Kiberbiztonság

Topical Requirement

Tematikus követelmény

Felhasználói útmutató

The Institute of
Internal Auditors

Tartalomjegyzék

A Tematikus követelmények áttekintése 1

Alkalmazhatóság, kockázat és szakmai megítélés 1

Megfontolások 4

A. melléklet. Gyakorlati alkalmazási példák 10

B. melléklet. A keretrendszerek leképezése 12

C. melléklet. Választható dokumentációs eszköz 17

A Tematikus követelmények áttekintése

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

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

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

Alkalmazhatóság, kockázat és szakmai megítélés

A Tematikus követelményeket akkor kell követni, amikor a belső ellenőrzési funkciók olyan témában végeznek bizonyosságot nyújtó megbízásokat, amelyekre vonatkozóan létezik Tematikus követelmény, vagy amikor a Tematikus követelmény komponenseit 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 kell alkalmazni a téma értékelésére a vonatkozó megbízásokon belül. Ezen felül, 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, ha olyan megbízást kérnek, amely eredetileg nem szerepelt a tervben, és tartalmazza a témát, akkor a Tematikus követelmény alkalmazhatóságát értékelni kell.

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

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

Míg a Kiberbiztonság Tematikus követelménye egy kiindulási alap a figyelembe veendő kontrollfolyamatokhoz, a kiberkockázatot nagyon magasra értékelő szervezeteknek további szempontokat is szükséges lehet értékelniük.

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). Még a kiszervezés sem mentesíti a belső ellenőrzési funkciót a Tematikus követelményeknek való megfelelésért viselt felelősség alól. 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 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 követelmény alkalmazása dokumentálható a belső ellenőrzési tervben vagy a megbízási munkadokumentumokban, a belső ellenőr szakmai megítélése alapján. Egy vagy több belső ellenőrzési megbízás is lefedheti a követelményeket. Valamint előfordulhat, hogy nem minden követelmény alkalmazható. Meg kell őrizni annak bizonyítékát, hogy a Tematikus követelmény alkalmazhatóságát értékelték, beleértve a kizárások indoklását is.

A C. mellékletben 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). Az eredményeket kommunikálni kell a vezetőtestület és a felsővezetés felé. A kommunikációnak be kell számolnia a belső ellenőrzési funkció Normáknak való megfeleléséről és a teljesítménycélok eléréséről.

A Tematikus követelményeknek való megfelelést a minőségértékelés során értékelik. A minőségértékelésre való felkészüléshez a belső ellenőrök a C. mellékletben található segédletet használhatják.

Kiberbiztonság

A kiberbiztonság széleskörű téma, amely bármely szervezet legtöbb technológiai aspektusához kapcsolódik. Az információtechnológia mellett a kiberbiztonság általában az üzleti folyamatok része, ami szükségessé teszi, hogy a belső ellenőrök a kibertérrel kapcsolatos kockázatokat értékeljék a megbízások tervezésekor, hatókör meghatározásakor és végrehajtásakor.

Az Egyesült Államok Kereskedelmi Minisztériumhoz tartozó Nemzeti Szabványügyi és Technológiai Intézet (NIST) a kiberbiztonságot egyszerűen így definiálja: " A kibertér használatának a kibertámadásokkal szembeni megóvásának vagy védelmének képessége". A Kiberbiztonság Tematikus követelménye arra a külső határterületre

összpontosít, amelyet a szervezetek biztosítanak az illetéktelen felhasználók és a rosszindulatú kiberfenyegetések kockázatainak csökkentése érdekében.

A kiberbiztonság az átfogó információbiztonság egy részhalmaza, amelyet a NIST a következőképpen határoz meg: "Az információk és információs rendszerek védelme a jogosulatlan hozzáférés, felhasználás, nyilvánosságra hozatal, működés megszakítása, módosítás vagy rombolás ellen a bizalmasság, sértetlenség és rendelkezésre állás biztosítása érdekében".

A kiberbiztonsági tematikus követelményhez tartozó kritériumok a következők:

- Irányítás - világosan meghatározott alapvető kiberbiztonsági célkitűzések és stratégiák, amelyek támogatják a szervezeti célokat, irányelveket és folyamatokat.
- Kockázatkezelés - a kiberfenyegetések azonosítására, elemzésére, kezelésére és nyomon követésére szolgáló folyamatok, beleértve a kiberkockázatok azonnali eszkalálására szolgáló folyamatot.
- Kontrollok - a vezetés által létrehozott, rendszeresen értékelt kontroll folyamatok a kiberkockázat mérséklésére.

Megfontolások

A belső ellenőrök a következő megfontolásokat használhatják a kiberbiztonsági Tematikus követelményben foglalt követelmények értékeléséhez. Ezek a megfontolások, amelyek kereszthivatkozást tartalmaznak a követelményekre, szemléltető jellegűek, de nem kötelezőek. A belső ellenőröknek szakmai megítélésükre kell hagyatkozniuk annak meghatározásakor, hogy mit vegyenek figyelembe az értékelésük során.

Irányítási megfontolások

Annak felmérése érdekében, hogy az irányítási folyamatok hogyan viszonyulnak a kiberbiztonsági célkitűzésekhez, a belső ellenőrök vizsgálhatják:

A. A hivatalos, dokumentált kiberbiztonsági stratégiai tervet és célkitűzéseket, beleértve annak bizonyítékát, hogy a vezetőtestület rendszeresen (általában negyedévente) felülvizsgálja az információbiztonsági funkció vezetője, például az információbiztonsági vezető (CISO) által készített kiberbiztonsági beszámolókat. A bizonyítékok közé tartozhat a következőkről szóló jelentés:
    - A stratégiai célok elérésének nyomon követése.
    - Költségvetési igények a kiberbiztonsági célok és célkitűzések támogatására.
    - A kockázatok és a belső kontrollok fókuszba helyezése, beleértve a kockázat csökkentés előrehaladásának jelentését is.
    - Kulcsfontosságú teljesítménymutatók (KPI-k) a siker mérésére.
    - A kiberbiztonsági munkatársak felvételéhez, képzéséhez és fejlesztéséhez szükséges emberi erőforrások.

B. A kiberbiztonsági folyamatok irányítására használt szabályzatok, folyamatok és egyéb vonatkozó dokumentáció, ideértve a következőket:
    - Legalább évente felülvizsgált és frissített szabályzatok. Az újonnan felmerülő kiberkockázatok szükségessé tehetik, hogy a felülvizsgálatokra és frissítésekre gyakrabban kerüljön sor.
    - Folyamat annak megállapítására, hogy az irányelvek és a folyamatok elegendőek-e a kiberbiztonsági működés támogatásához.
    - Széles körben elfogadott keretrendszerek (NIST, COBIT és mások) a kiberbiztonsági folyamatok és belső kontrollok megerősítésére.
C. A kiberbiztonsági célkitűzések elérését támogató szerepek és felelősségi körök, beleértve egy olyan struktúrát, amely biztosítja, hogy a kiberbiztonsági funkció a szervezet olyan szintjének jelentsen, amely kellő láthatósággal rendelkezik a szervezeti támogatás eléréséhez.
    - A kiberbiztonsági szerepköröket betöltő személyek ismereteinek, készségeinek és képességeinek rendszeres értékelésére szolgáló folyamat.
D. Az érintett érdekelt felekkel (például felsővezetéssel, üzemeltetéssel, kockázatkezeléssel, humán erőforrással, joggal, megfelelési területtel, stratégiai beszállítókkal és másokkal való együttműködés bizonyítéka, beleértve a meglévő és újonnan felmerülő kiberkockázatokról és az ismert potenciális sebezhetőségekről szóló kommunikációt. A kommunikáció bizonyítékai lehetnek értekezletek jegyzőkönyvei, jelentések vagy e-mailek.

Kockázatkezelési megfontolások

A. Annak felmérése érdekében, hogy a kockázatkezelési folyamatok hogyan viszonyulnak a kiberbiztonsági célkitűzésekhez, a belső ellenőrök vizsgálhatják:

   Hogyan értékeli és kezeli a szervezet a kiberbiztonsági kockázatot, beleértve azt, hogy a fenyegetéseket és sebezhetőségeket hogyan:

    - azonosítják és jelentik kezdetben.
    - elemzik, hogy felmérjék azok szervezeti célok elérésére gyakorolt kockázatát.
    - mérséklik, beleértve a kockázatot elfogadható szintre csökkentő cselekvési terveket.
    - kísérik figyelemmel, beleértve a folyamatos jelentéstételre vonatkozó tervet, amíg a fenyegetések teljes mértékben meg nem szűnnek.
B. Hogyan szerez a szervezet rendszeres időközönként információt a kiberbiztonsági kockázatkezeléshez a funkcionális területektől, például az információtechnológiától, a vállalati kockázatkezeléstől, a humánerőforrás-, a jogi, a megfelelési, az üzemeltetési, a számviteli és a pénzügyi területektől. Az információszerzésre egy keresztfunkcionális kiberbiztonsági csoport vagy informatikai irányító bizottság is alkalmazható.
C. Hogyan bízta rá a szervezet a kiberbiztonsági kockázatkezeléssel kapcsolatos elszámoltathatóságot és felelősséget egy személyre vagy csoportra.

- A felelős személy(ek)nek rendszeresen (negyedévente, havonta vagy szükség szerint) tájékoztatniuk kell a szervezetet a kiberbiztonsági kockázatok folyamatos aktualitásairól, és esetlegesen a kockázatcsökkentési stratégiák erőforrásigényeiről.

D. A kiberbiztonsági kockázatok eszkalációs folyamatait, beleértve a fenyegetés vagy kockázat szintjének értékelését, hozzárendelését és rangsorolását. A felülvizsgálat magában foglalhatja a következők azonosítását:
   - A szervezet által meghatározott kockázati szintek - például magas, közepes és alacsony - az egyes kockázati szintek részletes magyarázatával és az egyes kockázati kategóriákhoz tartozó eszkalációs eljárásokkal.
   - A már azonosított kiberbiztonsági kockázatok listája és az egyes kockázati események mérséklésének állapota.
   - Alkalmazandó jogszabályi és megfelelési követelmények.
   - Mind a pénzügyi, mind a nem pénzügyi (például hírnév) kockázatok hatásai.

E. A kiberbiztonsági kockázatoknak a vezetőség és az alkalmazottak felé történő kommunikálásának folyamatát, amely magában foglalja:
   - Az alkalmazottak rendszeresen (legalább évente) történő kiberbiztonsági képzését, például előre be nem jelentett, szimulált adathalász kampányokat a szervezeti tudatosság tesztelésére és mérésére.
   - A meglévő kiberbiztonsági problémák kijavításával kapcsolatos tájékoztatásokat, a várható befejezési dátumokkal.
   - A meg nem felelés nyomon követését, amely magában foglalja a vezetőtestület és a felsővezetés tájékoztatását.
   - A fenyegetések újraértékelését, amikor a szervezet kockázati hajlandósága és kockázattűrése megváltozik.

F. A szervezet által az incidensekre adott válaszlépéseket és a helyreállításra vonatkozóan bevezetett folyamatokat, amelyek magukban foglalják a következőket:
   - Dokumentált terv, amelyet felülvizsgálnak és frissítenek, ahogy a szervezet működése idővel változik. A tervnek tartalmaznia kell:
     - Az incidensek észlelésének és jelentésének módját.
     - Az incidensek megfékezésének módját a további károk megelőzése érdekében.
     - A szervezet helyreállításának és válaszlépéseinek módját a működés folytatása érdekében.
     - Az incidensek elemzésének módját a tanulságok levonása és a hasonló események megelőzése érdekében.
   - Rendszeres (legalább évente végzett) tesztelést (szimulációs gyakorlatot) és az eredmények jelentését a felsővezetésnek és az érintett érdekelt feleknek. A tesztelés eredményeképpen cselekvési tervek készülhetnek.

Kontrollfolyamatra vonatkozó megfontolások

Annak felmérése érdekében, hogy az kontrollfolyamatok hogyan viszonyulnak a kiberbiztonsági célkitűzésekhez, a belső ellenőrök vizsgálhatják

A. A vezetés megközelítését a hatékony kiberbiztonsági belső kontrollkörnyezet kialakítására, beleértve:
   - A megnövekedett kockázatok mérsékléséhez és az érzékeny, kritikus, személyes vagy bizalmas adatok védelméhez szükséges belső kontrollok felmérése és bevezetése a szervezeti kockázatértékelési folyamat alapján.
   - A kulcsfontosságú kiberbiztonsági kontrollok fenntartásához szükséges erőforrásigények meghatározása.
   - A szállítói kontrollok figyelembevétele a kontrollkörnyezet részeként, ami magában foglalja a szolgáltató szervezet kontrolljairól (SOC) szóló jelentések felülvizsgálatát az üzleti kapcsolat megkezdése előtt és az együttműködés teljes időtartama alatt.
   - Rendszeres tesztelése a kiberbiztonsági kontrolloknak, hogy úgy működnek-e, hogy csökkentsék a kockázatokat és támogassák a kiberbiztonsági célkitűzések elérését.
   - Folyamat a belső kontrollhiányosságok orvoslására, illetve a belső kontroll funkció vagy más bizonyosságot nyújtó szolgáltató által végzett értékelések (például penetrációs tesztek) megállapításainak kezelésére.

B. A szervezet tehetséggondozási folyamatát a kiberbiztonsági szakemberek toborzására és képzésére vonatkozóan, beleértve azt is, hogy a szervezet hogyan azonosítja a kiberbiztonsági szakemberek képességeinek növelésére irányuló lehetőségeket a technikai ismeretek támogatása, és a felmerülő problémákra vonatkozó szervezeti tudatosság javítása érdekében.
   - Ilyen például a képzésben, tudásmegosztó csoportokban való részvétel és a folyamatos szakmai képzés, amely magában foglalja a kibertérrel kapcsolatos minősítések megszerzését.

C. A vezetésnek a napi működésre összpontosító, az újonnan felmerülő kiberbiztonsági fenyegetések és sebezhetőségek azonosítására, rangsorolására, nyomon követésére és folyamatos jelentésére szolgáló folyamatát. A vizsgálat kiterjedhet arra is, hogy kialakítottak-e folyamatokat az új vagy kialakulóban lévő technológiákhoz, például a mesterséges intelligencia használatához, kapcsolódó fenyegetések és sebezhetőségek értékelésére.

D. Az informatikai eszközök teljes életciklusa során az informatikai eszközök kezelésére és védelmére létrehozott vezetői folyamatokat és kontrollokat, beleértve a hardver, a szoftver és a szállítói szolgáltatások kiválasztását, használatát, karbantartását és használatból történő kivonását. A hardverek közé tartoznak a szerverek, hálózati berendezések (például routerek vagy tűzfalak), asztali számítógépek, laptopok, mobiltelefonok, táblagépek és perifériák. A szoftverek közé tartoznak az operációs

rendszerek (például a Windows), a vállalatirányítási (ERP) szoftverek, alkalmazások, a vírusirtó programok és mások. A megfontolások a hardver és szoftver tekintetében a következők lehetnek:

- A szervezet által alkalmazott titkosítás, vírusirtó szoftverek, mobileszköz-kezelés, komplex jelszókövetelmények, virtuális magánhálózat (VPN)/zéró bizalom hálózat (ZTN) a hitelesítéshez, valamint a firmware-ek rendszeres frissítése.
- Olyan eszközkezelési folyamat, amely biztosítja, hogy a vállalat által kiadott hardverek megfelelő biztonsági konfigurációval rendelkezzenek a kiadáskor, és a kivezetett eszközök megfelelő módon legyenek selejtezve vagy megsemmisítve.
- Adatbázissal kapcsolatos kontrollok, amelyek magukban foglalják a felhasználói és rendszergazdai hozzáférés korlátozását, biztosítják a titkosítás használatát, az adatbázisok biztonsági mentését és tesztelését, valamint az erős hálózati biztonsági kontrollok meglétét.
- Hogyan veszik figyelembe a kiberbiztonsági fenyegetéseket vagy sebezhetőségeket a rendszerfejlesztési életciklusban (SDLC).
- A fejlesztés, a biztonság és az üzemeltetés (DevSecOps) által alkalmazott megközelítés, amely biztosítja, hogy a szoftverfejlesztési folyamat magában foglalja a kiberbiztonságot, a sebezhetőségek proaktív azonosítása érdekében.

E. A kiberbiztonság megerősítésére használt folyamatokat, többek között:

- Biztonsági beállítások konfigurálása a kiberbiztonsági kockázat minimalizálása érdekében.
- A mobileszközök kezelése (beleértve az e-mail és az alkalmazások használatát) úgy van konfigurálva, hogy csökkentse a kiberbiztonsági kockázatokat, és távolról kezelhető legyen, ha a felhasználó eszköze veszélybe kerül.
- A titkosítás használata mind a "nyugalmi állapotban lévő" adatok, például a merevlemezen tárolt információk, mind a "úton lévő" adatok, például az e-mailek esetében.
- Szerverek vagy szoftverek (például operációs rendszerek) frissítése a legújabb biztonsági verziókkal.
- A felhasználói hozzáférés kezelése, például többfaktoros hitelesítés (MFA) és egyedi felhasználói azonosítók használata komplex jelszavakkal, amelyek időszakosan lejárnak.
- Felügyeleti kontrollokat használatnak annak érdekében, hogy meghatározzák, vajon a rendelkezésre állás és az erőforrás-felhasználás eléri-e azt a szintet, amely lehetővé teszi a teljesítményt veszélyeztető potenciális kiberbiztonsági problémák vizsgálatát és elemzését.
- A kiberbiztonság integrálása az SDLC-be a kiberbiztonsági sebezhetőségek azonosítása és kezelése érdekében, mielőtt a szoftver éles alkalmazásba kerülne.

F. Hálózattal kapcsolatos kontrollokat, amelyek biztosítják a szervezet külső határterületét, beleértve azt is, hogy a szervezet hogyan használja a:

- Hálózati szegmentációt.
- Tűzfalakat.
- Felhasználói hozzáférés-ellenőrzést.
- Korlátozásokat mind a külső, mind a belső kapcsolatokra vonatkozóan.
- Dolgok internetét (IoT) körülvevő ellenőrzéseket az összekapcsolt hálózatok számára.
- Behatolásérzékelő/megelőző rendszereket a kiberbiztonsági támadások megelőzésére, észlelésére és az azutáni helyreállításra.

G. A végpont-kommunikációs biztonsági intézkedésekre vonatkozó kontrollokat, amelyek olyan szolgáltatásokra alkalmazandóak, mint az e-mail, az internetböngészők, a videokonferencia, az üzenetküldés (Zoom, MS Teams és mások), a közösségi média, a felhő és a fájlmegosztási protokollok. A kontrollok magukban foglalhatják bizonyos fájlkiterjesztések (például .exe fájlok) használatának korlátozását és a fájlmegosztás többfaktoros hitelesítését.

A. melléklet. Példák a gyakorlati alkalmazásra

Az alábbi példák olyan forgatókönyveket írnak le, amelyekben a Kiberbiztonság Tematikus követelménye alkalmazható:

1. Példa: A belső ellenőrzési tervben szerepel kiberbiztonsággal kapcsolatos belső ellenőrzési megbízás.

Ha a belső ellenőrzési funkció lezárja a kockázatalapú tervezési folyamatot, és a belső ellenőrzési terv egy vagy több kiberbiztonsággal 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 kiberbiztonság széleskörű 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 Kiberbiztonsági Tematikus követelmény egy vagy több követelménye nem alkalmazható a megbízás teljesítése során, akkor azt a belső ellenőröknek dokumentálniuk kell és meg kell őrizniük az adott követelmények kizárásának indoklását. Egyes követelmények kizárásának indoklása lehet például az, hogy a belső ellenőrzési funkció rotációs alapon végez különböző kiberbiztonsági megbízásokat, vagy megállapította, hogy a kockázat jelentősége a megbízás szempontjából alacsony.

2. Példa: A kiberbiztonsági kockázatokat egy olyan belső ellenőrzési megbízás során azonosítják, amely nem a kiberbiztonságra összpontosít.

A belső ellenőrök azonosíthatnak kiberbiztonsági kockázatokat egy olyan folyamat értékelése során, amely nem kapcsolódik közvetlenül a kiberbiztonsághoz. Például előfordulhat, hogy a belső ellenőrök a szállító számlák folyamatát értékelik egy olyan megbízás keretében, amely nem a kiberbiztonságra összpontosít, és a megbízás megtervezésekor nem azonosítják a kiberbiztonsági kockázatokat a megbízás hatókörében. Azonban az előzetes felmérés elvégzése után a belső ellenőrök megállapítják, hogy ezen kockázatoknak a megbízás hatókörébe kell tartozniuk; például azonosítják az előzetes megrendelés webalapú benyújtásával kapcsolatos kiberbiztonsági kockázatokat (13.2. norma: A megbízással kapcsolatos kockázatok felmérése).

A releváns kockázatok azonosítása után a belső ellenőröknek át kell tekinteniük a Kiberbiztonság Tematikus követelményét, és meg kell határozniuk, hogy mely követelmények alkalmazandók. Ebben a példában kizárhatják a kiberbiztonsági irányítási

folyamatot vagy a kiberbiztonsági kockázatkezelési folyamatot. A megbízás munkadokumentációban dokumentálniuk kell a Kiberbiztonság Tematikus követelmény többi követelményének kizárására vonatkozó indoklást, és a dokumentációt meg kell őrizniük.

3. Példa: Olyan kiberbiztonsági 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 kiberbiztonsági értékeléseket. Például amikor a szervezetek kibertámadás célpontjai, a vezetőtestület kérheti a belső ellenőrzés megbízását a kiberbiztonsági kontrollok értékelésére. A Tematikus követelmény alkalmazandó, a követelményeket értékelni kell, és dokumentálni kell az esetleges kizárásokat.

B. melléklet. Megfeleltetés a keretrendszerekhez

A szervezetnek lehetnek saját kiberbiztonsági erőfeszítései, amelyekhez olyan kockázatkezelési és irányítási keretrendszereket használnak, mint a COBIT vagy a NIST. A belső ellenőrök már kidolgozhattak ellenőrzési programokat és tesztelési eljárásokat e keretrendszerek alapján. A belső ellenőröknek össze kell hangolniuk a tervezett kiberbiztonsági kontrollok tesztelését a Tematikus követelménnyel a megfelelő lefedettség biztosítása érdekében. Az alábbi táblázat a Kiberbiztonság Tematikus követelményét három általánosan használt keretrendszernek felelteti meg: NIST Cybersecurity Framework 2.0, COBIT 2019 és NIST 800-53. Ezek a keretrendszerek azért kerültek összevetésre, mert könnyen és ingyenesen elérhetők.

Irányítási követelmények	Keretrendszeri referenciák		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Formális kiberbiztonsági stratégiát és célkitűzéseket alakítanak ki, amelyeket rendszeresen frissítenek. A kiberbiztonsági célkitűzések eredményeit rendszeresen megosztják és azokat a vezetőtestület felülvizsgálja, beleértve a kiberbiztonsági stratégiát támogató erőforrásokat és költségvetési megfontolásokat is.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. A kiberbiztonsággal kapcsolatos szabályzatokat és eljárásokat alakítanak ki, és azt rendszeresen frissítik a kontrollkörnyezet megerősítése érdekében.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11

C. A kiberbiztonsági célkitűzéseket támogató szerepek és felelősségi körök meg vannak határozva, és ki van alakítva egy folyamat a szerepköröket betöltő személyek ismereteinek, készségeinek és képességeinek rendszeres értékelésére.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07
D. Az érintett érdekelt felek bevonásával megvitatják a kiberbiztonsági környezet meglévő sebezhetőségeit és újonnan felmerülő fenyegetéseit, és ezekkel kapcsolatban intézkedéseket hoznak. Az érdekelt felek közé tartozik a felsővezetés, az üzemeltetés, a kockázatkezelés, a humánerőforrás-management, a jog, a megfelelési terület, a szállítók és egyéb szereplők.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Kockázatkezelési követelmények	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. A szervezet kockázatértékelési és kockázatkezelési folyamatai magukban foglalják a kiberbiztonsági fenyegetések és azok stratégiai célkitűzések elérésére gyakorolt hatásának azonosítását, elemzését, mérséklését és nyomon követését.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. A kiberbiztonsági kockázatkezelés a szervezet egészére kiterjed, és a következő területeket foglalhatja magában: információtechnológia, vállalati kockázatkezelés, humánerőforrás, jog, megfelelőség, üzemeltetés, ellátási lánc menedzsment, számvitel, pénzügy és egyéb területek.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12

C. A kiberbiztonsági kockázatkezeléssel kapcsolatos elszámoltathatóságot és felelősséget meghatározták. Kijelöltek egy személyt vagy csoportot, aki/amely rendszeresen figyelemmel kíséri és jelentést tesz a kiberbiztonsági kockázatok kezeléséről, beleértve a kockázatok mérsékléséhez és az újonnan felmerülő kiberbiztonsági fenyegetések azonosításához szükséges erőforrásokat.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12
D. Kialakítottak egy folyamatot a szervezet kockázatkezelési irányelvei vagy az alkalmazandó jogszabályi követelmények szerint elfogadhatatlan szintet elérő (új vagy korábban azonosított) kiberbiztonsági kockázat gyors eszkalálására. Figyelembe kell venni a kiberbiztonsági kockázat pénzügyi és nem pénzügyi hatásait.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Kialakítottak egy folyamatot a kiberbiztonsági kockázatok tudatosítására a vezetés és az alkalmazottak számára, valamint egy vezetői jelentést annak érdekében, hogy a problémákat, hiányosságokat vagy kontroll hibákat rendszeresen felülvizsgálják és javítsák.	PR.AT; GV.RR.01; GV.RRR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. A szervezet olyan kiberbiztonsági incidensekre való reagálási és helyreállítási folyamatot vezetett be, amely magában foglalja az észlelést, a megfékezést, a helyreállítást és az incidens utáni elemzést. Az incidensekre való reagálási és helyreállítási folyamatot rendszeresen tesztelik.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Kontrollfolyamat követelményei	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**

A. A belső és szállítói alapú kontrollok biztosítására folyamatot hoznak létre szervezet rendszerei és adatai bizalmasságának, sértetlenségének és rendelkezésre állásának védelme érdekében. Rendszeres időközönként értékeléseket végeznek annak megállapítására, hogy a kontrollok úgy működnek-e, hogy elősegítsék a szervezeti kiberbiztonsági célkitűzések elérését és a problémák gyors megoldását.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01
B. Olyan tehetséggondozási folyamatot alakítanak ki, amely magában foglalja a kiberbiztonsági műveletekhez kapcsolódó technikai kompetenciák fejlesztését és fenntartását célzó képzést. A folyamatot rendszeresen felülvizsgálják.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Kialakítanak egy folyamatot az újonnan felmerülő kiberbiztonsági fenyegetések és sebezhetőségek folyamatos nyomon követésére és jelentésére, valamint a kiberbiztonsági tevékenység javítására irányuló lehetőségek azonosítására, rangsorolására és végrehajtására.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. A kiberbiztonság az összes informatikai eszköz - beleértve a hardvert, a szoftvert és a szállítói szolgáltatásokat - életciklus-menedzsmentje (kiválasztás, használat, karbantartás és használatból való kivezetés) részét képezi.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06

E. A kiberbiztonság megerősítésére folyamatokat alakítanak ki, beleértve a konfigurációt, a végfelhasználói eszközök kezelését, a titkosítást, a szoftver javításokat, a felhasználói hozzáférés kezelését, valamint a rendelkezésre állás és a működés nyomon követését. A kiberbiztonsági megfontolások beépülnek a szoftverfejlesztésbe (DevSecOps).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
F. Hálózattal kapcsolatos kontrollokat vezetnek be, például a hálózati hozzáférés ellenőrzése és szegmentálása; tűzfalak használata és elhelyezése; korlátozott kapcsolatok külső hálózatokból és külső hálózatokhoz; virtuális magánhálózat (VPN)/zéró bizalom hálózati hozzáférés (ZTNA); a tárgyak internetének (IoT) hálózati kontrollja; és behatolásérzékelő/megelőző rendszerek (IDS és IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
G. Végpont-kommunikációs biztonsági kontrollokat alkalmaznak olyan szolgáltatásokra, mint az e-mail, az internetböngészők, a videokonferencia, az üzenetküldés, a közösségi média, a felhő és a fájlmegosztási protokollok.	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

C. melléklet. Opcionális dokumentációs segédlet

A belső ellenőröknek a kockázatértékelés alapján szakmai döntést kell hozniuk a követelmények alkalmazhatóságának meghatározásakor, és megfelelően dokumentálniuk kell egyes követelmények kizárását. A Tematikus követelményt a belső ellenőrzési tervben vagy a megbízás munkadokumentumaiban lehet dokumentálni a belső ellenőrök szakmai megítélése alapján. Egy vagy több belső ellenőrzési megbízás is kiterjedhet a követelményekre. Ezenkívül előfordulhat, hogy nem minden követelmény alkalmazható. Az alábbi nyomtatható űrlap a Kiberbiztonság Tematikus követelménynek való megfelelés dokumentálásának egyik lehetőségét kínálja, de használata nem kötelező.

Kiberbiztonság - Irányítás

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
A. Formális kiberbiztonsági stratégiát és célkitűzéseket alakítanak ki, amelyeket rendszeresen frissítenek. A kiberbiztonsági célkitűzések eredményeit rendszeresen megosztják és azokat a vezetőtestület felülvizsgálja, beleértve a kiberbiztonsági stratégiát támogató erőforrásokat és költségvetési megfontolásokat is.		
B. A kiberbiztonsággal kapcsolatos szabályzatokat és eljárásokat alakítanak ki. és azt rendszeresen frissítik a kontrollkörnyezet megerősítése érdekében.		
C. A kiberbiztonsági célkitűzéseket támogató szerepek és felelősségi körök meg vannak határozva, és ki van alakítva egy folyamat a szerepköröket betöltő személyek ismereteinek, készségeinek és képességeinek rendszeres értékelésére.		

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
D. Az érintett érdekelt felek bevonásával megvitatják a kiberbiztonsági környezet meglévő sebezhetőségeit és újonnan felmerülő fenyegetéseit, és ezekkel kapcsolatban intézkedéseket hoznak. Az érdekelt felek közé tartozik a felsővezetés, az üzemeltetés, a kockázatkezelés, a humánerőforrás-management, a jogi, a megfelelési terület, a szállítók és egyéb szereplők.		

Kiberbiztonság - Kockázatkezelés

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
A. A szervezet kockázatértékelési és kockázatkezelési folyamatai magukban foglalják a kiberbiztonsági fenyegetések és azok stratégiai célkitűzések elérésére gyakorolt hatásának azonosítását, elemzését, mérséklését és nyomon követését.		
B. A kiberbiztonsági kockázatkezelés a szervezet egészére kiterjed, és a következő területeket foglalhatja magában: információtechnológia, vállalati kockázatkezelés, humánerőforrás, jog, megfelelőség, üzemeltetés, ellátási lánc menedzsment, számvitel, pénzügy és egyéb területek.		

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
C. A kiberbiztonsági kockázatkezeléssel kapcsolatos elszámoltathatóságot és felelősséget meghatározták. Kijelöltek egy személyt vagy csoportot, aki/amely rendszeresen figyelemmel kíséri és jelentést tesz a kiberbiztonsági kockázatok kezeléséről, beleértve a kockázatok mérsékléséhez és az újonnan felmerülő kiberbiztonsági fenyegetések azonosításához szükséges erőforrásokat.		
D. Kialakítottak egy folyamatot a szervezet kockázatkezelési irányelvei vagy az alkalmazandó jogszabályi követelmények szerint elfogadhatatlan szintet elérő (új vagy korábban azonosított) kiberbiztonsági kockázat gyors eszkalálására. Figyelembe kell venni a kiberbiztonsági kockázat pénzügyi és nem pénzügyi hatásait.		
E. Kialakítottak egy folyamatot a kiberbiztonsági kockázatok tudatosítására a vezetés és az alkalmazottak számára, valamint egy vezetői jelentést annak érdekében, hogy a problémákat, hiányosságokat vagy kontroll hibákat rendszeresen felülvizsgálják és javítsák.		
F. A szervezet olyan kiberbiztonsági incidensekre való reagálási és helyreállítási folyamatot vezetett be, amely magában foglalja az észlelést, a megfékezést, a helyreállítást és az incidens utáni elemzést. Az incidensekre való reagálási és helyreállítási folyamatot rendszeresen tesztelik.		

Kiberbiztonság - Kontrollfolyamatok

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
A. A belső és szállítói alapú kontrollok biztosítására folyamatot hoznak létre szervezet rendszerei és adatai bizalmasságának, sértetlenségének és rendelkezésre állásának védelme érdekében. Rendszeres időközönként értékeléseket végeznek annak megállapítására, hogy a kontrollok úgy működnek-e, hogy elősegítsék a szervezeti kiberbiztonsági célkitűzések elérését és a problémák gyors megoldását.		
B. Olyan tehetséggondozási folyamatot alakítanak ki, amely magában foglalja a kiberbiztonsági műveletekhez kapcsolódó technikai kompetenciák fejlesztését és fenntartását célzó képzést. A folyamatot rendszeresen felülvizsgálják.		
C. Kialakítanak egy folyamatot az újonnan felmerülő kiberbiztonsági fenyegetések és sebezhetőségek folyamatos nyomon követésére és jelentésére, valamint a kiberbiztonsági tevékenység javítására irányuló lehetőségek azonosítására, rangsorolására és végrehajtására.		
D. A kiberbiztonság az összes informatikai eszköz - beleértve a hardvert, a szoftvert és a szállítói szolgáltatásokat - életciklus-menedzsmentje (kiválasztás, használat, karbantartás és használatból való kivezetés) részét képezi.		

Követelmény	Lefedett terület vagy a kizárás indoklása	Dokumentációs hivatkozás
E. A kiberbiztonság megerősítésére folyamatokat alakítanak ki, beleértve a konfigurációt, a végfelhasználói eszközök kezelését, a titkosítást, a szoftver javításokat, a felhasználói hozzáférés kezelését, valamint a rendelkezésre állás és a működés nyomon követését. A kiberbiztonsági megfontolások beépülnek a szoftverfejlesztésbe (DevSecOps).		
F. Hálózattal kapcsolatos kontrollokat vezetnek be, például a hálózati hozzáférés ellenőrzése és szegmentálása; tűzfalak használata és elhelyezése; korlátozott kapcsolatok külső hálózatokból és külső hálózatokhoz; virtuális magánhálózat (VPN)/zéró bizalom hálózati hozzáférés (ZTNA); a tárgyak internetének (IoT) hálózati kontrollja; és behatolásérzékelő/megelőző rendszerek (IDS és IPS).		
G. Végpont-kommunikációs biztonsági kontrollokat alkalmaznak olyan szolgáltatásokra, mint az e-mail, az internetböngészők, a videokonferencia, az üzenetküldés, a közösségi média, a felhő és a fájlmegosztási protokollok.		

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 szervezet világszerte a belső ellenőrzési szakma vezetőjeként ismerik el a normák, a minősítések, az oktatás, a kutatás és a technikai útmutatás terén. További információ a www.theiia.org oldalon.

Felelősségi nyilatkozat

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

Szerzői jog

2025. február

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