Szervezeti ellenállóképesség

Tematikus követelmény

Topical Requirement

The Institute of Internal Auditors

Fordította:

The Institute of Internal Auditors Hungary

Szervezeti ellenállóképesség Tematikus követelmény

Az IIA Nemzetközi Szakmai Gyakorlatok Keretrendszere (International Professional Practices Framework®) a Globális Belső Ellenőrzési Normákat (Global Internal Audit Standards™), a Tematikus követelményeket és a Globális útmutatásokat foglalja magában. A Tematikus követelmények kötelezőek, és azokat a Normákkal együtt kell alkalmazni, mivel azok biztosítják a követendő gyakorlatok hiteles alapját.

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, beleértve a helyi szabályozásokat.

A Tematikus követelményeknek való megfelelés növeli a belső ellenőrzési szolgáltatások következetességét, valamint javítja a belső ellenőrzési szolgáltatások, 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 alkalmazandó, ha a téma:

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

Nem minden egyes követelmény alkalmazható minden megbízás esetén, és egyes követelmények más megközelítések alkalmazásával is teljesíthetők. Amennyiben egy követelmény más jogszabályi vagy szerződéses előírások miatt nem alkalmazható, azok által felülíródik, vagy a Globális Belső Ellenőrzési Normáknak megfelelő eljárások alkalmazásával kerül teljesítésre, ennek indoklását dokumentálni kell és meg kell őrizni. A megfelelést a minőségértékelések során értékelik.

További információért lásd a Szervezeti ellenállóképesség Tematikus követelmény Felhasználói útmutatót.

Szervezeti ellenállóképesség

A Nemzetközi Szabványügyi Szervezet (ISO) meghatározása szerint a szervezeti ellenállóképesség „egy szervezet azon képessége, amelynek révén képes a változó környezet hatásait elviselni és azokhoz alkalmazkodni." (ISO 22316:2017). Bár ez a meghatározás egyértelmű törekvést fogalmaz meg, a gyakorlatban a szervezetek jelentős eltéréseket mutatnak abban, hogy miként készülnek fel a változásokra és a működést érő zavarokra, hogyan reagálnak azokra, hogyan alkalmazkodnak hozzájuk, illetve hogyan állítják helyre működésüket azok bekövetkezését követően. Mivel a szervezeti ellenállóképesség stratégiai, működési, technológiai, emberi, társadalmi és pénzügyi dimenziókra is kiterjed, egyes szervezetek képesek hatékonyan kezelni a változásokat, míg mások számára ez nehezebb, vagy eltérő megközelítéseket alkalmaznak a bizonytalanság kezelésére.

A szervezeti ellenállóképesség egy olyan átfogó fogalom, amely azokat a kockázatokat veszi figyelembe, amelyek jelentősen megzavarhatják vagy korlátozhatják a szervezet azon képességét, hogy alapvető termékeit és szolgáltatásait nyújtsa, fenntartsa az érdekelt felek bizalmát, illetve megvalósítsa stratégiai céljait. Ezek a kockázatok származhatnak hirtelen bekövetkező eseményekből (például természeti katasztrófákból, kibertámadásokból és geopolitikai konfliktusokból), tartós környezeti nyomásgyakorló tényezőkből (például erőforráshiányból és közegészségügyi válságokból), valamint a külső környezet változásaiból (például technológiai eredetű működési zavarból, szabályozási változásokból és a szervezeti hírnév romlásából).

E kockázatok megjelenhetnek fokozatos változások vagy lassan felépülő nyomásgyakorló tényezők formájában is, amelyek idővel aláásható a szervezet stabilitását és alkalmazkodóképességét. Az ilyen jellegű, fokozatosan kialakuló kockázatok könnyen elkerülhetik az ember figyelmét. Az ellenállóképes szervezetek a sikeres működés érdekében egyaránt képesek előre felismerni és kezelni a hirtelen jelentkező, valamint a nehezen észlelhető kockázatokat, továbbá alkalmazkodni azok hatásaihoz.

Az ellenállóképességet érintő eredendő kockázati tényezők közé tartoznak a rendkívül összetett működési környezetek, a globalizált ellátási láncok, a központosított infrastruktúra- vagy adatrendszerek, a munkaerő korlátozott rendelkezésre állása, az ingadozó piaci feltételek, valamint a kritikus harmadik felektől vagy meghatározott földrajzi térségektől való erős függés. A magas megbízhatóságot igénylő ágazatokban működő, illetve erős szabályozási felügyelet alatt álló szervezetek a közérdekre gyakorolt hatás és a megfelelési kötelezettségek miatt eredendően magasabb kockázatokkal szembesülhetnek.

A szervezeti ellenállóképesség a kockázatok kezelésére összpontosít a működési zavarok bekövetkezése előtt, azok fennállása alatt és azokat követően. A belső ellenőrök jellemzően az üzletmenet-folytonossággal és a katasztrófa utáni helyreállítással kapcsolatos informatikai (IT) folyamatokat és kontrollokat értékelik. Az üzletmenet-folytonossági terv részletezi azokat a lépéseket, amelyeket egy szervezet a kritikus működés fenntartása, valamint katasztrófa esetén a normál működés helyreállítása érdekében tesz. A katasztrófa utáni helyreállítási terv meghatározza, hogy a szervezet hogyan állítja helyre informatikai rendszereit, kritikus adatait és működését egy működési zavart okozó esemény bekövetkezését követően a normál üzleti működés helyreállítása érdekében.

Az előbb említett terveket magában foglaló szervezeti ellenállóképesség stratégiai tervezést, vállalati kockázatkezelést, hatékony vezetést és szervezeti kultúrát, valamint az egész szervezetre kiterjedő kontrollfolyamatokat igényel. A szervezeti ellenállóképességet támogató, jól kialakított kontrollfolyamatok nemcsak azt teszik lehetővé, hogy a szervezetek folyamatosan előre jelezzék a változásokat, felkészüljenek azokra, reagáljanak rájuk és alkalmazkodjanak hozzájuk, hanem azt is, hogy fennmaradjanak és fejlődjenek.

A szervezeti ellenállóképesség irányítási, kockázatkezelési és kontrollfolyamatainak értékelése és felmérése

Jelen Tematikus követelmény következetes, átfogó megközelítést biztosít a szervezeti ellenállóképességhez kapcsolódó irányítási, kockázatkezelési és kontrollfolyamatok tervezésének és végrehajtásának értékeléséhez. A követelmény a szükséges minimumot képviseli a szervezeti ellenállóképesség értékeléséhez.

Irányítás

Követelmények

A belső ellenőröknek a szervezeti ellenállóképesség irányításával kapcsolatban a következő szempontokat kell értékelniük:

A. A vezetés által kialakított, a vezetőtestület által elfogadott és felügyelt formális szervezeti ellenállóképességet szolgáló stratégia magában foglalja a változások kezeléséhez és a működés folytonosságának biztosításához szükséges működési, technológiai és pénzügyi elemeket. Az ellenállóképességgel kapcsolatos célkitűzések összhangban állnak a szervezet átfogó kockázatkezelési megközelítésével.

B. Az ellenállóképességgel kapcsolatos célkitűzések teljesítésének alakulásáról felülvizsgálati célból rendszeres időközönként tájékoztatják a vezetőtestületet. Ez biztosítja, hogy az ellenállóképesség beépüljön a stratégiai felügyeletbe, a hosszú távú tervezési folyamatokba, az utódlástervezésbe és a szervezeti kultúrába, beleértve a kritikus üzleti tevékenységek támogatásához szükséges erőforrás- és költségvetési szempontokat is.

C. A kritikus működési, technológiai és pénzügyi folyamatokra vonatkozó szabályzatok és eljárások kialakításra kerülnek, és a kontrollkörnyezet megerősítése érdekében rendszeresen felülvizsgálják, tesztelik és szükség szerint frissítik azokat.

D. A szervezeti ellenállóképességgel kapcsolatos célkitűzések felügyeletére és támogatására incidenskezelési struktúrát alakítanak ki és alkalmaznak. Ez magában foglalja a döntéshozatali struktúrát, a kommunikációs és eszkalációs protokollokat, valamint a vezetői és operatív szerepeket és felelősségi köröket.

E. Kialakítanak egy olyan folyamatot, amely rendszeres időközönként igazolja az ellenállóképesség biztosításához szükséges kompetenciák meglétét, valamint újraértékeli az ellenállóképességgel kapcsolatos folyamatokban kritikus szerepet betöltő személyek alkalmasságát.

F. Kialakítanak egy olyan folyamatot, amely biztosítja az érintett belső és külső érdekelt felek azonosítását, priorizálását és bevonását az ellenállóképességhez kapcsolódó célkitűzések elérését támogató információs és jelentéstételi struktúrák létrehozásába. Az érdekelt felek közé tartozhat a felsővezetés, a működési területek, a kockázatkezelés,

az IT, az ellátási lánc és a beszerzés, a létesítménygazdálkodás, a humánerőforrás, a pénzügy, a jogi terület, a bizonyosságot nyújtó funkciók (beleértve a belső ellenőrzést), a megfelelés, a külső kommunikáció, a kritikus beszállítók, az ügyfelek, a szabályozó hatóságok, valamint egyéb érintettek.

Kockázatkezelés

Követelmények

A belső ellenőröknek a szervezeti ellenállóképesség kockázatkezelésével kapcsolatban a következő szempontokat kell értékelniük:

A. A szervezeti ellenállóképességet érintő kockázatok azonosítása, értékelése és kezelése a szervezet egészében rendszeres időközönként megtörténik. A szervezeti ellenállóképességet érintő kockázatok és a szervezet stratégiai célkitűzései közötti összefüggések feltérképezése megtörténik. Az ellenállóképességhez kapcsolódó kockázatkezelési folyamat magában foglalja a kulcsfontosságú folyamatok értékelését.

B. A szervezeti ellenállóképességhez kapcsolódó kockázatkezelési folyamat keretében az elszámoltathatóság és a felelősségi körök egyértelműen meghatározottak. Kijelölt személy vagy szervezeti egység felel a szervezeti ellenállóképességet érintő kockázatok kezelésének rendszeres nyomon követéséért és az arról szóló jelentések elkészítéséért, beleértve a kockázatcsökkentéshez szükséges erőforrások, valamint az újonnan megjelenő fenyegetések figyelemmel kísérését is.

C. Olyan folyamat került kialakításra, amely a szervezeti ellenállóképességet érintő kockázatok szintjének folyamatos nyomon követését, valamint azon esetek gyors vezetői szintre emelését biztosítja, amelyek a szervezet kockázatkezelési irányelvei, kockázati tűrőképessége vagy a vonatkozó jogszabályi és szabályozói előírások alapján elfogadhatatlannak minősülő kockázati szintet érnek el. A szervezeti ellenállóképességet érintő kockázatok hatásainak értékelése során azok lehetséges következményeit figyelembe veszik.

D. A vezetés olyan folyamatot alakított ki és tesztel rendszeresen, amely biztosítja a válsághelyzetekre, működési zavarokra és vészhelyzetekre való reagálást, valamint az azokból történő helyreállítást. Az incidenskezelési és helyreállítási folyamat magában foglalja az észlelést, a rangsorolást, az elhárítást, a helyreállítást, valamint az incidens utáni elemzést. Az incidenskezelési megközelítés magában foglalja a forgatókönyv-elemzéseket, valamint a különböző működési zavart okozó eseményekre kiterjedő, rendszeresen végrehajtott stressztesztek.

Kontrollfolyamatok

Követelmények

A belső ellenőröknek a szervezeti ellenállóképességhez kapcsolódó kontrollfolyamatokkal összefüggésben a következő szempontokat kell értékelniük:

A. Olyan folyamat került kialakításra, amely biztosítja a kritikus külső szolgáltatók és beszállítók azonosítását, valamint az alapvető működés fenntartásához szükséges

minimális készletszintek meghatározását. A folyamat magában foglalja az alternatív beszállítók naprakész nyilvántartásának vezetését is.

B. A működés szempontjából kritikus adatokat azonosítják és osztályozzák. Az adatok osztályozása magában foglalja annak meghatározását, hogy hol találhatók az adatok, kiknek van szükségük hozzáférésre, hogyan történik a hozzáférés, valamint azt, hogy vészhelyzet esetén rendelkezésre áll-e biztonsági mentés, és az adatok helyreállíthatók-e.

C. Kritikus informatikai kontrollokat és folyamatos monitorozási mechanizmusokat alakítottak ki az információbiztonsági kockázatok, ideértve a kiberbiztonsági kockázatok mérséklése, valamint az érzékeny adatok válsághelyzetek, működési zavarok és vészhelyzetek alatti védelmének biztosítása érdekében. A kontrollok és a folyamatos monitoring magában foglalja a valós idejű fenyegetettségi információk felhasználását, valamint a hozzáférések kizárólag jogosult felhasználókra történő korlátozását.

D. A kritikus informatikai eszközöket nyilvántartják. Az eszközök közé tartoznak mindazon hardverek, szoftverek és szolgáltatások, amelyek a működés fenntartásához szükségesek válsághelyzetek, működési zavarok és vészhelyzetek esetén.

E. Az üzletmenet-folytonossági és a katasztrófa utáni helyreállítási tervek kialakításra kerültek, és egyértelműen meghatározzák a kijelölt munkatársak és helyreállítási csoportok szerepét és felelősségi körét. A terveket rendszeresen tesztelik (például forgatókönyv-alapú szimulációs gyakorlatok keretében), és a tesztelések eredményeiről, beleértve a fejlesztési lehetőségeket is, beszámolnak a vezetőtestületnek és a felsővezetésnek.

F. Olyan folyamat került kialakításra, amely lehetővé teszi a munkavégzési környezet szükség szerinti átalakítását válsághelyzetek, működési zavarok és vészhelyzetek esetén.

G. Olyan folyamat került kialakításra, amely a szervezeti ellenállóképességet érintő újonnan megjelenő fenyegetések és sérülékenységek folyamatos monitorozását és jelentését biztosítja. A folyamat a szervezeti ellenállóképességet támogató fejlesztési lehetőségek azonosítására, priorizálására és megvalósítására szolgál, ideértve a visszaélés-bejelentő rendszer, valamint a kockázati információk gyűjtését szolgáló mechanizmusok alkalmazását is.

H. Olyan folyamat került kialakításra, amely biztosítja a munkatársak szervezeti ellenállóképességgel kapcsolatos oktatását és képzését annak érdekében, hogy tisztában legyenek a válsághelyzetek, működési zavarok és vészhelyzetek bekövetkezése esetén követendő szabályzatokkal, eljárásokkal és a végrehajtandó intézkedésekkel. A folyamat magában foglal olyan gyakorlatokat, amelyek során működési zavart okozó eseményeket vagy helyzeteket szimulálnak.

I. Olyan folyamat került kialakításra, amely biztosítja, hogy a válsághelyzetek, működési zavarok és vészhelyzetek kezeléséhez szükséges működési, humán, technológiai és pénzügyi erőforrások tervezése megtörténjen, és azok rendelkezésre álljanak. Az ellenállóképesség támogatásához szükséges pénzügyi erőforrásokat rendszeres időközönként elemzik, és azokról beszámolnak a vezetőtestületnek.

J. Olyan folyamat került kialakításra, amely a válsághelyzetek, működési zavarok és vészhelyzetek utólagos felülvizsgálatát, valamint az eseményeket követő értékelések során levont tanulságok elemzését és azoknak a szervezeti ellenállóképességgel kapcsolatos jövőbeli tervezésbe történő beépítését biztosítja.

A Belső Ellenőrök Intézetéről

A Belső Ellenőrök Intézete (The Institute of Internal Auditors, IIA) egy nemzetközi szakmai szövetség, amelynek világszerte több mint 265.000 tagja van, és több mint 200.000 Certified Internal Auditor® (okleveles belső ellenőr, CIA®) tanúsítványt 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

2026. április

The Institute of Internal Auditors

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