikus információs rendszer (továbbiakban EIR) előzetes, a követelmények specifikálási fázisában történő biztonsági osztályba sorolásához, ezáltal támogassa, hogy a kockázati szinteknek megfelelően az információbiztonsági követelmények a Rendszer életciklusának legelején azonosításra kerüljenek és már a specifikálási/tervezési fázisban teljeskörűen figyelembe legyenek véve.

Az EIR-ek biztonsági osztályba sorolása egységes keretrendszert biztosít az információbiztonság növelésére tett törekvések hatékony irányításához és felügyeletéhez, lehetővé teszi az EIR védelmi képességeinek következetes meghatározását, mérését, ellenőrzését, valamint más rendszerek védelmi képességeivel való összehasonlítását.

# Az előzetes biztonsági osztályba sorolás folyamata

Az EIR védelmére fordított kiadásoknak arányosnak kell lenniük a felmerülő kockázatokkal, azaz csak a lehetségesen bekövetkező veszteségek és károk nagyságrendjével arányosan indokolt a védelemre költeni. Az információs rendszer védelmének kialakítására és fenntartására fordított költéségek a kezelt adatok, valamint az EIR elemeinek a bizalmasságának, a sértetlenségének vagy a rendelkezésre állásának elvesztésével okozott károk nagyságrendjével lehet megállapítani.

Az előzetes biztonsági osztályba sorolás tulajdonképpen az EIR kockázatok figyelembevételére épülő elvárt védelmi erősségének meghatározása. Az elvárt védelmi erősség előzetes, az EIR koncepcionálási fázisában történő azonosításának kettős célja, hogy

* a biztonsági szempontok és a kockázatokkal arányosan elvárt védelmi mechanizmusok az EIR tervezésének, belső kialakításának és működésének szerves részét képezzék, illetve
* a felhasználó és üzemeltető szervezet már a bevezetési projekt során, az EIR használatának megkezdése előtt fel tudjon készülni az EIR további életszakaszaiban elvárt védelmi intézkedések megfelelő kialakítására és működtetésére.

Az EIR előzetes biztonsági osztályba sorolása az alábbi lépések végrehajtásával történhet:

Az osztályba sorolás részletes szabályait 41/2015. (VII. 15.) BM rendelet tartalmazza. A rendelettel összhangban az előzetes biztonsági osztályba sorolás alkalmával az EIR vagy az általa kezelt adatok bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján 1-től 5-ig számozott fokozatot kell alkalmazni. A számozás emelkedésével párhuzamosan szigorodnak az EIR-re vonatkozó védelmi intézkedések.

Az EIR előzetes biztonsági osztályba sorolását az EIR-ek biztonságáért felelős személy készíti elő és az adott EIR adatgazdájával, valamint a szervezet adatvédelmi tisztviselőjével együttműködésben végzi el. Amiatt, hogy az EIR-rel kapcsolatos védelmi és információbiztonsági követelmények beépüljenek az EIR tervezési alapjául szolgáló követelményspecifikációba, műszaki leírásba, szervezeti oldalról megköveteli, hogy az elektronikus információbiztonságért felelős személyt már koncepcionálási szakaszban bevonják az új beszerzésekbe, illetve a fejlesztési prioritások meghatározásába.

Az olyan szoftverek és hardvermegoldások esetében, amelyek az általuk kezelt adatok vagy a bennük megvalósított funkciók alapján nem minősülnek önálló EIR-nek nem kell adatosztályozást elvégezni. Szoftverek esetében ilyenek például az irodai szoftverek, operációs rendszerek, segédprogramok, hardveres megoldások esetében a tűzfalak, switchek, routerek, szerverek, mentőeszközök.

## Az adatok azonosítása, adatvagyon felmérése

Az előzetes biztonsági osztályba sorolás első lépéseként azonosítani kell, hogy az EIR

1. milyen adatokat kezel a működése során
2. a meghatározott adatok milyen kategóriába tartoznak (személyes adat, különleges adat, bűnügyi személyes adat, közérdekű adat, közérdekből nyilvános adat, minősített adat)
3. az azonosított adatok milyen mennyiségben kerülnek az EIR-be (csekély, közepes, nagy, jelentős mennyiség)

A kezelt adatok teljeskörű felmérése érdekében érdemes az EIR által támogatandó üzleti és üzemeltetési folyamatokat azonosítani, majd meghatározni a folyamatok működtetésében érintett funkciókat. Az EIR által támogatott folyamatok és funkciók leltára alapot adhat a kezelt adatok teljeskörű meghatározásához. Az EIR által kezelt adatvagyonelemek leltárának készítésekor különösen figyelni kell a jogszabályok által definiált adatkategóriákba tartozó adatok azonosítására. A személyes adatkezelési és feldolgozási tevékenységhez kapcsolódóan a jogszabály nyilvántartási kötelezettséget ír elő valamennyi elvégzett adatkezelési tevékenység esetében[[1]](#footnote-1). Az EIR által kezelt adatok azonosítása támogatja a szervezet ezen nyilvántartási kötelezettségének teljesítését is.

## Fenyegetettségek meghatározása

Az EIR előzetes biztonsági osztályba sorolását előzetes kockázatelemzés alapján kell elvégezni. A jogszabály[[2]](#footnote-2) azt is lehetővé teszi a szervezetek számára, hogy a biztonsági osztályba sorolást saját kockázatelemzési módszertan alapján készítsék el. Ebben az esetben is célszerű kialakítani a jogszabályban felsorolt szempontok és a saját módszertan elemei közötti megfelelést.

A kockázatok meghatározása az EIR-re vonatkozó, illetve az általa kezelt adatok bizalmasságára, sértetlenségére, és rendelkezésre állásával kapcsolatos fenyegetettségek azonosításával kezdődik. Fenyegetettségnek hívjuk az olyan külső vagy belső irányultságú, kockázatot hordozó tényezőket, lehetséges műveletet, eseményt vagy mulasztásos cselekményt, amely sértheti az EIR, vagy valamely elemének védettségét, biztonságát. A fenyegetettségek feltárása az eddigi tapasztalatok felhasználásával, illetve az EIR elemzéséből felderített hiányosságok számbavételével történhet. Az egyes veszélyforrásokat, kockázatokat helyzetfelméréssel tudjuk meghatározni. A helyzetfelmérés történhet:

* fenyegetettség modellezéssel
* dokumentumok elemzésével (az EIR funkcionális követelményeinek felülvizsgálata, szabályzatok, dokumentációk vizsgálata);
* interjúkkal, csoportos módszerekkel;
* „mi lenne, ha” és forgatókönyv-elemzés módszerével (a stratégiai kockázatok és a folyamatok azonosítására);
* szemlével.

A fenyegetettségek listájának összeállításakor törekedni kell arra, hogy minden releváns számításba jöhető veszélyforrás azonosításra kerüljön. Az esetleg kimaradó veszélyforrások maradék kockázatként kezelhetjük.

A fenyegetettségek megjelenésének többféle rétegét különböztethetjük meg:

1. az adat, információ (pl. illetéktelen hozzáférés, módosítás),
2. az infrastruktúra (pl. szoftver sérülékenységek kezeletlensége, karbantartások elmaradása),
3. a fizikai környezet (pl. redundáns áramellátás, tűzvédelem hiánya)
4. az emberi tényezők (pl. hanyagság, ismeret hiány, szándékos károkozás).

A fenyegetettségek rangsorolása szükséges az előzetes kockázatelemzés megfelelő elvégzéséhez. A nem megfelelően vagy teljeskörűen elvégzett kockázatértékelés esetén az EIR előzetes biztonsági osztálya megállapított elvárt védelmi erősség - többletköltség vagy az adatokkal kapcsolatos kockázatok kezeletlenül maradnak.

## Kockázatok értékelése

Ahogy azt korábban említettük, az EIR biztonsági osztályának megállapítása a 41/2015 BM rendelet 2. mellékletében felsorolt káresemények szempontjából kialakított ötfokozatú skálán, az EIR által kezelt adatok sérülésének és az ebből fakadó következményeknek, a szervezettel szembeni bizalomvesztésnek, illetve a közvetlen- és közvetett anyagi kár mértékének a megadott szintek alapján történő besorolásával történik.

***A kockázati tényezők származtatásakor nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetettségek által okozható kárt, káros hatást kell figyelembe venni***. Ezt a kockázati szorzótáblával tudjuk elérni. A szorzótábla sorát a fenyegetettség előfordulási valószínűsége, oszlopát a bizalmasság, sértetlenség és rendelkezésre állás szempontokhoz tartozó kárérték közül a legmagasabb kategória határozza meg.

Kockázati szorzótábla minta:

| **Kárérték szint** | **Előfordulási valószínűsége** | | | | |
| --- | --- | --- | --- | --- | --- |
| **1. nem értelmezhető** | **2. csekély** | **3. közepes** | **4. nagy** | **5. nagyon nagy** |
| **1. nem értelmezhető** | Alacsony | Alacsony | Alacsony | Közepes | Közepes |
| **2. csekély kár** | Alacsony | Alacsony | Közepes | Közepes | Közepes |
| **3. közepes kár** | Alacsony | Közepes | Közepes | Közepes | Magas |
| **4. nagy kár** | Közepes | Közepes | Közepes | Magas | Magas |
| **5. nagyon nagy kár** | Közepes | Közepes | Magas | Magas | Magas |

A káresemény mértékének a meghatározása során az adattípusokhoz és adatmennyiségekhez elsődlegesen a jogszabály, az összeghatárokhoz elsődlegesen a szervezet kockázatkezelési szabályzata szolgálhat forrásként. Az alábbiakban található kárérték táblázatok az NEIH honlapján 2019 márciusában kiadott [NEIH OVI] Osztályba sorolás és védelmi intézkedés űrlap v4.60 [[3]](#footnote-3) alapján készültek.

### Bizalmasság sérüléséből adódó kárérték megállapítása

A bizalmasság az adat arra vonatkozó tulajdonsága, hogy az adatot csak az arra jogosultak és csak a jogosultságuk mértékéig ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. A bizalmasság elsődlegesen a (különleges) személyes-, és üzleti adatokat kezelő EIR-eknél lehet fontos, tehát minden olyan esetben, ahol nem szeretnénk, ha az információ illetéktelen kezekbe kerülne.

Az EIR vagy az általa kezelt adatok bizalmasságának elvesztése esetén a kár mértéke[[4]](#footnote-4):

| **Kárérték szint/Kárfajta** | **Közvetlen anyagi kár** | **Társadalmi-politikai hatás** | **Bizalmasság sérülése** |
| --- | --- | --- | --- |
| **1. nem értelmezhető** | Az érintett szervezet költségvetéséhez képest jelentéktelen | Nincs bizalomvesztés, a probléma a szervezeten belül marad és meg is oldható | Elhanyagolható |
| **2. csekély kár** | Eléri a szervezet költségvetésének 1%-át | Az érintett szervezeten belül kezelhető | Belső szabályozóval védett adat vagy néhány személyes adat bizalmassága sérülhet.  Az üzlet vagy ügymenet szempontjából csekély értékű, és/vagy csak belső szabályzóval védett adat vagy EIR bizalmassága sérül. |
| **3. közepes kár** | Eléri a szervezet költségvetésének 5%-át | Bizalomvesztés a szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettség sérülhet | Nagy mértékű személyes adat bizalmassága vagy különleges adat bizalmassága sérülhet |
| **4. nagy kár** | Eléri a szervezet költségvetésének 10%-át | Jogszabályok betartása vagy végrehajtása elmaradhat, bizalomvesztés a szervezeten belül, a felső vezetésben vagy vezetésben személyi felelősségre vonást kell alkalmazni. | Tömeges különleges személyes adat bizalmassága sérülhet |
| **5. nagyon nagy kár** | Eléri a szervezet költségvetésének 15%-át | Súlyos bizalomvesztés a szervezettel szemben, alapvető emberi vagy társadalom működése szempontjából kiemelt jogok sérülhetnek. | Kiemelten tömeges különleges adat bizalmassága sérülhet |

### Sértetlenség sérüléséből adódó kárérték megállapítása

Az sértetlenség az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanság) is, illetve az EIR elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az EIR eleme rendeltetésének megfelelően használható́. A sértetlenség olyan EIR-eknél lehet vezető̋ szempont, ahol fontos, hogy a kezelt adatokat illetéktelenül senki ne változtathassa meg, pl. nemzeti adatvagyont kezelő EIR-ek, közhiteles nyilvántartások, mérő-, érzékelő rendszerek.

Az EIR vagy az általa kezelt adatok sértetlenségének elvesztése esetén a kár mértéke[[5]](#footnote-5):

|  |  |  |  |
| --- | --- | --- | --- |
| **Kárérték szint/Kárfajta** | **Közvetlen anyagi kár** | **Adat, információs rendszer sérülés** | **Társadalmi-politikai hatás** |
| **1. jelentéktelen kár** | Az érintett szervezet költésvetéséhez képest jelentéktelen | Az érintett szervezet költésvetéséhez képest jelentéktelen | A probléma a szervezeten belül marad és meg is oldható |
| **2. csekély kár** | Eléri a szervezet költségvetésének 1%-át | Az üzlet vagy ügymenet szempontjából csekély értékű, és/vagy csak belső szabályzóval védett adat, vagy EIR sérül. | A társadalmi hatás az érintett szervezeten belül kezelhető |
| **3. közepes kár** | Eléri a szervezet költségvetésének 5%-át | Az üzlet- vagy ügymenet szempontjából érzékeny folyamatokat kezelő EIR, információt képező adat vagy egyéb jogszabállyal védett adat sérül. | Bizalomvesztés a szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettség sérülhet |
| **4. nagy kár** | Eléri a szervezet költségvetésének 10%-át | Az üzlet- vagy ügymenet szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő EIR vagy információt képező adattömegesen, vagy jelentősen sérül | Jogszabályok betartása vagy végrehajtása elmaradhat, bizalomvesztés a szervezeten belül, a felső vezetésben vagy vezetésben személyi felelősségre vonást kell alkalmazni. |
| **5. nagyon nagy kár** | Eléri a szervezet költségvetésének 15%-át | A nemzeti adatvagyon helyreállíthatatlanul megsérül | Súlyos bizalomvesztés a szervezettel szemben, alapvető emberi vagy társadalom működése szempontjából kiemelt jogok sérülhetnek. |

### Rendelkezésre állás sérüléséből adódó kárérték megállapítása

A rendelkezésre állás az adat, illetve az EIR elemeinek olyan állapota, amelyben az az arra jogosultak által a szükséges időben és időtartamra használható́. Azoknál a EIR-eknél, ahol alapvető igény a működés fenntartása, pl. a létfontosságú EIR elemek és rendszerek a rendelkezésre állás kiemelt fontosságú.

Az EIR vagy az abban tárolt adatok rendelkezésre állásának elvesztése esetén (nem elérhető a rendszer vagy az adat) a kár mértéke[[6]](#footnote-6):

| **Kárérték szint/Kárfajta** | **Közvetlen anyagi kár** | **Társadalmi-politikai hatás** | **Rendelkezésre állás** |
| --- | --- | --- | --- |
| **1. jelentéktelen kár** | Az érintett szervezet költésvetéséhez képest jelentéktelen | A probléma a szervezeten belül marad és meg is oldható | Az érintett szervezet működése szempontjából jelentéktelen adat vagy EIR rendelkezésre állása nem biztosított. |
| **2. csekély kár** | Eléri a szervezet költségvetésének 1%-át | A társadalmi hatás az érintett szervezeten belül kezelhető | Az üzlet vagy ügymenet szempontjából csekély értékű, és/vagy csak belső szabályzóval védett adat vagy EIR rendelkezésre állása nem biztosított. |
| **3. közepes kár** | Eléri a szervezet költségvetésének 5%-át | Bizalomvesztés a szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettség sérülhet | Az üzlet- vagy ügymenet szempontjából érzékeny folyamatokat kezelő EIR, információt képező adat vagy egyéb jogszabállyal védett adat rendelkezésre állása nem biztosított. |
| **4. nagy kár** | Eléri a szervezet költségvetésének 10%-át | Jogszabályok betartása vagy végrehajtása elmaradhat, bizalomvesztés a szervezeten belül, a felső vezetésben vagy vezetésben személyi felelősségre vonást kell alkalmazni. | Az üzlet- vagy ügymenet szempontjából nagy értékű üzleti adat vagy EIR rendelkezésre állása nem biztosított. |
| **5. nagyon nagy kár** | Eléri a szervezet költségvetésének 15%-át | Súlyos bizalomvesztés a szervezettel szemben, alapvető emberi vagy társadalom működése szempontjából kiemelt jogok sérülhetnek.  Az ország, a társadalom működőképességének fenntartását biztosító EIR rendelkezésre állása nem biztosított. | Az ország, a társadalom működőképességének fenntartását biztosító létfontosságú EIR rendelkezésre állása nem biztosított; |

A következő lépésként - az előbbiekben felállított kárérték táblázatok felhasználásával - meg kell ítélnie az adatgazdának, hogy mekkora kár éri a szervezetet, hogy ha az EIR sértetlensége, rendelkezésre állása vagy az EIR-ben kezelt adat bizalmassága, sértetlensége vagy rendelkezésre állása sérül.

A táblázatunkat kiegészítettük három oszloppal (B- bizalmasság, S-sértetlenség, R- rendelkezésre állás), melyek a bizalmasság, sértetlenség és a rendelkezésre állás becsült kárérték szintjeit tartalmazzák.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Rendszer funkció** | **Támogatott folyamat** | **A rendszerben kezelt adatok** | **B** | **S** | **R** | **Besorolás indoklása** |
| Funkció X | Folyamat Y | Adatkör1 | **2** | **2** | **3** |  |

## EIR előzetes biztonsági osztályba sorolása

A kapott értékeket a maximum elv alapján összesíteni kell, úgy, hogy az alkalmazások bizalmasság, sértetlenség és rendelkezésre állás szerinti kárértékeit nem átlagoljuk, hanem azok maximumát vesszük. Az alkalmazás biztonsági osztályát összevonva úgy fejezzük ki, hogy a bizalmasság, sértetlenség, rendelkezésre állás hármasból a legnagyobb értéket vesszük.

Az alábbi táblázat egy mintát mutat az EIR és rendszerelemeinek biztonsági osztályainak meghatározásához:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A Rendszer által kezelt adatkörök** | **B** | **S** | **R** | **Az informatikai rendszer biztonsági osztálya** |
| Adatkör1 | 2 | 2 | 3 | 3 |
| Adatkör2 | 3 | 3 | 2 | 3 |
| Adatkör3 | 2 | 4 | 3 | 4 |
| Az EIR biztonsági osztálya | **3** | **4** | **3** | **4** |

Amellett, hogy az érintett szervezetre érvényes minden kötelezettséget figyelembe kell venni, az EIR kialakítása során implementálni kell és fent kell tartani a fenti folyamat eredményeként kapott biztonsági osztályhoz tartozó, 41/2015 BM rendelet 3. pontja szerinti védelmi intézkedés katalógusban meghatározott minimális követelményeket.

## Az előzetes biztonsági osztályba sorolás jóváhagyása és felülvizsgálata

Az EIR előzetes osztályba sorolás eredményét az érintett szervezet vezetőjének kell jóváhagynia. A szervezet vezetője felel azért, hogy az EIR biztonsági osztályának meghatározása megfelel a jogszabályoknak és kockázatoknak, valamint a besorolásban felhasznált adatok teljeskörűek.

A projekteken belül minden egyes újonnan implementálandó EIR esetében el kell végezni az előzetes biztonsági osztályba sorolást, illetve a projekt hatókörének, illetve a kezelt adatok körének minden változása esetén azt dokumentált módon felül kell vizsgálni.

A biztonsági osztályba sorolási kötelezettséget a jogszabály szerint a szervezet informatikai biztonsági szabályzatában elő kell írni, új EIR-ek implementálásának esetén az előzetes biztonsági osztályba sorolást a szervezeteknek célszerű a beszerzéssel, illetve a projekt menedzsmenttel kapcsolatos szabályozási környezetük részévé tenni, hogy ezzel is támogassák az információbiztonság növelésére tett törekvések hatékony irányításához és felügyeletéhez szükséges intézkedések hatékony megvalósítását.

A fejlesztendő EIR előzetes biztonsági osztályba sorolását úgy kell elvégezni, hogy abból a besorolás megfelelősége megítélhető legyen. Amennyiben a szervezet az előzőekben leírtaktól eltérő kockázatértékelési módszertant használ, a dokumentációnak tartalmazni kell a kockázatértékelés módszertani leírását és eredmény dokumentumát is.

Az információbiztonsági tervben szerepeltetni kell az elvégzett kockázatelemzés releváns adatait és következtetéseit, valamint az előzetes biztonsági osztályba sorolás eredményét.

1. GDPR 30. cikk. [↑](#footnote-ref-1)
2. 41/2015. BM rend. 1. melléklet 1.2 [↑](#footnote-ref-2)
3. https://nki.gov.hu/wp-content/uploads/2019/03/ovi460.xltm [↑](#footnote-ref-3)
4. NEIH által kiadott „Osztályba sorolás és védelmi intézkedés űrlap v4.60” – „Osztályba sorolás” munkalap [↑](#footnote-ref-4)
5. NEIH által kiadott „Osztályba sorolás és védelmi intézkedés űrlap v4.60” – „Osztályba sorolás” munkalap [↑](#footnote-ref-5)
6. NEIH által kiadott „Osztályba sorolás és védelmi intézkedés űrlap v4.60” – „Osztályba sorolás” munkalap [↑](#footnote-ref-6)