Harmadik fél

Tematikus követelmény

Topical Requirement

The Institute of Internal Auditors

Fordította:

The Institute of Internal Auditors Hungary

Harmadik fél Tematikus követelmény

A Nemzetközi Szakmai Gyakorlatok Keretrendszere (International Professional Practices Framework®) a Globális Belső Ellenőrzési Normákat (Global Internal Audit Standards™), a Tematikus követelményeket és a Globális iránymutatásokat foglalja magában. A Tematikus követelmények kötelezőek, és azokat a Normákkal együtt kell alkalmazni, amelyek az előírt gyakorlatok hiteles alapját képezik.

A Tematikus követelmények egyértelmű elvárásokat támasztanak a belső ellenőrökkel szemben azáltal, hogy a szükséges minimumot határozzák meg a megjelölt kockázati területek ellenőrzésére vonatkozóan. A szervezet kockázati profilja megkövetelheti, hogy a belső ellenőrök a téma további szempontjait is figyelembe vegyék.

A Tematikus követelményeknek való megfelelés növeli a belső ellenőrzési szolgáltatások következetességét, valamint javítja a belső ellenőrzési szolgáltatások és eredmények minőségét és megbízhatóságát. Végső soron a Tematikus követelmények fejlesztik a belső ellenőrzési szakmát.

A belső ellenőröknek a Globális Belső Ellenőrzési Normákkal összhangban kell alkalmazniuk a Tematikus követelményeket. A Tematikus követelményeknek való megfelelés a bizonyosságot nyújtó szolgáltatások esetében kötelező, a tanácsadói szolgáltatások esetében pedig ajánlott. A Tematikus követelmény akkor alkalmazható, ha a téma:

1. A belső ellenőrzési tervben szereplő megbízás tárgya.
2. Egy megbízás teljesítése során azonosított.
3. Az eredeti belső ellenőrzési tervben nem szereplő soron kívüli megbízás tárgya.

Dokumentálni kell, és meg kell őrizni annak bizonyítékát, hogy a Tematikus követelményben szereplő minden egyes követelmény alkalmazhatóságát értékelték. Nem minden egyes követelmény alkalmazható minden megbízás esetén; ha a követelményeket nem alkalmazzák, az indoklást dokumentálni kell és meg kell őrizni. A Tematikus követelménynek való megfelelés kötelező, és azt a minőségértékelések során vizsgálják.

Harmadik felek

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 szerződéssel, megállapodással vagy más módon formalizálható. Ez a Tematikus követelmény a „harmadik fél” kifejezést használja a beszállítókra, szolgáltatókra, vállalkozókra, alvállalkozókra, kiszervezett szolgáltatást nyújtókra, egyéb ügynökségekre és tanácsadókra. A kifejezés azokra a megállapodásokra is kiterjed, amelyek a harmadik fél és annak alvállalkozói között jönnek létre, akik az ellátási lánc alacsonyabb szintjén helyezkednek el.

A Tematikus követelmény akkor alkalmazandó, amikor a belső ellenőrzési funkció harmadik felekre és/vagy alvállalkozói kapcsolatokra vonatkozóan végez ellenőrzési tevékenységet, beleértve azokat is, amelyek a harmadik fél szerződése vagy megállapodása alapján az adott szervezettel további (negyedik

vagy annál mélyebb) szinteken engedélyezettek. A belső ellenőröknek a harmadik és a további szinteken lévő feleket a kockázat alapján szükséges besorolniuk a későbbi kockázatkezelési szakaszban leírtak szerint. A belső ellenőröknek a kockázatértékelés eredményei által jelzett valamennyi követelményt alkalmazniuk kell, és a kivételeket kell.

Ez a Tematikus követelmény nem vonatkozik az elsődleges szervezettel fennálló olyan közvetett külső kapcsolatokra, érdekeltségekre vagy érintettségekre, mint például a szabályozó hatóságok, ügynökök, brókerek, befektetők, vagyonkezelők/vezetőtestületi tagok, közszolgáltatók és a nyilvánosság tagjai, 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 rugalmasságra, és szakmai megítélésükre javasolt hagyatkozniuk, hogy a Tematikus követelményt az elsődleges szervezet harmadik félre vonatkozó meghatározásához igazítsák.

Az elsődleges szervezet (a harmadik féllel megállapodást kötő szervezet) változatlanul felelős a célkitűzéseinek elérésével kapcsolatos kockázatokért, akkor is, ha egy harmadik felet bíz meg egy vagy több célkitűzés elérésének elősegítésével. A harmadik felekkel való együttműködés olyan kockázatokat rejt magában, amelyeket megfelelő irányítási, kockázatkezelési és kontrollfolyamatokon keresztül kell azonosítani, értékelni és kezelni, a jelen Tematikus követelményben foglaltak szerint. Ha egy harmadik fél nem teljesíti a szerződésben foglaltakat, etikátlan gyakorlatot folytat, vagy üzleti működésében zavar keletkezik, az elsődleges szervezetet is hátrányos érinthetik a következmények. A harmadik felekkel kapcsolatos kockázatok kategóriái és példái a következők:

- Stratégiai, például az elsődleges 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 érdekeltekkel való kapcsolatában és bizalmában okozott kár.
- Etikai, mint például feddhetetlenség, összeférhetetlenség, kenőpénz és korrupció.
- Működési, például fizikai és információbiztonsági, bennfentes kockázat, szolgáltatási zavarok 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 harmadik fél életciklusa a kiválasztásból, a szerződéskötésből, a beillesztésből, a nyomon követésből és a szerződés megszüntetéséből áll. A belső ellenőröknek ezeket a szakaszokat is figyelembe kell venniük az irányítási, kockázatkezelési és kontrollfolyamatokra vonatkozó követelmények értékelésekor.

Harmadik felek irányítási, kockázatkezelési és kontrollfolyamatainak értékelése és felmérése.

Ez a Tematikus követelmény következetes, átfogó megközelítést biztosít a harmadik felekhez kapcsolódó irányítási, kockázatkezelési és kontrollfolyamatok kialakításának és végrehajtásának értékeléséhez. A követelmény a szükséges minimumot képviseli az értékeléshez.

IRÁNYÍTÁS

Követelmények:

A belső ellenőröknek az elsődleges szervezet harmadik feleinek irányításával kapcsolatban a következő szempontokat kell értékelniük, beleértve a vezetőtestület által gyakorolt felügyeletet is:

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.

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.

KOCKÁZATKEZELÉS

Követelmények:

A belső ellenőröknek értékelniük kell a szervezet harmadik felekkel kapcsolatos kockázatkezelésének az alábbi szempontjait:

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 az ellátási-lánc alsóbb szintjén lévő 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.

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.

KONTROLLOK

Követelmények:

A belső ellenőröknek értékelniük kell az alábbi kontrollokat a kockázatok alapján besorolt harmadik felek vonatkozásában. Az értékelésnek ki kell terjednie a vezetés által alkalmazott folyamatokra, amelyek a szervezet harmadik feleinek folyamatos értékelésére és nyomon követésére irányulnak.

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.

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 számukra 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.

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.

Szerzői jog

2025. szeptember

The Institute of Internal Auditors

Globális központ
A Belső Ellenőrök Intézete
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Telefon: +1-407-937-1111
Fax: +1-407-937-1101