

Kiberbiztonság

Topical Requirement

Tematikus követelmény



The Institute of
Internal Auditors

Kiberbiztonsági tematikus követelmény

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

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

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

A belső ellenőröknek a Globális Belső Ellenőrzési Normákkal összhangban kell alkalmazniuk a Tematikus követelményeket. Az aktuális követelményeknek való megfelelés a bizonyosságot nyújtó szolgáltatások esetében kötelező, a tanácsadói szolgáltatások esetében pedig ajánlott.

A Tematikus követelmény akkor alkalmazható, ha a téma:

- A. a belső ellenőrzési tervben szereplő megbízás tárgya vagy
- B. egy megbízás teljesítése során azonosított vagy
- C. az eredeti belső ellenőrzési tervben nem szereplő megbízási kérelem tárgya.

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

[További információért lásd a Kiberbiztonság Tematikus követelmény Felhasználói útmutatót.](#)



Kiberbiztonság

A Nemzeti Szabványügyi és Technológiai Intézet (NIST) a kiberbiztonságot a következőképpen határozza meg: "A kibertér használatának a kibertámadásokkal szembeni megóvásának vagy védelmének képessége". 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 kiberbiztonság csökkenti a kockázatot azáltal, hogy megerősíti az általános kontrollkörnyezetet, és megvédi a szervezet információs eszközeit a jogosulatlan hozzáféréstől, működés megszakításától, módosítástól vagy a rombolástól. A kibertámadások közvetlen és közvetett hatásokhoz vezethetnek, amelyek gyakran jelentősek, mivel a számítógépek, hálózatok, programok, adatok és érzékeny információk a legtöbb szervezet kritikus összetevői.

A kiberbiztonsági irányítási, kockázatkezelési és kontrollfolyamatok értékelése és felmérése

Ez a Tematikus követelmény következetes, átfogó megközelítést biztosít a kiberbiztonsági irányítási, kockázatkezelési és kontroll folyamatok kialakításának és végrehajtásának értékeléséhez. A követelmények a szükséges minimumot képviselik a szervezet kiberbiztonságának értékeléséhez.

IRÁNYÍTÁS: A kiberbiztonsági irányítás értékelése és felmérése

Követelmények:

A belső ellenőröknek a szervezet kiberbiztonsági irányításával kapcsolatban a következőket kell értékelniük:

- A.** Formális kiberbiztonsági stratégiát és célkitűzéseket alakítanak ki, amelyeket rendszeresen frissítenek. A kiberbiztonsági célkitűzések eredményeit rendszeresen megosztják és azokat a vezetőttestület 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.
- 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 megfelelés, a szállítók és egyéb szereplők.



KOCKÁZATKEZELÉS: A kiberbiztonsági kockázatkezelés értékelése és felmérése

Követelmények:

A belső ellenőröknek a szervezet kiberbiztonsági kockázatkezelésével kapcsolatban a következőket kell értékelniük:

- 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, megfelelés, üzemeltetés, ellátási lánc menedzsment, számvitel, pénzügy és egyéb területek.
- 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 eskalálására. 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.

KONTROLLOK: A kiberbiztonsági kontrollfolyamatok értékelése és felmérése

Követelmények:

A belső ellenőröknek a szervezet kiberbiztonsági kontrollfolyamataival kapcsolatban a következőket kell értékelniük:

- A.** A belső és szállítói kontrollok biztosítására folyamatot hoznak létre szervezet rendszerei és adatai bizalmosságának, 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.
- 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)/zéro 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 szervezetet világszerte a belső ellenőrzési szakma vezetőjeként ismerik el a normák, a minősítések, az oktatás, a kutatás és a technikai útmutatás terén. További információ a www.theiia.org oldalon.

Szerzői jog

© 2025 The Institute of Internal Auditors, Inc. Minden jog fenntartva. Sokszorosítási kérelmeket a copyright@theiia.org e-mail címen fogadunk.

2025. február



The Institute of
Internal Auditors

Globális központ

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

