Szervezeti ellenállóképesség

Tematikus követelmény

Felhasználói útmutató

Topical Requirement

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 (4.1 norma: Megfelelés a Globális Belső Ellenőrzési Normáknak) 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 belső ellenőrzés mandátuma egyértelműen meghatározza a belső ellenőrzési funkció által végzett szolgáltatások hatókörét és típusait, amely magában foglalja a Tematikus követelmények figyelembevételét (6.1. norma: A belső ellenőrzés mandátuma). 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, hogy egy minimális követelményrendszert biztosítsanak a téma következetes és megbízható értékeléséhez.

A Tematikus követelmények egyértelműen kapcsolódnak az IIA Három Vonal Modelljéhez és a Normákhoz. Az irányítási, kockázatkezelési és kontrollfolyamatok a 9.1 „Az irányítási, kockázatkezelési és kontrollfolyamatok megértése” című normához igazodó Tematikus követelmények fő összetevői. A Három Vonal Modellre vetítve az irányítás az vezetőtestülethez/irányítótestülethez, 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/irányítótestületnek 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 megköveteli 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 (lásd 9.4. normát, amely tartalmazza a belső ellenőrzési terv módosításait).

A szakmai megítélés kulcsfontosságú szerepet játszik a Tematikus követelmény alkalmazásában. A kockázatértékelések határozzák meg a belső 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), valamint azonosítják a megbízás célkitűzéseinek eléréséhez szükséges erőforrásokat (13.5 norma: A megbízáshoz rendelt erőforrások). Az A. függelék: „Példák a gyakorlati alkalmazásra” leírja, hogy a belső ellenőrök hogyan használják a Tematikus követelményt.

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 Normáknak megfelelő eljárások alkalmazásával kerül teljesítésre, ennek indoklását dokumentálni kell és meg kell őrizni. A megfelelést a minőségértékelések során értékelik.

A Tematikus követelménynek való megfelelést a 14.6 A megbízás dokumentációja normában leírtak szerint a belső ellenőr szakmai megítélése alapján kell dokumentálni.

Míg a Szervezeti ellenállóképesség 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 vezető úgy ítéli meg, hogy a belső ellenőrzési funkció nem rendelkezik a szükséges szakmai ismeretekkel egy, a Tematikus követelmény tárgyában történő ellenőrzési megbízás elvégzéséhez, a megbízás elvégzése kiszervezhető (3.1 norma: Kompetencia, 7.2 norma: A belső ellenőrzési vezető képesítései, 10.2 norma: Emberi erőforrás-gazdálkodás). A belső ellenőrzési vezetők számára hasznos forrás lehet a Belső Ellenőrök Intézete által közzétett Belső Ellenőrzési Kompetencia Keretrendszer. A Normák minden olyan személyre vagy funkcióra vonatkoznak, aki vagy amely belső ellenőrzési szolgáltatásokat nyújt, függetlenül attól, hogy az adott szervezet közvetlenül alkalmaz-e belső ellenőröket, külső szolgáltatón keresztül szerződik-

e velük, vagy mindkettő. A belső ellenőrzési vezető továbbra is viseli a végső felelősséget a megfelelés biztosításáért. Ezen túlmenően, ha a belső ellenőrzési vezető úgy ítéli meg, hogy a belső ellenőrzési erőforrások nem elegendőek, az ellenőrzési vezetőnek tájékoztatnia kell a vezetőtestületet az elégtelen erőforrások hatásáról és arról, hogy az erőforráshiányt hogyan fogják kezelni (8.2 norma: Erőforrások).

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 fejezettel 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 és magas színvonalú belső ellenőrzési gyakorlatokat. Ezeket a vonatkozó helyi törvényekkel, rendeletekkel, felügyeleti elvárásokkal és más, szakmailag elismert keretrendszerekkel együtt kell alkalmazni, amelyek további vagy specifikusabb követelményeket írhatnak elő. Előfordulhat, hogy a belső ellenőrök már kidolgozták a megbízási munkaprogramokat és vizsgálati eljárásokat ezen szabályzatok és keretrendszerek alapján. A belső ellenőröknek össze kell hangolniuk a szervezeti ellenállóképességhez kapcsolódó tervezett kontrolltesztelést és más belső és külső bizonyosságot nyújtó szolgáltatók által végzett megbízható tesztelést (9.5. norma: Koordináció és együttműködés) a Tematikus követelménnyel a megfelelő lefedettség biztosítása érdekében.

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 kiterjedhet a követelményekre. Ezenkívül előfordulhat, hogy nem minden követelmény alkalmazható. Meg kell őrizni annak bizonyítékát, hogy a Tematikus követelmény alkalmazhatóságát értékelték, beleértve a kivételek indoklását is.

A D. függelékben található segédlet használható referenciaként és a belső ellenőrök által végzett munka dokumentálására.

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, 8.4 norma: Külső minőségértékelés, 12.1 norma: Belső minőségértékelés). Az eredményeket kommunikálni kell a vezetőtestület és a felsővezetés felé. A kommunikáció során be kell számolni a belső ellenőrzési funkció Normáknak való megfeleléséről és a teljesítménycélok eléréséről.

A Tematikus követelményeknek való megfelelést célszerű figyelembe venni a megbízás szintjén végzett felügyeleti tevékenységek során (12.3 norma: A megbízások végrehajtásának felügyelete és fejlesztése), és a minőségértékelések keretében is vizsgálják. A minőségértékelésre való felkészüléshez a belső ellenőrök a D. függelékben található segédletet használhatják.

Szervezeti ellenállóképesség

A szervezeti ellenállóképesség a szervezet azon képességét jelenti, hogy ellenálljon a változások hatásainak és alkalmazkodjon azokhoz, különösen működési zavarok időszakában. A Nemzetközi Szabványügyi Szervezet ISO 22316 keretrendszerének meghatározása szerint ez „egy szervezet azon képessége, amelynek révén képes a változó környezet hatásait elviselni és azokhoz alkalmazkodni." Bár ez a meghatározás egyértelmű törekvést fogalmaz meg, a gyakorlatban a szervezetek jelentős különbségeket 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.

Gyakorlati szempontból az ellenállóképes szervezetek jobb helyzetben vannak ahhoz, hogy túléljék a váratlan kihívásokat, valamint azokkal szembesülve fejlődjenek és sikeresen működjenek tovább.

Számos tényező akadályozhatja a szervezetet stratégiai céljai megvalósításában, többek között:

- Természeti katasztrófák, például földrengések, tüzek, árvizek, hurrikánok, cunamik, trópusi viharok és egyéb szélsőséges időjárási jelenségek.
- Kibertámadások, például zsarolóprogramok, rosszindulatú szoftverek, szolgáltatásmegtagadásos támadások, adatvédelmi incidensek, belső fenyegetések, valamint egyéb rosszindulatú tevékenységek, amelyek célja a szervezet megkárosítása vagy működésének akadályozása.
- Geopolitikai konfliktusok, például gazdasági szankciók, vámok, terrorizmus, háború és egyéb nemzetek közötti feszültségek.
- Környezeti nyomások, például erőforráshiány, közegészségügyi válságok, fenntarthatósági tényezők vagy éghajlatváltozás.
- Külső tényezők változásai, például a technológia fejlődése (beleértve a mesterséges intelligenciát), a megfelelési követelmények változásai (jogi, szabályozási és pénzügyi beszámolási területen), a foglalkoztatottsági szint, a fogyasztói kereslet és a szervezeti megítélésének alakulása.
- Pénzügyi kihívások, például infláció vagy defláció, kamatlábak, devizaárfolyamok és az uralkodó piaci feltételek, például recesszió vagy gazdasági növekedés.
- Működési kihívások, például összetett folyamatok, harmadik felektől való erős függés, földrajzi elhelyezkedés, kulturális kihívások, korlátozott munkaerő-kapacitás, valamint nem hatékony vezetés vagy kockázatkezelés.
- Ellátási lánccal kapcsolatos kihívások, így különösen a nyersanyagok beszerzésének akadályai, a megfelelően diverzifikált beszállítói kör hiánya, valamint a nyersanyagárak jelentős ingadozása.
- Belső események, például kulcsfontosságú munkavállalók fluktuációja és működési hibák.

Bár a működési zavart okozó események jellege eltérő lehet, a szervezet számára célszerű, hogy rendelkezzen egy jól meghatározott ellenállóképességi stratégiával és formalizált folyamatokkal, amelyek lehetővé teszik a változások folyamatos előrejelzését, az azokra való felkészülést, a megfelelő reagálást és az azokhoz való alkalmazkodást. A szervezeti ellenállóképesség egy gyűjtőfogalom és a kapcsolódó stratégia a szervezet sajátosságaitól függően különböző elemeket foglalhat magában, például az üzletmenet-folytonosságot, a katasztrófa utáni helyreállítást, a kritikus funkciók nyilvántartását, az utódlási terveket és a helyreállítási teszteket.

A Szervezeti ellenállóképesség Tematikus követelményhez tartozó kritériumok a következők:

- **Irányítás** – világosan meghatározott, az ellenállóképességhez kapcsolódó alapvető célkitűzések és stratégiák, amelyek támogatják a szervezet küldetésének és jövőképének megvalósítását.
- **Kockázatkezelés** – az ellenállóképességet érintő fenyegetések azonosítására, elemzésére, kezelésére és nyomon követésére szolgáló folyamatok, beleértve az ellenállóképességhez kapcsolódó incidensek azonnali eszkalálását biztosító folyamatot.
- **Kontrollok** – a vezetés által kialakított, rendszeresen értékelt kontrollfolyamatok az ellenállóképességhez kapcsolódó kockázatok mérséklésére.

Megfontolások

A belső ellenőrök a következő megfontolásokat használhatják a Szervezeti ellenállóképesség Tematikus követelményben foglalt követelmények értékeléséhez. Az egyes megfontolások betűjelzései az ahhoz kapcsolódó Tematikus követelményekre hivatkoznak. Ezek a megfontolások szemléltető jellegűek, de nem kötelezőek. A belső ellenőröknek szakmai megítélésükre kell hagyatkozniuk annak meghatározásakor, hogy mit vegyenek figyelembe az értékelésük során.

A közszféra belső ellenőrzési megbízásai során a jogszabályokból, a kormányzati struktúrából vagy a politikai környezetből adódó korlátozások potenciális akadályt jelenthetnek ezen munka bizonyos aspektusainak kezelésében. A közszféra belső ellenőreinek a kockázatértékelési folyamat részeként dokumentálniuk kell az ilyen hatókör-korlátozásokat, majd szakmai megítélésük alapján egyértelműen kell meghatározniuk és kommunikálniuk vizsgálatuk testreszabott hatókörét.

Irányítási megfontolások

Annak értékelése érdekében, hogy az irányítási folyamatok miként támogatják a szervezeti ellenállóképességi célkitűzések megvalósítását, a belső ellenőrök az alábbiakra vonatkozó bizonyítékokat vizsgálhatják:

A. A vezetés által kialakított és dokumentált, az ellenállóképességhez kapcsolódó stratégiát, amelyet a vezetőtestület hagy jóvá és felügyel. A stratégiát formálisan kommunikálják valamennyi munkatárs felé, továbbá szorosan illeszkedik a szervezet küldetéséhez, jövőképéhez, kultúrájához és kockázatkezelési megközelítéséhez, valamint támogatja azok megvalósítását. Az ellenállóképességhez kapcsolódó stratégiai terv célkitűzéseit a vezetőtestület hagyja jóvá, összhangban állnak a szervezet átfogó kockázatkezelési megközelítésével, és azokat rendszeresen tesztelik és felülvizsgálják. A terv tartalmazhat működési, technológiai és pénzügyi elemeket, például:

   - Működési – a szervezeti ellenállóképesség szervezetszintű koordinációja; az ellenállóképességhez kapcsolódó kockázatértékelési folyamatok; üzletmenet-folytonossági tervezés, beleértve az időszakos tesztelést és a jelentéstételt; válságkezelés; a munkaerő alkalmazkodóképessége (például távoli munkavégzés gyors bővíthetősége, minimális helyszíni létszám, valamint a kritikus szerepkörök több munkatárs általi elláthatóságát biztosító keresztképzés); a kulcsfontosságú munkavállalók utódlástervezése; az ellátási lánc ellenállóképessége; kulcsfontosságú teljesítménymutatók (KPI-ok) kialakítása; valamint a vezetőtestület tagjainak képzése a megfelelő tudatosság biztosítása érdekében.

- Technológiai – az IT-infrastruktúrára vonatkozó követelmények meghatározása; a kritikus adatok azonosítása és osztályozása; adatmentések; kiberbiztonsági intézkedések és a fenyegetések monitorozása; a kritikus technológiai eszközök karbantartása; valamint a kritikus adatok helyreállítási pont és helyreállítási idő célértékeinek meghatározása (helyreállítási tesztekkel igazolva).
- Pénzügyi – az ellenállóképességhez kapcsolódó költségvetési források elkülönítése; készpénztartalékok a működés fenntartására zavarok esetére; olyan pénzügyi beszámolási folyamatok, amelyek biztosítják a működési zavarokhoz kapcsolódó tranzakciók pontos nyilvántartását; a működési zavarokból eredő kockázatok mérséklését szolgáló biztosítási fedezetek; valamint rendkívüli finanszírozást lehetővé tevő hitelkeretek rendelkezésre állása.

B. Az ellenállóképességért felelős személy vagy csoport rendszeresen (például havi vagy negyedéves gyakorisággal) tájékoztatást nyújt a vezetőtestületnek, amely tartalmazhat meghatározott kockázattűrési küszöbértékeket, teljesítménymutatókat, illetve egyéb olyan információkat, amelyek a megfigyelt jelenségek és tendenciák bemutatását szolgálják. A jelentések bemutatják az ellenállóképességhez kapcsolódó stratégiai célkitűzések teljesítésének állapotát, ideértve a stratégiai felügyeletet, a monitoring tevékenységet és a hosszú távú tervezést is. A jelentések többek között az alábbi területekre vonatkozó monitoringeredményeket tartalmazhatják:

- A stratégiai ellenállóképességi célkitűzések megvalósulása, valamint az azok elérését esetlegesen akadályozó tényezők.
- Az ellenállóképességhez kapcsolódó stratégiai célkitűzések támogatásához szükséges költségvetési igények, például a technológiai eszközökkel kapcsolatos szükségletek.
- Az ellenállóképességhez kapcsolódó kockázatok alakulása, beleértve a kockázati környezetben bekövetkező jelentős változásokat, amelyek hatással vannak a meghatározott kockázattűrési szintekre.
- A szervezeti ellenállóképességet szolgáló belső kontrollok hatékonysága, beleértve a helyesbítő intézkedések végrehajtásának előrehaladását.
- A szervezeti ellenállóképesség eredményességének mérésére szolgáló kulcsfontosságú teljesítménymutatók (KPI-k);
- Az ellenállóképességhez kapcsolódó feladatokat ellátó munkavállalók felvételéhez, képzéséhez és továbbfejlesztéséhez szükséges emberi erőforrások.

C. A működési, technológiai és pénzügyi ellenállóképességi folyamatok irányítására szolgáló szabályzatok, eljárások és egyéb releváns dokumentumok, ideértve a következőket:

- Az ellenállóképességhez kapcsolódó kritikus folyamatok azonosítása és rendszeres elemzése annak megállapítására, hogy továbbra is megfelelően tükrözik-e a szervezet legfontosabb folyamatait.
- A szabályzatok legalább éves rendszerességgel (magasabb kockázati szint esetén ennél gyakrabban) történő felülvizsgálata és aktualizálása, továbbá az újonnan megjelenő, az ellenállóképességet érintő kockázatok, illetve a tesztelésekből vagy

tényleges működési zavart okozó eseményekből levont tanulságok alapján szükségessé váló soron kívüli módosítása.

- A szabályzatok és eljárások szervezeti ellenállóképesség célú alkalmazhatóságának és megfelelőségének rendszeres felülvizsgálata annak érdekében, hogy megfelelően támogassák a szervezeti ellenállóképességgel kapcsolatos tevékenységeket.
- Annak vizsgálata, hogy az ellenállóképességi folyamatok és a belső kontrollok megerősítése során alkalmaznak-e széles körben elfogadott keretrendszereket a kapcsolódó területeken, például a kockázatkezelés, az informatika vagy az irányítás területén. Figyelembe vehető például a NIST, a COSO vagy az ISO által kidolgozott keretrendszerek alkalmazása, különösen az ISO 22300-as szabványsorozat (például az ISO 22316 vagy 22336 szabványok).

D. Kialakított és dokumentált eseményirányítási struktúra áll rendelkezésre, amely meghatározza a szervezeti ellenállóképességi célkitűzések megvalósításához kapcsolódó vezetői szerepeket és felelősségi köröket. Rendelkezésre állnak a döntéshozatali hierarchia kialakítását igazoló bizonyítékok, beleértve a működési zavarok idején a szervezeti ellenállóképességgel kapcsolatos döntésekért felelős személyek kijelölését, valamint az olyan működési döntésekhez szükséges jóváhagyási rend meghatározását, mint a pénzügyi források felhasználása vagy a szervezet támogatását szolgáló, harmadik féllel kötendő szerződések jóváhagyása. További szempontként értékelhető a dokumentált eszkalációs rend és a működési zavarok időszakára meghatározott ideiglenes döntési jogosultságok megléte, beleértve a pénzügyi döntési jogkörök delegálására és a harmadik felekkel kötött szerződések jóváhagyási értékhatáraira vonatkozó rendelkezéseket is.

E. Kialakított folyamat működik a szervezeti ellenállóképességhez kapcsolódó folyamatok működtetéséért és irányításáért felelős személyek ismereteinek, készségeinek és képességeinek rendszeres (például éves vagy féléves) értékelésére. A folyamat magában foglalhatja a képzési lehetőségek azonosítását, ideértve a jelenléti vagy online képzéseket, konferenciákat, igény szerint elvégezhető tanfolyamokat és szakmai minősítéseket. Rendelkezésre állnak az utódlási tervezésre vonatkozó bizonyítékok a szervezeti ellenállóképesség szempontjából kulcsfontosságú szerepkörök azonosítása érdekében, beleértve olyan forgatókönyv-alapú teszteket is, amelyek feltárják azokat a tevékenységeket, amelyeket kizárólag egyetlen személy vagy csak korlátozott számú munkatárs képes ellátni. A helyettesítést biztosító személyekkel szemben támasztott kompetenciakövetelmények meghatározottak.

F. Kialakított folyamat működik a releváns belső és külső érdekelt felek – az adott körülményeknek megfelelő – azonosítására, priorizálására és bevonására azon információs és jelentési struktúrák kialakításába, amelyek támogatják a szervezeti ellenállóképességi célkitűzések elérését veszélyeztető meglévő sérülékenységek és újonnan megjelenő fenyegetések azonosítását, valamint az azokra adandó válaszintézkedéseket. Rendelkezésre állnak bizonyítékok az érdekelt felek részvételéről a szervezeti ellenállóképességet érintő sérülékenységekkel kapcsolatos egyeztetésekben. Ilyen bizonyíték lehet például elektronikus levél, értekezleti jegyzőkönyv vagy jelentés, beleértve a szervezeti szintű mutatószámok alkalmazásának igazolását is a szervezeti ellenállóképesség eredményességének mérésére és nyomon követésére.

Kockázatkezelési megfontolások

Annak értékelése érdekében, hogy a kockázatkezelési folyamatok miként támogatják a szervezeti ellenállóképességi célkitűzések megvalósítását, a belső ellenőrök az alábbiak fennállását alátámasztó bizonyítékokat vizsgálhatják:

A. A szervezet kockázatértékelési és kockázatkezelési folyamatai magukban foglalják a szervezeti ellenállóképességet érintő kockázatok azonosítását, folyamatos végrehajtásuk és dokumentálásuk biztosított, eredményeikről pedig a szervezet egészében tájékoztatást nyújtanak A szervezeti ellenállóképességet érintő kockázatok kezelésének folyamata kiterjed a kulcsfontosságú területek értékelésére, így többek között a működés, a vállalati szintű kockázatkezelés, az informatika, az ellátásilánc- és beszerzésmenedzsment, a létesítményüzemeltetés, a humánerőforrás-gazdálkodás, a pénzügyek, a jogi terület, a megfelelőség, a szabályozási környezet, a külső kommunikáció, a kritikus beszállítók, a szervezet megítélése, az újonnan felmerülő kockázatok és egyéb releváns területek vizsgálatára. A szervezeti ellenállóképességet érintő kockázatok azonosításán túl a folyamatok magukban foglalják annak értékelését is, hogy az üzleti működést megzavarni képes fenyegetések és sérülékenységek:

   - miként kerülnek azonosításra és jelentésre;
   - hogyan kerülnek elemzésre annak értékelése érdekében, hogy milyen kockázatot jelentenek a szervezeti célkitűzések megvalósítására nézve;
   - milyen módon kerülnek kezelésre, beleértve a kockázatok elfogadható szintre történő csökkentését célzó intézkedési tervek kidolgozását és végrehajtását;
   - valamint miként biztosított nyomon követésük, ideértve a fenyegetések teljes körű megszüntetéséig tartó folyamatos jelentéstételt is.

További bizonyítékok lehetnek többek között az alábbiak:

- a folyamatban részt vevő szervezeti területeket bemutató dokumentumok, például jelentések, elektronikus levelek vagy értekezleti jegyzőkönyvek; ezek olyan kockázati tényezőkre is kiterjedhetnek, mint a hatás, a bekövetkezési valószínűség, a bekövetkezés gyorsasága és egyéb releváns szempontok;
- Szorosan összefüggő vagy egymástól kölcsönösen függő kockázati tényezők elemzése annak meghatározása érdekében, hogy a többféle kockázati kitettség együttesen milyen összesített hatást eredményez;
- a kockázatértékelés magában foglalja a kritikus eszközök védelmi rétegeinek és a kapcsolódó erőforrások értékelését annak érdekében, hogy megelőzhető legyen az egyetlen hibapontból eredő kockázat;
- a kockázatértékelés aktualizálása a tényleges válsághelyzetekből, működési zavarokból, valamint a tesztek és forgatókönyv-alapú szimulációk eredményeiből levont tanulságok figyelembevételével;
- a szervezet az üzleti hatáselemzés eredményei alapján, a potenciális hatás és a bekövetkezési valószínűség figyelembevételével rangsorolja a legnagyobb kockázatot jelentő területeket.

B. A szervezet kijelölt egy személyt vagy szervezeti egységet, amely számára egyértelmű felelősséget és elszámoltathatóságot határozott meg a szervezeti ellenállóképességet érintő kockázatok nyomon követésével, valamint az azokról történő jelentéstétellel kapcsolatban és ezt rendszeresen felülvizsgálja. A kijelölt személynek, illetve a kijelölt szervezeti egység tagjainak megfelelő képesítéssel és a szervezeti ellenállóképességhez kapcsolódó tevékenységek kezelésében szerzett tapasztalattal kell rendelkezniük, lehetőség szerint a szervezet működési területén (például az egészségügyben, a pénzügyi szektorban vagy a közszférában). A személy vagy a szervezeti egység tagjai rendszeres képzéseken vesznek részt annak érdekében, hogy naprakész ismeretekkel rendelkezzenek a szervezeti ellenállóképességet érintő kockázatok területén megjelenő új tendenciákról.

C. A szervezet olyan folyamatot alakított ki, amely biztosítja a szervezeti ellenállóképességet érintő (újonnan felmerülő vagy korábban azonosított) kockázatok nyomon követését, valamint azon esetek haladéktalan eszkalációját, amelyek a szervezet kockázatkezelési szabályzatai, kockázati tűrőképesség vagy a vonatkozó jogszabályi és szabályozói előírások alapján elfogadhatatlan kockázati szintet érnek el. A folyamat során figyelembe veszik a szervezeti ellenállóképességet érintő kockázatok hatásait, ideértve a pénzügyi és nem pénzügyi mutatókat is. A pénzügyi mutatók közé tartozik például az árbevétel, a költségek, a jövedelmezőség, a pénzforgalom, az adósságállomány, a részvényárfolyam és az összesített vállalatérték. A nem pénzügyi mutatók közé tartozik például a márka megítélése, az ügyfél-elégedettség, a környezeti hatások és a munkavállalók fluktuációja. A folyamat a következőket foglalja magában:

- A kockázatok korai azonosítása és időben történő jelentése.
- A kockázatok elemzését annak értékelése érdekében, hogy azok milyen mértékben veszélyeztethetik a szervezeti célkitűzések megvalósítását.
- A kockázatcsökkentő intézkedési tervek kidolgozását és jóváhagyását, beleértve annak meghatározását, hogy a kockázatok miként csökkenthetők elfogadható szintre megfelelő időn belül. Az intézkedési tervek a szervezet átfogó kockázatkezelési stratégiáján alapulnak. A javaslatnak tartalmaznia kell a kockázatcsökkentéshez szükséges erőforrásokat, így különösen a pénzügyi forrásokat, munkaidő-ráfordítást, valamint a képességek fejlesztéséhez szükséges további technológiát és szoftvereket.
- A kockázatok folyamatos nyomon követését és a kulcsfontosságú kockázati mutatókkal kapcsolatos jelentéstételt mindaddig, amíg a fenyegetések megszüntetése meg nem történik.

D. A szervezet olyan folyamatot vezetett be, amely biztosítja a válsághelyzetekre, működési zavarokra, vészhelyzetekre vagy egyéb eseményekre való reagálást, valamint az azokból történő helyreállítást. A folyamatot rendszeresen, például negyedévente vagy évente teljeskörűen tesztelik, emellett szükség szerint gyakoribb, részleges teszteléseket is végeznek, például havi rendszerességgel. A kritikus szolgáltatások ennél gyakoribb tesztelést is indokolhatnak. Az incidensekre való reagálási és helyreállítási folyamat magában foglalhatja a következőket:

- Észlelés – a kibereseményekfolyamatos monitorozása. Ez magában foglalhatja például behatolás-észlelő rendszerek, fenyegetettségi információk, vagy biztonsági információ- és eseménykezelési rendszerek alkalmazását. A biztonsági információ- és eseménykezelési rendszerek mesterséges intelligenciával is támogathatják a folyamat hatékonyságát. Természeti katasztrófák vagy a létesítményekben érintő működési zavarok esetén a szervezet olyan kommunikációs rendszert alakított ki (például riasztási protokollokat vagy értesítési rendszereket), amely biztosítja a gyors tájékoztatást és az információk megosztását. A szervezet valamennyi eseménytípusra meghatározta az illetékes vészhelyzeti beavatkozó szervek és hatóságok értesítésének rendjét. Az eseményeket azok kritikus jellege alapján szükséges priorizálni.
- Reagálás és elszigetelés – az eseménykezelési megközelítés magában foglalja a forgatókönyv-alapú elemzéseket, valamint a különböző működési zavart okozó eseményekre kiterjedő rendszeres stressztesztek. Kiberbiztonsági események esetén a további károk megelőzése érdekében a szervezet folyamatot alakított ki az érintett eszközök elkülönítésére, például a hálózati forgalom átirányításával vagy a felhasználói hozzáférések korlátozásával. Fizikai események esetén a szervezet olyan intézkedéseket alkalmaz, amelyek az esemény hatásainak korlátozása érdekében lehetővé teszik az érintett terület elkülönítését, ideértve szükség esetén a munkatársak másik helyszínre történő áttelepítését is.
- Helyreállítás – kiberbiztonsági vagy informatikai eseményekhez kapcsolódó helyzetekhez a szervezet olyan eljárásokat alakított ki, amelyek a működés helyreállításához szükséges kritikus eszközök helyreállítását priorizálja (például adatok biztonsági mentésekből történő visszaállítása vagy szerverek újbóli üzembe helyezése útján). A működés újraindításához szükséges nem informatikai erőforrások helyreállításának priorizálása ugyancsak biztosított. Ez magában foglalhatja a kulcsfontosságú munkatársak vagy alapvető működési funkciók fokozatos visszaállításának megtervezését is.
- Incidenst követő elemzés – a szervezet elemzi az eseményeket, hogy meghatározza:
  - a működési zavart okozó események kiváltó okait;
  - a megtett intézkedések eredményességét;
  - milyen fejlesztések szükségesek a szervezeti ellenállóképességet támogató folyamatok megerősítéséhez, így például a szabályzatok, eljárások, kockázatértékelések vagy a stratégia aktualizálásához.

A reagálási és helyreállítási folyamat alaposságának és eredményességének tesztelése során alkalmazott forgatókönyv-alapú szimulációk, szimulációs gyakorlatok, amelyek kiterjednek a kritikus szolgáltatásokra és funkciókra, valamint azok függőségeire, a szervezet kockázattűrési szintjeihez igazítható. Ezek az események lehetnek belső vagy külső eredetűek. A gyakorlatok eredményeit a vezetőtestület és a felsővezetés felülvizsgálhatja, a kapcsolódó javító intézkedések előrehaladását nyomon követik és azokról rendszeres jelentést készítenek. A javaslatoknak végrehajthatóaknak kell lenniük, egyértelmű felelőssel és határidőkkel.

Kontrollfolyamatra vonatkozó megfontolások

Annak értékelése érdekében, hogy a kontrollfolyamatok miként támogatják a szervezeti ellenállóképességhez kapcsolódó célkitűzések megvalósítását, a belső ellenőrök az alábbiak fennállását alátámasztó bizonyítékokat vizsgálhatják:

A. Olyan folyamat működik, amely biztosítja a kritikus harmadik fél szolgáltatók (külső szolgáltatók és beszállítók), valamint az alapvető működés fenntartásához szükséges minimális készletszintek azonosítását és értékelését. Az értékelés kiterjedhet a harmadik felek szervezeti ellenállóképességének és üzletmenet-folytonossági képességének vizsgálatára, valamint tartalmazhatja az egyes szállítók kockázati besorolását. A szervezet a szerződéskötést megelőzően, valamint azt követően is rendszeresen felülvizsgálhatja a beszállítókat a kockázati besorolások folyamatos értékelése érdekében. A szervezet nyilvántartást vezet azokról a potenciális helyettesítő beszállítókról, amelyekhez egy meglévő beszállítói kapcsolat megszűnése esetén fordulhat.

B. A vezetés elvégezte az adatok osztályozását, különös tekintettel azon kritikus adatok azonosítására, amelyek a működési zavart okozó eseményeket követő helyreállításhoz és a működés fenntartásához szükségesek. A szervezet hatékony belső kontrollokat alakított ki a kritikus adatok védelme érdekében, ideértve a hozzáférés kizárólag jogosult személyekre történő korlátozását, valamint annak biztosítását, hogy a kritikus adatokról rendszeres biztonsági mentés készüljön, és azok megfelelő időn belül visszaállíthatók legyenek.

C. A vezetés kritikus informatikai kontrollokat és folyamatos monitoringfolyamatokat alakított ki az információbiztonsági (ideértve a kiberbiztonsági) kockázatok mérséklése, valamint az érzékeny adatok működési zavart okozó események alatti védelme érdekében. Az érzékeny adatok védelmét titkosítás biztosítja. A folyamatos monitoring és a valós idejű fenyegetettségi információk riasztásokat küldenek a vezetés számára, az azonosított problémákat pedig megfelelő időn belül kezelik. A szervezet alkalmazhat széles körben elfogadott kontrollkeretrendszereket, mint például a NIST, a COSO, az ISO vagy más szervezetek által kidolgozott megoldásokat.

D. A szervezet nyilvántartást vezet a kritikus IT-eszközökről, ideértve a hardvereket, szoftvereket és szolgáltatásokat, amelyek a működés támogatásához szükségesek válsághelyzetek, működési zavarok és vészhelyzetek idején. Azokat az informatikai eszközöket, amelyek rövid idő alatt nehezen szerezhetők be vagy pótolhatók, kiemelt prioritásúként azonosították.

E. Üzletmenet-folytonossági és katasztrófa utáni helyreállítási terv került kialakításra, amelyek az üzleti hatáselemzés eredményei alapján kijelölik a helyreállítási csoportok tagjait. A terveket rendszeresen, például negyedévente vagy évente tesztelik forgatókönyv-alapú szimulációs gyakorlatok és stressztesztek keretében, amelyek során a működési zavarok valós vészhelyzeteket modelleznek, és magukban foglalják a belső és külső érintettekkel folytatott kommunikációs protokollok tesztelését is. A tesztelések eredményeiről, valamint a feltárt fejlesztési lehetőségekről jelentést készítenek a vezetőtestületnek és a felsővezetésnek.

F. Olyan folyamat került kialakításra, amely lehetővé teszi a munkavégzési környezet átalakítását működési zavart okozó események esetén. Ez magában foglalhatja alternatív munkavégzési helyszínek igénybevételét, például az otthoni munkavégzést vagy ideiglenes iroda gyors és hatékony kialakítását. A szervezet a helyszíni munkavégzés kiváltására hibrid vagy távmunkára vonatkozó megoldásokat alkalmazhat. További elemek lehetnek az informatikai és humán erőforrásokat is érintő erőforrások gyors és hatékony mozgósítására, illetve átcsoportosítására vonatkozó eljárások.

G. Olyan folyamat működik, amely biztosítja a szervezeti ellenállóképességet érintő újonnan megjelenő fenyegetések és sérülékenységek folyamatos monitorozását és az azokról történő jelentéstételt, továbbá a szervezeti ellenállóképességet támogató fejlesztési lehetőségek azonosítását, priorizálását és megvalósítását. A monitoringtevékenységek magukba foglalhatják a kulcsfontosságú kockázati mutatók (KRI-k), a kockázatokat összefoglaló kimutatások (dashboardok), valamint a kockázati környezet jövőbeli kialakulását vizsgáló elemzések alkalmazását. A szervezet az újonnan megjelenő fenyegetésekről minden munkavállaló számára tájékoztatást nyújthat a tudatosság növelése érdekében, beleértve a kockázatcsökkentő intézkedések és kontrollok ismertetését is. A bejelentő rendszeren keresztül érkező bejelentéseket nyilvántartásba veszik, elemzik és megfelelő időn belül kezelik, és a felsővezetés részére jelentik. A problémák megoldásához folyamatos monitoringra és további jelentések készítésére is szükség lehet.

H. Olyan folyamat működik, amely biztosítja a munkatársak felkészítését a szervezeti ellenállóképességhez kapcsolódó szabályzatok és eljárások alkalmazására válsághelyzetek, működési zavarok és vészhelyzetek esetére. A folyamat magában foglalja a működési zavart okozó forgatókönyveket modellező gyakorlatokat és képzéseket. A képzésekre rendszeres időközönként, például negyedéves vagy éves gyakorisággal kerül sor. A kritikus szolgáltatások ennél gyakoribb tesztelést is igényelhetnek.

I. Olyan folyamat működik, amely biztosítja, hogy a válsághelyzetek, működési zavarok és vészhelyzetek kezeléséhez szükséges működési, humán, technológiai és pénzügyi erőforrások tervezése megtörténjen, és azok rendelkezésre álljanak. A vezetés rendszeresen, például negyedévente vagy évente felülvizsgálja a rendelkezésre álló erőforrások megfelelőségét az érzékelt kockázati szintek figyelembevételével, és az erőforrásigényekről tájékoztatják a vezetőtestületet. A kritikus szolgáltatások ennél gyakoribb tesztelést is igényelhetnek. Az elemzés magában foglalja a likviditás, a biztosítási fedezet és a rendkívüli finanszírozási megoldások értékelését. A pénzügyi erőforrásigényeket a szervezet mérete, összetettsége, ágazati sajátosságai és kockázati profilja alapján tervezik meg. A folyamat magában foglalhatja a finanszírozás előzetes jóváhagyását.

J. Olyan folyamat működik, amely biztosítja a válsághelyzetek, működési zavarok és vészhelyzetek bekövetkezését követő felülvizsgálatot, valamint az incidenseket követő elemzések során levont tanulságok hasznosítását. A felülvizsgálatokat formálisan dokumentálni kell, a levont tanulságokat pedig be kell építeni a szervezeti ellenállóképesség jövőbeli tervezésébe.

A. függelék: Példák a gyakorlati alkalmazásra

A következő forgatókönyvek leírják, hogy mikor alkalmazható a Szervezeti ellenállóképesség Tematikus követelmény. Ezenfelül a Belső Ellenőrök Intézete által közzétett „Tematikus követelmények alkalmazási útmutatója" gyakorlati segítséget nyújt a kötelező követelmények alkalmazásához, az esetleges korlátozások kezeléséhez, valamint a kritikus kockázati küszöbértékek azonosításához.

1. forgatókönyv: A belső ellenőrzési tervben szerepel a szervezeti ellenállóképességgel kapcsolatos belső ellenőrzési megbízás.

Amennyiben a belső ellenőrzési funkció lezárja a kockázatalapú tervezési folyamatot, és a belső ellenőrzési terv egy vagy több szervezeti ellenállóképességgel kapcsolatos megbízást tartalmaz, a Tematikus követelmény alkalmazása kötelező az ilyen megbízások elvégzése során. A megfelelés úgy érhető el, hogy a követelményeket belefoglalják a belső ellenőrzési terv érintett megbízásaiba.

A szervezeti ellenállóképesség széles körű téma, és nem biztos, hogy a Tematikus követelmény minden követelménye minden megbízás esetében alkalmazandó. Ha a belső ellenőrök szakmai megítélés alapján úgy döntenek, hogy a Szervezeti ellenállóképesség Tematikus követelmény egy vagy több követelménye nem releváns az adott megbízás szempontjából, és ezért annak vizsgálata mellőzhető, az erre vonatkozó indokolást dokumentálni kell és megkell őrizni. Egyes követelmények kizárásának indoklása lehet például az, hogy a belső ellenőrzési funkció a szervezeti ellenállóképesség különböző területeit rotációs rendszerben vizsgálja, vagy megállapította, hogy az adott kockázat jelentősége a megbízás szempontjából alacsony.

2. forgatókönyv: A szervezeti ellenállóképességgel kapcsolatos kockázatokat egy olyan belső ellenőrzési megbízás során azonosítják, amelynek nem ez az elsődleges tárgya.

A belső ellenőrök azonosíthatnak ellenállóképességgel kapcsolatos kockázatokat egy olyan folyamat értékelése során, amely nem kapcsolódik közvetlenül az ellenállóképességhez. Előfordulhat például, hogy a belső ellenőrök egy olyan megbízás keretében vizsgálják az humánerőforrás-gazdálkodási folyamatokat (például a munkaerő felvételét és megtartását), amely eredetileg nem a szervezeti ellenállóképességre irányul, és a tervezési szakaszban az ellenállóképességet érintő kockázatokat nem tekintik a vizsgálat hatókörébe tartozónak. Az előzetes folyamatmegismerést követően azonban arra a következtetésre juthatnak, hogy ezek a kockázatok mégis a vizsgálat körébe tartoznak. Például azonosíthatják a munkatársak megtartásával összefüggő utódlástervezési kockázatokat (13.2 norma: A megbízással kapcsolatos kockázatok felmérése).

A releváns kockázatok azonosítását követően a belső ellenőröknek át kell tekinteniük a Szervezeti ellenállóképesség Tematikus követelményt, és meg kell határozniuk, hogy mely követelmények alkalmazandók. Ebben a példában előfordulhat, hogy kizárólag az Irányítás témakörébe tartozó E. követelményre összpontosítanak, és kizárják a kockázatkezelési és kontrollkövetelményeket. Az ilyen kizárások indoklását a megbízás munkalapjaiban kell dokumentálniuk kell és a dokumentációt meg kell őrizni.

3. forgatókönyv: Olyan ellenállóképességgel kapcsolatos megbízás esetén, amely eredetileg nem szerepelt a belső ellenőrzési tervben.

Az érdekelt felek, például a vezetőtestület, a vezetőség vagy a szabályozó hatóság felkérheti a belső ellenőröket, hogy az eredeti ellenőrzési terven kívül végezzenek ellenállóképességgel kapcsolatos értékeléseket. Például amikor egy szervezet kibertámadás célpontjává válik, a vezetőtestület belső ellenőrzési megbízás elrendelését kezdeményezheti a szervezeti ellenállóképességhez kapcsolódó kontrollok értékelésére annak felmérése érdekében, hogy a szervezet mennyire felkészült egy hasonló kibertámadás utáni helyreállításra. Ilyen esetben a Tematikus követelmény alkalmazandó, a követelményeket értékelni kell, és minden kizárást megfelelően dokumentálni kell (9.4 norma: Belső ellenőrzési terv).

B. függelék: Példák ellenőrzési megbízásokra az alkalmazandó forgatókönyvek alapján

1. forgatókönyv: **A téma szerepel a belső ellenőrzési tervben.**

Központi nagybani piacért felelős állami szerv

A belső ellenőrzési funkció az éves kockázatalapú tervezési folyamat során az alapvető piaci működés folytonosságát magas kockázatú területként azonosítja, a logisztikai zavaroknak, a közegészségügyi eseményeknek, valamint a kritikus infrastruktúrától való függőségnek való kitettség miatt. Az értékelés alapján a belső ellenőrök megállapítják, hogy a Szervezeti ellenállóképesség Tematikus követelmény alkalmazandó a tervezett megbízás során.

Az irányítás követelményei értékelése érdekében a belső ellenőrök áttekintik a vezetőtestületi jegyzőkönyveket, a stratégiai terveket és a költségvetési dokumentumokat annak megállapítására, hogy a szervezeti ellenállóképességgel kapcsolatos célkitűzések formálisan meghatározásra kerültek-e, és megfelelő felügyelet alatt állnak-e. Értékelik, hogy a vezetés rendszeresen beszámol-e a vezetőtestületnek a kritikus sérülékenységekről, például a szállítási függőségekről, az infrastrukturális korlátokról és az egészséggel kapcsolatos kockázatokról. Amennyiben nem áll rendelkezésre egységes, a szervezeti ellenállóképességre vonatkozó stratégiai dokumentum, a belső ellenőrök értékelik, hogy az ellenállóképesség elemei következetesen beépülnek-e az operatív és stratégiai dokumentumokba.

Kockázatkezelési szempontból a belső ellenőrök megvizsgálják a szervezet kockázatnyilvántartást, és interjúkat készítenek az operatív vezetéssel annak megerősítésére, hogy az ellátás folytonosságát veszélyeztető kockázatok azonosítása, értékelése és felelősökhöz rendelése megtörténik-e. Tesztelik, hogy a korábbi események, például ideiglenes leállások vagy hozzáféréskorlátozások során alkalmazták-e az eszkalációs folyamatokat, valamint megállapítják, hogy a válaszintézkedések összhangban álltak-e a meghatározott kockázattűrési szintekkel.

A kontrollfolyamatok magukban foglalják a működés folytonosságát biztosító intézkedések felülvizsgálatát, az időszakos tesztgyakorlatok dokumentált bizonyítékainak vizsgálatát, valamint a működési zavart okozó események során a közfeladatot ellátó hatóságokkal folytatott együttműködést igazoló dokumentumok felülvizsgálatát. A belső ellenőrök áttekintik az incidenseket követő jelentéseket is annak megállapítására, hogy a levont tanulságok beépültek-e a folyamatok fejlesztésébe. Amennyiben a Tematikus követelmény egyes követelményei jogszabályi vagy szervezeti korlátok miatt nem alkalmazhatók, a belső ellenőrök a Normákkal összhangban dokumentálják a kizárás indoklását.

2. forgatókönyv: Egy megbízás teljesítése során azonosított téma.

Nemzetközi jelenléttel rendelkező szakmai szolgáltató vállalat

Az irányításra és a vállalati szintű kockázatkezelésre fókuszáló megbízás során a belső ellenőrök sérülékenységet tárnak fel a decentralizált döntéshozatal, a kulcsfontosságú helyi vezetőktől való függés, valamint több joghatóságon átnyúló szabályozási kitettség területén. E megállapítások alapján a belső ellenőrök arra a következtetésre jutnak, hogy a Szervezeti ellenállóképesség Tematikus követelmény egyes elemei alkalmazandók a megbízás során.

Az irányítás követelményeinek értékelése érdekében a belső ellenőrök áttekintik a globálisan alkalmazott szabályzatokat, a vezetőtestületnek készített beszámolókat és a válságkezelési protokollokat annak megállapítására, hogy a szervezet meghatározta-e hogyan biztosítja a működés folytonosságát a szabályozási változások, a kritikus munkavállalók jelentős fluktuációja, illetve egy adott országban bekövetkező, szélesebb körű hatással járó reputációs események esetén. Értékelik, hogy a vezetőtestület kap-e összevont beszámolót a különböző országokat érintő kritikus kockázatokról, valamint, hogy a szervezeti ellenállóképesség felügyeletéért való felelősség egyértelműen meghatározott-e.

Kockázatkezelési szempontból a belső ellenőrök megvizsgálják a vállalati szintű kockázatkezelési keretrendszert annak megerősítésére, hogy a kulcs munkavállalóktól való függéshez, a határokon átnyúló szabályozási megfeleléshez, valamint a reputációs kitettséghez kapcsolódó kockázatok hozzárendelésre kerültek-e a szervezet stratégiai céljaihoz. Mintavételes tesztelést végeznek a kiválasztott incidens esetén annak megállapítására, hogy a helyi események megfelelően eszkalálásra kerültek-e a globális vezetés felé, illetve, hogy a válaszintézkedésekről szóló döntések a meghatározott döntési jogosultsági szinteknek megfelelően születtek-e meg.

A kontrollokhoz kapcsolódó folyamatok vizsgálata magában foglalja a különböző országokban alkalmazott üzletmenet-folytonossági intézkedések áttekintését, annak értékelését, hogy a kritikus szerepkörök megfelelően lefedettek-e, rendelkezésre állnak-e helyettesítő munkatársak vagy megfelelően kialakított utódlási folyamatok, továbbá annak felmérését, hogy a technológiai infrastruktúra megfelelően támogatja-e az összehangolt távoli munkavégzést. A belső ellenőrök áttekintik az eseményeket követő elemzések dokumentációját is annak megerősítésére, hogy a javító intézkedéseket végrehajtották-e. Amennyiben a Tematikus követelménynek csak bizonyos elemei alkalmazandók, a belső ellenőrök dokumentálják az alkalmazás vagy kizárás szakmai indokait.

3. forgatókönyv: **A téma egy felkérésre indult megbízás tárgya.**

Kritikus nemzeti infrastruktúráért felelős szervezet

Egy szomszédos országban pusztító hurrikán hatására a vezetőtestület egyik tagja kezdeményezi, hogy a belső ellenőrzési funkció vegyen fel a tervbe egy, a szervezeti ellenállóképességre irányuló megbízást annak felmérésére, hogy a szervezet milyen mértékben van kitéve a működési zavaroknak, a speciális szaktudással rendelkező szolgáltatóktól való függőségnek, a szabályozási kötelezettségeknek és a súlyos környezeti eseményeknek. Ebben az esetben a Szervezeti ellenállóképesség Tematikus követelményt teljeskörűen alkalmazzák.

Az irányítás követelményeinek értékelése érdekében a belső ellenőrök áttekintik a vezetőtestület által jóváhagyott stratégiai tervet és a kapcsolódó dokumentumokat annak megerősítésére, hogy a kritikus szolgáltatások folytonossága formálisan beépül a hosszú távú tervezésbe. Megvizsgálják a vezetőtestületnek készített beszámolókat annak megállapítására, hogy rendszeresen felülvizsgálják-e a működési rendelkezésre álláshoz, a kritikus eszközök fenntartásához és a pénzügyi tartaléktervezéshez kapcsolódó kulcsmutatókat, ideértve a biztosítási fedezeteket és a tartalékképzést is.

Kockázatkezelési szempontból a belső ellenőrök értékelik, hogy az infrastruktúra-kieséssel, a szolgáltatói koncentrációval, a szabályozási megfeleléssel, valamint a környezeti kitettséggel kapcsolatos kockázatokat miként azonosítják, értékelik és követik nyomon a vállalati szintű kockázatkezelési keretrendszerben. Megvizsgálják, hogy ezen kockázatok nyomon követéséért viselt felelősség egyértelműen meghatározott-e, valamint, hogy a korábbi szolgáltatáskiesések során követték-e az eszkalációs eljárásokat, beleértve a szabályozó és a katasztrófavédelmi hatóságokkal való koordinációt.

A kontrollok tesztelése keretében vizsgálják az üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervek meglétét és rendszeres tesztelését, a kritikus eszközök nyilvántartásait, az alternatív szolgáltatókkal kötött szerződéses megállapodásokat, valamint értékelik az incidensek utáni elemzések dokumentációját annak megállapítására, hogy a javító intézkedéseket nyomon követték-e és végrehajtották-e. Amennyiben egyes követelmények a szabályozási rendelkezések miatt nem alkalmazhatók, a belső ellenőrök a Normákkal összhangban dokumentálják ennek indokait.

C. függelék: Kapcsolódás egyéb keretrendszerekhez

A szervezet kialakíthatta saját, a szervezeti ellenállóképességet támogató megközelítését, amely olyan keretrendszereken alapulhat, mint például az ISO szabványai. A belső ellenőrök ezen keretrendszerek alapján már kidolgozhatták ellenőrzési programjaikat és tesztelési eljárásaikat. A belső ellenőröknek a szervezeti ellenállóképességet támogató kontrollok tervezett tesztelését összhangba kell hozniuk a Tematikus követelménnyel annak érdekében, hogy biztosítsák a megfelelő lefedettséget (13.4 norma: Az értékelés kritériumai). Az alábbi táblázat bemutatja a Szervezeti ellenállóképesség Tematikus követelmény és az ISO 22336 keretrendszer közötti megfeleltetést. További keretrendszerekre vonatkozó hivatkozások az E. függelékben találhatók.

Irányítási követelmények	ISO 22336 keretrendszer
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.	4.1; 6.1; 6.2; 7.1; 8.4; 8.5; 9.1; 9.5
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.	6.4; 8.6; 10.2
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.	4.2; 6.3; 8.3; 8.4; 9.4
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.	5.4

Irányítási követelmények	ISO 22336 keretrendszer
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.	9.6
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.	9.2; 9.5

Kockázatkezelési követelmények	ISO 22336 keretrendszer
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.	4.4; 5; 7.3; 7.4; 7.5, 7.6, 9.2, 9.3
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.	4.3; 8.2; 9.6
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.	7.2; 7.6; 10.1
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 stressztesteket.	7.2; 7.6; 7.8

Kontrollfolyamat követelményei	ISO 22336 keretrendszer
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.	7.7
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.	6.1
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.	7.5
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.	9.2
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.	8.6; 9.6; 10.3
F. Olyan folyamat került kialakításra, amely lehetővé teszi a munkavégzési környezet szükség szerinti átalakítását válsághelyzetek, működési zavarok és vészhelyzetek esetén.	9.3
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.	7.6
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.	10.2; 10.3

Kontrollfolyamat követelményei		ISO 22336 keretrendszer
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.	6.4; 7.6; 9.6
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.	10.2, 10.3

D. függelék: 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 követelménynek való megfelelést a belső ellenőrzési tervben vagy a megbízás munkalapjaiban lehet dokumentálni a belső ellenőrök szakmai megítélése alapján. Egy vagy több belső ellenőrzési megbízás is lefedheti a követelményeket. Emellett előfordulhat, hogy nem minden követelmény alkalmazandó. Az alábbi nyomtatható űrlap lehetőséget biztosít a Szervezeti ellenállóképesség Tematikus követelménynek való megfelelés dokumentálására, de alkalmazása azonban nem kötelező.

Szervezeti ellenállóképesség - Irányítás

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
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.		

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
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.		

Szervezeti ellenállóképesség – Kockázatkezelés

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
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.		

Szervezeti ellenállóképesség – Kontrollok

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
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.		

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
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.		

E. függelék: További keretrendszer-referenciák

Terület	ISO-hivatkozás	Hatókör/Szakaszcímek
Irányítás	ISO 22316:2017	Szabályzat és stratégia; vezetői elkötelezettség; közös jövőkép; szervezeti kultúra; kommunikáció; folyamatos fejlesztés
Kockázatkezelés	ISO 31000:2018	Hatókör/kontextus/kritériumok; kockázatértékelés; kockázatkezelési intézkedések; nyomon követés; kommunikáció.
Az üzletmenet-folytonosság és a katasztrófa utáni helyreállítás alapjai	ISO 22301: 2019; ISO/TS 22317:2021	Üzletmenet-folytonossági irányítási rendszer, vezetés, tervezés, működés; üzleti hatáselemzéshez kapcsolódó tevékenységek és eredmények.
Az ellátási lánc ellenállóképessége	ISO/TS 22318:2021	Beszállítói függőségek elemzése; folytonossági stratégiák; alternatív megoldások; bizonyossághoz kapcsolódó követelmények.
Az információs és kommunikációs technológia felkészültsége	ISO/IEC 27031	Információs és kommunikációs technológia folytonossága; helyreállítási célkitűzések; tesztelés és fejlesztés; üzletmenet-folytonossági irányítási rendszerrel való összhang.

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® (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 egyedi körülményekre, és mint ilyen, csak útmutatásként használható. Az IIA azt ajánlja, hogy minden konkrét helyzetre vonatkozóan kérjen független szakértői tanácsot. Az IIA nem vállal felelősséget azért, ha valaki kizárólag erre az anyagra hagyatkozik.

Szerzői jog

2026. április

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