ÁLLAMI
SZÁMVEVŐSZÉK

MÓDSZERTANI ÚTMUTATÓ

IT alkalmazások folyamatorientált ellenőrzéséhez

Jóváhagyom:

.....

Domokos László
elnök

2018. április 09.

A módszertani munkát felügyelte:

Holman Magdolna
főtitkár

A végrehajtásért felelős:

Tótpál Szabolcs
osztályvezető

A módszertani munkát irányította:

Borsos Ferenc
elnöki megbízott

Összeállították:

Molnár Bálint
számvevő tanácsos

Weltherné Szolnoki Dóra
számvevő tanácsos

TARTALOMJEGYZÉK

RÖVIDÍTÉSEK JEGYZÉKE

ÁSZ	Állami Számvevőszék
INTOSAI	„International Organization of Supreme Audit Institutions", Legfőbb Ellenőrző Intézmények Nemzetközi Szervezete
INTOSAI IDI	„INTOSAI Development Initiative", INTOSAI Fejlesztési Kezdeményezés
ISACA	„Information Systems Audit and Control Association", Információs Rendszer Auditorok és Ellenőrök Szervezete
IT	információs technológia
SLA	„service level agreement", a szolgáltatás minőségi elvárásait rögzítő megállapodás

ÉRTELMEZŐ SZÓTÁR

adatok integritása	Annak a feltételnek a megléte, hogy az adat helyes, és semmiféle művelet, mint például adatátvitel, tárolás, visszaállítás nem károsította meg az eredeti adatot. Az adat helyesen áll rendelkezésre a kezelés számára. Meghatározott műveletek szempontjából alapvető adat minőségi elvárás. Más szempontok alapján az adat integritás biztosíték arra nézve, hogy az adathoz csak felhatalmazott, jogosult fér hozzá, vagy módosíthatja azt.
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.
elektronikus információs rendszer	A működés és gazdálkodás során felhasznált és keletkező elektronikus eszközökkel feldolgozott és elektronikus adathordozókon rögzített adatok és információk elektronikus formában tárolt összessége, mely az adatok befogadását, feldolgozását, kibocsátását és tárolását biztosító informatikai hardver és szoftver eszközökkel együtt alkot rendszert.
ellenőrzési modul	A számvevőszéki ellenőrzési programok egy főbb ellenőrzési szempont köré csoportosított, önálló ellenőrzési rész-feladatként értelmezhető szempont- és kritériumrendszere, mely más fő szempont ellenőrzési feladatától elkülöníthető.
folyamatorientált megközelítés	Az ellenőrzés felépítésének módja: az ellenőrzött szerv valamely közpénz- vagy közvagyon gazdálkodással kapcsolatos működési folyamatának végigkísérésével határozza meg az ellenőrzés tárgyát, hatókörét, szempontjait és módszereit.

hardver	A hardver olyan fizikai - elektromos, elektromágneses eszközök, részek összessége, melyek lehetővé teszik az informatikai rendszer működését
IT alkalmazás	Olyan informatikai eszközökkel támogatott szoftver vagy szoftver csomag, mely(ek) egy feladat ellátását, valamely folyamat végrehajtását, a szervezet működtetését vagy működését, konkrét ügyleti folyamatok végrehajtását támogatja (támogatják).
input	Az IT alkalmazás által kezelt bemeneti adatok összessége.
output	Az IT alkalmazás által előállított kimeneti adatok összessége.
komplexitás	A teljeskörűség és a rendszer elemek közötti összefüggések együttes teljesülése.
middleware	Szoftverek, melyek kapcsolatot alkotnak az IT alkalmazások és az operációs rendszerek, hálózati szoftverek között.
rendelkezésre állás	Annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.
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.
szoftver	Elektronikus adatfeldolgozó berendezések memóriájában elhelyezkedő, azokat működtető program és mellékelt írásos dokumentáció(k).

BEVEZETÉS

Az Állami Számvevőszékről szóló törvény rögzíti, hogy a szervezet az általa végzett ellenőrzések szakmai szabályait, módszereit maga alakítja ki. Az ÁSZ stratégiájában rögzítette, hogy a magas színvonalú feladatellátás alapfeltétele a célokhoz, feladatokhoz illeszkedő módszertan kidolgozása, továbbfejlesztése, a folyamatos, minőségközpontú módszertani fejlesztés fenntartása, a nemzetközi jó gyakorlat adaptálása. Jelen módszertani dokumentum a nyilvános számvevőszéki ellenőrzés-szakmai szabályok rendszerében a módszertani útmutatók szintjén jelenik meg. Ezáltal a Limai Nyilatkozat alapulvétele mellett a második szinten található, a Számvevőszék működése és a számvevőszéki ellenőrzés alapelveire ráépül.

A módszertani útmutató bármely ellenőrzési típus szerinti, az ÁSZ ellenőrzési feladatai és jogosultságai figyelembevételével meghatározott ellenőrzés lefolytatásához az informatikai alkalmazásokkal támogatott feladatellátás megítélése terén nyújt háttértámogatást.

Jelen módszertani útmutató (a továbbiakban: Útmutató) az ellenőrzés tárgyát képező folyamatok vagy feladatok informatikai alkalmazásokkal való támogatottsága megfelelőségének megítéléséhez nyújt módszertani hátteret.

Az Útmutató alkalmazott elvek és gyakorlati szempontok bemutatásával kívánja az ellenőrzési feladatellátást támogatni függetlenül attól, hogy az ellenőrzési feladat mely ellenőrzési típusba sorolható.

Az Útmutató célja az, hogy:

- támogassa az ellenőrzési feladat kiválasztása, az ellenőrzési előtanulmány és az ellenőrzési program elkészítésének feladatait azon ellenőrzések esetében, ahol az ellenőrzés tárgya, vagy ahhoz kapcsolódó folyamat IT alkalmazásokkal támogatott;

- gyakorlati szempontok bemutatásával támogassa a helyszíni ellenőrzés megvalósításának megtervezését, végrehajtását, kiértékelését, az ellenőrzési megállapításokhoz vezető okok feltárását, a lehetséges hatások feltérképezését, a javaslatok megfogalmazását, valamint az ellenőrzés hasznosulásának megtervezését, előkészítését és nyomon követését.

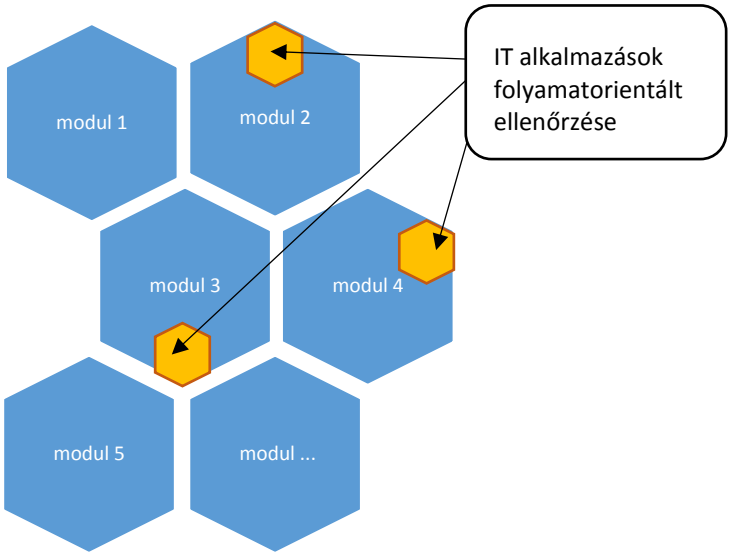
Az Útmutató az INTOSAI IDI számvevőszékek részére készített „IT ellenőrzési kézikönyve", a Svájci Számvevőszék „Útmutató az IT alkalmazások ellenőrzéséhez" című útmutatója, az INTOSAI 5310 „Információs rendszer biztonsági felülvizsgálatának módszertana" című módszertani útmutatója, valamint 5450 „Az államadósság informatikai rendszerének ellenőrzése" című módszertani útmutatójának tervezete, az ISACA „Általános alkalmazás kontroll ellenőrzés programja" című dokumentum, az Ausztrál Számvevőszék „Emberi Erőforrás Menedzsment Informatikai Rendszere – kockázatok és kontrollok" című dokumentum, valamint a szakirodalom további tanulmányai, cikkei feldolgozásával az ellenőrzés teljes folyamatának korszerű támogatását célozza az ellenőrzési témaválasztástól kezdve a hasznosulásig.

1. IT ALKALMAZÁSOK FOLYAMATORIENTÁLT ELLENŐRZÉSE

Az IT alkalmazások folyamatorientált ellenőrzése **nem ellenőrzési típus**.

Az Útmutatóban foglaltak modulszerű alkalmazását mutatja be az 1. sz. ábra. Bármely ellenőrzési típus szerint lefolytatott ellenőrzés során az IT alkalmazások folyamatorientált ellenőrzése lehet ellenőrzési modulban megtervezett ellenőrzési feladat. Az Útmutató az IT alkalmazások ellenőrzési feladatának megtervezéséhez és végrehajtásához nyújt módszertani támogatást.

1. sz. ábra - Az IT alkalmazások folyamatorientált ellenőrzésének moduláris alkalmazása



Forrás: ÁSZ grafika

Az Útmutatónak nem része egy-egy szervezet teljes informatikai rendszere általános kontrolljainak ellenőrzése.

Mind a közpénzzel, a közvagyonnal való gazdálkodás (folyamata), mind a jogszabályok által előírt feladatok, közfeladatok ellátása, valamint e tevékenységekről való beszámolás informatikai alkalmazásokkal támogatottak. Az elektronikus információk keletkezése és kezelése környezetének ellenőrzési szempontú megítélése elengedhetetlen. Az adatok és információk a szakmai folyamatok elemei, azok megbízhatósága, helyénvalósága, teljes körűsége és pontossága a feltétele a szabályszerűségi, eredményességi, hatékonysági és gazdaságossági követelmények teljesítésének.

2. AZ ELLENŐRZÉS KERETEI

2.1. Az ellenőrzés célja

A közpénzekkel és közvagyonnal való gazdálkodást leképező információs rendszer megbízhatóságát többek között a működést és gazdálkodást támogató informatikai alkalmazások megfelelő működésének (funkcionalitásának és biztonságának) értékelésével ítélhetjük meg.

Az IT alkalmazások folyamatorientált ellenőrzésnek célja, hogy az ÁSZ független és szakmailag megalapozott megállapítást tegyen arról, hogy a kiválasztott

folyamat, feladat szabályszerű és megbízható végrehajtását megfelelően támogatják-e az informatikai alkalmazások és azok kontrolljai.

A működés és gazdálkodás IT alkalmazással való megfelelő támogatásának ellenőrzése két tényező együttes ellenőrzéséből adódik:

- az IT alkalmazás funkcionalitásának megfelelésére vonatkozó ellenőrzés (biztosított-e az alkalmazás funkcionalitása az elvárt működés szerint);
- az IT alkalmazás, és az abban feldolgozott, kezelt és létrehozott adatok és információk ellenőrzése a biztonsági követelmények érvényesülése szempontjából (az alkalmazás megbízhatósága és az alkalmazással kezelt és előállított adatok integritása, időszerűsége, biztonsága, bizalmassága, sértetlensége, rendelkezésre állása, megbízhatósága, teljes körűsége és pontossága).

Az IT alkalmazások folyamatorientált ellenőrzése során az ÁSZ a kiválasztott alkalmazás funkcionalitásának és megbízhatóságának megfelelőségéről (vagy hatékonyságáról) szerez ésszerű bizonyosságot, ezáltal hozzájárul a kontroll hiányosságok és a le nem fedett kockázatok feltárásához.

A fentiekből következően az ellenőrzés célja kettős:

- elsődleges cél az ellenőrzött IT alkalmazásból nyert adatok és információk ellenőrzési szempontú felhasználhatóságának megítélése;
- másodlagos cél az IT alkalmazás funkcionalitása és megbízhatósága terén fennálló, le nem fedett kockázatok feltárása, értékelése, azok lehetséges hatásának bemutatása.

Az ellenőrzés fő szempontját, illetve alszempontjait az az ellenőrzési típus és ellenőrzési cél határozza meg, amelyhez az IT alkalmazás ellenőrzési modulként kapcsolódik.

2.2. Az ellenőrzés és kritérium rendszerének alapja

Az ÁSZ jogállását és hatáskörét az ÁSZ tv. határozza meg. Az ellenőrzések általános hatáskörrel kiterjedhetnek a közpénzekkel és a közvagyonnal való felelős gazdálkodás, ezáltal a működés és gazdálkodás IT alkalmazásokkal való támogatásának ellenőrzésére is.

Az ellenőrzés célja szerinti megállapítás kialakítása az ellenőrzés szempontrendszerének az ellenőrzés típusától függően – az IT alkalmazás megfelelőségére vonatkozó kritériumokkal kiegészített – előre meghatározott kritérium rendszer felállításán alapszik. Az IT alkalmazás megfelelősége, szabályszerű működése, az alkalmazás kontrolljainak eredményessége, hatékonysága és gazdaságossága kritériumainak kialakítása során mind a jogszabályi követelmények, mind az általános sztenderdek, a jó gyakorlatok és az IT szakmai sztenderdek, ajánlások irányadóak.

2.3. Az ellenőrzés hatóköre és tárgya

Az ellenőrzés (modulszerű alkalmazás mellett és önálló ellenőrzési formában) szervezeti felépítéstől függetlenül egy működési, működtetési folyamat, feladatellátás vagy ügylet(csoport) információs folyamataiból kiindulva, a

folyamatban azonosított releváns kockázati pontokon a támogató informatikai alkalmazás külső és belső kontrollrendszerére irányul.

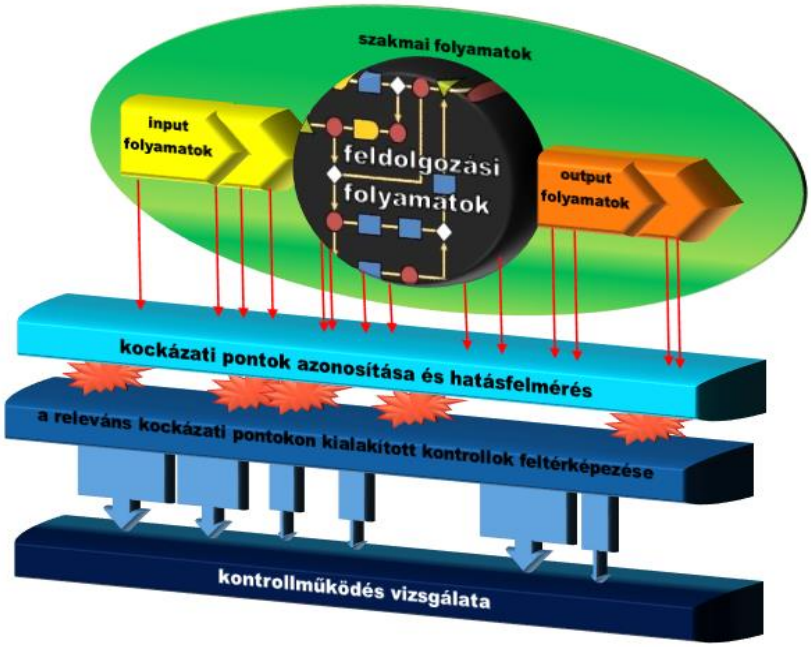
Az ellenőrzés hatóköre a kiválasztott folyamat vagy feladatellátás kontroll rendszerére, a folyamatot támogató informatikai rendszerekre és azok kontroll rendszerére terjed ki. Ugyanakkor az ellenőrzésnek nem tárgya a folyamatokat támogató IT alkalmazások middleware és hardware infrastruktúrája, ezt mutatja be a 2. sz. ábra.

2. sz. ábra - Ellenőrzési hatókör a szakmai folyamatok, illetve annak támogatása rendszerében

Forrás: ÁSZ grafika

A 3. sz. ábra azt mutatja be, hogy az IT alkalmazások folyamatorientált ellenőrzése a szakmai folyamatokban azonosított releváns kockázati pontokon az IT alkalmazások kockázatait kezelő külső kontroll környezet és belső kontroll rendszer ellenőrzésére irányul. Ezáltal az ellenőrzési hatókör kiterjed az alkalmazás által kezelt és feldolgozott, valamint az alkalmazás által előállított adatok (output) és információk integritására, időszerűségére, biztonságára, bizalmasságára, sértetlenségére, rendelkezésre állására, megbízhatóságára, teljes körűségére és pontosságára.

3. sz. ábra - Az ellenőrzés hatóköre és folyamata



Forrás: ÁSZ grafika

2.4. A kockázati megközelítés alkalmazása

Az IT alkalmazások folyamatorientált ellenőrzésének előkészítése és végrehajtása során több szinten és egymásra épülő módon szükséges értelmezni a kockázati megközelítést.

Az IT alkalmazások folyamatorientált ellenőrzése esetén az ellenőrzés tárgyát képező folyamat vagy feladatellátás részletes lépéseinek, folyamatának részletes elemzése mutat rá a kockázati pontokra. A kockázati megközelítés alkalmazásával - az azonosított kockázati pontokon a kockázati tűrőképesség meghatározása mellett - döntést kell hozni az adott kockázat elfogadható szintre csökkentésének szükségességéről (relevanciájáról) és módszeréről. Az ellenőrzés során a kockázati tűrés felülvizsgálata mellett szükséges megítélni, hogy a kockázatok kezelésére megtörtént-e az alkalmazás kontrolljainak kiépítése és a kiépített kontrollok működnek-e, működésük megfelel-e – ellenőrzési típustól függően – a szabályszerűségi, eredményességi, hatékonysági és gazdaságossági kritériumoknak.

Az ellenőrzés tárgyát képező folyamatot támogató informatikai alkalmazás(ok) és az alkalmazás kontrolljai közül tesztelésre történő kiválasztás, illetve a tesztadatbázisok összeállítása során a kockázati megközelítés alkalmazása biztosítja azt, hogy az ellenőrzés megállapításai a releváns, jelentős hatással bíró elemekre vonatkozzanak. Így végső soron az ellenőrzés megállapításai olyan következtetések levonására lesznek alkalmasak, melyekkel az ellenőrzés célja elérhető. Az ellenőrzés a kockázatosnak tekintett területekre fókuszál.

Az ellenőrzés során az informatikai kulcskontrollok meghatározása az - ellenőrzés tárgyát képező folyamat vagy feladatellátás részletes megismerését követően - azonosított kockázatok bekövetkezésének és hatásának felmérésével lehetséges.

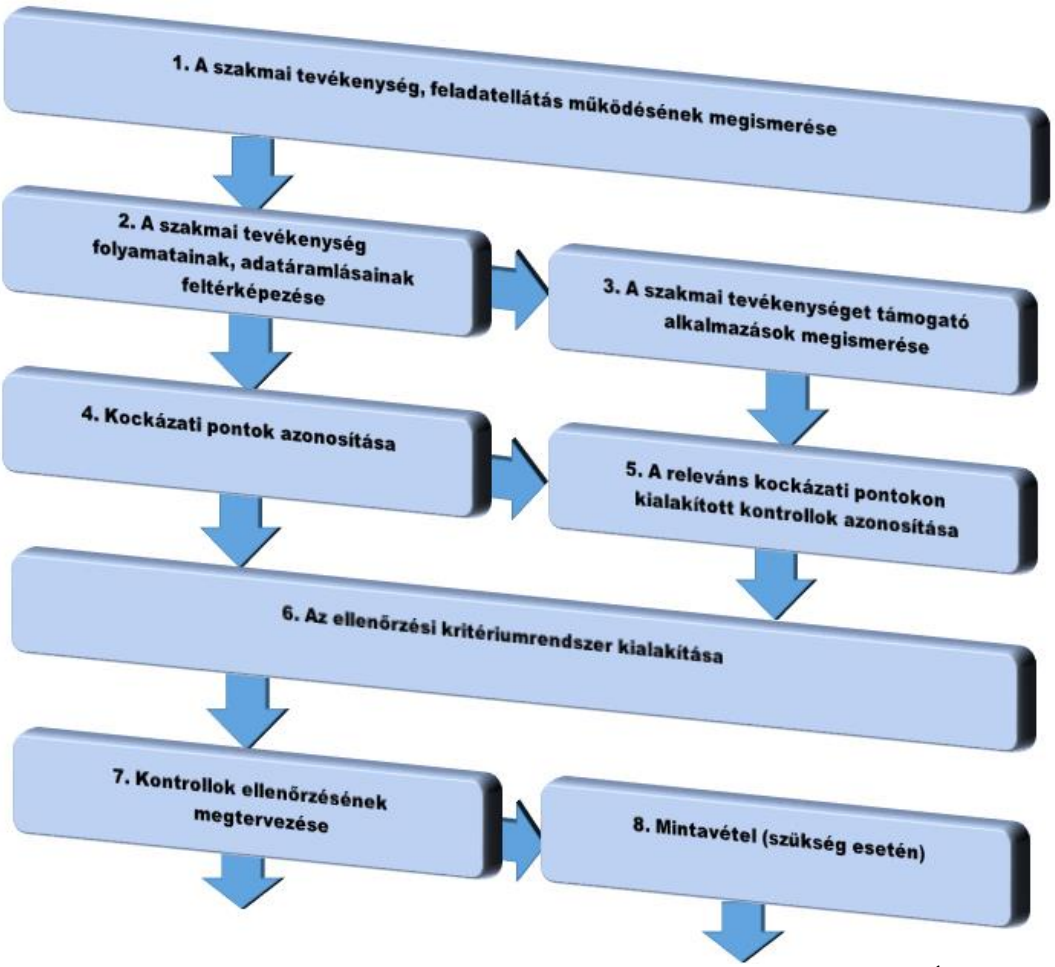
3. AZ ELLENŐRZÉS LEFOLYTATÁSA

Az IT alkalmazások folyamatorientált ellenőrzése során a Számvevőszék működésére vonatkozó alapelvek mellett az előkészítés és a végrehajtás során szükséges figyelemmel lenni az ellenőrzés típusához kapcsolódó alapelvben és módszertani útmutatóban rögzítettekre.

3.1. Az ellenőrzés előkészítése

Az IT alkalmazások folyamatorientált ellenőrzésének előkészítése szerves részét képezi a szervezet, a feladatellátás, vagy folyamat ellenőrzése előkészítésének (mely ellenőrzéshez modulszerűen tartozik). Modulszerűen megtervezett ellenőrzés esetén az előtanulmány és az ellenőrzési program kialakításánál az egyes ellenőrzési modulok szinkronitásának megteremtése biztosítja azt, hogy az ellenőrzés megállapításai és következtetései összehangolt egészet alkossanak. Az Útmutató az IT alkalmazás ellenőrzés sajátos lépéseit és az ellenőrzési típusok alapelveiben és módszertani útmutatóiban nem tárgyalt jellegzetességeit mutatja be. Az ellenőrzés előkészítésének folyamatát a 4. sz. ábra jeleníti meg, és a következő lépésekre tagolja:

4. sz. ábra - Ellenőrzési folyamat – előkészítés



Forrás: ÁSZ grafika

3.1.1. Az ellenőrzött terület megismerése

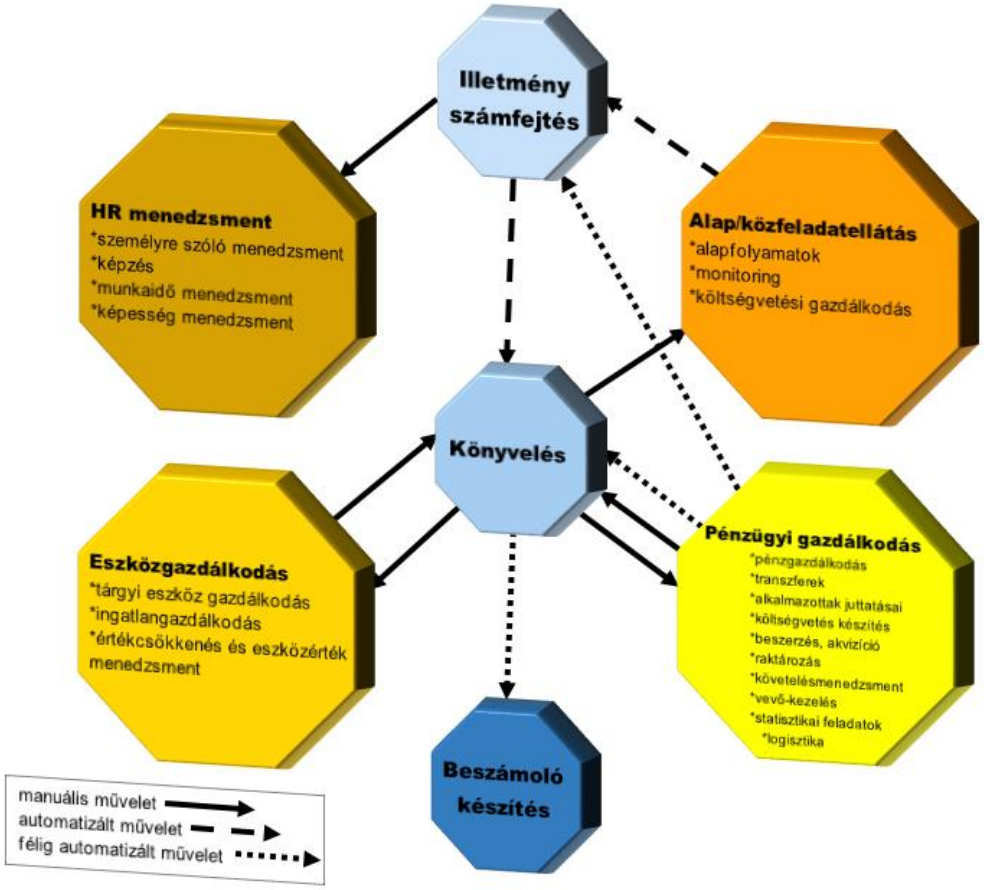
Az IT alkalmazások folyamatorientált ellenőrzése jellegéből adódóan nagy hangsúlyt helyez a kiválasztott feladat, folyamat megismerésére, adatáramlásai, valamint az azokat támogató IT alkalmazások feltérképezésére. Szintén a megismerési szakasz fontos eleme a feltérképezett folyamatok releváns kockázati pontjainak feltárása, valamint az azok kezelésére alkalmazott kontrollok azonosítása. A megismerés gyakorlati módszereit tekintve a folyamatfelbontás és –analizálás ábrázolás-technikai megoldásait célszerű alkalmazni.

3.1.2. A szakmai folyamatok értelmezése, az adatáramlások feltérképezése

Az ellenőrzés tárgyát képező folyamat vagy feladatellátás részletes megismerésének az IT alkalmazás ellenőrzés szempontjából alkalmas módja a folyamat alapú megközelítés.

Amint azt az 5. sz. ábra is szemlélteti egy leegyszerűsített elméleti példa segítségével, az alkalmazás nem kizárólag automatizált funkciókat jelent, hanem olyan eljárások és műveletek összességét, melyek valamely (rész)feladat ellátásához szükségesek. A feladat lehet továbbá pénzügyi természetű, nyilvántartás létrehozásával vagy nyilvántartások közötti műveletek lebonyolításával kapcsolatos, működtetéssel, vagyongazdálkodással, HR menedzsmenttel (humán erőforrás gazdálkodással) összefüggő, illetve más, a szervezet által ellátott (köz)feladathoz (közvetlenül vagy közvetve) kapcsolódó.

5. sz. ábra – Példa a szakmai feladatok és adatkapcsolatok ábrázolására



Forrás: ÁSZ grafika

Az ellenőrzött folyamat (pl. beszámoló-készítés, illetményszámfejtés, stb.) vagy feladatellátás (pl. nyugdíjszerű ellátások folyósítása) működési környezetének megismerése során ismereteket kell szerezni arról, hogy a szakterületi előírások alapján milyen adat és információs folyamatok relevánsak az ellenőrzés szempontjából (pl. nyugdíjszerű ellátások folyósítása esetén a vonatkozó jogszabályok megismerése, az igénylés, igényelbírálás, és a tényleges folyósításhoz kapcsolódó előírások, belső szabályozások és elvárások, stb.) Az ellenőrzés alá vont folyamat vagy feladatellátás működési környezetéből adódó információs folyamatok megismerése egyúttal az információáramlásra és az információs életciklusra is rámutathat.

A szakmai folyamatok elemzésének lehetséges lépései:

1. Az ellenőrzött terület szabályozási környezetének megismerése
   a. külső szabályozási környezet megismerése
   b. belső szabályozási környezet megismerése
2. Az ellenőrzött terület adatáramlásainak feltérképezése
   a. az adatáramlás bemeneti elemeinek (adatok, információk, egyéb elemek) meghatározása
   b. az adatáramlás bemeneti elemei főbb jellemzőinek megismerése (pl. elektronikus-e, aggregált-e, stb.);
   c. az adatáramlás kimeneti elemeinek megismerése;

d. az adat- és információáramlások jellegének (manuális, automatizált) és kapcsolódási pontjainak feltérképezése;
e. a folyamatokhoz és kapcsolódási pontokhoz tartozó szereplők, felelősök, rendszerek megismerése.

Az ellenőrzött folyamat részfolyamatokra bontása során meg kell állapítani, hogy melyek az egyes részfolyamatok - ellenőrzés célja szempontjából - releváns eredményei, kimenetei. Azonosítani kell azokat a műveleteket, folyamatokat, alfolyamatokat és szereplőket (szervezeti egységek, rendszerek, felelősök), amelyek ezeket az eredményeket, az adatáramlás kimeneti elemeit generálják. A részfolyamatok kockázati megközelítésű elemzése biztosítja az ellenőrzött folyamat vagy feladatellátás megvalósítására, eredményére és működésére hatást gyakorló kockázati pontok felismerését.

Az ellenőrzött folyamat vagy feladatellátás eredményét, kimenetét befolyásoló rutin eseményeken (alfolyamat, művelet, stb.) túl az ellenőrzött időszakban jelentkező – szintén befolyással bíró – nem rutin események megismerésére is nagy hangsúlyt kell fektetni. (pl.: új IT rendszer, vagy új alkalmazások bevezetése, jogszabályi változások, felelősségi viszonyok változása, stb.)

A megismerés és a kockázati megközelítés alkalmazásának szemléletes módszere az ábrázolással egybekötött „feltérképezés" (mapping). E technika segít az ellenőrzés célja szemszögéből nem releváns részfolyamatok azonosításában is. Szükséges lehet a megismert adatáramlások és kapcsolódások részfolyamatonként történő ábrázolása. A folyamatokhoz kapcsolódó kockázatok és kontrollok együttes megjelenítése történhet táblázatos formában vagy folyamatábrák készítésével. Az ellenőrzés szempontjából releváns elemek, folyamatok korai meghatározásának előnye, hogy még a kockázatelemzés előtt ki lehet szűrni a kevésbé lényeges alfolyamatokat, elemeket.

Az ábrázolásnak minden esetben átlátható módon kell bemutatnia az egyes alfolyamatok be- és kimeneti elemeit, a feldolgozási folyamatokat, az alfolyamatok kapcsolódási pontjait, az adatáramlásokat, a feldolgozás, folyamat és adatáramlások jellegét (manuális, automatikus), valamint a folyamatban résztvevő szereplőket (felelősök, rendszerek, szervezeti egységek).

Pl. a bérszámfejtés az alábbi alfolyamatokat tartalmazhatja: alkalmazottak törzsadatainak kezelése; bérjegyzékek előkészítése; munkabér és juttatások kifizetése; bérfizetés könyvelése, stb. Az értékesítés az alábbi alfolyamatokat tartalmazhatja: vevői törzsadatbázis kezelése, karbantartása; értékesítés tárgyi megvalósítása; bevétel könyvelése, stb.

3.1.3. Az ellenőrzött folyamat, feladatellátás kockázati pontjainak azonosítása

Az ellenőrzési terület megismerésének következő lépése az ellenőrzött folyamat, feladatellátás kockázati térképének elkészítése. Kockázatként értelmezzük azokat a tényezőket, amelyek az ellenőrzött folyamat, feladatellátást támogató informatikai megoldás által előállított kimenet integritását, időszerűségét, biztonságát, bizalmasságát, sértetlenségét, rendelkezésre állását, megbízhatóságát, teljes körűségét és pontosságát veszélyeztetik. Gyakorlatilag minden feltárt adatáramláshoz (mind a bemeneti, mind a kimeneti ponttal együtt), minden feldolgozási ponthoz, illetve adatáramlás szempontjából

releváns elemhez fel kell tenni a kérdést, hogy mi okozhat hibát, rendellenességet.

A felmérendő kockázatok alapvetően két forrásból eredhetnek, elsősorban a folyamat vagy feladatellátás szakterületi környezetéből és másodsorban az informatikai eszközök alkalmazásából. Ha az ellenőrzésben érintett szervezet rendelkezik a folyamataira vonatkozó kockázatelemzéssel, az az ellenőrzés során felhasználható.

A kockázati pontok feltárása során kiemelt figyelmet kell szentelni annak azonosítására, meghatározására, hogy az adott kockázat az ellenőrzés mely alszempontjára van hatással. Így a kockázati pontok kezelésére alkalmazott kontroll kritériumoknak való megfelelés alapján adható válasz az ellenőrzési cél és annak alszempontjai kérdéseire.

Valamennyi beazonosított kockázatról el kell dönteni, hogy az ellenőrzött folyamat jellegéből, környezetéből adódó kockázatot, vagy az informatikai alkalmazásból eredő kockázatot jelent.

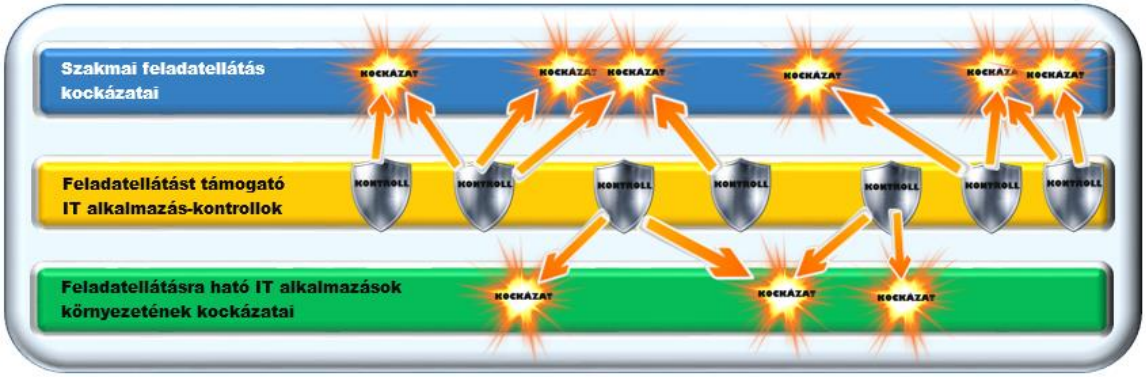
Informatikai alkalmazásból eredő kockázat lehet többek között az adatok kezelésére, feldolgozására és kibocsátására alkalmatlan informatikai infrastruktúra vagy informatikai kontroll környezet kialakításának, az adatvesztés és -sérülés, az adat hozzáférés korlátozottsága, helytelen adathozzáférés, az adatok és információk precizitása sérülésének, a helytelen/nem érvényesített adatok bevitelének és feldolgozásának, az adatok kibocsátása során a helytelen érzékenyítés, az alkalmazások komplexitásából eredő adatkapcsolatok asszinkronitásának, stb. kockázata.

A feltárt szakmai folyamatokhoz kapcsolódó kockázati pontok egy része megfeleltethető az adott (al)folyamatot támogató, azt végrehajtó IT alkalmazásokból adódó kockázatoknak. A folyamat elemeinek automatizálása ugyanis számos újabb kockázati pont kialakulását eredményezheti (pl. a felelősség megosztások beépítésének problémái, a magas fokú integráció következtében fellépő általánossá vált manuális kontrollok hiánya, a valós idejű feldolgozások). A működési és gazdálkodási folyamatok kockázati pontjainak informatikai alkalmazásokra történő kivetítése, megfeleltetése ugyanakkor nem feltétlenül ad teljes körű képet a folyamat és az alkalmazások szintjén megjelenő kockázatokról. Ezért az informatikai alkalmazások megismerése során megszerzett információk alapján meg kell vizsgálni, hogy az adott alkalmazás milyen további kockázati pontokkal rendelkezik.

Ezen túl fel kell mérni az ellenőrzésre kiválasztott folyamat végső kimenetével, illetve annak paramétereivel kapcsolatban, hogy azok mely esetekben nem tekinthetőek megfelelőnek és ennek milyen okai lehetnek.

A 6. ábra a feladatellátás szakmai és informatikai adat folyamatainak elemzése alapján azonosított kockázatok és az IT alkalmazással való támogatásból eredő önálló kockázatok, valamint az alkalmazásba beépített kontrollok közötti viszony egyes eseteit mutatja be. Az ábrából látható, hogy egy-egy kockázatot több kontroll is kezel, egyes kontrollok rendszerbe építése több kockázathoz, általános kockázatokhoz, az informatikai környezet meglétéhez vagy a teljes szakmai folyamathoz is kapcsolódhat.

6. sz. ábra – Példa a folyamatok elemzése alapján azonosított és az IT alkalmazással való támogatásból eredő önálló kockázatok, valamint a beépített kontrollok viszonyának ábrázolására



Forrás: ÁSZ grafika

A kockázati hatások csoportosítása

Amennyiben a kockázatok azonosítása megtörtént, szükséges bekövetkezési valószínűségük meghatározását követően azok hatását felmérni. A kockázat típusok hatás alapján történő csoportosítása lehet pl. a következő (egy-egy kockázat több hatással is járhat):

- pénzügyi, vagyoni kockázat – azaz a szervezet pénzügyi vagy vagyoni helyzetére gyakorolt negatív hatás;
- megfelelőségi kockázat – azaz a szervezet nem tud eleget tenni a szabályszerűségi és egyéb követelményeknek, elvárásoknak;
- információ biztonsági kockázat – azaz illetéktelenek hozzáférnek meghatározott, számukra nem nyilvános információkhoz, vagy az adat/információ nyújtása nem megfelelő;
- működési kockázat (a feladatellátás minőségi megvalósításának kockázata) – pl. validálás, vagy helytelen feldolgozás kockázata; csökkent rendelkezésre állás kockázata; költséges kompenzációs kontrollok beépítési kötelezettségének kockázata; az információ hitelességének kockázata, stb.;
- csalás kockázata – azaz egyéni haszon reményében szándékos megtévesztés vagy szándékos károkozás történik a szervezetet vagy a szervezetben dolgozó személyeket érintően.

A kockázatok lehetséges hatásainak meghatározása során minden esetben szükséges az ellenőrzési célokkal való kapcsolat feltérképezése. A kockázatok hatás alapján történő kategorizálása a végső következtetések, javaslatok kialakításához szintén fontos segítséget nyújt.

Annak ellenére, hogy az ellenőrzés fókuszát elsősorban a szakmai folyamatok és az azokat támogató informatikai alkalmazások képezik, az általános informatikai kontrollok kiválasztott IT alkalmazás vonatkozásában történő ellenőrzését el kell végezni. Ezek jelentős hatással vannak nem csak a szakmai folyamatok, de az informatikai alkalmazások kockázataira is (például: változáskezelés- és fejlesztés menedzsment, összeférhetetlenség szabályozás, adatbázis kontrollok, konfiguráció menedzsment).

3.1.4. Az IT alkalmazás részletes megismerése

Az IT alkalmazások folyamatorientált ellenőrzése nem ellenőrzött szervezethez, hanem az ellenőrzés célja szerinti ellenőrzött folyamathoz vagy feladatellátáshoz kapcsolódik. Ezáltal az ellenőrzés fókuszába egyes esetekben egy szervezet informatikai alkalmazásai, más esetekben olyan IT alkalmazások kerülnek, melyeket több szervezet vagy (különböző szervezetekhez tartozó) szervezeti egység(ek) együttesen hoznak létre, kezelnek, vagy nyernek abból információt további feldolgozás céljából. Az ellenőrzésre kerülő IT alkalmazások nem szükségszerűen ugyanazon szervezet informatikai rendszerének részei, melynek a folyamatait támogatják.

Az ellenőrzött folyamat, feladatellátás egy vagy több, kapcsolódó vagy különálló informatikai alkalmazással való támogatásának feltérképezése mellett az alkalmazások kapcsolódási pontjainak ábrázolása is segítheti a kontrollpontok feltárását, mert azok összhangja vagy kapcsolata a feltárt adatáramlások ábrázolásakor esetenként nem egyértelmű. Különösen igaz ez az integrált alkalmazásokra. Néhány szakmai folyamatot pl. ugyanazon alkalmazás is támogathat, míg más folyamatok kiszolgálása több alkalmazással történik meg.

Az informatikai alkalmazások alábbi három típusát különböztetjük meg:

- Standard (dobozos) informatikai alkalmazások: olyan általánosan használt, illetve forgalmazott szoftvereket értünk alatta, melyeket szakmai felhasználásra fejlesztettek ki, de nem szervezet-specifikusan. Ilyenek például a szektor-specifikus szakmai szoftverek, irodai multifunkcionális programok, az ügyviteli vagy dokumentumkezelő speciális informatikai alkalmazások, a nyilvántartási szoftverek, a számviteli és a HR menedzsment szoftverek. Ellenőrzési szempontból a szabványos alkalmazások előnye, hogy magas színvonalon tervezettek, fejlesztettek, teszteltek és dokumentáltak. Leggyakoribb készen beszerezhető szoftverek a pénzügyi, bérszámfejtési, személyzeti, eszköznyilvántartó szoftverek.
- Dedikált (testreszabott) informatikai alkalmazások: szervezet specifikus alkalmazások, melyeket egy adott szervezet igényei szerint fejlesztettek ki. A szabványos alkalmazásokkal szemben számos előnye és hátránya lehet (előny lehet pl. a folyamatok pontos leképezése, igények szerinti kialakítása, a felhasználók által végrehajtott tesztek; hátrány lehet pl. a hardver korlátozottság, a fejlesztés során a fejlesztő nem kap meg minden szükséges információt, a külső fejlesztő nem bocsátja rendelkezésre a dokumentációt, szerződési garanciák problémái, stb.).
- Saját fejlesztésű informatikai alkalmazások: a szervezeten belül, saját erőforrással fejlesztett szoftverek előnye lehet, hogy a dedikált alkalmazásokhoz hasonlóan a szervezet jellemzőihez, egyedi igényeihez igazított fejlesztés, a fejlesztők szakmai folyamatokkal kapcsolatos informáltsága magas szintű. Hátrányként jelentkezhet a legújabb, legmagasabb minőségi szintű informatikai eszközök és technikák ismeretének, gyakorlatának hiánya, illetve a költségvetési korlátok fokozott alkalmazása.

Az ellenőrzött területhez kapcsolódó informatikai alkalmazások megismeréséhez, kockázatainak feltárásához az alábbi információkkal szükséges rendelkezni:

- az alkalmazás neve, azonosítója, verziószáma
- az alkalmazás rövid leírása (felhasznált adat típusa, adatmozgás, előállított adat típusa, adatfeldolgozási művelet, feldolgozási gyakoriság, kapcsolódás más alkalmazásokkal)
- az alkalmazás felelőse és az adatgazdák
- az alkalmazás típusa
- az alkalmazás fizikai környezete (milyen technikai infrastruktúrába ágyazottan működik – csak amennyiben az IT alkalmazás kockázatait és kontrolljait e tényezők befolyásolják)
- összes felhasználó száma
- kapcsolódó szerepkörök, jogosultságok
- egyéb IT alkalmazásokkal való kapcsolatok
- telepítés dátuma
- utolsó (forráskód) módosítás dátuma
- az utolsó és a tervezett módosítások oka
- az alkalmazás ismert (általános és specifikus) problémái, korlátai.
- az alkalmazás garanciái és fejlesztői támogatása.

Az alkalmazások megismerésének forrásai elsősorban a szervezeti kontrollkörnyezet alkalmazás-specifikus elemei (szabályzatok, eljárásrendek), az alkalmazás fejlesztői specifikációja és dokumentációja, a tervezett biztonsági eljárások leírása, a program szerkezet, a felhasználói kézikönyv, a működtetési leírás, a megrendelés, a tesztelési dokumentum, a helpdesk jelentés, az adatleltár, az archívum, a háttértár, a visszaállítási eljárások jegyzőkönyve, stb.

3.1.5. Kontrollok azonosítása

A kontrollok azonosításának módszere a végigkövetés (walkthrough), melynek alkalmazásakor a tipikus bemeneti adatok útját kell dokumentáltan követni egy-egy szakmai folyamatban, annak valamennyi lépésén át. A végigkövetés által a már feltérképezett szakmai folyamatok valós működéséről (automatikus és manuális lépéseiről) és a folyamatba épített kontrollok meglétéről kapunk információkat.

A végigkövetés egy ellenőrzést támogató eszköz annak biztosítására, hogy az ellenőrzést végző teljes egészében beazonosítsa és megértse a folyamat, feladatellátás működésének és működtetésének valamennyi elemét, a releváns kockázatokat és kontrollokat. Végigkövetés adhat segítséget a következőkhöz:

- az adatáramlások és folyamatok megértéséhez;
- a meglévő dokumentumok és folyamatábrák konzisztenciájának és szignifikanciájának megítéléséhez;
- a kontrollpontok feltérképezéséhez;
- az érintett tevékenységi terület fő felelősei megismeréséhez;
- a tevékenységgel kapcsolatos dokumentumok körének megismeréséhez;
- a kontroll tevékenység elemei, működése megismeréséhez;
- a kontroll jellegének azonosításához: megelőző, feltáró vagy javító; automatikus, vagy manuális (és működési szükségességének gyakorisága);

- a kapcsolódó ellenőrzési nyomvonallal való viszony megismeréséhez.

A kockázatok kezelésére alkalmazásba épített és az alkalmazás környezetében kialakított kontrollok egyaránt alkalmazhatóak. Az alkalmazás kontrollok azok az automatizmusok és eljárások, amelyek biztosítják az adatfeldolgozási műveletek és adatok (nyilvántartások) jóváhagyását, integritását (sértetlenségét), precizitását (hibamentességét) és érvényességét (hatályosságát). Az informatikai eszközökkel támogatott alkalmazás kontrollok az informatikai alkalmazásba beágyazottak. Céljuk az adatáramlások komplexitásának, megbízhatóságának és precizitásának biztosítása.

A kiépített kontroll típusát tekintve lehet teljes egészében automatizált, részben automatikus és manuális. Jelleg szerint megkülönböztethetünk megelőző, feltáró és javító kontroll mechanizmusokat.

- Megelőző (preventív) kontrollok: a kockázatok bekövetkezését, illetve valószínűségének csökkentését hivatottak szolgálni.
- Feltáró (detektív) kontrollok: a kockázatok hatását segítenek észlelni, de a „hibát" nem korrigálják.
- Javító (korrektív) kontrollok a bekövetkezett és feltárt hiba kijavítását, helyreállítást szolgálják.

A kontrollok rendszert alkotnak, melyben a folyamat vagy feladatellátás jellegétől függően meghatározhatók a kulcskontrollok. E kiemelt kontrollok játsszák az ellenőrzés kritérium- és súlyozási rendszerének kialakításakor a legfontosabb szerepet.

A 7. sz. ábra egy leegyszerűsített példát mutat be arra, hogy a kockázatok és kockázati pontokhoz kapcsolódó kontrollok feltárását az összefüggések táblázatos formában történő feltérképezése segíti.

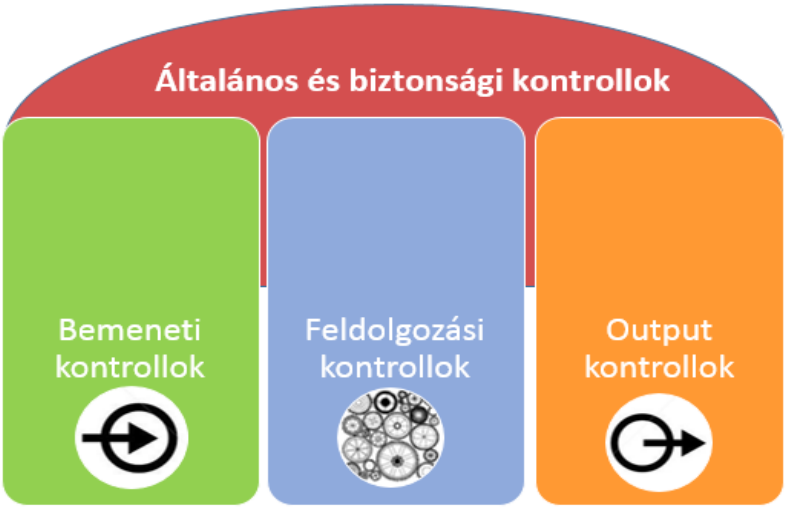
7. sz. ábra – Példa a kockázati pontokhoz kapcsolódó kontrollok feltérképezésére, bemutatására

kockázati pont	kontrollok	a kontroll működtetése			kontroll típus			mely követelményt elégíti ki az adott kontroll működtetése										
"mi romolhat el?"		ki a felelőse?	mikor lép működésbe?	hogyan működik?	feltáró	megelőző	javító	validálás	értékhelyesség	helyes időszak terhelése	jogok és kötelezettségek	allokáció	pozícionálás	érvényesítés	dokumentálás elve	naplózás	adat rendelkezésre tartás	ellenőrizhetőség
A	A1	pl. rendszergazda	pl. előzetes	pl. leírás a dokumentáció 6. oldalán		*	*				*			*		*	*	*
	A2	pl. felhasználó	pl. tranzakció futtatásakor	pl. felhasználó indítja a szabályzatban meghatározott esetekben	*					*			*					
B	B1	pl. felhasználó munkahelyi vezetője	pl. kizárólag adott értékhatár felett, utólagos	pl. teljesen automatizált, ld User Manual 17. o.	*			*	*		*					*		
…	…																	
…	…																	

Az alkalmazás kontrollok adatáramlásbeli pozíciója szerinti főbb csoportjait a 8. sz. ábra mutatja be, melyek jellemzőit e fejezet a következők szerint taglalja:

A általános és biztonsági kontrollok
B bemeneti (input) kontrollok
C feldolgozási kontrollok
D kimeneti (output) kontrollok

8. sz. ábra – Az alkalmazás kontrollok adatáramlásbeli pozíciója szerinti főbb csoportjai



Forrás: ÁSZ grafika

Az ábrán is látható módon az IT alkalmazások általános és biztonsági kontrolljai átjárják a bemeneti, feldolgozási és kimeneti kontrollokat, azokkal közös metszetet is képeznek.

A - Az alkalmazás általános és biztonsági kontrolljai

Az általános kontrollok lényeges, elsődlegesen meghatározó hatást gyakorolnak az alkalmazás megbízható és megfelelő működésére, funkcionalitására. A biztonsági kontrollok biztosítják az alkalmazás megbízhatóságát és az alkalmazással kezelt és előállított adatok integritását, bizalmasságát, sértetlenségét és rendelkezésre állását.

Ezen kontrollok ellenőrzése kiemelten fontos, mivel az alkalmazás bemeneti, feldolgozási és kimeneti kontrolljainak működésére is jelentős hatással vannak, illetve specifikusan megjelennek azok szintjén is.

A teljes informatikai rendszer általános kontrolljainak ellenőrzéséhez képest lényegesen szűkebb terület az adott IT alkalmazáshoz közvetlenül kapcsolódó általános és biztonsági kontrollok ellenőrzése.

Hangsúlyosak az adott alkalmazás funkcionalitást érintő általános kontrolljai, melyek jellemzően a fejlesztésmenedzsment és a változáskezelés területeihez kapcsolódhatnak:

- rögzített eljárások a feladat vagy folyamat végrehajtásában bekövetkező (jogszabályi és egyéb) változások alkalmazásba építésére;
- az alkalmazással szemben támasztott funkcionális és biztonsági követelmények dokumentáltsága;
- alkalmazás fejlesztési terv és részletes terv dokumentációja;
- szakmai jóváhagyások;
- minőségbiztosítási eljárások kidolgozottsága, tesztelési tervek (funkcionális, integrációs, stb.) és dokumentáltan végrehajtott tesztelés;
- fejlesztés szakmai igazolása;
- dokumentált konfigurációs menedzsment;
- változások végrehajtásának dokumentált megtervezése és végrehajtása, stb.

Az adott alkalmazás általános és biztonsági kontrolljai jellemzően a következők lehetnek:

- alkalmazás és egyes műveleteinek speciális hozzáférési kontrolljai (fizikai és logikai);
- alkalmazás felhasználói, fejlesztői, felelősei és rendszergazdái közötti feladatkörök szétválasztása;
- az alkalmazás, illetve forráskódjainak tulajdonjogi helyzete,
- az alkalmazás működtetésében résztvevő szervezettel (szervezetekkel) kötött szerződések garanciális elemei, az SLA-k;
- az alkalmazás üzletmenet-folytonossági kontrolljai (mentés, tárolás, katasztrófa-kezelés, archiválás, stb.);
- adatbáziskontrollok;
- konfigurációs kontrollok, stb.

Az alkalmazásokhoz kapcsolódó általános és biztonsági kontrollok általában nem csak az alkalmazások szintjén jelennek meg, hanem szervezeti és szabályozási szinten is (pl.: jogszabályváltozásból eredő alkalmazás fejlesztések és kiegészítések dokumentáltságának előírásai nem egy-egy alkalmazás dokumentumaiban, hanem szervezeti szintű szabályozásokban jelennek meg).

B - Bemeneti (input) kontrollok

Az input kontrollok célja részben az alkalmazás funkcionalitásának biztosítása, részben az alkalmazásba bekerülő adatok és információk pontosságának, teljeskörűségének és ellenőrzöttségének biztosítása. Az input adatok kontrollja a manuális és az alkalmazásba beépített automatizált, fél-automatizált kontrollok kombinációja. Az input kontrollok biztosítják az alkalmazásba bejövő adatok, információk integritását, azaz érvényesítettségét (validitását, jóváhagyását), pontosságát, teljeskörűségét és időszerűségét (időbeli relevanciáját).

Biztonsági input kontrollok lehetnek:

- az input adattartalom megfelelő időben történő rendelkezésre állásának ellenőrzése;
- az input adatokhoz való hozzáférések kontrolljai;
- sztenderdizált adat input mezők (pl. strukturált képernyő mezők, adatbeviteli mezők, választómezők, mezőszintre delegált jogosultságok)
- adatbeviteli jóváhagyás, melynek célja, hogy minden bejövő adatot rögzítsen és jóváhagyjon az erre kijelölt személy vagy jogosultsági csoport (pl. jelszó, manuális adatrögzítés esetén jogosultsági napló, érzékeny információt érintő adatbevitel esetén „négy szem" elvű jóváhagyási funkció);
- input dokumentum késleltetés, mely az eredeti dokumentum ellenőrzésére és karbantartására szolgál;
- input adat érvényesítése, hatályosítása (pl. hiányzó értékek automatikus hibalistázása, külön jogosultsággal bevihető adatmezők definiálása és a kapcsolódó engedélyezés hitelesítése, bevitt adat módosításának akadályozása, összefüggő adatmezőkön az adatbevitel logikai kapcsolása, sajátos „adatbeszúrás" szabályai, logikai korlát az időadatokra vonatkozóan – pl. jövőre vonatkozó adatbevitel korlátozása);
- adatbeviteli hibák kezelése (pl. felelősség meghatározása mellett a hibás tevékenységek naplózása, a kezeletlen hibákról rendszeres összesítés készítése, hibajavítás kezelése, automatikus adatfeltöltés esetén az adatfolyamban fellelt folytonossági hiány esetén automatikus jelzés készítése, rendszeres összefoglaló készítése a nem javított hibákról azok keletkezési idejének és a javítás prioritásának megjelenítésével);
- az adatbevitel technikai megoldásába épített kontrollok (pl. kezdőérték újrakalkulálás, a felhasználók tevékenységének monitorozása a meghatározott szabályoktól való eltérő tevékenységek kiküszöbölésére).

Funkcionalitáshoz kapcsolódó input kontrollok lehetnek:

- az input adattartalom szükségességének és elégségességének ellenőrzése;
- adat előállítási rutinok, melyeknek célja az adatbeviteli hibák keletkezésének megakadályozása;
- az alkalmazás nem engedi meg a duplikációt (tiltó kontrollok és a megszüntetésre irányuló automatizmusok);

- érzékeny adatok többszörös érvényesítése, jóváhagyása;
- egyszeres adatbevitel, vagy előre meghatározott szabály szerinti adatbeviteli ismétlődés engedélyezése; stb.

További lehetséges biztonsági input kontrollok:

- egyes, minősített adatok bevitele nélkül az alkalmazás nem futtatja le a feldolgozási folyamatot;
- az alkalmazás nem fogad helytelen (a definiálttól eltérő) vagy feldolgozásra alkalmatlan adatot;
- nem lehetséges átfedés vagy rés, az alkalmazás kontrolljai logikai ellenőrzést végeznek az adatok és folyamatok időbeli keletkezésére nézve figyelembe véve az egymásutániságot; (pl. az adatok időbeli keletkezését illetően, vagy az adatok keletkezési ideje szerinti sorrend megbomlása esetén szűr).

C - Feldolgozási (process) kontrollok

A feldolgozási kontrollok biztosítják az adatfeldolgozás precizitását, teljeskörűségét, időszerűségét és funkcionalitását a folyamatban. Ezek a kontrollok hozzájárulnak ahhoz, hogy az adatok alkalmazás által történő feldolgozása precíz legyen, azaz sem a folyamatba nem tartozó adat hozzáadása, sem a ténylegesen szükséges adat elvesztése vagy módosítása ne következzen be.

A feldolgozási folyamatok ellenőrzése során meg kell győződni arról is, hogy a jogszabályokban, belső szabályzatokban foglalt előírásokat és egyéb elvárásokat az alkalmazás műveletei teljes körűen és pontosan teljesítik-e.

A komplexitáshoz kapcsolódó kontroll lehet például az input adatok mennyisége, értéke és az output adatok mennyisége, értéke közötti egyensúly. Amennyiben az alkalmazás megosztott, vagy egyértelműen meghatározható szabály hiányában változó mennyiségű, más alkalmazásból származó adatot dolgoz fel, akkor kontrollként felhasználható az alkalmazások által használt adatlisták összevetése is. Alkalmanként a folyamat során feldolgozott adatok értékeiből kiindulva a folyamat logikai pontjain meghatározott részösszegek és a következő munkafolyamat bemeneti adatértékének összevetése jelenthet kontrollt.

Biztonsági folyamat kontrollok lehetnek:

- hiba-fájl automatikus létrehozása, rögzítése;
- az alkalmazás által végzett feldolgozási lépésekhez (tasks) kapcsolódó feladatok, parancsok ütemezésének hozzárendelése;
- hiba esetén az alkalmazás automatikus üzenetet generál;
- valamely parancs, feladat végrehajtását követően az alkalmazás erről automatikus üzenetet generál;
- (adat) módosítást követően az alkalmazás erről automatikus üzenetet generál, a módosítás tartalmának megjelölésével;
- (adat) törlést követően az alkalmazás erről automatikus üzenetet generál, a törölt adat megjelölésével;
- amennyiben a törlés az adatbázis integritásának sérülését okozná, az alkalmazás nem teszi lehetővé a törlés végrehajtását;

- jogosulatlan vagy rossz szándékú beavatkozás esetén a beavatkozás rögzítése;
- az adat módosítása esetén a módosított adattal megismételt folyamat ellenőrzése, stb.

Funkcionalitáshoz kapcsolódó folyamat kontrollok lehetnek:

- az adatfeldolgozás lépései végrehajtási ismétlődésének előre meghatározott szempontok szerinti korlátozása;
- számításokat tartalmazó adatfeldolgozási lépések esetén matematikai kontrollok;
- adat módosítás esetén az adattal logikai kapcsolatban álló adatok módosítása megtörténtének ellenőrzése, stb.

D - Kimeneti (output) kontrollok

Az output kontrollok biztosítják a külső és belső szabályozó eszközökben foglalt előírásoknak és egyéb elvárásoknak való megfelelést, az alkalmazás kimeneti adatainak és információinak sértetlenségét, integritását és a hibamentes, időben történő kibocsátását. Alkalmanként a folyamat kontrollok hiányosságai output kontrollokkal kompenzálhatóak, azonban az input- és folyamat kontrollok működését a nem megfelelő output kontrollok ronthatják.

Az output fájlok jogosulatlan módosítása (jogosulatlan adat módosítás és manipuláció) elleni védelmet kontrollokkal kell biztosítani.

Az adott alkalmazás kimeneti adatai vagy információi, illetve ezek egy meghatározott része lehet egy másik alkalmazás inputja. Az ellenőrzési feladattól függően az ellenőrnek lehet feladata az is, hogy meggyőződjön az alkalmazások közötti adattranszfer kockázati pontjain kiépített kontrollok meglétéről és működéséről.

Biztonsági kimeneti (output) kontrollok lehetnek:

- az alkalmazás üzenete a feldolgozottság szintjéről;
- az adatfeldolgozás végeztével az alkalmazás automatikus üzenete a felhasználóknak;
- az output kibocsátásának rögzítése (kinek, mikor, milyen címen stb.);
- esetleges lekérdezésekhez kapcsolódó biztonsági kontrollok (pl. jogosultságok), illetve a lekérdezések eredményéhez kapcsolódó logikai kontrollok;
- az output és a lekérdezés eredménye pontosan megegyezik az alkalmazásban végrehajtott adatfeldolgozás eredményeként létrejövő és rögzített adattal (és a folyamat bármikor és bármennyiszer reprodukálható);
- az alkalmazások, feldolgozási szintek közötti precíz, hibamentes, teljes adat transzfer biztosítása, stb.

Funkcionalitáshoz kapcsolódó kimeneti (output) kontrollok lehetnek:

- automatikus mennyiségi és értékbeli összehasonlítás;
- a létrejött output formai, logikai összevetése az elvárt (rögzített paraméterek szerinti) outputtal;
- az output információtartalma teljeskörűségének ellenőrzése, stb.

Fontos kiemelni, hogy bizonyos kockázatok lefedése nem csak közvetlen kontrollokkal lehetséges, hanem ún. kompenzációs kontrollokkal csökkenthető

a kockázat bekövetkezésének valószínűsége, avagy feltárható a bekövetkezett kockázati esemény, és csökkenthető annak hatása.

Például amennyiben nem alkalmaznak hozzáférés kontrollokat (megelőző kontroll) a szakmai folyamat adott szintjén, de a naplózással kapcsolatos kontrollokat (feltáró kontroll) működtetik ugyanezen szinten, akkor ezek a kontrollok a sértetlenség és a bizalmasság kockázatainak kontroll hiányosságait kompenzálhatják.

3.1.6. Az ellenőrzés kritériumrendszerének kialakítása

A feltárt kockázatok, azok bekövetkezési valószínűsége és várható hatása ismeretében deklarált kockázati tűréshatárt meghaladó kockázatok kezelésére kontrollcélokat kell meghatározni. Kontrollcélként az az igény vagy követelmény definiálható, mely az elvárt eredmény eléréséhez szükséges kontrollokkal van összefüggésben (ellenőrzési szemszögből: elvárt kontroll).

Az ellenőrzés kritériumrendszerét az azonosított kockázatok lefedésére

- a jogszabályokban és belső szabályokban meghatározott,
- a szakterület speciális szabályozása szerinti,
- az IT szakmai sztenderdek szerinti, vagy
- az elvárt, tipikus, illetve ismert jó gyakorlat szerinti kontrollok alapján szükséges kialakítani.

A kockázati alapú megközelítés alkalmazásával a kritériumként meghatározott kontrollok értékelése során figyelembe kell venni azt is, hogy a kontroll hiánya vagy helytelen működése által kiváltott hatás alapján kulcskontroll vagy egyéb kontroll kategóriába tartozik-e. Kulcskontrollként szükséges megjelölni azokat a kontrollokat, amelyek elengedhetetlenek a kockázatok egy elfogadható vagy elfogadott szintre való csökkentése érdekében.

A kritériumrendszer kialakításakor azt kell meghatározni, hogy mely kontrolloknak milyen minőségi szinten történő kiépítése jelenti azt az elvárt szintet, amely az ellenőrzés során a minősítés alapja lesz.

Az elvárt kontrollok meghatározásakor figyelembe kell venni, hogy az adott kontroll működése összhangban van-e az ellenőrzött folyamatra vagy feladatellátásra vonatkozó jogszabályi, belső szabályzat szerinti előírásokkal, illetve a folyamat vagy feladatellátás felelősének (pl. a hatékony közpénzfelhasználás szempontját is tükröző) érdekeivel, szándékaival.

Az ellenőrzés a kontrollok működésének megfelelőségére és - az ellenőrzés típusától függően - hatékonyságára irányul.

A kontrollok működési hatékonyságának elemzése rávilágíthat arra is, hogy a választott kontrollmegoldás alternatívájának alkalmazásával lehetséges-e hatékonyabb megoldást elérni.

3.1.7. Kontrollok ellenőrzésének megtervezése

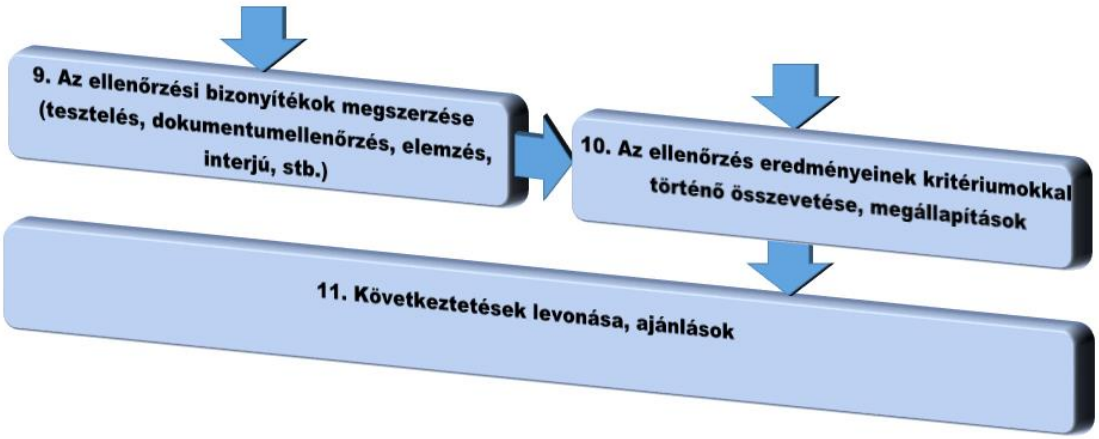
Az IT alkalmazás folyamatorientált ellenőrzése fő kérdésének megválaszolása a jelentős hatással bíró, kockázati megközelítéssel kiválasztott kontrollok részletes elemzésén és tesztelésén keresztül történik. Az ellenőrzési eljárások megtervezése során figyelembe kell venni a meghatározott kritériumot és az ellenőrzésre

kiválasztott kontroll jellemzőit. Szükség esetén mintavételezési eljárások alkalmazására is sor kerülhet.

3.2. Az ellenőrzés végrehajtása

Az ellenőrzés végrehajtása a 9. sz. ábrán bemutatott tagolás szerint a bizonyítékok megszerzésére, az ellenőrzés eredményeinek kiértékelésére, a megállapítások írásba foglalására, majd a releváns következtetések levonására tagolódnak.

9. sz. ábra - Ellenőrzési folyamat – az ellenőrzés végrehajtása



Forrás: ÁSZ grafika

3.2.1. Az ellenőrzési bizonyítékok megszerzése

Az ellenőrzési eljárás és az ellenőrzési bizonyíték megszerzésének módszere nem különbözik a Számvevőszéki ellenőrzés általános alapelvei 4.2 fejezetében rögzítettektől. A bizonyíték megszerzésének eszközei azonban eltérhetnek, mivel a bizonyítékok informatikai eszközök segítségével, illetve az ellenőrzött alkalmazás kifejezett használata során szerezhetőek meg. Tekintettel a bizonyítékszerzés technikai megvalósításának specialitására (pl. számítógépes adatelemzés, tesztrendszer tesztelése, és más számítógéppel támogatott ellenőrzési eljárások), különös hangsúlyt kap az ellenőrzést végző személy tesztelési eljárásairól készített jegyzőkönyv, (elektronikus) napló, képernyőképek, stb. ellenőrzési bizonyítékként történő rögzítése. Az ellenőrzési eljárások részletes megtervezése során mindezen körülményekre tekintettel kell lenni.

Az ellenőrzést végző személynek a kontrollok jellege, és az alkalmazható ellenőrzési technikák feltérképezésével meg kell ítélnie, hogy szükséges-e egyes kontrollok ellenőrzéséhez speciális szaktudással rendelkező ellenőr közreműködése.

A kontrollok működésének részletes ellenőrzése során fel kell mérni, hogy valójában rendelkeznek-e a feltárt kockázatokat mérséklő, feltáró vagy javító kontrollokkal, s azok megfelelően, (ellenőrzési típustól függően: hatékonyan) működnek-e.

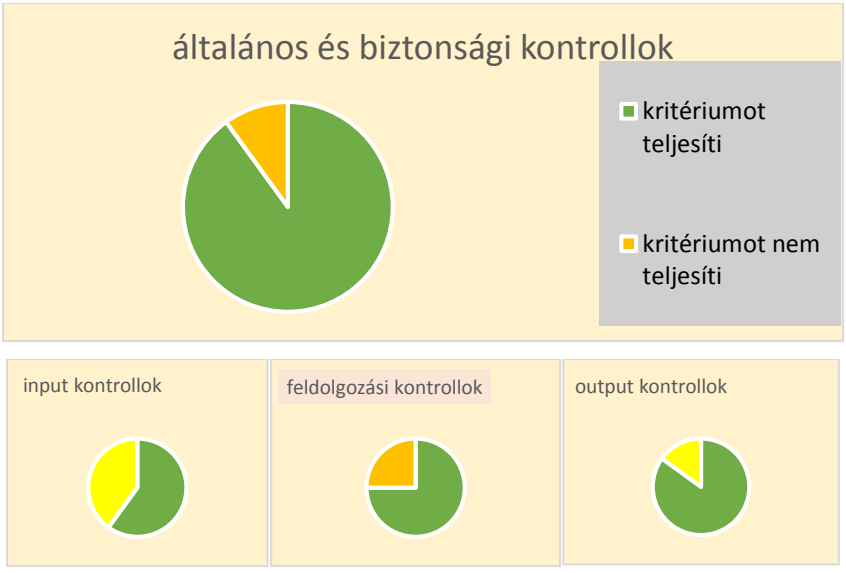
3.2.2. Az ellenőrzés eredményeinek kiértékelése, megállapítások

Az ellenőrzött folyamat, feladatellátás IT alkalmazással való támogatottsága megfelelőségének (és ellenőrzés típustól függően: hatékonyságának) ellenőrzési eredményeit több, egymásra épített lépéssel lehet kiértékelni. Az ellenőrzés előkészítési szakaszában megszerzett információk és az ellenőrzés lefolytatása szakaszában összegyűjtött ellenőrzési bizonyítékok kiértékelésekor a tesztelés, valamint az elemzés, dokumentumellenőrzés, stb. eredményeit össze kell vetni a kritériumokkal.

Az ellenőrzés végrehajtása – részben - a kontrollok tesztelésén keresztül valósul meg. Az ellenőrzés eredményeinek összefoglalásakor vagy a megállapítások megfogalmazásakor azonban az ellenőrzött folyamat vagy feladat környezeti (szabályozottsági, szervezeti, informatikai) beágyazottságáról szerzett információkat és ellenőrzési bizonyítékokat is fel kell használni.

Megfelelőségi ellenőrzés esetén az értékelés a kontroll meglétére és alapfunkciójának betöltésére (kezeli-e a kockázatot, melyhez kontroll célként kitűzték), teljesítmény-ellenőrzési elemként való alkalmazás esetén a kontroll eredményességének, hatékonyságának és gazdaságosságának értékelésére terjed ki. Az ellenőrzés tervezésekor kialakított súlyozás figyelembevételével kell a kulcskontrollok működésének ellenőrzési tapasztalatait a kiértékelésben megjeleníteni. A megfelelőségi ellenőrzés eredményei kontrollcsoportonkénti összefoglalásának ábrázolására példa a 10. sz. ábra szerinti diagram. Az ábra kiemeli, hogy az általános és biztonsági kontrollok működésének kiértékelésben betöltött szerepe magasabb súlyt képviselhet egyéb értékelt kontrollokkal szemben. Egy-egy kontroll-csoportban az egyedi, kiválasztott kontrollok működésének százalékos megosztása alapján lehetséges összesített értékelést adni, az esetlegesen kiválasztott kulcskontrollok figyelembevétele mellett.

10. sz. ábra – Kontrollcsoportonkénti értékelés, ábrázolás



Forrás: ÁSZ grafika

A megszerzett bizonyítékok kiértékelését követően a megállapítások megfogalmazásánál figyelembe kell venni azt, hogy a feltárt rendellenesség

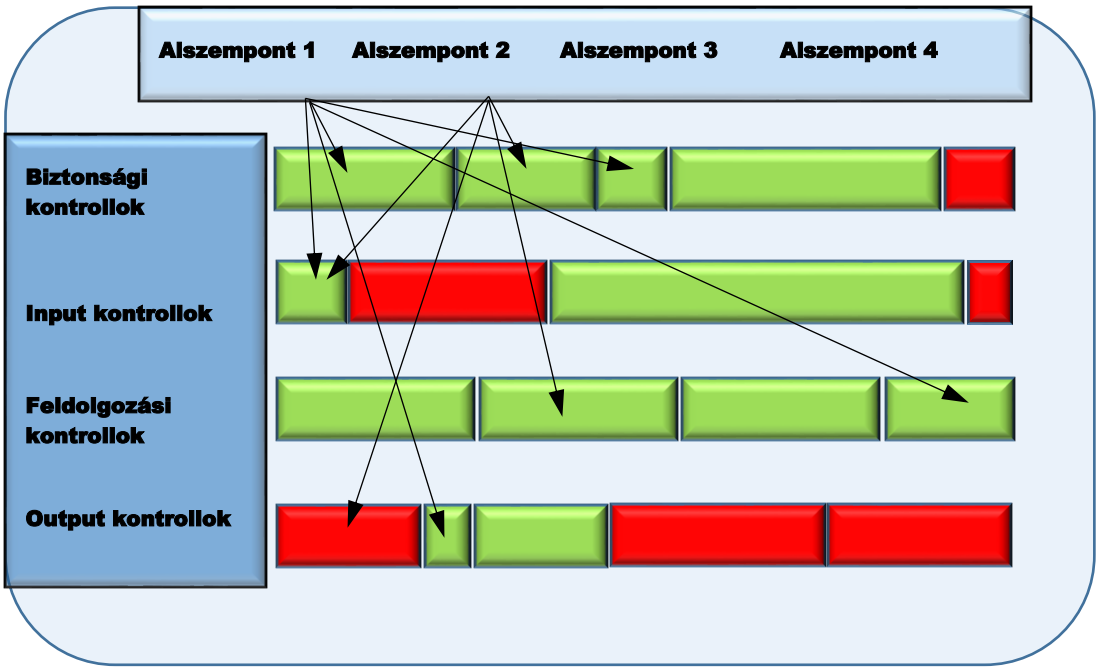
milyen hatást gyakorol az ellenőrzés tárgyát képező folyamat vagy feladatellátás megfelelőségére, minőségére.

Az azonosított kockázatok alapján meghatározott kontrollcélok teljesítésére alkalmazott kontrollok rendszere összességében akkor megfelelő, ha a kontrollok kiépítettek, működnek, azaz a kapcsolódó kockázatokat csökkentik, valamint véletlen vagy szándékos hiba (a folyamat, feladatellátás valamely pontján az elvárt szintű működéstől való eltérés) nem gyakorol jelentős hatást a kimeneti adatok és információk megbízhatóságára, integritására, pontosságára, kommunikációs időszerűségére, bizalmasságára, sértetlenségére és rendelkezésre állására.

Az egyes alszempontok megítélése a hozzá kapcsolódó kontrollok működésétől függ. Egy-egy kontroll megléte és működésének minősége több alszempontra adott válaszra is hatással lehet.

A 11. ábra példát jelenít meg az ellenőrzési alszempontok és a kontrollok értékelésének kapcsolatára. Az ábra azt mutatja meg, hogy az egyes kontroll fajtákba tartozó, a kritériumot teljesítő (világoszölddel jelölt), és a kritériumot nem teljesítő (sötétpirossal jelölt) kontrollok összesített és súlyozott kiértékelése mely alszempontok szerinti kérdések megválaszolását segíti. Az első alszempont kérdése e példában az volt, hogy az adott feladat ellátást az IT alkalmazás megfelelő funkcionalitását biztosító kontrolljai megfelelően támogatják-e. A kérdés megválaszolásához e példában figyelembe kell venni, hogy az első és harmadik biztonsági kontroll, az első input kontroll, valamint a negyedik feldolgozási kontroll a kritériumot teljesíti, azaz az alszempont kérdésére a kapcsolódó kontrollok súlyozott kiértékelése alapján pozitív válasz adható.

11. sz. ábra – Ellenőrzési alszempontok és kontrollok értékelésének kapcsolata

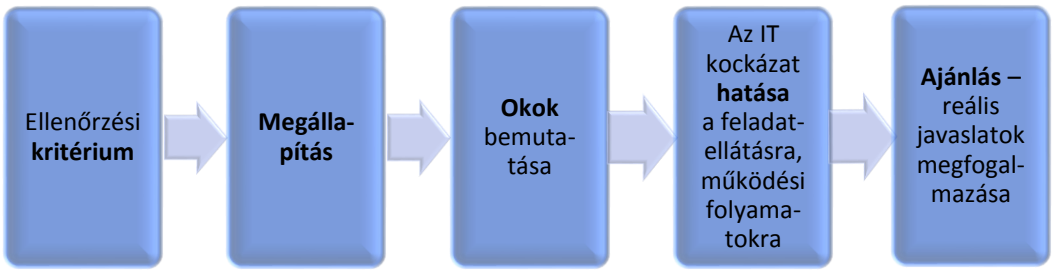


Forrás: ÁSZ grafika

Minden esetben szem előtt kell tartani a kritériumok kialakításától kezdődően a megállapításokon keresztül a következtetésekhez és javaslatokhoz vezető logikai

láncolatot, melyet a 12. sz. ábra szemléltet. Az ellenőrzési *kritériumok* felállítását követően azok teljesüléséről tesz az ellenőrzés *megállapításokat*. Az ellenőrzés folyamatorientált megközelítése lehetővé teszi a feltárt tények, hiányosságok *okainak* bemutatását is (valamint azt is, hogy pl. meghatározott kontrollok működésének hiánya esetén a kockázatokat kompenzáló kontrollok csökkentik-e a kockázatot a kívánt szintre). A megállapítások és okok együttes elemzésével szükséges bemutatni a kontrollokkal nem csökkentett IT kockázatok *hatását* a működésre és feladatellátásra. Annak érdekében, hogy reális, megvalósítható *javaslatokat* tegyen az ellenőrzés, figyelembe kell venni a megállapításokat, az okokat és a lehetséges hatásokat is.

12. sz. ábra – Logikai láncolat a kritériumok kialakításától a megállapításokon keresztül a következtetésekhez és javaslatokhoz



Forrás: ÁSZ grafika

3.3. Az ellenőrzés hasznosulása

A folyamatorientált IT alkalmazás ellenőrzés hasznosulása négy szinten jelentkezhet.

A közvélemény és adófizető állampolgárok

- tájékoztatást kaphatnak az ellenőrzött folyamatok szabályszerű működéséről, megbízhatóságáról, a kapcsolódó informatikai kockázatokról, azok lehetséges hatásairól és kezeléséről;
- az ÁSZ jelentésekben foglalt megállapításokon keresztül információt nyerhetnek a közpénzekkel és közvagyonnal való gazdálkodás informatikai eszközökkel való támogatottságában rejlő biztonsági és funkcionalitási kontrollok működéséről;

A jogalkotó, végrehajtó, irányító szervezetek

- megfelelő alátámasztást és információkat szerezhetnek a megalapozott döntéshozatalhoz mind a jogszabály és jogi irányítási eszközök megalkotása, mind azok végrehajtása tekintetében;
- információt kapnak a közpénzekkel és közvagyonnal való gazdálkodás IT eszközökkel történő megbízható támogatásához szükséges döntéshozatalhoz az irányított szervezetek tekintetében;

Az ellenőrzött szervezetek vezetése, menedzsmentje, döntéshozói, felelős vezetői és informatikai szervezete

- információt nyerhet az IT alkalmazással támogatott folyamat vagy feladatellátás megbízhatóságáról, a megbízhatóságot veszélyeztető kockázatokról;
- információt nyerhet továbbá azokról a kockázatokról, amelyeket általános biztonsági, bemeneti, folyamat vagy kimeneti biztonsági kontrollok nem csökkentenek a kívánt szintre, s melyek esetében hátrányt okozó kockázati hatás léphet fel;
- valamint információt nyerhet azokról a kockázatokról is, amelyek a folyamatot vagy feladatellátást támogató IT alkalmazás funkcionalitási kontrolljainak nem megfelelő működéséből erednek.

A Számvevőszék az ellenőrzési eredmények visszacsatolásaként

- az ellenőrzés eredményeit, megállapításait, következtetéseit felhasználhatja a későbbi témaválasztás és a kockázatelemzés terén mind az ellenőrzés témája (közpénzekkel és közvagyonnal való gazdálkodás fajtája, szegmense) mind az ellenőrzött szervezetek, folyamatok és feladat ellátási típusok potenciális köre, mind a tipikus, IT alkalmazásokkal összefüggő (általánosítható és egyedi) kockázatok és kontrollok körének meghatározásakor;
- az ellenőrzés eredményeit alkalmazhatja a jövőbeni ellenőrzések témájának, tárgyának, hatókörének, fókuszterületeinek megtervezése, a konkrét ellenőrzések technológiai megvalósításának, módszertani segédleteinek megtervezése (pl. mintaméret, speciális ellenőrzési eljárások, speciális kompetenciák igénye, stb.) során.