

BUDAPEST FŐVÁROS XV. KERÜLETI ÖNKORMÁNYZAT
JEGYZŐJE

BUDAPEST FŐVÁROS XV. KERÜLETI ÖNKORMÁNYZAT
JEGYZŐJÉNEK

18/2020. (VI.24.) SZÁMÚ

UTASÍTÁSA

AZ INTEGRÁLT KOCKÁZATKEZELÉSI SZABÁLYZATRÓL

Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 119. § (3) bekezdésében biztosított jogkörömben eljárva, a Budapest Főváros XV. kerületi Polgármesteri Hivatalra (továbbiakban: Hivatal), a Budapest Főváros XV. kerületi Önkormányzatra és a Budapest Főváros XV. kerületi Nemzetiségi Önkormányzatokra (továbbiakban Önkormányzat) vonatkozó integrált kockázatkezelési tevékenységgel összefüggő szabályokat a helyi sajátosságok figyelembevételével - az államháztartásról szóló 2011. évi CXCV. törvény (Áht.), az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.), az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (továbbiakban: technológiai vhr), a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről szóló 370/2011. (XII. 31.) Korm. rendelet (továbbiakban Bkr.), valamint az államháztartásért felelős miniszter által közzétett módszertani útmutatókban foglaltakra figyelemmel - az alábbiak szerint szabályozom.

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályzat célja, érvényessége, alapelvek

1.1. A szabályzat célja

- (1) A szabályzat célja a Hivatal, az Önkormányzat és a Nemzetiségi Önkormányzatok integrált kockázatkezelési eljárásának a szabályozása, mely a kockázati tényezők meghatározására, azok értékelésére, a kockázatokra adott válaszreakciókra, a kockázatok felülvizsgálatára, az ezzel összefüggő feladatokat ellátók hatáskörére, felelősségre és a dokumentálás rendjére terjed ki.
- (2) Megfelelő kockázatkezelési tevékenység révén csökkenthetőek a kockázatok hatásai, illetve megelőzhető a feltárt kockázatok tényleges bekövetkezése a Hivatal, az Önkormányzat és a Nemzetiségi Önkormányzatok által kitűzött célok megvalósítása érdekében.
- (3) A szabályzat rendelkezései arra irányulnak, hogy az Áht., az Ibtv., a technológiai vhr, a Bkr. és egyéb jogszabályok, módszertani útmutatók előírásai, követelményei érvényesüljenek.

1.2. A szabályzat hatálya

- (1) A szabályzat hatálya az Önkormányzatra, a Hivatalra és a Nemzetiségi Önkormányzatokra terjed ki.
- (2) A szabályzat tárgyi hatálya a Hivatal, az Önkormányzat és a Nemzetiségi Önkormányzatok kockázatkezelésével összefüggő munkafolyamatokra, azok végrehajtása során kifejtett tevékenységekre terjed ki. A tárgyi hatály kiterjed továbbá a Hivatal által működtetett elektronikus információs rendszerekre.

1.3. Az integrált kockázatkezelés során érvényesítendő alapelvek

- (1) A rendszerszemlélet elvének érvényre jutása érdekében a jegyző az Önkormányzat, a Nemzetiségi Önkormányzatok és a Hivatal valamennyi tevékenységére kiterjedő integrált kockázatkezelési rendszert alakít ki és működtet.
- (2) Az alkalmazott módszerek megválasztásának szabadsága alapján a jegyző a kialakított célokhoz és sajátosságokhoz legteljesebb mértékben illeszkedő kockázatkezelési módszert alkalmazza.

Értelmező rendelkezések

- a) *Belső kontrollrendszer:* a szervezeti célok megvalósítását segítő eszközök összessége. Egymásra épülő és egymást kiegészítő elemei a kontrollkörnyezet, az integrált kockázatkezelési rendszer, a kontrolltevékenységek, az információs- és kommunikációs rendszer valamint a monitoring.
- b) *Folyamatgazda:* az adott folyamatleírás létrehozásáért felelős személy, aki általában is felel a folyamat kialakításáért, dokumentálásáért és fejlesztéséért, valamint ellátja a folyamatok kockázatainak felmérését, azonosítását, elemzését, továbbá javaslatot tesz a feltárt kockázatok kezelésére.
- c) *Főfolyamat:* a szervezet által végzett tevékenységek legnagyobb csoportjai, általában szervezeti – külső és belső – funkciókkal azonosítható.
- d) *Integrált kockázatkezelési intézkedési terv:* az integrált kockázatkezelési folyamat eredményeként létrejövő kockázatkezelési intézkedési terv, amely a szervezet céljaival kapcsolatos valamennyi olyan kockázat kezelését magában foglalja, amelyek kezelése a szervezet kockázati tűréshatárára tekintettel indokolt.
- e) *Integrált kockázatkezelési koordinátor:* a Bkr. 7. § (4) bekezdése alapján az integrált kockázatkezelési rendszer koordinálására kijelölt szervezeti felelős.
- f) *Integrált kockázatkezelési rendszer:* olyan folyamat alapú kockázatkezelési rendszer, amely a Hivatal minden tevékenységére kiterjed, egységes módszertan és eljárások alkalmazásával, a Hivatal és az Önkormányzat célkitűzéseinek és értékeinek figyelembevételével biztosítja a Hivatal kockázatainak teljes körű azonosítását, azok meghatározott kritériumok szerinti értékelését, valamint a kockázatok kezelésére vonatkozó intézkedési terv elkészítését és az abban foglaltak nyomán követését.
- g) *Interjú:* két vagy több ember beszélgetése, melynek célja, hogy az interjú készítői az interjú alanyától információkat nyerjenek egy meghatározott témakörben.
- h) *Kérdőív:* adatgyűjtési eszköz, amely az adatközlők válaszainak rögzítésére szolgál, általában strukturált, előre rögzített kérdéssorok mentén.
- i) *Kiscsoportos beszélgetés:* egyszeri moderált brainstorming a kockázatok azonosítása érdekében.
- j) *Kockázat:* a jövőben valamilyen valószínűséggel bekövetkező esemény, ami bizonyos mértékben, negatív vagy pozitív irányban befolyásolja a szervezeti célok elérését.
- k) *Kockázatelemzés:* objektív módszer az ellenőrizendő területek kiválasztására, mely meghatározza a költségvetési szerv tevékenységében és belső kontrollrendszerében rejlő kockázatokat.
- l) *Kockázati tényező:* kockázat okaként azonosítható körülmény.
- m) *Kockázatkezelési stratégia:* egyes kockázatokkal kapcsolatos, tudatosan választott magatartás.
- n) *Kockázati tűréshatár:* a kockázati kitettségnek az a szintje, amely felett a hivatali szervezet vezetője mindenképpen válaszintézkedést kíván tenni a felmerülő kockázatokra.

- o) *Kontrollkörnyezet*: a vezetők és alkalmazottak belső kontrollokhoz való viszonyának, tudatosságának külső szemlélő számára megfigyelhető jelei. A kontrollkörnyezet magában foglalja az egyéni és szervezeti integritás fejlesztését, az etikai értékeket, az érintettek szakmai kompetenciáját, a szervezet vezetésének filozófiáját és stílusát, a felelősségi körök kijelölésének, a beszámoltatásnak, valamint teljesítményértékelésnek a módszereit, továbbá a vezetők vezetési tevékenységének minőségét. Beletartoznak ugyanakkor a szervezet tevékenységét szabályozó intézkedések, a szabályozók rendszere és a szervezetet leíró dokumentumok is.
- p) *Kontrolltevékenység*: mindazok az eljárások, amelyek biztosítják, hogy a vezetés által megfogalmazott célok és elvárások végrehajtásra kerüljenek, és az azokat veszélyeztető kockázatokat a tevékenység során a szervezet kezelje. A kontrolltevékenységek a kockázatok kezelésének eszközei.
- q) *Korrupció*: a Büntető Törvénykönyvről szóló 2012. évi C. törvény XXVII. Fejezetén belüli tényállások és ezen belül a kötelezettség vagy joggyakorlás elmulasztásának, hivatali helyzettel való visszaélésnek, a hatáskör túllépésének ígérete, megtörténte vagy erre vonatkozó felhívás megfogalmazása jogtalan előny ellenében vagy ennek reményében.r)
Monitoring: nyomon követési mechanizmusok rendszere, amely lehetővé teszi, hogy a folyamatok és a belső kontrollrendszer folyamatos megfigyelés és értékelés alatt álljon, így a szervezet kontrollrendszere rugalmasan tud reagálni a változó külső és belső körülményekhez.
- s) *Projekt*: egy olyan egyedi folyamatrendszer, amely kezelési és befejezési időpontokkal megjelölt, specifikus követelményeknek - határidő, költség, erőforrás - megfelelő célkitűzés elérése érdekében vállalt, koordinált és kontrollált tevékenységek csoportja. Az építési beruházások tekintetében projektnek tekintendő a költségvetésben biztosított forrás alapján, meghatározott időkeretben, új épület megépítése, vagy nagyobb, mint 400 m² össz. bruttó szintterületű meglévő épület átalakítása, felújítása érdekében végzett elsősorban építésügyi, másodsorban gazdasági és jogi tevékenységek összessége.
- t) *Részfolyamat*: egy főfolyamatba tartozó, elkülönülő eredménnyel járó, egymáshoz kapcsolódó tevékenységek láncolata.
- u) *Valószínűség*: egy esemény bekövetkezésének esélye.
- v) *Vezetői nyilatkozat*: a Bkr. 11. § (1) bekezdése által előírt, a Bkr. 1. melléklete szerinti, a belső kontrollrendszer működéséről szóló vezetői nyilatkozat.

2. A kockázat fogalma, típusai

3.1. A kockázat fogalma

- (1) A kockázat *szűkebb értelemben* a kitűzött célokat veszélyeztető tényező.
- (2) A kockázat *tágabb értelemben* valamely esemény, tevékenység vagy annak elmulasztása, amelyek bekövetkezése általában negatív, de egyes esetekben pozitív hatással lehet a kitűzött célok elérésére.
- (3) *A kockázat lehet:*
 - a) véletlenszerű esemény,
 - b) hiányos ismeret vagy információ,
 - c) az ellenőrzés hiánya, illetve gyengesége,
 - d) a vezetés magatartása.

3.2. A kockázatok típusai

- (1) *A szervezetet érintő kockázatok*
 - a) *Eredendő kockázat:* a szervezet által nem befolyásolható, többnyire külső kockázatok.
 - b) *Belső kontroll kockázat:* a költségvetési szerv belső kontroll rendszerének nem megfelelő kialakítása, illetve működtetése miatt fellépő kockázat (ha a szerv a saját hibájából nem képes, vagy tudatosan nem tárja fel, illetve nem előzi meg a hibákat, szabálytalanságokat).
 - c) *Megmaradó kockázat:* a vezetés által tudatosan elfogadott kockázatok.
 - d) *Információbiztonsági kockázat:* a Hivatal elektronikus információs rendszereire ható nemkívánatos események bekövetkezési valószínűsége szorozva az okozott kár mértékével.
- (2) *Szervezetet működésének fontosabb kockázati tényezői*
 - a) *Külső eredetű, környezeti kockázatok:* függetlenek a szerv működésétől, de bekövetkezésükre a Hivatal megfelelő stratégiával képes felkészülni, hatásait mérsékelni és/vagy kiküszöbölni.
 - b) *Belső működési kockázatok:* a szervezet működésének, tevékenységének, folyamatainak velejárói, melyek kiküszöbölése, vagy mérséklése a vezetéssel szemben támasztott követelmény.
- (3) A fontosabb kockázati kategóriákat az 1. számú függelék tartalmazza azzal a kitéttel, hogy a kategóriákhoz tartozóan felsorolt kockázatok nem taxatívák, azok időről időre változhatnak, bővíthetnek, kikerülhetnek a felsorolásból.

II. FEJEZET

AZ INTEGRÁLT KOCKÁZATKEZELÉS RENDJE

1. A kockázatkezelési hatókör

- (1) A kockázatelemzés felöleli az Önkormányzat, a Nemzetiségi Önkormányzatok és a Hivatal teljes tevékenységi területét.

2. A kockázatkezelői szintek

- (1) A **jegyző** felelős a belső kontrollrendszer keretében - a szervezet minden szintjén érvényesülő – megfelelő kontrollkörnyezet, integrált kockázatkezelési rendszer, kontrolltevékenységek, információs és kommunikációs rendszer és nyomon követési rendszer (monitoring) kialakításáért, működtetéséért és fejlesztéséért. (Bkr. 3.§)
- (2) A **Hivatal dolgozói** saját munkaterületükön aktívan közreműködnek a tevékenységek kockázati szempontú vizsgálatában és kezelésében. A munkavállaló köteles munkaköri feladatát megfelelő szakmai hozzáértéssel ellátni, valamint az irányadó jogszabályok, szabályzatok és vezetői utasítások betartásával hozzájárulni a tevékenységi kockázatok csökkentéséhez, továbbá a vezetője felé köteles jelezni a tudomására jutott, veszélyeztető eseményeket.
- (3) A **folyamatgazdák** végzik a felelősségi körükbe tartozó folyamatok kockázatainak beazonosítását, elemzését és értékelését - a Kockázatkezelő Munkacsoport ajánlásai alapján-, az elemzések eredményét megosztják az önálló szervezeti egység vezetőjével és javaslatot tesznek a kockázatok kezelésére.

- (4) Az **önálló szervezeti egységek vezetői** saját hatáskörön belül, a rendelkezésre álló eszközökkel kezelik a szervezeti egységet érintő kockázatokat, melynek keretében meghatározzák a kockázatviselési hajlandóságot és a kockázatra adott válaszokat azon kockázatok esetében, amelyet a saját szintjükön képesek kezelni.
- (5) A hivatali, önkormányzati, illetve nemzetiségi önkormányzati szintű kockázatokat a **Kockázatkezelő Munkacsoport** (továbbiakban: Munkacsoport) elemzi, kezeli.
- (6) Az **integrált kockázatkezelési koordinátor**, az integrált kockázatkezelési rendszer koordinálására kijelölt szervezeti felelősként segíti a jegyző, a Munkacsoport és a szervezeti egységek munkáját.
- (7) A Hivatal által megbízott **elektronikus információs rendszerek biztonságáért felelős személy** (továbbiakban: IBF) végzi az információbiztonsági kockázatelemzést együttműködve a jelen fejezetben rögzített szerepekkel.

3. A kockázatkezelési rendszer felelősei

- (1) A Bkr. szerint a jegyző felelőssége és kötelessége a kockázati tényezők, elemek azonosítása, a kockázati hatás mérése, a kockázatok bekövetkezésének valószínűsítése, és ennek a valószínűségnek a szervezet tűréshatárán belüli szintre történő csökkentése, illetve a bekövetkezés megelőzése.
- (2) Az önálló szervezeti egységek vezetői felelnek a saját szervezeti egységük hatáskörébe tartozó folyamatok, tevékenységek kockázatainak felismeréséért, kezeléséért. Amennyiben a kockázat meghaladja a szervezeti egység hatáskörét, illetve az szervezeten belül nem kezelhető - a kockázat hatásának jelentőségétől függően - azonnal értesítik az integrált kockázatkezelési koordinátoron keresztül a Munkacsoportot.
- (3) Az önálló szervezeti egységen belül kijelölt folyamatgazda felelős az általa irányított folyamatok, tevékenységek kockázatainak felméréséért, értékeléséért és kezelésének előkészítéséért, illetve végrehajtásáért.
- (4) A Munkacsoport készíti el a célkitűzések végrehajtását akadályozó kockázatok elemzését (azonosítás, értékelés), annak kezelési módját. A Munkacsoport meghatározza, hogy milyen mértékű kockázattal lehet számolni, és a meghatározott kockázati mérték függvényében milyen intézkedéseket kell végrehajtani.
- (5) Az integrált kockázatkezelési koordinátor az integrált kockázatkezelési rendszer működését koordinálja és kezeli a dokumentumokat.
- (6) A Hivatal által megbízott elektronikus információs rendszerek biztonságáért felelős személy végzi az információbiztonsági kockázatelemzést.
- (7) A jegyző az integrált kockázatkezelési feladatellátásban részt vevő személyek számára biztosítja a szükséges feltételeket.
- (8) A kockázatkezelési tevékenység feladat és hatáskörét a szabályzat és a munkaköri leírások tartalmazzák.

4. A Kockázatkezelő Munkacsoport szervezete, működése, feladatai

4.1 A Kockázatkezelő Munkacsoport szervezete, működése

- (1) A Munkacsoport vezetője a jegyző.
- (2) A Munkacsoport tagjai:
 - az aljegyző,
 - az önálló szervezeti egységek vezetői,
 - a humánpolitikai feladatokat ellátó szervezeti egység vezetője,
 - a minőségügyi vezető,
 - a Hivatal nemzetiségi referense,
 - az integrált kockázatkezelési koordinátor, valamint
 - az IBF.
- (3) A Munkacsoport titkári feladatait, az üléseinek dokumentációját, a kockázatok nyilvántartását az integrált kockázatkezelési koordinátor végzi.
- (4) A Munkacsoport a kockázatelemzés módszertanát évente felülvizsgálja, szükség szerint aktualizálja és jóváhagyja, valamint kialakítja a kockázatkezelési stratégiát.
- (5) A belső ellenőrzés megfigyelőként vehet részt a Munkacsoport munkájában, tanácsadói tevékenysége keretében független értékelés nyújtásával segítheti a munkát.

4.2. A Kockázatkezelési Munkacsoport kiemelt feladatai:

- (1) Feladatát képezi a kockázatok feltárása, elemzése, értékelése, a kockázati tűréshatárok meghatározása, a belső ellenőrzési feladatokat ellátó szervezeti egység és a külső ellenőrző szerv által feltárt kockázatok elemzése, valamint javaslattétel a kockázatkezelésre vonatkozóan.
- (2) Az önálló szervezeti egységek szintjén nem kezelhető kockázatok esetében elvégzi a kockázatok értékelését, csoportosítását és rendszerezését, a delegált kockázatok tűréshatárát meghatározza és kialakítja a kockázatok kezelésének stratégiáját.
- (3) Felülvizsgálja az egyes szervezeti egységek által elkészített elemzéseket és intézkedési javaslatokat – ezeket összefoglalja és felterjeszti a jegyzőnek jóváhagyásra.
- (4) A kockázatkezelési folyamatok előírása, feltételeinek biztosítása és betartásának megkövetelése, továbbá az integrált kockázatkezelési folyamatba épített ellenőrzés.
- (5) A kockázatokkal kapcsolatos információk folyamatos szolgáltatása az integrált kockázatkezelési koordinátoron keresztül.
- (6) A Hivatal és az Önkormányzat egészét átfogó kockázatkezelési intézkedési terv kialakítása, javaslatok megfogalmazása.
- (7) A kockázatkezeléssel kapcsolatos elszámoltathatóság biztosítása.
- (8) Az integrált kockázatkezelési intézkedési terv előkészítése a jegyző általi aláírásra, illetve intézkedésre. Az integrált kockázatkezelési intézkedési terv végrehajtásának a nyomon követése, értékelése.
- (9) Évente legalább egyszer, január 31-ig felülvizsgálja az előző évi integrált kockázatkezelési intézkedési tervek megvalósulását és arról beszámolót készít a jegyző felé.

5. Az integrált kockázatkezelési koordinátor feladatai

- (1) A jegyző által kijelölt szervezeti felelősként az integrált kockázatkezelési rendszer működését koordinálja (technikai és személyorientált koordináció).

- (2) Szakértői tevékenységet végez, amelyben megismerteti az érintettekkel az integrált kockázatkezelési tevékenység tartalmát, továbbá szakmai támogatást biztosít a kockázatkezelési lépések szakmailag megfelelő végrehajtásához.
- (3) Biztosítja a szervezeti kommunikációt az integrált kockázatkezelési folyamatban résztvevők számára.
- (4) Ellátja a Munkacsoport tevékenységével kapcsolatos ügyviteli feladatokat.
- (5) Az integrált kockázatkezelés dokumentumainak kezelése, a kockázatok nyilvántartása.

III. FEJEZET

A KOCKÁZATKEZELÉS VÉGREHAJTÁSÁNAK SZABÁLYAI

1. A kockázatkezelés folyamata

- (1) A kockázatkezelés egy állandóan változó folyamat, az Önkormányzat, a Hivatal és a Nemzetiségi Önkormányzatok céljai elérésével kapcsolatos kockázatok azonosításának és elemzésének, valamint a megfelelő válaszok meghatározásának folyamata.
- (2) Az integrált kockázatkezelés keretében meg kell állapítani az Önkormányzat, a Nemzetiségi Önkormányzatok és a Hivatal tevékenységében, gazdálkodásában rejlő kockázatokat, meg kell határozni az egyes kockázatokkal kapcsolatban a szükséges intézkedéseket, valamint azok teljesítésének folyamatos nyomon követésének a módját.
- (3) *A kockázatkezelés az alábbi lépéseket tartalmazza:*
- (4) *A kockázatok azonosítása/feltárása*, melyek a működést, a kiemelt célok elérését veszélyeztetik, valamint az azokhoz kapcsolható keretek meghatározása.
- (5) *A kockázatok elemzése, kiértékelése és rangsorolása* jellegük, felmerülési helyük, hatásuk súlyossága és bekövetkezési valószínűségük szerint.
- (6) *Az elfogadható kockázati szint (kockázati tűréshatár) meghatározása.* Az Önkormányzat, a Nemzetiségi Önkormányzatok és a Hivatal egészére, valamint azon belül a Hivatal egyes szervezeti egységeire vonatkozó ún. „tűréshatárok” meghatározása, amelyek felett intézkedéseket kell fogantatni.
- (7) *A kockázatok kezelésére kockázatkezelő javaslatok megfogalmazása, döntés a kockázatok kezeléséről:* a kockázatokat, illetve hatásukat milyen módon kívánja a vezetés mérsékelni, elkerülni, és/vagy bekövetkezési valószínűségüket csökkenteni, a kockázatkezelési stratégia meghatározása. *A válaszintézkedések beépítése az integrált kockázatkezelési intézkedési tervekbe.*
- (8) *Az integrált kockázatkezelési intézkedési tervek megvalósítása, a kockázatok és a kockázatokra kialakított válaszok folyamatos monitoringja.*

2. A kockázatok azonosítása, feltárása

- (1) A kockázat azonosítás célja annak megállapítása, hogy melyek az Önkormányzat, a Nemzetiségi Önkormányzatok és a Hivatal célkitűzéseit veszélyeztető fő kockázatok.
- (2) A kockázatokat minden esetben a célokhoz kapcsolódóan a szervezet egészére nézve és az egyes folyamatokhoz kapcsolódóan is azonosítani kell. A kockázatok azonosításakor az eredendő kockázatokat kell feltárni.
- (3) Alapvető követelmény a szervezetet érintő valamennyi kockázat (támogató és funkcionális folyamatok kockázatainak) beazonosítása és a szerv vezetése általi megismertetése.
- (4) A kockázat beazonosításának folyamatához elengedhetetlen a célkitűzések alapos ismerete, a legmagasabb céloktól egészen a napi működés céljainak szintjéig.

- (5) Az azonosítás meghatározó eleme a tevékenység jellege. A kockázatokat ezen ismeretek alapján lehet felismerni, azonosítani, illetve az egyes kategóriák mentén csoportosítani.
- (6) A kockázatok felmérését a folyamatleírások mentén kell előkészíteni.
- (7) A kockázatok azonosítását célszerű csoportmunkában folyamatonként, az adott folyamatban résztvevők bevonásával megszervezni, lebonyolítani – integrált kockázati leltár kialakításával. A csoportmunka mellett kiegészítő technikaként alkalmazható az interjú, a kérdőív és a kics csoportos megbeszélés.
- (8) A projekteket külön egységként kell kezelni a kockázatkezelési rendszerben.
- (9) A stratégiai jellegű kockázatok feltárása a Munkacsoport feladata.
- (10) A vezetésnek gondoskodnia kell egy naprakész nyilvántartási rendszer kialakításáról az Integrált Kockázati Leltár létrehozásával, amely alkalmas a kockázatok nyilvántartására és változásainak folyamatos nyomon követésére.
- (11) *A kockázatok beazonosításának folyamata:*
- *A folyamatgazda a felügyelete alá tartozó folyamatokra vonatkozóan - a Munkacsoport ajánlásából kiindulva - munkatársai bevonásával elvégzi a folyamatok (főfolyamatok, részfolyamatok) kockázatainak feltárását és azonosítását. (A folyamatokra jellemző kockázati kategóriák értékelésére, meghatározására az 1. számú függelék szolgál segítségül.)*
 - *Az önálló szervezeti egységek vezetői felülvizsgálják a folyamatgazda által összegyűjtött folyamatokat, és a hozzájuk tartozó kockázati kategóriákat. Ennek során bővíthetik a folyamatokat, illetve a kiemelt kockázatok körét, vagy abból az általuk felügyelt szervezet számára nem releváns kockázatokat el is hagyhatják.*
 - *A kockázatok azonosításának eredményeképpen el kell készíteni szintenként az Integrált Kockázati Leltárt, amibe minden azonosított kockázatot fel kell vezetni.*
 - *A Munkacsoport feladata a különböző szinteken azonosított kockázatok rendszerezése, az esetleges duplikációk kiszűrése, valamint a kockázatok rangsorolása, továbbá az integrált kockázati leltár kezelése.*
 - *A kockázatok feltárását és beazonosítását minden év február 28-ig kell elvégezni.*
- (12) *A kockázatelemzés során beazonosított kockázatok három főbb kategóriába sorolhatók:*
- a) *Hivatali, önkormányzati, illetve nemzetiségi önkormányzatiszintű kockázatok:* A Munkacsoport által beazonosított kockázatok, melyek kezeléséről a Munkacsoport dönt.
 - b) *Kiemelt kockázatok:* Olyan magas bekövetkezési hatással bíró hivatali, illetve önkormányzati, illetve nemzetiségi önkormányzati kockázatok, melyeket valamennyi önálló szervezeti egység vezetőnek kötelező elemeznie és ezekre vonatkozóan intézkedési tervet kell készíteniük.
 - c) *A szervezeti egység szintjén a folyamatgazdák által beazonosított kockázatok:* A folyamatgazdák által beazonosított olyan további kockázatok, amely speciálisan az ő szakmai feladatukra, gazdálkodási körükre vonatkozik.
- (13) Az információbiztonsági kockázatelemzés elvégzéséhez fel kell mérni, meg kell ismerni az elektronikus információs rendszereket és azok környezetét, valamint azok jelenlegi információbiztonsági szintjét.
- (14) A következő területeket kell a dokumentációk bekérésével, illetve szakmai interjúk lefolytatásával megismerni:
- a) Adminisztratív védelmi intézkedések
 - i. A Hivatalra vonatkozó jogszabályok, szabályzatok
 - ii. Az elektronikus információs rendszerre vonatkozó szabályzatok
 - iii. Szerződések, külső felek kezelése
 - iv. Alkalmazásfejlesztés, változáskezelés

- v. Jogosultságigénylés
 - vi. Biztonsági események kezelése
 - vii. Üzemeltetési eljárások
 - viii. Szervizelés, eszközcsere, selejtezés
- b) Logikai védelmi intézkedések
- i. Mentési megoldások
 - ii. Kártékony kód elleni védekezés
 - iii. Biztonsági frissítések telepítése
 - iv. Hálózat felépítése
 - v. Biztonsági rendszerek
 - vi. Kriptográfiai megoldások
- c) Fizikai biztonság
- i. Beléptetés
 - ii. Számítógépterem kialakítása
 - iii. Épületben történő közlekedés
 - iv. Irodák kialakítása, tiszta asztal, üres képernyő politika.
- (15) Az informatikai erőforrásokra ható fenyegetettségek vagy fenyegető tényezők (például: üzleti hírszerzés, rosszindulatú hackerek, természeti katasztrófák) mindig a sérülékeny pontokon keresztül fejtik ki hatásukat, így az ellenük való védekezés legfőbb eleme a sérülékenységek azonosítása és megszüntetése.
- (16) A sérülékenység egy bizonyos gyenge pont kihasználása a rá ható fenyegetettség által. Meg kell vizsgálni, hogy a beazonosított gyenge pontokon keresztül mely fenyegetettségek tudják kifejteni a káros hatásukat.

3. A kockázatok elemzése, kiértékelése és rangsorolása

- (1) A kockázatok elemzésének célja annak megállapítása, hogy a beazonosított kockázatok milyen mértékben befolyásolják a Hivatal, az Önkormányzat és a Nemzetiségi Önkormányzatok fő célkitűzéseit.
- (2) A kockázatelemzés során, a kockázatok azonosítását követően el kell végezni a kockázatoknak a kockázati tényezőkre való visszavezetését és a kockázati tényezők közötti összefüggések feltárását.
- (3) A kockázatok elemzését kockázatkezelési szintenként (folyamatgazda, szervezeti egység vezetője, Munkacsoport) kell elvégezni, lehetőség szerint csapatmunkában.
- (4) Az elemzés során alkalmazott értékelési kritériumok egységes értelmezése és alkalmazása érdekében, a szervezetre jellemző kockázati tényezők alapján *Kockázatértékelési Kritérium Mátrixot* kell kialakítani, melyről a Munkacsoport dönt.
- (5) Az értékelés során meg kell határozni a feltárt kockázati tényezők bekövetkezésének valószínűsítését, illetve a szervezetre gyakorolt hatását.
- (6) A beazonosított kockázati tényezőkről tájékoztatni kell azokat a dolgozókat és vezetőket, akiknek a tevékenységét az adott kockázat érinti.
- (7) A hivatali és önkormányzati szintű *kockázatok rangsorolását* a Munkacsoport végzi.
- (8) A kockázatok elemzését és értékelését tárgyév március 31-ig kell elvégezni.

4. Elfogadható kockázati szint (tűrészhatár) meghatározása

- (1) A fő kockázati prioritások meghatározásához figyelembe kell venni a Hivatal, az Önkormányzat és adott Nemzetiségi Önkormányzat adott kockázattal szembeni tűrőképességét.
- (2) A tűrészhatár a kockázati kitettségnek azt a szintjét jelenti, amire az érintett szervezet vezetése mindenképpen válaszingédkedést kíván tenni.
- (3) A tűrészhatárokat a szervezet minden szintjén ismertté kell tenni az érintettek azonosulása érdekében, amely alapot biztosít a releváns kockázatok mennyiségi és minőségi méréséhez, valamint a szükséges válaszlépések meghozatalához.
- (4) A kockázattűrő képesség meghatározása a megfelelő kockázati stratégia kialakításának elengedhetetlen feltétele.
- (5) *A kockázati tűrészhatárokat a következő csoportok szerint lehet értelmezni:*
 - a) *Hivatali, önkormányzati, nemzetiségi önkormányzati szintű kockázati tűrészhatár:* Az egész szervezetre vonatkozó összes kockázat mértékét figyelembe véve kerül kialakításra. A Munkacsoport megítéli a kockázatoknak való kitettség elfogadható mértékét, és egy általános tolerancia szintet határoz meg a szervezet számára, amely egészének működése során felmerülő kockázatokra vonatkozó kockázati tűrészhatárt jelenti.
 - b) *Delegált kockázati tűrészhatár:* A szervezet egészére megállapított kockázati tűrészhatárt alapul véve kerül meghatározásra, hogy az egyes folyamatok vonatkozásában vagy szervezeti szinteken a kockázatoknak még mekkora mértéke fogadható el.
 - c) *Projekt kockázati tűrészhatár:* A projektekre vonatkozó tűrészhatárt is a szervezet egészére megállapított kockázati tűrészhatár figyelembe vételével kell meghatározni. A projekt időtartama alatt változhat az elfogadhatónak ítélt kockázat mértéke.
- (6) *A tűrészhatárok meghatározásánál figyelembe veendők:*
 - a) A gyakorlati tapasztalatok alapján mindenképpen kezelendők azok a kockázatok, amelyeknek ugyan kicsi a bekövetkezési valószínűségük, de a hatásuk nagy.
 - b) Azok a kockázatok, amelyeknek nagy a bekövetkezési valószínűségük, de a hatásuk minimális, nem feltétlenül kezelendők. Ez alól kivételt képez, ha év közben a gyakori bekövetkezés miatt a veszteség olyan mértékűvé válik, amely meghaladja az adott területre meghatározott tolerancia szintjét.
- (7) A kockázati tűrészhatárt a Munkacsoport határozza meg.
- (8) Információbiztonsági szempontból minden közepes, illetve annál magasabb kockázatot kezelni szükséges.

5. A kockázatokra adott válaszreakciók, a kockázatkezelés módszerei

- (1) A szervezet vezetésének rendelkeznie kell olyan eszközökkel, amelyekkel képes a szervezet működését érintő, negatív hatású kockázatos eseményeket felismerni, és azok racionálisan csoportosítását követően meghatározni a szükséges válaszreakciókat (válaszlépéseket).
- (2) A kockázati tűrészhatárt meghaladó kockázatok esetében kockázatkezelő szintenként, a kockázatkezelői szinteken kockázatonként megfelelő kockázatkezelési stratégiákat kell meghatározni, a felelősök és a végrehajtási határidők megjelölésével.
- (3) A kockázatkezelési stratégiákat a várható kockázatsökkentő hatásuk és megvalósítási költségük összevetésével kell értékelni. Az intézkedéseket az eredményesség, hatékonyság, gazdaságosság követelményeit figyelembe véve kell meghatározni.

- (4) A vezetésnek a válaszlépés melletti döntés meghozatalakor, figyelemmel kell lennie arra, hogy az adott kockázat:
- milyen mértékű hatást gyakorol a Hivatalra, az Önkormányzatra, illetve a Nemzetiségi Önkormányzatokra
 - a célhierarchia melyik szintjét érinti,
 - melyik folyamatba van beágyazva,
 - mely szervezeti egységek vesznek részt a válaszlépésben,
 - milyen anyagi ráfordítással jár a választott megoldás,
 - milyen eredményt várnak a válaszlépéstől.
- (5) *A kockázatkezelés módszerei (a teljesség igénye nélkül)*
- a) *A kockázat megszüntetése, elkerülése:* A módszer alapvetően a kockázati események bekövetkezésének kivédését, illetve a gyors felfedezését szolgáló eljárásokat foglalja magában. Akkor alkalmazandó, ha az adott kockázati tényező gyakran következik be, és bekövetkezése esetén a hatása jelentős. A hivatali és az önkormányzati tevékenységek (folyamatok) megszüntetésének, áthárításának jogszabályi korlátai miatt ez nem, vagy csak kivételes esetekben alkalmazható.
- b) *A kockázat kezelése, csökkentése:* A legtöbb kockázat esetében alkalmazható módszer, melynek célja a kialakított módszerek, technikák és eszközök alkalmazásával a kockázatelemzés eredménye alapján megfogalmazott kockázati kitettség csökkentése, a vezetés által tudatosan vállalható kockázati kitettség (tűrőhatáron belüli) szintjére. Irányulhat a kockázat bekövetkezési valószínűségének befolyásolására, a kockázat bekövetkezésének lehetőségére való felkészülésre (a várható hatás mértékének meghatározása), azon keresztül a reagáló képesség növelésére, illetve a kockázatok hatásának mérséklésére, a folyamatokba beépített kontrollok felhasználásával.
- c) *A kockázat megosztása, áthárítás:* A kockázat bekövetkezésének valószínűsége nem csökken, hatása nem változik, azonban a kockázatviselő személye módosul (pl.: kiszervezés, biztosítás).
- d) *A kockázat elviselése, elfogadása:* Alkalmazása esetén a vezetés dönthet úgy, hogy nem tesz intézkedéseket a kockázat csökkentésére, mert:
- a szervezet kialakult működési rendjében az adott kockázat hatásának kiküszöbölése, vagy csökkentése többbe kerülne, mint a kockázatos tevékenységből származó lehetséges kár, vagy
 - a kockázatkezelés személyi, technikai akadályokba, idő-, illetve anyagi korlátba ütközik.
- (6) A jegyző a válaszintézkedések kiválasztásában, illetve jóváhagyásában a *Munkacsoport, valamint* belső ellenőrzési vezető ajánlásaira, javaslataira támaszkodik.
- (7) A kiemelten nagy kockázatú tevékenységek esetében a jegyző intézkedik a legmagasabb kockázatú terület/tevékenység ellenőrzéséről (preventív ellenőrzés), folyamatos jelentést, beszámolót kér, illetve helyszíni vizsgálatot tart, vagy felkéri a belső ellenőrzési feladatokat ellátó szervezeti egységet a vizsgálat elvégzésére.
- (8) A kockázatok kezelésének elsődleges eszköze a hatékony folyamatba épített ellenőrzés. Az ellenőrzés hatékonyságát támogatja az ellenőrzési nyomvonal kialakítása és annak rendszere.
- (9) A kockázatok csökkentésére kialakított stratégiákat és válaszlépéseket Integrált Kockázatkezelési Intézkedési Tervbe kell foglalni, melyet a jegyző hagy jóvá.
- (10) Az Integrált Kockázatkezelési Intézkedési Tervet tárgyév április 15. napjáig el kell készíteni és a jegyzővel jóváhagyatni.

6. A kockázatkezelés monitoringja, felülvizsgálata

- (1) A kockázatok nyilvántartására és elemzésére a jegyző olyan monitoring rendszert működtet, amely alkalmas minden egyes kockázat esetében, a kezelésére kialakított módszer tényleges alkalmazásának, és azon keresztül hatékonyságának nyomon követésére, mérésére, a hozott intézkedésektől eltérő gyakorlat jelzésére. Továbbá lehetővé teszi a vezetés számára menetközben a korrekciós intézkedések szükség szerinti meghozatalát.
- (2) A Munkacsoport és a kockázat felméréseért és kezeléséért felelős vezetők kötelezettsége, az Integrált Kockázatkezelési Intézkedési Terv végrehajtásának folyamatos nyomon követése, ellenőrzése és értékelése, valamint a tevékenységek változásaihoz igazodóan a kockázati szint fenntartására, a kockázatok kezelésére hozott intézkedések megtétele.
- (3) A kockázatértékelést és az Integrált Kockázatkezelési Intézkedési Tervet soron kívül aktualizálni kell a tevékenység, a szervezet, a külső és belső környezet, a kockázatok jelentős változása, valamint a bekövetkezett kockázati események alapján.
- (4) A befejezetlen kockázatkezelési eljárásokról haladéktalanul jelentést kell küldeni az Integrált Kockázatkezelési Koordinátor útján a jegyzőnek.
- (5) A (2) – (5) bekezdésben foglalt feladatok ellátására a folyamatgazda köteles.
- (6) Évente legalább egyszer felül kell vizsgálni az előző évi Integrált Kockázatkezelési Intézkedési Tervek hatékonyságát, megvalósulását. A vizsgálatot a Munkacsoport végzi és arról beszámolót készít a jegyző felé.
- (7) A kockázatok kezelésének felülvizsgálatát kockázatkezelő szintenként tárgyév december 15. napjáig kell elvégezni

7. A kockázatok és intézkedések nyilvántartása

- (1) A jegyzőnek gondoskodnia kell egy naprakész nyilvántartási rendszer kialakításáról az Integrált Kockázati Leltár létrehozásával, amely alkalmas a kockázatok nyilvántartására, változásainak és a kezelés során tett intézkedések következményeinek folyamatos nyomon követésére.
- (2) *A nyilvántartásból bármely időpontban egyértelműen láthatónak kell lennie, hogy:*
 - melyek a tűréshatárt meghaladó azonosított kockázatok,
 - azokat kik és mikor határozták meg,
 - kezelésükre milyen intézkedéseket javasoltak,
 - az intézkedések végrehajtásáért ki a felelős,
 - az intézkedésnek mi a határideje,
 - az intézkedés milyen eredménnyel járt, milyen változást eredményezett az adott kockázat helyzetében (értékében),
 - a kockázat jelenlegi státusza (kezelt, kezeletlen, kezelés folyamatban).
- (3) A feltárt kockázatok, és intézkedések nyilvántartását az Integrált Kockázatkezelési Koordinátor kezeli és vezeti, mely nyilvántartásra a belső ellenőrzés is támaszkodik éves munkarendjének kialakításakor.

IV. FEJEZET

ZÁRÓ RENDELKEZÉSEK

- (1) Jelen szabályzat 2020. június 25. napján lép hatályba.
- (2) Jelen szabályzat hatálybalépésével egyidejűleg a 15/2019.(XI.14.) számú jegyzői utasítással kiadott Kockázatelemzési Szabályzat hatályát veszti.

- (3) A szabályzattal érintett kollégáknak az utasítás rendelkezéseit meg kell ismerniük és a megismerés tényét megismerési nyilatkozaton igazolniuk kell.

Budapest, 2020. június „24”

dr. Filipisz Andrea
jegyző

Mellékletek:

1. melléklet Az integrált kockázatkezelés felelősei és feladatai

Függelékek:

1. függelék A költségvetési szervet érintő kockázatok (nem taxatív)

Az integrált kockázatkezelés felelősei és feladatai

Integrált kockázatkezelés	Jegyző	Folyamatgazdák	Önálló szervezeti egységek vezetői	Munkatársak	Kockázatkezelési Munkacsoport	Integrált kockázatkezelési koordinátor	Belső Ellenőr	IBF
Kockázatkezelési rendszer kialakítása és működtetése	<ul style="list-style-type: none"> • Felelős a belső kontrollrendszer keretében - a szervezet minden szintjén érvényesülő – integrált kockázatkezelési rendszer, kialakításáért, működtetéséért és fejlesztéséért; • Integrált kockázatkezelési Szabályzat kiadása; • Kockázatkezelési Munkacsoport felállítása; • Integrált kockázatkezelési koordinátor kijelölése; 	<ul style="list-style-type: none"> • Integrált kockázatkezelési szabályzat véleményezése; • Felelős az általa irányított folyamatok, tevékenységek kockázatainak felméréseért, értékeléséért és kezelésének előkészítéséért, illetve végrehajtásáért; 	<ul style="list-style-type: none"> • Integrált kockázatkezelési szabályzat véleményezése; • Felelős a saját szervezeti egysége hatáskörébe tartozó folyamatok, tevékenységek kockázatainak felismeréséért, kezeléséért; 	<ul style="list-style-type: none"> • A saját munkaterületükön aktívan közreműködnek a tevékenységek kockázati szempontú vizsgálatában és kezelésében; 	<ul style="list-style-type: none"> • Integrált kockázatkezelési Szabályzat, illetve módosításának előkészítése; • Az integrált kockázatkezelési rendszer működésének legfőbb szerv; • A kockázatkezelési folyamatok előírása, feltételeinek biztosítása és betartásának megkövetelése, az integrált kockázatkezelési folyamatba épített ellenőrzés és felülvizsgálat; 	<p><i>A Bkr.7.§ (4) bekezdése alapján a költségvetési szerv vezetője az integrált kockázatkezelési rendszer koordinálására szervezeti felelőst jelöl ki. Ha a költségvetési szerv integritás tanácsadó foglalkoztat, akkor az integrált kockázatkezelési rendszer koordinálásával kapcsolatos feladatokat az integritás tanácsadó látja el. Ha van integritás tanácsadó és ettől függetlenül kockázatkezelési koordinátor is kijelölésre került, akkor együttműködnek a feladatok ellátásában.</i></p> <ul style="list-style-type: none"> • Az integrált kockázatkezelési rendszer működésének koordinálása (technikai és személyorientált koordináció); • Dokumentumok kezelése; 	<p>Bizonyosságot nyújtó tevékenysége</p> <p>értékeli a szervezet kockázatkezelési rendszerét és javaslatot tesz annak fejlesztésére.</p> <p>Tanácsadó tevékenysége keretében- a szervezetről és a szervezeti kockázatokról való átfogó ismereteivel-támogatja a kockázatok elemzését.</p> <p>A belső ellenőrzés folyamatgazdáj</p> <p>a-ként azonosítja és értékeli a saját folyamatának kockázatait, meghatározza a kockázatok csökkentésére vonatkozó intézkedéseket.</p>	<p>Kialakítja az információbiztonsági kockázatelemzési módszertant a jelen szabályzat keretein belül.</p>
Kockázatok azonosítása	<ul style="list-style-type: none"> • Közreműködik a szervezeti szintű kockázatok azonosításában; • Munkatársak tájékoztatásának biztosítása az azonosított kockázatokról; 	<ul style="list-style-type: none"> • Felelős a felelősségi körébe tartozó saját szervezeti és a folyamatok szintű kockázatok feltárásában, azonosításában; 	<ul style="list-style-type: none"> • Felelős a szervezeti egység tevékenységi körébe tartozó szervezeti és a folyamatok szintű kockázatok meghatározásában; 	<ul style="list-style-type: none"> • Közreműködik a szervezeti és a folyamatok szintű kockázatok azonosításában (interjú, kérdőív, stb.) 	<ul style="list-style-type: none"> • Az azonosított kockázatok csoportosítása, rangsorolása, átfedések kiszűrése; • Integrált Kockázati Leltár készítése; 	<ul style="list-style-type: none"> • A kockázatok feltárásának és azonosításának koordinálása kockázatkezelési szintenként. • Munkatársak tájékoztatása az azonosított kockázatokról; 	<p>A belső ellenőrzés folyamatgazdáj</p> <p>a-ként azonosítja és értékeli a saját folyamatának kockázatait, meghatározza a kockázatok csökkentésére vonatkozó intézkedéseket.</p>	<ul style="list-style-type: none"> • Azonosítja a Hivatal elektronikus információs rendszereire ható információbiztonsági kockázatok; • Dokumentálja az információbiztonsági kockázatok az Integrált Kockázati Leltárban.
Kockázatok értékelése	<ul style="list-style-type: none"> • Jóváhagyás; 	<ul style="list-style-type: none"> • A Kockázati Kritérium Matrix alkalmazásával értékeli a kockázatok; • A kockázatok értékelésével meghatározza a folyamat kockázatosságát. 	<ul style="list-style-type: none"> • Felelős a szervezeti egység tevékenységi körébe tartozó szervezeti és a folyamatok szintű kockázatok értékelésének végrehajtásáért; • Javaslatot tesz a Munkacsoport felé a szervezeti egység hatáskörét, illetve azon belül nem kezelhető kockázatokra; 	<ul style="list-style-type: none"> • Közreműködik a kockázatok értékelésében; 	<ul style="list-style-type: none"> • Kockázati Kritérium Matrix kialakítása; • Integrált Kockázatelemzési Matrix meghatározása; • A hivatal és önkormányzati szintű kockázatok elemzése, értékelése; • Kockázatok értékelésének összegzése; 	<ul style="list-style-type: none"> • A kockázatkezelési szinteken a kockázatelemzés koordinálása, • A szervezeti kommunikáció biztosítása; 	<p>Értékeli a Hivatal elektronikus információs rendszereire ható információbiztonsági kockázatok.</p>	

Integrált Kockázatkezelési Intézkedési Terv készítése	<ul style="list-style-type: none"> • Kockázati tőrés határok jóváhagyása; • Az Integrált Kockázatkezelési Intézkedési Terv jóváhagyása; • Munkatársak tájékoztatásának biztosítása az intézkedési tervben foglaltakról, 	<ul style="list-style-type: none"> • Javaslatot tesz a kockázatok csökkentésére vonatkozó stratégiára és a szükséges intézkedések megtételére; 	<ul style="list-style-type: none"> • Felelős a szervezeti egység tevékenységi körébe tartozó szervezeti és a folyamat szintű kockázatok stratégiájának, valamint a Kockázatkezelési Intézkedési Terv kidolgozásáért; 	<ul style="list-style-type: none"> • Megismeri a szervezet azonosított kockázatait és közreműködik a kockázatok csökkentésére kialakított válaszlépések végrehajtásában; 	<ul style="list-style-type: none"> • Szervezeti szintenként a kockázati tőrés határok meghatározása; • Integrált Kockázatkezelési Intézkedési terv előkészítése, a jegyző jóváhagyására. 		<ul style="list-style-type: none"> • Kockázatkezelési Munkacsoport feladatainak koordinálása; • Az Integrált Kockázatkezelési Intézkedési terv előkészítésének koordinálása; • A szervezeti kommunikáció biztosítása. 	Az Integrált Kockázatkezelési Intézkedési terv kiegészítése az információbiztonsági kockázatokkal.
Az integrált Kockázatkezelési Intézkedési terv nyomon követése, éves felülvizsgálata.	<ul style="list-style-type: none"> • Beszámoltatás 	<ul style="list-style-type: none"> • Beszámol az Integrált Kockázatkezelési Intézkedési terv végrehajtásáról a vezetője felé. 	<ul style="list-style-type: none"> • Beszámol az Integrált Kockázatkezelési Intézkedési terv végrehajtásáról a Munkacsoport felé. 	<ul style="list-style-type: none"> • Visszacsatolást ad a bevezetett intézkedések hatásosságáról. 	<ul style="list-style-type: none"> • Az Integrált Kockázatkezelési Intézkedési terv nyomon követéséről szóló beszámoló összeállítása a jegyző felé; 		<ul style="list-style-type: none"> • Kockázatkezelési Bizottság/ Munkacsoport monitoring feladatainak segítése, koordinálása; • A beszámoló előkészítése. 	Felülvizsgálja az Integrált Kockázatkezelési Intézkedési tervet információbiztonsági szempontból.

1. függelék a 18/2020. (VI.24.) számú jegyzői utasításhoz

A szervezetet érintő kockázatok
(nem taxatív jellegű felsorolás)

I. **A kockázatok forrása szerinti csoportosítása**

a) **Külső kockázatok**

KÜLSŐ KOCKÁZATOK	
Infrastrukturális	Az infrastruktúra elégtelenségei vagy hiányosságai fennakadást okozhatnak a normál működésben.
Gazdasági	Költségvetési támogatások csökkenése, elvonása, árbevételek elmaradása, nem tervezhető központi intézkedések, kamatláb-változások, árfolyam-változások, infláció negatív hatással lehetnek a tervekre.
Jogi és szabályozási	A jogszabályok, fenntartói, felügyeleti rendelkezések és egyéb szabályok korlátozhatják a kívánt tevékenységek terjedelmét, az erős jogi szabályozás akár túlzott megkötéseket is előírhat.
Környezetvédelmi	A környezetvédelmi megszorítások a szervezet működési területén korlátot szabhatnak a lehetséges tevékenységeknek.
Politikai	Egy kormányváltás/politikai döntés megváltoztathatja a kitűzött célokat. Egy szervezet tevékenysége magára vonhatja a politika érdeklődését vagy nem kívánt politikai reakciót válthat ki.
Piaci	Versenyhelyzet kialakulása, vevői/szállítói problémák megjelenése negatív hatással lehet a tervekre.
Elemi csapások	Tűz, árvíz vagy egyéb elemi csapások hatással lehetnek a kívánt tevékenység elvégzésének képességére. A katasztrófavédelmi terv elégtelennek bizonyulhat.

b) **Belső kockázatok**

JOGI SZABÁLYOZÁS HIÁNYOSSÁGAIBÓL EREDŐ KOCKÁZATOK	
Jogi	<ul style="list-style-type: none"> • A jogi szabályozási, politikai, gazdasági stb. környezeti változásokat nem követik a belső szabályozások. Az új feladatokhoz kapcsolódó belső szabályzatok késve készülnek el, vagy nem megfelelőek. • A szakmai és adminisztratív feladatokat befolyásoló szabályok túl bonyolultak, a költségvetési szerv túlszabályozott, párhuzamos tevékenységek fordulnak elő. A szabályozási környezet túl gyakran változik. A jogszabályok nincsenek egymással összhangban / a jogharmonia hiánya. • Szabályozás és gyakorlat különbözik. Eltérő a jogszabály-értelmezés és/vagy alkalmazás az egyes költségvetési szerveknél. • A Hivatal nem időben értesül a vonatkozó szakmai jogszabályok teljes köréről / azok változásáról. • Szakpolitikai stratégia gyakran változik.
PÉNZÜGYI KOCKÁZATOK	
Költségvetési	A kívánt tevékenység ellátására nem elég a rendelkezésre álló forrás.
Csalás, hamisítás	Vagyonvesztés. A források nem elegendők a kívánt megelőző

	intézkedésre.
Biztosítási	Nem lehet a megfelelő biztosítást megszerezni elfogadható költségen. A biztosítás elmulasztása.
Tőke beruházási	Nem megfelelő beruházási döntések.
Felelősségvállalási	A szervezetre mások cselekedete negatív hatást gyakorol, és a szervezet jogosult kártérítést követelni.
Közbeszerzési	A legalacsonyabb ajánlati ár is magasabb a tervezettnél jogorvoslati eljárás miatti kései projektkezdés
TEVÉKENYSÉGI KOCKÁZATOK	
Stratégiai	Nem megfelelő stratégia követése. A stratégia elégtelen vagy pontatlan információra épül.
Működési	<ul style="list-style-type: none"> • Elérhetetlen/megoldhatatlan célkitűzések. A célok csak részben valósulnak meg. • a szervezeti struktúra csak részben megfelelő • nem megfelelő kontrollrendszer kialakítása
Információs	A döntéshozatalhoz nem elegendő információ a szükségesnél kevesebb ismeretre alapozott döntést eredményez.
Hírnév	A nyilvánosságban kialakult rossz hírnév negatív hatást fejthet ki.
Üzemeltetési	A hatékonysági kritériumok érvényesülése érdekében az üzemeltetés fenntarthatóságának, fejlesztésének igénye (pl. energiatakarékos megoldások keresése). Ha az üzemeltetés nem gazdaságos, jelentős bevételkiesést, vagy többletkiadást idézhet elő. A karbantartásra fordítható összegek elégtelensége miatti épületkárosodások a működést veszélyeztetik
Projekt	Megfelelő előzetes kockázatelemzés, hatástanulmány nélkül készült el a projekt-tervezet. A projektek nem teljesülnek a költségvetési vagy funkcionális határidőre.
Innováció	Elmulasztott újítási lehetőségek.
Informatikai	<ul style="list-style-type: none"> • az elavult hardverek meghibásodása • az előregedett szerverek a megnövekedett adattartalom tárolására, futtatására nem alkalmasak • a régi gépeket az új alkalmazások futtatása lelassítja • az új gépeken a Microsoft alapú szoftverek hiánya miatt egyes alkalmazások nem működnek (Forrás SQL, statisztikai szoftver) • a szükséges új szoftverek beszerzése elmarad • integráltság hiánya • új alkalmazások bevezetésekor felmerülő egyéb üzemeltetési és emberi erőforrás kockázat • üzemeltetési és működésfolytonossági kockázatok (vírus, stb.)
EMBERI ERŐFORRÁS KOCKÁZATOK	
Humán erőforrás mennyisége és minősége	<ul style="list-style-type: none"> • A megfelelő szakképzettséggel rendelkező munkaerő biztosítása <ul style="list-style-type: none"> ○ munkateherben lévő különbségek ○ kompetenciában jelentkező különbségek ○ a legjobb tisztviselőket más szervek elcsábítják jobb fizetési feltételekkel • Jogszabályváltozásból eredő humán erőforrás kockázat <ul style="list-style-type: none"> ○ nők 40 éves munkaviszonyt követő nyugdíjazásának lehetősége ○ a bírák nyugdíjazására vonatkozó jogszabály-módosítás ○ létszámstop • A tartósan távollévők kiesett munkaerejének pótlása

	<ul style="list-style-type: none"> ○ várandósság, szülési szabadság, CSED, GYED, GYES idejére történő határozott idejű foglalkoztatás ○ váratlan, hosszantartó betegség
Személycserék	A hatékony működést korlátozza, vagy teljesen ellehetetleníti a szükséges számú, megfelelő képesítésű személyi állomány hiánya. Vezetőváltás Kulcsfontosságú munkaerő kiesése, távozása
Egészségügyi	A személyi állomány egészségügyi állapota befolyásolhatja a hatékony munkavégzést. Az alkalmazottak túlterheltsége, fásultsága Általános érdektelenség, kiégés A beléptetési, adatvédelmi, informatikai biztonsági előírások nem megfelelő betartása
Munkafeltételek	A hatékony munkavégzést akadályozzák a nem megfelelő munkaköri környezet és a munkavégzéshez szükséges feltételek biztosításának hiányosságai. A tárgyi feltételek nem megfelelő biztosítása (informatikai eszközök)
INTEGRITÁSI KOCKÁZAT	
<ul style="list-style-type: none"> • a szervezet célkitűzéseit, értékeit, elveit sértő vagy veszélyeztető visszaélés, szabályoktól eltérő tevékenység, vagy egyéb esemény lehetősége: pl: <ul style="list-style-type: none"> ○ a szervezet munkatársai nem azonosulnak a szervezeti etikai szabályokkal; ○ az összeférhetetlenségi követelményeket nem tartják be ○ a belső kontrollrendszer hiányos, vagy működése nem megfelelő; ○ aköztsztszviselői jogviszonyból fakadó kötelezettség vétkes megszegése; 	
KORRUPCIÓS KOCKÁZAT (Olyan integritási kockázat, amely korrupciós (bűn)cselekmény bekövetkezésének a lehetőségét jelenti)	
<ul style="list-style-type: none"> • jogtalan előny kérése, a jogtalan előny vagy ennek ígéretének elfogadása, illetve a harmadik személynek adott vagy ígért jogtalan előny kéréjével vagy elfogadójával történő egyetértés; • ajándékok elfogadása; • korrupciós helyzetről a bejelentési kötelezettség elmulasztása; • hivatali helyzettel történő visszaélés 	

II. Más csoportosításban a szervezet tevékenységével, folyamataival összefüggésben az alábbi kockázati kategóriák és kockázatok alakíthatók ki:

Kockázati kategóriák	Lehetséges kockázatok	hatás 1-5	valószínűség 1-5
Szakmai feladatellátással kapcsolatos kockázatok	<ul style="list-style-type: none"> • A szakmai feladatellátást szabályozó belső szabályzatok, utasítások nincsenek összhangban a stratégiai és a rövid távú tervekkel. • A szakmai feladatellátásra vonatkozó belső szabályzatokat, utasításokat nem tartják be. • A szakmai feladatellátásra vonatkozó jogszabályi követelményeket nem tartják be. 		
Szabályozásból és annak változásából eredő kockázatok	<ul style="list-style-type: none"> • Egyes folyamatok nem kerülnek pontos szabályozásra a belső eljárásrendekben. • A jogi szabályozási, politikai-gazdasági stb. környezeti változásokat nem követik a belső szabályozások. • Az új feladatokhoz, környezeti változásokhoz 		

	<p>kapcsolódó belső szabályzatok egyáltalán nem készülnek el, csak hiányosan készülnek el, vagy nem időben készülnek el.</p> <ul style="list-style-type: none"> • A költségvetési tervek összeállításához nem állnak rendelkezésre a tervezést befolyásoló jogi és egyéb szabályok. • Az előre nem tervezhető jogi vagy belső szabályozási változások előre nem tervezhető hatásokkal járnak. • A szakmai és adminisztratív feladatokat befolyásoló szabályok túl bonyolultak. • A szakmai és adminisztratív feladatokat befolyásoló jogi vagy belső szabályozási környezet túl gyakran változik, és ezzel folyamatos bizonytalanságot eredményez. • Külföldi partnerek eltérő szabályozása, nem megfelelő harmonizáció. • Szabályozás és gyakorlat különbözik. • Lassú a szabályozás változásáról szóló információ átültetése a gyakorlatba. • Szervezet nem időben értesül a vonatkozó szakmai jogszabályok teljes köréről / azok változásáról. 		
A koordinációs és kommunikációs rendszerekben rejlő kockázatok	<ul style="list-style-type: none"> • Az egyes szervezeti egységek közötti koordináció és kommunikáció nem biztosított. • A belső kommunikációs folyamatok nem megfelelően működnek. • A munkatársak nem kommunikálnak egymással, nem működik a felülről lefelé, illetve az alulról felfelé történő kommunikáció. • Negatív sajtóvisszhang vagy a pozitív kommunikáció lehetősége nincs megfelelően kezelve. • PR, tájékoztatásra vonatkozó jogszabályokat, szervezeti arculati elemeket nem ismerik vagy használják előírászerűen. 		
Külső szervezetekkel való együttműködésben rejlő kockázatok	<ul style="list-style-type: none"> • A tervezéshez, illetve a szakmai és adminisztratív feladatok ellátásához szükséges adatokat, információkat a partnerek nem bocsátják időben rendelkezésre. • A partner szervezetektől érkező adatszolgáltatás hiányos, nem megbízható, nem megalapozott. • A partner szervezetekkel folytatott kommunikáció nem megfelelő. 		
Szervezetek/partnerek változásából eredő kockázatok	<ul style="list-style-type: none"> • A partner szervezetek előre nem látható változásai negatívan befolyásolják a szakmai vagy adminisztratív feladatok ellátását. • A partner szervezetek változásairól nem értesül időben a szervezet, ami negatív következményekkel jár a szakmai vagy adminisztratív feladatok ellátására. 		
Tervezésből, pénzügyi és egyéb erőforrások rendelkezésre állásából eredő kockázatok	<ul style="list-style-type: none"> • A költségvetési tervek nincsenek összhangban a jogi szabályozási előírásokkal, a célkitűzésekkel. • A költségvetési tervek nem térnek ki a terv végrehajtásához szükséges erőforrásokra. • A költségvetési tervek nem számolnak a terv végrehajtását akadályozó kockázatokkal, a költségvetési terv nem tartalmaz tartalékokat. • A feladatok, erőforrások és kapacitások változását a tervezésnél nem veszik figyelembe. • A költségvetési források esetleges csökkenését, az előre nem látható pénzügyi krízisek bekövetkezésének lehetőségét nem veszik figyelembe a tervezés során. • Az árfolyamváltozások lehetséges kockázatait, az 		

	<p>inflációs várakozások nem kerülnek figyelembevételre a tervezés során.</p> <ul style="list-style-type: none"> • A szakmai és adminisztratív feladatok ellátásának erőforrás szükséglete (pénzügyi, fizikai, egyéb) nem biztosított, vagy nem a megfelelő mennyiségben és minőségben biztosított. • Források nem állnak rendelkezésre a kifizetés időpontjában. • A likviditási előrejelzés nem megfelelő (késik, pontatlan). • A betervezett kötelezettségvállalás nem valósul meg. 		
<p>Az irányítási, a belső kontrollrendszerben és a belső ellenőrzésben rejlő kockázatok</p>	<ul style="list-style-type: none"> • A szervezet vezetői nincsenek tisztában a stratégiai és rövid távú célokkal. • A szervezet vezetői nem motiváltak. • A szervezet vezetői nem mutatnak etikus magatartást munkájuk során. • A belső kontrollrendszer egyes elemei (pl. kontrolltevékenység, monitoring, stb.) hiányoznak a szervezetenél, vagy nem megfelelően működnek. • A korábbi ellenőrzések során tett javaslatokat a vezetőség nem hajtotta végre vagy az intézkedések nem hatékonyak. • Egyes folyamatokat hosszabb ideje nem ellenőrizték. • Egyes folyamatokra vonatkozóan a korábbi ellenőrzések súlyos hibákat tártak fel. • A projektek előrehaladását gátló tényezőkről az információ késve vagy nem jut el az intézkedésre alkalmas szintre. • Rendhagyó ügyek nagy száma/komplexitása miatt nehéz a nyomon követés. • Jelentéstételi határidők elmulasztása. • Külső szolgáltató általi ellenőrzés megszervezése, leszerződés audit céggel késedelmes. • Jelentések hiányosan, késve kerülnek összeállításra. • Jelentéstételi, adatszolgáltatási kötelezettség határidejét nem tartják be. • Szakmai tapasztalat hiánya a munkatársak körében. • Biztosítékok meglétének ellenőrzése nem kellően alapos / elmarad. • A helyszíni ellenőrzésen feltárt problémák nyomon követése nem megfelelő. • Dokumentum alapú és helyszíni ellenőrzések lebonyolítása elmarad, vagy nem kellően részletes / alapos • Helyszíni ellenőrzések kockázatelemzése nem megfelelő. • A helyszíni ellenőrzésen feltárt problémák nyomon követése / visszacsatolása nem megfelelő. • Nem vagy nem megfelelően ellenőrzik a beszerzési /közbizterzési kötelezettséget. • Az ellenőrzésen feltárt problémák nyomon követése nem megfelelő. • A szervezeti integritást sértő események kezelésének eljárásrendje nincs / hiányos. • Csak EU-s / hazai ellenőrző szervek tárják fel a szabálytalanságot • A szabálytalanság tényének megállapítása és annak kezelése, szankcionálása nem egységes. • Követeléskezelés eredménytelen / elhúzódik. • Minőségileg kifogásolható tervek műszaki és időbeli nehézségeket okoznak a végrehajtás során. • Formális kontrollok lassítják a folyamatot. • Korrupció veszélye a közbizterzésben. 		

	<ul style="list-style-type: none"> • Közbeszerzésre vonatkozó minőségbiztosítási és szabályossági javaslatokat (EKKE) nem veszik figyelembe. 		
Humán erőforrás-gazdálkodásban rejlő kockázatok	<ul style="list-style-type: none"> • A szakmai és adminisztratív feladatok ellátására nem áll rendelkezésre elegendő munkaerő-kapacitás. • A rendelkezésre álló munkaerő nem rendelkezik megfelelő végzettséggel és/vagy szakmai tapasztalattal. • Új munkatársak betanítására nincs megfelelő kapacitás, idő. • A munkatársak elkötelezettsége, lojalitása, munkabírása, motiváltsága nem megfelelő. • A szervezet munkatársai nem azonosulnak a szervezeti etikai szabályokkal. • A munkatársak feladat- és felelősségi köre nem kellően részletes/meghatározott, nem megfelelően elhatárolt, nem megfelelően kommunikált. • A vezetők szakmai és etikai megítélése nem megfelelő. • A munkaerő-felvételnek nem megfelelő a gyakorlata, ezáltal nem biztosított a minőségi munkaerő, megfelelő időben történő rendelkezésre állása. • A szervezet motivációs és bérpolitikái nem készültek el, hiányosak, nem megfelelőek, nem illeszkednek az aktuális szervezeti célokhoz. • A szervezetnél nincs kialakult képzési rendszer vagy elavult, esetleg „diszkriminatív” (pl. folyamatosan csak bizonyos szervezeti egységek / munkavállalók részesülnek képzésben). • A szervezet nem rendelkezik teljesítménymenedzsment rendszerrel vagy a kialakított rendszer nincs összhangban a stratégiai és rövid távú célkitűzésekkel. • Magas fluktuáció. • Munkatársaknak nincs megfelelő kapacitásuk a feladatok végrehajtására. • Szervezeti bizonytalanság (pl. várható átalakulás, megszűnés, működési támogatás hiánya, stb.) . • A munkavégzéshez szükséges technikai / fizikai erőforrások nem állnak megfelelően rendelkezésre. • Összeférhetetlenségi követelmények teljesítése nehézségekbe ütközik. 		
A megbízható gazdálkodást és a pénzkezelést befolyásoló kockázatok	<ul style="list-style-type: none"> • Az egyes szakmai vagy adminisztratív intézkedéseknek a kiadásokra gyakorolt hatását nem megfelelően mérik fel. • Nem megfelelő a szervezet likviditásmenedzsmentje. • A szervezetnél nem kialakult vagy nem megfelelő a közbeszerzési rendszer. • A pénzkezeléssel kapcsolatos jogi és belső szabályozási előírások betartása nem biztosított. • A pénzkezeléssel kapcsolatos biztonsági előírásokat nem tartják be. • Az egyes szakmai, illetve adminisztratív folyamatok végrehajtása során nem törekednek a költségek minimalizálására. • A szervezet nem rendelkezik kontrolling, illetve teljesítményértékelési rendszerrel. • A szervezeti célok és az elért eredmények értékelése rendszeres időközönként nem történik meg. 		
Számviteli folyamatokkal kapcsolatos kockázatok	<ul style="list-style-type: none"> • A szervezet nem rendelkezik megfelelő számviteli nyilvántartási rendszerrel. • A szervezet beszámolási rendszere nem megbízható. 		

	<ul style="list-style-type: none"> • A szervezet nem tesz időben eleget a beszámolási kötelezettségeknek. • A szervezet nem követi folyamatosan nyomon a könyvvetéssel kapcsolatos jogi szabályozási előírások változásait. • A könyvvetés informatikai támogatottsága nem megoldott. 		
Működésből, üzemeltetésből eredő kockázatok	<ul style="list-style-type: none"> • A szervezet nem rendelkezik fizikai biztonsági tervekkel és előírásokkal. • A szervezet nem rendelkezik beruházási, fejlesztési tervekkel, illetve a tervek nem aktualizáltak, azok felülvizsgálata nem biztosított. • A szervezeti vagyon, eszközök megfelelő működtetése és állagmegóvása nem biztosított. • Az üzemeltetési feladatoknak nincs felelőse a szervezeten belül. • A szervezeti vagyon, eszközök megóvását szolgáló biztonsági előírások nem kerülnek betartásra. 		
Az iratkezeléssel, irattározással kapcsolatos kockázatok	<ul style="list-style-type: none"> • A szervezet nem rendelkezik pontos, naprakész iratkezelési és irattározási rendszerrel. • Az irattározás fizikai, biztonsági követelményei nem megoldottak. • A nyilvántartási rendszerek nem megfelelőek, nem naprakészek, vagy a hozzáférési korlátok nem működnek. 		
Informatikai rendszerekkel, valamint adatkezeléssel és adatvédelemmel kapcsolatos kockázatok	<ul style="list-style-type: none"> • A szervezet nem rendelkezik informatikai stratégiai tervvel. • A szervezet nem rendelkezik informatikai biztonsági és katasztrófa tervvel. • A szakmai, illetve adminisztratív folyamatok támogatására a szükséges időpontban nem áll rendelkezésre informatikai alkalmazás. • A szervezet informatikai alkalmazásai elavultak. • A szervezet hardver ellátottsága nem megfelelő. • Az informatikai alkalmazások nem felelnek meg a biztonságosság követelményének. • Az archiválási rendszerek egyáltalán nem vagy nem megfelelően működnek. • Egyes informatikai alkalmazások nem kompatibilisek más, a szervezet által alkalmazott informatikai rendszerekkel. • A szervezet adatkezelése és adatvédelme nem felel meg a jogi és belső szabályozási előírásoknak. 		

Kockázatok értékelése

1) **Valószínűségi skála meghatározása:** A rendelkezésre álló tapasztalatok alapján a feltárt kockázatok az elemzés évében milyen valószínűséggel fognak bekövetkezni.

2) **Hatásskála meghatározása:** A kockázatok felmerülése esetén azok hatása milyen nagyra becsülhető.

1) **Az alkalmazott valószínűségi skála meghatározása:**

1. 1-20 % közötti valószínűség (nagyon alacsony valószínűségű)
2. 21-40 % közötti valószínűség (alacsony valószínűségű)
3. 41-60 % közötti valószínűség (közepes valószínűségű)
4. 61-80 % közötti valószínűség (magas valószínűségű)
5. 81-99 % közötti valószínűség (nagyon magas valószínűségű)

Kritérium Mátrix Valószínűség vizsgálathoz

Értékelési Kritérium skála	Hatás	Érték
1-20 % közötti valószínűség (nagyon alacsony valószínűségű)	Bekövetkezhet, de nagyon alacsony a valószínűsége és ritkán, egyedi, szórvány esetek	1
21-40 % közötti valószínűség (alacsony valószínűségű)	Elképzelhető, hogy bekövetkezik, alacsony a valószínűsége, több, de nem rendszer szerű eset	2
41-60 % közötti valószínűség (közepes valószínűségű)	Bekövetkezik, közepes a valószínűsége, több, rendszer szerű eset	3
61-80 % közötti valószínűség (magas valószínűségű)	Nagy valószínűséggel bekövetkezik éven belül és/vagy havi szinten	4
81-99 % közötti valószínűség (nagyon magas valószínűségű)	Nagyon magas valószínűséggel bekövetkezik és/vagy heti, napi szinten	5

2) Az alkalmazott hatásskála meghatározása:

1. 0-20 % (nagyon alacsony hatású)
2. 21-40 % (alacsony hatású)
3. 41-60 % (közepes hatású)
4. 61-80 % (nagy hatású)
5. 81-99 % (nagyon nagy hatású)

Kritérium Mátrix Hatás vizsgálathoz

Értékelési Kritérium skála	Hatás	Érték
0-20 % (nagyon alacsony hatású)	kis munkával, alacsony költséggel helyreállítható, jogszabályt nem sértő, munkavégzést nehezíti, de nem akadályozza	1
21-40 % (alacsony hatású)	többlet erőforrás bevonását igényli, de a funkciók ellátását nem akadályozza meg, munkavégzést nehezíti	2
41-60 % (közepes hatású)	egyres határidők, követelmények nem teljesülnek, anyagi károkat okozhat	3
61-80 % (nagy hatású)	kárt okoz (akár anyagi is), funkció ellátását akadályozza, az Önkormányzat hírnevét befolyásolja	4
81-99 % (nagyon nagy hatású)	jelentős (akár anyagi) kárt okoz, alapfunkció nem működik, az Önkormányzat hírnevét súlyosan befolyásolja, jogi lépések, perek indulhatnak	5

Az Integrált kockázatkezelés feladatainak ütemezése:

Feladat	Határidő
Évente legalább egyszer felül kell vizsgálni az előző évi integrált kockázatkezelési intézkedési tervek megvalósulását és arról beszámolót készíteni a jegyző felé.	január 31-ig
A kockázatok feltárása és beazonosítása	minden év február 28-ig kell
A kockázatok elemzése és értékelése	tárgyév március 31-ig
Az Integrált Kockázatkezelési Intézkedési Terv elkészítése.	tárgyév április 15. napjáig
A kockázatok kezelésének felülvizsgálata kockázatkezelő szintenként	tárgyév december 15. napjáig