Harmadik fél

Tematikus követelmény

Topical Requirement

Felhasználói útmutató

The Institute of Internal Auditors

Fordította:

The Institute of Internal Auditors Hungary

Tartalomjegyzék

A tematikus követelmények áttekintése

A Tematikus követelmények a Nemzetközi Szakmai Gyakorlatok Keretrendszer (International Professional Practices Framework®) alapvető részét képezik, a Globális Belső Ellenőrzési Normákkal (Global Internal Audit Standards™) és a Globális Iránymutatásokkal együtt. A Belső Ellenőrök Intézete megköveteli, hogy a Tematikus követelményeket a Globális Belső Ellenőrzési Normákkal együtt használják, amelyek az előírt gyakorlatok kötelező érvényű bázisául szolgálnak. A Normákra való hivatkozások ebben az útmutatóban a részletesebb információk forrásaként jelennek meg.

A Tematikus követelmények meghatározzák azt, hogy a belső ellenőrök hogyan kezelik az aktuális kockázati területeket a minőség és a szakmán belüli következetesség előmozdítása érdekében. A Tematikus követelmények megteremtik az alapot, és releváns kritériumokat biztosítanak a Tematikus követelmény tárgyához kapcsolódó bizonyosságot nyújtó szolgáltatások elvégzéséhez (13.4 norma: Az értékelés kritériumai). A Tematikus követelményeknek való megfelelés kötelező a bizonyosságot nyújtó megbízások esetében, és ajánlott a tanácsadói szolgáltatások során történő értékeléshez. A Tematikus követelmények nem arra szolgálnak, hogy lefedjék az összes lehetséges szempontot, amelyet a bizonyosságot nyújtó megbízások teljesítésekor figyelembe kell venni; inkább arra szolgálnak, hogy egy minimális követelménykészletet biztosítsanak a téma következetes és megbízható értékeléséhez.

A Tematikus követelmények egyértelműen kapcsolódnak az IIA Három Vonal Modelljéhez és a Globális Belső Ellenőrzési Normákhoz. Az irányítási, kockázatkezelési és kontrollfolyamatok a 9.1 „Az irányítási, kockázatkezelési és kontrollfolyamatok megértése” normához igazodó Tematikus követelmények fő összetevői. A Három Vonal Modellre vetítve az irányítás az vezetőtestülethez/irányító testülethez, a kockázatkezelés a második vonalhoz, a kontrollok vagy kontrollfolyamatok pedig az első vonalhoz kapcsolódnak. Míg a vezetés az első és a második vonalban is képviselteti magát, a belső ellenőrzési funkció a harmadik vonalban, független és tárgyilagos bizonyosságnyújtóként jelenik meg, amely az vezetőtestületnek/irányító testületnek jelent (8. alapelv: A vezetőtestület felügyeleti szerepe).

Alkalmazhatóság, kockázat és szakmai megítélés

A Tematikus követelményeket akkor kell követni, amikor a belső ellenőrzési funkciók olyan témában végeznek bizonyosságot nyújtó megbízásokat, amelyekre vonatkozóan létezik Tematikus követelmény, vagy amikor a Tematikus követelmény elemeit más bizonyosságot nyújtó megbízásokon belül azonosítják.

A Normákban leírtak szerint a kockázatértékelés a belső ellenőrzési vezető tervezési feladatának fontos része. A belső ellenőrzési tervbe foglalandó bizonyosságot nyújtó megbízások meghatározása megkövetelik a szervezet stratégiáinak, céljainak és kockázatainak legalább évenkénti értékelését (9.4 norma: Belső ellenőrzési terv). Az egyes bizonyosságot nyújtó megbízások tervezésekor a belső ellenőröknek fel kell mérniük a megbízás szempontjából releváns kockázatokat (13.2 norma: A megbízással kapcsolatos kockázatok felmérése).

Ha egy Tematikus követelmény témáját a kockázatalapú belső ellenőrzési tervezési folyamat során azonosítják, és az szerepel az ellenőrzési tervben, akkor a Tematikus követelményben szereplő követelményeket alkalmazni kell a téma értékelésére a vonatkozó megbízásokon belül. Ezen túlmenően, amikor a belső ellenőrök megbízást végeznek (akár szerepel a tervben, akár nem), és a Tematikus követelmény elemei felmerülnek, a megbízás részeként értékelni kell a Tematikus követelmény alkalmazhatóságát. Végül, olyan megbízásra vonatkozó kérés esetén, amely eredetileg nem szerepelt a tervben, de a téma szerepel a Tematikus követelmények között, akkor is kell azt alkalmazni.

A szakmai megítélés kulcsfontosságú szerepet játszik a Tematikus követelmény alkalmazásában. A kockázatértékelések határozzák meg az ellenőrzési vezetők döntését arról, hogy mely megbízásokat vegyék fel a belső ellenőrzési tervbe (9.4 norma: Belső ellenőrzési terv). Ezen túlmenően a belső ellenőrök szakmai megítélés alapján mérlegelik és határozzák meg, hogy az egyes megbízások milyen szempontokra terjedjenek ki (13.3 norma: A megbízás célkitűzései és hatóköre, 13.4 norma: Az értékelés kritériumai és 13.6 norma: Munkaprogram).

Meg kell őrizni annak bizonyítékát, hogy a Tematikus követelményben szereplő minden egyes követelmény alkalmazhatóságát értékelték, beleértve a kivételek indoklását is. A Tematikus követelménynek való megfelelést a 14.6 „A megbízás dokumentációja” normában leírtak szerint a belső ellenőr szakmai megítélése alapján kell dokumentálni.

Míg a Tematikus követelmény egy kiindulási alap a figyelembe veendő kontrollfolyamatokhoz, azok a szervezetek, amelyek az adott témát nagyon magas kockázatúnak értékelik, további szempontokat is szükségesnek tarthatnak az értékeléshez.

Ha a belső ellenőrzési funkció nem rendelkezik a szükséges szakmai kompetenciákkal egy, a Tematikus követelmény tárgyában történő megbízás elvégzéséhez, a belső ellenőrzési vezetőnek meg kell határoznia, hogyan szerezze meg az erőforrásokat, és időben tájékoztatnia kell a vezetőtestületet és a felsővezetést a korlátok következményeiről, valamint arról, hogy az erőforráshiányt hogyan fogják kezelni. A belső ellenőrzési vezető továbbra is viseli a végső felelősséget azért, hogy a belső ellenőrzési funkció megfeleljen a Tematikus követelményeknek, függetlenül attól, hogy az erőforrásokat milyen módon biztosítja (3.1 norma: Kompetencia, 7.2 norma: A belső ellenőrzési vezető képesítései, 8.2 norma: Erőforrások, 10.2 norma: Emberi erőforrás-gazdálkodás).

Teljesítmény, dokumentáció és jelentéstétel

A Tematikus követelmények alkalmazása során a belső ellenőröknek is meg kell felelniük a Normáknak, és munkájukat az V. terület „A belső ellenőrzési szolgáltatások nyújtása” című résszel összhangban kell végezniük. Az V. terület normái leírják a megbízások tervezését (13. alapelv: Tervezzük megbízásainkat hatékonyan!), a megbízások végrehajtását (14. alapelv: Végezzük el a megbízásokhoz kapcsolódó feladatokat!) és a megbízások eredményeinek közlését (15. alapelv: Kommunikáljuk a megbízás eredményeit és kövessük nyomon az intézkedési terveket!).

A Tematikus követelmények célja, hogy támogassák a következetes, magas színvonalú belső ellenőrzési gyakorlatot. A jogszabályok és szabályozások, a felügyeleti elvárások és más, szakmailag elismert keretrendszerek további vagy specifikusabb követelményeket írhatnak elő. A belső ellenőröknek meg kell érteniük és be kell tartaniuk azokat a jogszabályokat és szabályozókat, amelyek arra az ágazatra és joghatóságokra vonatkoznak, ahol a szervezet működik – ideértve a szükséges közzétételek megtételét is –, az 1.3 Jogkövető és etikus magatartás norma szerint. A belső ellenőrök ezeket a további

követelményeket már beépíthették az ellenőrzési programokba és tesztelési eljárásokba, de a megfelelő lefedettség biztosítása érdekében szükséges azokat összeegyeztetniük a Tematikus követelménnyel.

A Tematikus követelmény alkalmazása dokumentálható a belső ellenőrzési tervben vagy a megbízási munkadokumentumokban, a belső ellenőr szakmai megítélése alapján. Egy vagy több belső ellenőrzési megbízás is lefedheti a követelményeket. Valamint előfordulhat, hogy nem minden követelmény alkalmazható. Meg kell őrizni annak bizonyítékát, hogy a Tematikus követelmény alkalmazhatóságát értékelték, beleértve a kivételek indoklását is.

Minőségbiztosítás

A Normák megkövetelik, hogy a belső ellenőrzési vezető dolgozzon ki, vezessen be és tartson fenn egy minőségbiztosítási és -fejlesztési programot, amely a belső ellenőrzési funkció minden aspektusára kiterjed (8.3 norma: Minőség). Az eredményeket kommunikálni kell a vezetőtestület és a felsővezetés felé. A kommunikációnak be kell számolnia a belső ellenőrzési funkció Normáknak való megfeleléséről és a teljesítménycélok eléréséről.

A Tematikus követelményeknek való megfelelést a minőségértékelés során értékelik.

Harmadik fél

A harmadik fél olyan külső személy, csoport vagy szervezet, akivel egy szervezet („az elsődleges szervezet”) üzleti kapcsolatot létesít termékek vagy szolgáltatások beszerzése céljából. A kapcsolat formalizálható szerződés, megállapodás vagy más eszköz útján annak érdekében, hogy a szervezet termékeket, szolgáltatásokat, munkaerőt, gyártási vagy informatikai megoldásokat – például adattárolást, adatfeldolgozást és karbantartást – vehessen igénybe.

> Megjegyzés
>
> A Tematikus követelmények a Globális Belső Ellenőrzési Normákban meghatározott általános belső ellenőrzési terminológiát használják. Az olvasóknak a Normák fogalomjegyzékében található fogalmakra és meghatározásokra ajánlott hivatkozniuk.

A „harmadik fél” kifejezés ágazattól vagy más kontextustól függően eltérő módon használható. Minden belső ellenőrzési funkció rugalmasan alkalmazhatja a saját szakmai megítélését a Tematikus követelmény alkalmazását illetően, annak megfelelően, hogy az elsődleges szervezet (a harmadik féllel megállapodást kötő szervezet) hogyan definiálja a harmadik feleket. A Harmadik fél Tematikus követelményben és a Felhasználói útmutatóban a „harmadik fél” kifejezés az eladókra, beszállítókra, vállalkozókra, alvállalkozókra, kiszervezett szolgáltatást nyújtókra, egyéb ügynökségekre és tanácsadókra vonatkozik. A „harmadik fél” kifejezés minden erre vonatkozó megállapodást magában foglal, beleértve a harmadik fél és alvállalkozói közötti megállapodásokat is, amely alvállalkozókat gyakran az ellátási láncban alsóbb szinten elhelyezkedő „negyedik feleknek”, „ötödik feleknek” vagy „n-edik feleknek” neveznek.

Ez a Tematikus követelmény nem vonatkozik az elsődleges szervezettel fennálló közvetett külső kapcsolatokra, érdekeltségekre vagy érintettségekre, mint például a szabályozó hatóságok, ügynökök, brókerek, befektetők, vagyonkezelők/vezetőtestületi tagok, közszolgáltatók és a lakosság, vagy belső kapcsolatokra, mint például alkalmazottak vagy csoporton belüli szolgáltatók.

A „harmadik fél” fogalmát ágazattól vagy más kontextustól függően eltérő módon lehet meghatározni és használni. A belső ellenőrök számára biztosított a rugalmasság, és szakmai megítélésükre kell

hagyatkozniuk, hogy a Tematikus követelményt az elsődleges szervezet harmadik félre vonatkozó meghatározásához igazítsák.

A szervezet harmadik felekkel fennálló kapcsolatainak kezelésére szolgáló folyamatok hatékonyságát a szervezet egészére és/vagy egy vagy több egyedi szerződés, megállapodás vagy kapcsolat szintjén lehet értékelni. A belső ellenőröknek felülről lefelé irányuló megközelítést kell alkalmazniuk a szervezet harmadik félre vonatkozó szabályzatainak, folyamatainak, eljárásainak, keretrendszerének és életciklusának megértése során. A belső ellenőröknek ítélőképességük alapján szükséges megérteniük a harmadik felek kockázatainak árnyalatait az egyes ágazatok, szervezetek és megbízási témák alapján. Az 5.1 normával („Információ felhasználása”) összhangban a belső ellenőröknek ajánlott tisztában lenniük az általuk esetlegesen hozzáférhető, harmadik féltől származó információkkal kapcsolatos szabályzatokkal és folyamatokkal, és meg kell felelniük azoknak.

A Tematikus követelmény akkor alkalmazandó, amikor a belső ellenőrzési funkció harmadik felek és/vagy bármely alvállalkozói kapcsolat – beleértve a negyedik vagy azt követő szinteken lévő kapcsolatokat is – vonatkozásában bizonyosságot nyújtó megbízásokat végez, amelyeket a harmadik félnek az elsődleges szervezettel kötött szerződése vagy megállapodása tesz lehetővé. A belső ellenőröknek a harmadik és további alvállalkozói szinteken lévő feleket a kockázat alapján ajánlott besorolniuk, az alábbi kockázatkezelési szakaszban leírtak szerint. A belső ellenőröknek a kockázatértékelés eredményeiből következő követelményeket kell alkalmazniuk, és a kivételeket dokumentálni kell.

A Harmadik fél Tematikus követelmény és a Felhasználói útmutató a szervezet harmadik felekkel való kapcsolatának szakaszaira, más néven életciklusára utal: kiválasztás, szerződéskötés, beillesztési folyamat, nyomon követés és a szerződés megszüntetésére irányuló folyamat. A Harmadik fél Tematikus követelmény és a Felhasználói útmutató céljaira ezeket a szakaszokat használják, még akkor is, ha egyes ágazatok az életciklusnak saját változataival rendelkeznek. A szakaszok a következők:

- Kiválasztás: magában foglalja a harmadik fél szükségességének meghatározására irányuló folyamatokat, a harmadik fél igénybevételének tervét és a kellő körültekintéssel történő kiválasztást. A kiválasztásnak emellett szükséges magában foglalnia a potenciális és megbízott harmadik felek kockázatainak értékelését is.
- Szerződéskötés: magában foglalja a harmadik féllel kötendő jogi megállapodás kidolgozásának, megtárgyalásának, jóváhagyásának és végrehajtásának kellő gondossággal végzett folyamatait.
- Beillesztési folyamat: a szerződés aláírásakor kezdődik, amikor a kapcsolat megkezdődik, és megteremti az alapot ahhoz, hogy a harmadik felek megfeleljenek a szerződés vagy megállapodás feltételeinek.
- Nyomon követés: magában foglalja a szerződés megkötése és jóváhagyása után a harmadik fél életciklus-menedzsmentjére, koordinációjára és folyamatos nyomon követésére vonatkozó folyamatokat. A megközelítés általában szisztematikus és kockázatalapú, és figyelembe kell vennie a folyamatos fejlesztést. A nyomon követés magában foglalja a fennálló, harmadik féllel kötött szerződés vagy megállapodás szükség szerinti megújítását.
- Szerződés megszüntetésére irányuló folyamat: magában foglalja a szerződés és megállapodás megszüntetésére, a kockázati szint alapján besorolt harmadik felek kilépési stratégiájának fenntartására és szükség szerint a szerződéses kapcsolatok megszüntetésére

vonatkozó folyamatokat. A folyamatok jellemzően kockázatalapú megközelítést alkalmaznak, és tartalmazhatnak hivatalos kilépési tervet.

Az elsődleges szervezet megtartja az elszámoltathatóságot a céljai elérésével kapcsolatos kockázatokért, még akkor is, ha egy harmadik felet bíz meg egy vagy több cél elérésének elősegítésével. A harmadik felekkel való együttműködés csökkentheti a szervezet egyes folyamatainak elvégzésével kapcsolatos költségeit. Ugyanakkor működési kockázatokat is jelenthet, mivel az elsődleges szervezetnek kevesebb rálátása és ráhatása van a harmadik fél kontroll folyamataira. Ha egy harmadik fél nem teljesíti a szerződésben foglaltakat, etikátlan gyakorlatot folytat, vagy üzletmenetében zavar keletkezik, az elsődleges szervezetet is hátrányosan érinthetik a következmények.

Az elsődleges szervezetnek megfelelő irányítási, kockázatkezelési és kontrollfolyamatok révén azonosítania, értékelnie és kezelnie kell a kockázatokat. A harmadik felekkel kapcsolatos kockázatok kategóriái és példái a következők:

- Stratégiai, például a szervezet küldetésének és/vagy magas szintű célkitűzéseinek megvalósítására vagy az egyesülések és felvásárlások hatásainak kezelésére való képesség csökkenése.
- Reputációs, például a környezetnek vagy az elsődleges szervezetnek az ügyfelekkel, vevőkkel és érdekelt felekkel való kapcsolatában és bizalmában okozott kár.
- Etikai, mint például feddhetetlenség, összeférhetetlenség, kenőpénz és korrupció.
- Működési, például fizikai és információbiztonsági, bennfentes kockázat, szolgáltatáskimaradás és a célok elmaradása.
- Pénzügyi, például harmadik fél fizetésképtelensége és visszaélés.
- Megfelelési, a vonatkozó helyi, nemzeti és nemzetközi szabályozási követelmények alapján
- Kiberbiztonsági és egyéb adatvédelmi, például az érzékeny adatok veszélyeztetése és kiszivárgása.
- Információtechnológiai, például a kritikus műveleteket támogató szolgáltatások hiánya.
- Jogi, például összeférhetetlenség, jogviták és szerződésszegés miatti pereskedés.
- Fenntarthatósági, például környezeti, társadalmi és irányítási szempontok. Ilyen például a szervezet természeti környezetre gyakorolt hatásával kapcsolatos kockázatok, valamint a szervezet és a közösségek közötti interakciókkal kapcsolatos kockázatok.
- Geopolitikai, például kereskedelmi viták/szankciók és politikai instabilitás.

A belső ellenőröknek a harmadik fél életciklusának minden egyes szakaszát szükséges figyelembe venniük az irányítási, kockázatkezelési és kontrollfolyamatokra vonatkozó követelmények értékelésekor.

A Harmadik fél Tematikus követelményben foglalt követelmények három szakaszra oszlanak, a 9.1 Az irányítási, kockázatkezelési és kontrollfolyamatok megértése norma szerint:

- Irányítás – világosan meghatározott minimális elvárások és stratégiák a harmadik felek igénybevételére a szervezeti célok, irányelvek és eljárások támogatása érdekében.

- Kockázatkezelés – folyamatok a harmadik felek igénybevételével járó kockázatok azonosítására, elemzésére, kezelésére és nyomon követésére, beleértve az incidensek haladéktalan jelentésére és kezelésére szolgáló folyamatot.
- Kontrollok – a vezetés által létrehozott, rendszeresen értékelt kontrollfolyamatok a harmadik felek igénybevétele során felmerülő kockázatok mérséklésére.

A Tematikus követelményen és ezen a Felhasználói útmutatón kívül a belső ellenőröknek érdemes a harmadik felekre vonatkozó további szakmai útmutatókat, például az IPPF Globális útmutatóit és az ágazatspecifikus forrásokat is figyelembe venniük.

Megfontolások

Az alábbi megfontolások segíthetnek a belső ellenőröknek a Harmadik fél Tematikus követelményben foglaltak végrehajtásában. Az alábbiakban az egyes szakaszokban található, betűvel jelölt állítások a Tematikus követelmény megfelelő követelményeit újrafogalmazzák vagy értelmezik. Ezek a nem kötelező megfontolások szemléltető jellegűek, hogy példákat adjanak a követelmények értékelésének módjaira. A belső ellenőröknek szakmai megítélésük alapján szükséges meghatározniuk, mit foglaljanak bele az értékeléseikbe.

Irányítási megfontolások

Annak felmérése érdekében, hogy az irányítási folyamatokat, beleértve az vezetőtestület felügyeletét is, hogyan alkalmazzák a harmadik fél célkitűzéseire, a belső ellenőrök megvizsgálhatják a következő bizonyítékokat:

A. Szabályozott és dokumentált kockázatalapú megközelítés vagy stratégia annak meghatározására, hogy igénybe vegyenek-e harmadik felet. A megközelítést rendszeresen felülvizsgálják, és a következőkre terjed ki:

- Egy világosan meghatározott és szabályozott folyamat a megközelítés megvalósítására, amelyet a szervezet jóváhagyott a használatra.
- A költség-haszon elemzésen alapuló tervezett erőforrások igazolják a harmadik fél bevonását, biztosítva a stratégiai összhangot és az erőforrások hatékony felhasználását.
- A vezetőség értékelése a kockázatokról és a kontrollokról, beleértve azokat is, amelyek a harmadik felekkel kapcsolatosak.
- Megfelelő erőforrások a harmadik felek szerződéskötéséhez, irányításához és teljesítményének nyomon követéséhez.
- Az érdekelt felek visszajelzéseinek beépítése a megközelítésbe vagy stratégiába.

B. A harmadik féllel való kapcsolatok meghatározására, értékelésére és kezelésére szolgáló szabályozások, folyamatok és egyéb vonatkozó dokumentáció az életciklus során. A szabályzatok és folyamatok a következőket foglalhatják magukban:

- Egységesen kialakított eszközök és sablonok a kulcsfontosságú irányítási, kockázatkezelési és kontrollfolyamatok megkönnyítésére.
- Eljárások a szabályzatok és folyamatok rendszeres értékelésére, megfelelőségük megállapítására és szükség szerinti frissítésére.
- A harmadik felek kiválasztására, szerződéskötésére, beillesztésére, nyomon követésére és a szerződés megszüntetésére irányuló folyamat kritériumainak megállapítása.
- Az alkalmazandó jogszabályi követelmények azonosítása és rendszeres felülvizsgálata a szabályzatokkal és folyamatokkal való összehangolás érdekében.

- Összehasonlító elemzések elvégzése a vezető harmadik fél menedzsment gyakorlatok azonosítása és összevetése céljából.

C. Meghatározott szerepkörök és felelősségi körök, amelyek támogatják a harmadik felekkel kapcsolatos célkitűzések elérését. További bizonyítékok lehetnek:

- Folyamatok annak értékelésére, hogy a harmadik fél értékei, etikai értékrendje és társadalmi felelősségvállalása összhangban van-e az elsődleges szervezet alapelveivel. A folyamatnak tartalmaznia kell, hogy miként lehet azonnal kezelni a lehetséges összeférhetetlenségeket vagy etikátlan gyakorlatokat.
- A harmadik felek kezelését végző munkaköröket betöltő munkatársak rendszeres képzése, valamint kompetenciáik időszakos értékelése.
- Folyamat annak értékelésére, hogy alkalmaznak-e olyan képzést, mely az egész szervezetre kiterjedő, harmadik felekkel kapcsolatos tudatosságot alakít ki.
- A szerepek és felelősségi körök igazodnak a Három Vonal Modellhez.

D. Kellő időben történő kommunikáció és együttműködés az érintett érdekelt felekkel a harmadik fél életciklusa során (például a vezetőtestület, a felsővezetés, a beszerzés, az üzemeltetés, a kockázatkezelés, a megfelelés, a jogi, információtechnológiai, információbiztonsági, humánerőforrás területek és mások), amely magában foglalja:

- A harmadik fél kockázatairól és az ismert potenciális sebezhetőségekről szóló információkat az értekezletek jegyzőkönyveiben, jelentéseiben vagy e-mailben.
- Információcsere a harmadik fél koordinációjáról és az együttműködés előremozdításáról (például rendszeres, több szakterületet érintő találkozókon keresztül).

Kockázatkezelési megfontolások

Annak értékeléséhez, hogy a kockázatkezelési folyamatokat hogyan alkalmazzák a harmadik féllel kapcsolatos célkitűzésekre, a belső ellenőrök megvizsgálhatják az alábbi bizonyítékokat:

A. A harmadik féltől származó szolgáltatások igénybevételére vonatkozó szabályozott és átfogó kockázatkezelési folyamatok meghatározott szerepköröket és felelősségi köröket tartalmaznak, és érdemben kezelik a szervezetre vonatkozó kulcskockázatokat:

- A harmadik felek kockázatainak értékelésére és kezelésére szolgáló folyamatok közé tartozik, hogy a kulcskockázatok:
  - Hogyan kerülnek elsődlegesen azonosításra és jelentésre.
  - Hogyan kerülnek elemzésre annak érdekében, hogy értékeljék a szervezeti célok elérésének képességére gyakorolt hatásukat.
  - Hogyan kerülnek mérséklésre, beleértve a kockázatot elfogadható szintre csökkentő cselekvési terveket.
  - Hogyan követik őket nyomon, beleértve a korai figyelmeztetések észlelését és az azokra való reagálást, valamint a folyamatos jelentéstételre vonatkozó tervet, amíg a fenyegetések teljes mértékben el nem hárulnak.

- Nyomon követési mechanizmusok vannak érvényben a folyamatok betartása, az esetleges eltérések esetén intézkedési tervek végrehajtása érdekében, hogy megakadályozzák a szervezet hosszú távú céljainak vagy stratégiájának meghiúsulását.
- Egy kockázatkezelési bizottság vagy más csoport szakmai felügyeletet gyakorol a harmadik felekkel kapcsolatos kockázatokkal kapcsolatban és tájékoztatást nyújt a vezetőtestületnek. A bizottságnak meghatározott célja van, és rendszeresen ülésezik. A bizonyítékok közé tartozhatnak az ülések jegyzőkönyvei.

B. A harmadik felekkel kapcsolatos kockázatokat a szerződéses életciklus során rendszeresen azonosítják és értékelik. A kockázatértékelés besorolja és priorizálja a harmadik feleket. A kockázatokra adott válaszokat besorolják és priorizálják.

- A harmadik felek kockázatértékelésének kidolgozásakor az elsődleges szervezet olyan tényezőket vesz figyelembe, mint a mérete, érettsége és a bevont harmadik felek száma.
- A kockázatértékelés dokumentált, és meghatározza az eredendő és a maradványkockázatokat.
- A szervezet belső eljárásrend szerint végzi a kockázatértékelés felülvizsgálatát és frissítését.
- A harmadik felek kockázatok szerinti besorolásra és priorizálására kritériumokat állapítanak meg. Példák az ilyen kritériumokra:
  - A nyújtott szolgáltatások kritikusak a szervezet működése szempontjából.
  - A megállapodás pénzügyi értéke jelentős.
  - A kapcsolat új, gyorsan létrejött és/vagy hosszú ideig tart.
  - Több külső fél is bevonásra került.
  - A harmadik fél a munka egy részét vagy egészét alvállalkozásba kívánja adni.
- A szervezet betartja a széles körben elfogadott kockázatértékelési gyakorlatokat, beleértve azt is, hogy a kockázatértékelést a lehető legkorábbi szakaszban kell elvégezni, jellemzően akkor, amikor az ajánlatot a kiválasztási szakaszban elemzik, és még a beillesztési folyamat előtt.
- A szállítók kérdőívet töltenek ki, amely alapján a szervezet meghatározza kockázati besorolásukat és prioritásukat az eredendő kockázatok alapján. A szervezet biztosítja, hogy a kérdőíveket az érintett személyzet kitölti, és a pontosság biztosítása érdekében felülvizsgálják.
- A szervezet a harmadik féllel szembeni kockázatkezeléssel kapcsolatban rendszeres időközönként tájékoztatást kap olyan funkcionális területektől, mint az informatika, a beszerzés, a kockázatkezelés, a humánerőforrás, a jogi, a megfelelési, az üzemeltetési, a számviteli és a pénzügyi területek.

C. A kockázatra adott válaszok, mint például a kockázatcsökkentés, elfogadás, megszüntetés és megosztás, a kockázati besorolásnak megfelelően kerülnek meghatározásra.

- A kockázatra adott válaszok dokumentáltak, és figyelembe veszik a harmadik fél kontrollkörnyezetét.

- Dokumentáció arról, hogy az elsődleges szervezet kockázattűrő képességét meghaladó kockázatokra adott válaszokat felülvizsgálják a megfelelőség szempontjából, különösen akkor, ha a kockázatokat elfogadják. A kockázatokra adott válaszok tartalmazzák azokat is, amelyek a harmadik felekkel kapcsolatos lehetséges összeférhetetlenségek kezelésére vonatkoznak.

D. A harmadik féllel kapcsolatos kockázatok kezelésére és jelentésére szolgáló folyamatok, beleértve a fenyegetés vagy kockázat szintjének értékelését, hozzárendelését és rangsorolását. A felülvizsgálat magában foglalhatja a következők meghatározását:

- A szervezet kockázati szintjeinek – például magas, közepes és alacsony – meghatározása és magyarázatai, valamint az egyes kockázati kategóriákra vonatkozó jelentési eljárások.
- A harmadik felek listája az azonosított kockázatok szerint besorolva, valamint a kockázati események mérséklésének állapota.
- Alkalmazandó jogszabályi és megfelelési követelmények.
- Mind a pénzügyi, mind a nem pénzügyi (például reputációs) kockázatok hatásai.
- A harmadik felek kockázatainak a vezetőség és a munkavállalók felé történő kommunikálására szolgáló eljárások, beleértve a kockázati profil rendszeres jelentését a vezetőtestületnek (vagy más megfelelő testületnek). A kommunikációnak szükséges tartalmaznia a kiemelten kezelt harmadik feleknél észlelt problémák orvoslásával kapcsolatos aktualitásokat.
- A besorolások és a prioritások újraértékelésére szolgáló folyamatok, amikor az elsődleges szervezet kockázati étvágya és kockázattűrési szintje megváltozik.

Kontrollmegfontolások

Annak felmérése érdekében, hogy a harmadik féllel fennálló kapcsolatokra hogyan alkalmazzák a kontrollfolyamatokat, a belső ellenőrök megvizsgálhatják az alábbi bizonyítékokat:

A. A harmadik felek bevonására és kiválasztására alapos átvilágítási eljárást alkalmaznak, amelyhez dokumentált és jóváhagyott üzleti indoklás vagy más vonatkozó dokumentáció tartozik, amely leírja és indokolja a harmadik féllel való kapcsolat szükségességét és jellegét.

- Az üzleti indoklás:
  - Megcélozhatja a harmadik fél elvárásoknak való megfelelésével kapcsolatos kockázatokat és a szervezetre gyakorolt lehetséges hatásait.
  - Tartalmazhat részletes költség-haszon elemzést.
- A kialakított beszerzési eljárások – mint például a versenyeztetés, az ajánlattételi felhívás és az egyedi beszerzés – követése. A folyamatok tartalmazzák a következőket:
  - Fontos szempontokra vonatkozó kritériumok, például a kiberbiztonsági protokollok felülvizsgálata, a banki adatok ellenőrzése, pénzügyiháttér-ellenőrzés, valamint a harmadik fél szervezeti felépítésének, bűnügyi és jogi nyilvántartásának, gépjárművezetői előéletének, politikai tevékenységének és bűncselekményekhez köthető kapcsolatainak feltárása.

- Jól meghatározott kiválasztási kritériumok, beleértve a korábbi teljesítmények, a referenciák, a reputáció és a megállapodás költségének értékelését.
- Kellő körültekintés az ajánlattevők megfelelő kiválasztásának biztosítása érdekében, például az ajánlatok felülvizsgálatát végző többfunkciós csoportok létrehozása. Az elfogultság kockázatának csökkentése érdekében a felülvizsgálati csoportok kontrolljai magukban foglalják a csoportok létrehozására vonatkozó eljárásokat és a lehetséges összeférhetetlenségek nyilvánosságra hozatalára vonatkozó követelményeket.
- A harmadik fél kontrollkörnyezetének kellő gondossággal történő értékelése; például helyszíni látogatás vagy a harmadik félnél az alábbiak áttekintése:
  - Rendszer- és Szervezeti Kontrollokról szóló (SOC) jelentések.
  - Pénzügyi stabilitás.
  - Alapító okirat vagy cégkivonat.
  - Átláthatóság a kulcsfontosságú vezetőség és az érdekelt felek döntéshozatalában.
  - Szervezeti felépítés.
  - Működési stabilitás.
  - Kiberbiztonsági protokollok.
  - A vonatkozó jogszabályoknak, szabályozóknak és szabványoknak való megfelelés.
  - Etikai értékrend.
  - Az elsődleges szervezettel való kapcsolatának előzményei.
  - Reputáció.
- Bizonyíték arra, hogy a potenciális szállítók vagy vállalkozók csak a megfelelő átvilágítási folyamatok elvégzése és az eredmények elemzése után jutnak el az ellátási-lánc életciklusának szerződéskötési szakaszába.

B. A szerződéskötésre vonatkozó szabályzatokat és folyamatokat kialakították és azokat betartják.

- A szerződésekben a szerződéses feltételeket egyértelműen írják meg.
- A szerződésszerkesztés során figyelembe veszik a főbb kockázatokat, és a vonatkozó rendelkezéseket beépítik. A megoldást igénylő kérdéseket ebben a szakaszban kommunikálják a harmadik fél felé.
- A szerződések lényeges elemeit a szervezet szerződéskötésre vonatkozó szabályzatok és folyamatok, valamint a harmadik fél kockázati szintje alapján határozzák meg. Az elemek közé tartozhatnak:
  - Titoktartási (adatvédelmi) megállapodások.
  - Megszüntetési rendelkezések és meghatározott paraméterek az adathozzáféréshez.
  - Kiberbiztonsági követelmények, beleértve az összes adathoz való hozzáférésre és azok megosztására, valamint az incidensekről vagy jogsértésekről meghatározott időn belül történő jelentéstételre vonatkozó követelményeket.
  - Az elsődleges szervezet adatait érintő jogsértésről szóló értesítésekre vonatkozó követelmények.

- Egy szabályozott eljárás a harmadik fél azonosítására, beleértve a teljes nevet, címet, telephelyeket és weboldalt. A szokásos gyakorlat az, hogy az azonosítási folyamat során ellenőrzőlistát használnak, és felülvizsgálják az információk pontosságát.
- Világosan meghatározott szolgáltatási-szint megállapodások, amelyek meghatározzák az elvárt teljesítményt és az egyes felek jogait, kötelezettségeit, szankcióit, ösztönzőit és felelősségét, beleértve a munkaerőköltségek kifizetésének felelősségét (beleértve az ellátási-lánc alsóbb szinteken elhelyezkedő alvállalkozókat is).
- Az ellenőrzésre való jogra vonatkozó záradék, amely az ellátási-lánc alsóbb szintjén elhelyezkedő alvállalkozókra is kiterjed, vagy annak bizonyítására vonatkozó követelmény, hogy egy jó hírű, független bizonyosságot nyújtó szolgáltató ellenőrizte a feleket. Ellenőrzési jogra vonatkozó záradék nélkül a belső ellenőrzési funkció képessége a bizonyosság megszerzésére vagy nyújtására korlátozott lehet.

- A szervezet hozzáféréssel rendelkezik független auditorok kontrollértékelési jelentéseihez – például pénzügyi, megfelelőségi és adatbiztonsági területeken –, mint amilyenek az International Standard on Assurance Engagements (ISAE) vagy a SOC jelentések.
  - A harmadik fél külső bizonyosságot nyújtó szolgáltatóinak munkájára való támaszkodás esetén, a dokumentumokat a megbízhatóság biztosítása érdekében felül kell vizsgálni.
  - A SOC-jelentéseket a nem megfelelő kockázatkezelési és változáskezelési folyamatok azonosítására használják.

- A szabályzatok és folyamatok az egyes szervezetek vagy szerződéstípusok szempontjából lényeges összetevőkkel foglalkoznak:
  - Környezetvédelmi és fenntarthatósági záradékok.
  - Visszaélés bejelentési protokollok.
  - A teljesítmény mérésére vonatkozó követelmények.
  - A harmadik fél által tesztelt üzletmenet-folytonossági terv.
  - A mesterséges intelligencia használata a szolgáltatásnyújtásban.
  - Egyértelműen meghatározásra kerülnek az ellátási-lánc alsóbb szintjén lévő alvállalkozók azonosítási adatai, a közzétételi kötelezettségek, a szerződéses feltételek és a teljesítési kör.
  - Változáskezelési folyamat, amely meghatározza, hogyan kell kezelni a szerződés időtartama alatt bekövetkező változásokat a szerződés hatályában, a feltételekben vagy a működési követelményekben (például technológiai módosulások vagy jogszabályi változások esetén).
  - Korlátozások a változtatásra vonatkozó megrendelések számára és a számlázható összegekre.

- A szabályzatok és folyamatok megkövetelik a végtermékek hivatalos elfogadását, mielőtt a kifizetés megtörténne, vagy bármilyen visszatartott összeget elengednének.
- A harmadik felek kötelesek megosztani etikai irányelvüket vagy magatartási kódexüket és/vagy betartani az elsődleges szervezet etikai politikáját vagy magatartási kódexét.

- Ha a harmadik fél bocsátja rendelkezésre a szerződést, az elsődleges szervezet jogi felülvizsgálatot végez, a fő kockázatok ismertek és megfelelő kockázatcsökkentési stratégiával kezelik őket.

C. A véglegesített szerződéseket vagy megállapodásokat a megfelelő érdekelt felek – beleértve a jogi és megfelelési területet is – felülvizsgálják és jóváhagyják, biztonságosan tárolják, majd a szerződéskezelő vagy adminisztrátor felelősségi körébe rendelik.

- Szerződés vagy más hivatalos dokumentum, amely magában foglalja a kiszervezett kapcsolatot és a harmadik fél kötelezettségét, valamint a szükséges jogi és megfelelési felülvizsgálatok bizonyítékát.

D. Minden harmadik féllel fennálló kapcsolatról pontos, teljes és naprakész listát vezetnek, például egy központosított szerződéskezelő rendszerben.

- A harmadik féllel kötött új szerződések vagy megállapodások nyilvántartásba vagy nyilvántartó rendszerbe történő felvételének folyamata.
- Folyamat a potenciális harmadik felek szállítói rendszerbe való bevitelére és eltávolítására, ha a szerződést nem hagyják jóvá.
- A harmadik fél szerződéseinek vagy megállapodásainak a nyilvántartásból vagy a rendszerből való eltávolítására szolgáló folyamat.
- Nyomon követési rendszer az egyes vállalkozókkal vagy szállítókkal kapcsolatos problémák dokumentálására a jövőbeni hivatkozás céljából.
- Felülvizsgálati folyamat annak megállapítására, hogy vajon a harmadik feleket tartalmazó nyilvántartás pontos és teljes-e.

E. Dokumentált beillesztési folyamatokat alakítanak ki és követnek annak érdekében, hogy a harmadik felek teljesíteni tudják a szerződés vagy megállapodás feltételeit. A felülvizsgálatok kiterjedhetnek annak ellenőrzésére, hogy:

- Az egységes beillesztési eljárások biztosítják, hogy minden szükséges dokumentáció, képzés és megfelelési felülvizsgálat megtörténjen.
- A harmadik fél rendszerei és folyamatai zökkenőmentesen integrálhatók az elsődleges szervezet technológiájával.
- A megosztott rendszerek kompatibilisek és biztonságosak. A bizonyítékok tartalmazhatják a szolgáltatást igénybe vevő szervezet kiegészítő kontrolljait is a SOC-jelentés részeként.
- Az elsődleges szervezet értékeli a harmadik fél üzletmenet-folytonossági terveit, amelyek biztosítják a szolgáltatás folytonosságát vészhelyzet esetén. Ebben az esetleges zavarok kezelésére vészhelyzeti tervek is szerepelhetnek.

F. A szerződés vagy megállapodás célkitűzéseihez viszonyított szállítói teljesítmény folyamatos nyomon követésére szolgáló folyamatok, beleértve a kulcsfontosságú teljesítménymutatók értékelését.

- A nyomon követési folyamat visszacsatolásként szolgál a harmadik fél kockázatértékeléséhez, és az azonosított kontrollhiányosságokat felülvizsgálatra kerülnek, valamint szükség esetén kezelésükre intézkedések történnek.
- A valós idejű nyomon követést támogató folyamatok, technológiák és eszközök jelentései vagy megállapításai.
- Folyamatok, amelyek biztosítják, hogy a kifizetések a szerződés vagy megállapodás feltételeinek megfelelően történjenek, például a projektütemtervnek, mérföldköveknek és kommunikációs követelményekn való megfelelés.ek A kifizetések csak olyan jóváhagyott szerződéses partnereknek történnek, akik befejezték a beillesztési szakaszt és bekerültek a szállítói fizetési rendszerbe. Ha a szerződésben meghatározott teljesítendő feladatok szerepelnek, a végső kifizetésekre csak akkor kerül sor, ha a teljesítendő feladatok ellenőrzése megtörtént.
- A harmadik féllel kötött megállapodásokkal kapcsolatos költségek ellenőrzése az érték biztosítása és a befektetés megtérülésének meghatározása érdekében. A költség-haszon elemzések eredményeinek felhasználása a szerződések újratárgyalásához.
- A szerződésben vagy megállapodásban szereplő szolgáltatási szint be nem tartása esetén alkalmazandó szankciók megállapítására szolgáló eljárások. A szerződésszegéshez kapcsolódó pénzügyi következmények kiszámítása és érvényesítése a tényleges bekövetkezéskor történik.
- A kiemelten kezelt harmadik felek kockázatalapú besorolását rendszeresen újraértékelik, amikor a megállapodásban változások történnek, illetve amikor egy szerződés közeledik a lejárathoz vagy az automatikus megújuláshoz.
- A kiemelten kezelt harmadik felek felülvizsgálata, például helyszíni vagy negyedéves üzleti felülvizsgálatok a kontrollok és a működési integritás igazolására.
- A további folyamatos nyomon követés bizonyítéka lehet:
    - A harmadik fél pénzügyi stabilitásának elemzése.
    - Harmadik féllel szembeni panaszok elbírálása.
    - Független könyvvizsgálói jelentések, például a International Standard on Assurance Engagements, Statements on Standards for Attestation Engagements, a harmadik felek által szolgáltatott pénzügyi, ellenőrzési, megfelelőségi és adatbiztonsági jelentések; ISO tanúsítványok
    - A harmadik fél által végzett üzleti ellenálló képességi tesztek vezetőség által végzett felülvizsgálata, beleértve az azonosított jelentős problémákat.
    - Az alvállalkozók vagy az ellátási láncban alsóbb szintén lévő további partnerek igénybevételére vonatkozó feltételek és korlátozások.
    - Harmadik fél etikai értékeinek, kultúrájának és magatartásának értékelése.
    - Válaszok a média megkereséseire.
    - Az adatvédelmi és kiberbiztonsági protokollok értékelése az elsődleges szervezet adatainak és információinak továbbítása és tárolása védelmére, beleértve a fejlett technológiák, például a mesterséges intelligencia használatát.

- A szervezet által a teljesítmény folyamatos javítására és a szerződés vagy megállapodás célkitűzéseinek teljesítésére irányuló lehetőségek azonosítása.
- A feladatok elkülönítésének felülvizsgálata.

G. Javító intézkedések kezdeményezésére vonatkozó protokollok az azonosított incidensekkel kapcsolatban, ha egy harmadik fél nem teljesíti a szerződés vagy megállapodás követelményeit, vagy ha a harmadik fél tevékenységei növelik az elsődleges szervezetre jelentett kockázatot.

- Protokollok az incidensek súlyossága és a harmadik fél prioritása alapján történő továbbítására.
- Az incidenst követő felülvizsgálat, beleértve a kiváltó okok elemzését.

H. Folyamatok a lejáró vagy automatikusan megújuló szerződésekre és megállapodásokra vonatkozó figyelmeztetések biztosítására. Az automatikus megújítási folyamatok magukban foglalják az alábbiak felülvizsgálatát:

- A harmadik fél teljesítménye.
- A szerződés vagy megállapodás feltételei és bármely kiegészítés.
- Kockázati tényezők.

I. A szerződés megszüntetési folyamatra vonatkozóan formalizált terv kerül kialakításra és alkalmazásra, amely biztosítja a szerződéses követelmények – különösen az időzítés és az elvárások – megfelelő teljesítését, beleértve az ellátási-lánc alsóbb szintén lévő érintett alvállalkozókat is.

- Ellenőrző listák vagy interjúk a kulcsfontosságú érdekelt felekkel a biztonsági intézkedések hatékonyságának biztosítása érdekében.
- A harmadik fél által őrzött szervezeti információkat vagy adatokat visszajuttatták vagy megsemmisítették.
- A harmadik fél hozzáférése a szervezet adataihoz, rendszereihez vagy létesítményeihez visszavonásra került.
- Az elsődleges szervezet eszközeinek, például készülékek/berendezések, szoftverlicencek, szellemi tulajdon és dokumentáció visszajuttatása megtörtént.
- Ha a szerződés megszüntetése a harmadik félnek felróható okkal történik, a kiváltó körülményeket vagy kockázatokat azonosítják és a felsővezetés és/vagy a vezetőtestület elé terjesztik.
- Amennyiben egy kiemelten kezelt harmadik féllel kötött szerződés megszűnik, a felet ugyanazon kockázatértékelés alapján kell pótolni, kivéve, ha a szerződés teljesült vagy további együttműködésre nincs szükség.

A. függelék. Gyakorlati alkalmazási példák

Az alábbi példák olyan forgatókönyveket írnak le, amelyekben a Harmadik Fél Tematikus követelmény alkalmazható:

1. példa: A belső ellenőrzési tervben szereplő belső ellenőrzési megbízás olyan szolgáltatást vagy teljesítményt érint, amelyet jelenleg egy harmadik fél nyújt.

Amikor a belső ellenőrzési funkció befejezi kockázatalapú tervezési folyamatát, és a belső ellenőrzési tervbe egy vagy több olyan szolgáltatásra vagy teljesítményre vonatkozó megbízást vesz fel, amelyet jelenleg harmadik felek nyújtanak szerződés vagy megállapodás alapján, a Tematikus követelményt kötelező alkalmazni.

A Tematikus követelményben szereplő követelmények közül nem mindegyik alkalmazható minden vizsgálatra. Ha a belső ellenőrök szakmai megítélés alapján úgy döntenek, hogy a harmadik félre Tematikus követelmény egy vagy több követelménye nem alkalmazható, és ezért ki kell zárni a megbízásból, a belső ellenőröknek dokumentálniuk kell és meg kell őrizniük az adott követelmények ellenőrzésből történő kizárásának indoklását. Bizonyos követelmények kizárásának indoklása lehet például az, hogy a belső ellenőrzési funkció megállapította, hogy a szervezet a küldetése szempontjából kritikus szolgáltatások tekintetében kevésbé támaszkodik harmadik felekre, vagy hogy ez egy olyan kialakult kapcsolat, amelynek pénzügyi hatása alacsony.

2. példa: A harmadik féllel kapcsolatos kockázatokat a harmadik feleken vagy a szerződéskezelésen kívüli más témában végzett megbízás során azonosítják.

A belső ellenőrök jelentős harmadik féllel kapcsolatos kockázatot azonosíthatnak egy olyan folyamat értékelése során, amelyről eredetileg nem állapították meg, hogy harmadik féllel vagy szerződéskezeléssel kapcsolatos. Például az adattárolás értékelésére irányuló megbízás megtervezésekor a belső ellenőrök megtudják, hogy a felhőszolgáltatásokat egy harmadik fél nyújtja. A harmadik fél által nyújtott szolgáltatásokért felelős vezetéssel folytatott interjúk során a belső ellenőrök azonosítják a harmadik féllel kapcsolatos kiberbiztonsági kockázatokat.

A releváns kockázatok azonosítása után a belső ellenőröknek át kell tekinteniük mind a Harmadik fél, mind a Kiberbiztonság Tematikus követelményét, és meg kell határozniuk, hogy mely követelmények alkalmazandók. A belső ellenőrök kizárhatják a harmadik fél irányítási folyamatát vagy a harmadik fél kockázatkezelési folyamatát a megbízás hatóköréből, és a szolgáltatásokra vonatkozó, harmadik fél által működtetett kontrollokra összpontosíthatnak. Ugyanez a szakmai megítélés vonatkozik a Kiberbiztonsági Tematikus követelmény alkalmazására is. A belső ellenőröknek a megbízási munkadokumentumokban dokumentálniuk kell a Harmadik fél vagy a Kiberbiztonság Tematikus követelmények bármely követelményének kizárására vonatkozó indoklást, és a dokumentációt meg kell őrizniük.

3. példa: A belső ellenőrzési tervben eredetileg nem szereplő, harmadik félre vonatkozó ellenőrzési vizsgálat válik szükségessé.

A szervezeten belül olyan probléma merül fel egy kiemelt harmadik féllel kapcsolatban, amely a belső ellenőrzési funkció haladéktalan bevonását igényli. A probléma egy kontrollhiányosság volt. A belső ellenőrzési vezetőnek célszerű kommunikálnia a vezetőtestületnek a belső ellenőrzési funkció ellenőrzési tervének és erőforrásainak átcsoportosítását a felmerült igényekhez való igazodás érdekében. A belső ellenőrnek együtt kell működnie az érintett vezetéssel a megbízás célkitűzéseinek kidolgozása érdekében, hogy értékelje a helyzetet, és javaslatokat fogalmazzon meg a hasonló esetek jövőbeni előfordulásának megelőzésére. A belső ellenőrzési vezetőnek át kell tekintenie a Tematikus követelményt annak érdekében, hogy meghatározza az ellenőrzés hatókörét, eldöntse, mely követelmények alkalmazandók és dokumentálja az esetleges kivételeket.

B. melléklet. Opcionális dokumentációs segédlet

A belső ellenőröknek a kockázatértékelésre támaszkodva szakmai megítélésük alapján kell meghatározniuk, hogy mely követelmények alkalmazandók, és megfelelő módon dokumentálniuk kell az egyes követelmények vizsgálatának kizárását. A Tematikus követelményt a belső ellenőrzési tervben vagy a megbízás munkadokumentumaiban lehet dokumentálni a belső ellenőrök szakmai megítélése alapján. Egy vagy több belső ellenőrzési megbízás is kiterjedhet a követelményekre. Ezenkívül előfordulhat, hogy nem minden követelmény alkalmazható. Az alábbi nyomtatható űrlap a Harmadik fél Tematikus követelménynek való megfelelés dokumentálásának egyik lehetőségét kínálja, de használata nem kötelező.

Harmadik fél – Irányítás

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
A. Szabályozott megközelítést alakítanak ki, hajtanak végre, és rendszeresen felülvizsgálnak annak meghatározására, hogy szerződést kössenek-e harmadik féllel. A megközelítés megfelelő kritériumokat tartalmaz annak meghatározására és értékelésére, hogy milyen erőforrások szükségesek és állnak rendelkezésre a célok eléréséhez egy termék vagy szolgáltatás nyújtása révén.		
B. Szabályzatokat és folyamatokat alakítottak ki a harmadik felekkel való kapcsolatok és kockázatok meghatározására, értékelésére és kezelésére a harmadik felek teljes kapcsolati életciklusa során. A szabályzatok és folyamatok összhangban vannak az alkalmazandó jogszabályi követelményekkel, és a kontrollkörnyezet megerősítése érdekében rendszeresen felülvizsgálják és frissítik azokat.		

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
C. A szervezet harmadik felek kezelésére vonatkozó szerepeit és felelősségi köreit meghatározzák, részletezve, ki választja ki, irányítja, kezeli a harmadik feleket, ki kommunikál velük, ki végzi a nyomon követésüket, és kinek kell tájékoztatást kapnia a harmadik felek tevékenységéről. Kialakítottak egy olyan folyamatot, amely biztosítja, hogy a harmadik félhez rendelt szereppel és felelősséggel megbízott személyek rendelkezzenek a megfelelő kompetenciákkal.		
D. Meghatározásra kerültek olyan kommunikációs eljárásrendek, amelyek biztosítják az érintett érdekelt felek számára a kiemelten kezelt harmadik felek teljesítményére, kockázataira és megfelelésére (különösen a jogszabályok és szabályozók megsértése esetére) vonatkozó információk kellő időben történő jelentését. A harmadik feleket a kockázatuk alapján besorolják. Az érintett érdekelt felek közé tartozhatnak többek között a vezetőtestület, a felsővezetés, a beszerzés, az üzemeltetés, a kockázatkezelés, a megfelelés, a jog, az információtechnológia, az információbiztonság, a humánerőforrás területei és egyéb szereplők.		

Harmadik fél – Kockázatkezelés

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
A. A harmadik felek és szolgáltatásaik kockázatkezelésére vonatkozó folyamatok szabályozottak és átfogóak, meghatározott szerepeket és felelősségi köröket tartalmaznak, és érdemben kezelik a szervezet szempontjából releváns kulcsfontosságú kockázatokat, mint például a stratégiai, reputációs, etikai, működési, pénzügyi, megfelelési, kiberbiztonsági, információtechnológiai, jogi, fenntarthatósági és geopolitikai kockázatok. A folyamatok betartását nyomon követik, és az eltérések esetén javító intézkedéseket valósítanak meg.		
B. A harmadik felekkel kapcsolatos kockázatokat az életciklus során rendszeresen azonosítják és értékelik. A kockázatértékelést a harmadik felek besorolására és priorizálására használják, beleértve a partnerek láncolatának alsóbb szintjein elhelyezkedő feleket is. A kockázatokra adott válaszokat besorolják és priorizáljak. A kockázatértékelést rendszeresen felülvizsgálják és frissítik.		
C. A kockázatokra adott válaszok megfelelőek és pontosak, és összhangban vannak a besorolásukkal. A kockázatokra adott válaszokat végrehajtják, felülvizsgálják, jóváhagyják, nyomon követik, értékelik és szükség szerint módosítják.		

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
D. Kialakítottak olyan folyamatokat, amelyek biztosítják a harmadik felektől eredő problémák kezelését és – szükség esetén – jelentését, elősegítve a teljesítményekért való elszámoltathatóságot, valamint növelve a szerződésekben vagy egyéb megállapodásokban foglalt feltételek teljesülésének esélyét. Ha egy harmadik fél nem reagál a továbbított aggályokra, kialakított folyamatok állnak rendelkezésre annak érdekében, hogy a vezetés értékelje a fennálló üzleti kapcsolatból eredő kockázatokat, és – az indokoltságtól függően – további intézkedéseket, kockázatcsökkentő lépéseket tegyen vagy a szerződéses kapcsolat megszüntetését kezdeményezze.		

Harmadik fél – Kontrollok

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
A. A harmadik felek bevonására és kiválasztására alapos átvilágítási eljárás van érvényben, amelyhez dokumentált és jóváhagyott üzleti indoklás vagy más releváns dokumentum tartozik, amely részletesen ismerteti és alátámasztja a harmadik féllel való kapcsolat szükségességét és jellegét.		
B. A szerződéskötés és jóváhagyás a szervezet harmadik felekre vonatkozó kockázatkezelési irányelvei és eljárásai szerint valósul meg, és magában foglalja az érintett szervezeti egységek együttműködését.		
C. A végleges szerződéseket vagy megállapodásokat minden releváns érdekelt fél – beleértve a jogi és a megfelelési területet – felülvizsgálja és jóváhagyja, mindkét fél felhatalmazott képviselői aláírják, és biztonságos módon kerülnek tárolásra. Minden szerződéshez felelős szerződéskezelő vagy adminisztrátor kerül kijelölésre.		

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
D. A szervezet minden harmadik féllel fennálló kapcsolatáról pontos, teljes és naprakész nyilvántartást vezet, például egy központosított szerződéskezelő rendszerben.		
E. Dokumentált beillesztési folyamatokat alakítottak ki és követnek a harmadik felekre vonatkozóan, amelyek megalapozzák a szerződés vagy megállapodás feltételeinek betartását.		
F. Folyamatos nyomon követési folyamatokat alakítottak ki annak érdekében, hogy értékelni lehessen, vajon a harmadik felek az együttműködés teljes életciklusa során a szerződés vagy megállapodás feltételeinek megfelelően teljesítenek-e, illetve eleget tesznek-e szerződéses kötelezettségeiknek. A folyamatok magukban foglalják a szolgáltatott információk megbízhatóságának ellenőrzését, valamint a teljesítmény újraértékelését meghatározott időközönként, továbbá minden olyan esetben, amikor a szerződés vagy megállapodás módosul.		
G. Kialakított eljárások biztosítják a javító intézkedések kezdeményezését abban az esetben, ha egy harmadik fél nem felel meg az elvárásoknak, illetve fokozott, vagy váratlan kockázatot jelent. Az eljárások magukban foglalják az incidensek súlyosság szerinti továbbítását, az incidenseket követő felülvizsgálatok elvégzését, valamint a kiváltó okok elemzését.		
H. A szerződések lejárati és megújítási időpontjait nyomon követik, és szükség esetén megteszik a szükséges megújítási intézkedéseket.		

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
I. A szerződéses követelmények – beleértve az ütemezés és az elvárások – megfelelő kezelésének biztosítása érdekében szabályozott, a szerződés megszüntetésre vonatkozó tervet alakítanak ki és követnek. A folyamatok kiterjednek arra, hogyan kell: • Megszüntetni a harmadik féllel fennálló szerződéses kapcsolatot. • Szükség esetén másik harmadik felet választani. • Biztosítani, hogy a harmadik félnél tárolt érzékeny adatok kezelésére új felelős kerüljön kijelölésre, és az adatok visszakerüljenek a szervezethez, vagy megsemmisítésre kerüljenek. • Visszavonni a harmadik fél hozzáférését a szervezet rendszereihez, eszközeihez és létesítményeihez.		

A Belső Ellenőrök Intézetéről

A Belső Ellenőrök Intézete (The Institute of Internal Auditors, IIA) egy nemzetközi szakmai szövetség, amelynek világszerte több mint 255 000 tagja van, és több mint 200 000 Certified Internal Auditor® (CIA®) okleveles belső ellenőrzési képesítést adott ki. Az 1941-ben alapított nemzetközi szervezetet világszerte a belső ellenőrzési szakma vezetőjeként ismerik el a normák, a minősítések, az oktatás, a kutatás és a technikai útmutatás terén. További információ a www.theiia.org oldalon.

Felelősségi nyilatkozat

Az IIA ezt a dokumentumot tájékoztató és oktatási céllal teszi közzé. Ez az anyag nem arra szolgál, hogy végleges válaszokat adjon konkrét egyedii körülményekre, és mint ilyen, csak útmutatóként használható. Az IIA azt ajánlja, hogy bármely konkrét helyzetre vonatkozóan közvetlenül független szakértői tanácsot kérjenek. Az IIA nem vállal felelősséget azért, ha valaki kizárólag erre az anyagra hagyatkozik.

Szerzői jog

Szeptember 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101