

Kibernetinis saugumas

Topical Requirement

Teminis reikalavimas



The Institute of
Internal Auditors

Kibernetinio saugumo teminis reikalavimas

Kibernetinio saugumo teminiai reikalavimai yra privaloma Tarptautinės profesinės praktikos sistemos (Professional Practices Framework®) sudedamoji dalis kartu su Pasauliniais vidaus audito standartais (Global Internal Audit Standards™) ir Pasaulinėmis gairėmis. Teminiai reikalavimai turi būti naudojami kartu su Pasauliniais vidaus audito standartais, kurie yra autoritetingas privalomos praktikos pagrindas.

Teminiai reikalavimai pateikia aiškius lūkesčius vidaus auditoriams, nustatydami minimalius bazinius konkrečios rizikos temos audito reikalavimus. Atsižvelgiant į organizacijos rizikos profilį, vidaus auditoriams gali tekti atsižvelgti į papildomus temas aspektus.

Atitiktis teminiams reikalavimams padidins vidaus audito paslaugų atlikimo nuoseklumą ir pagerins vidaus audito paslaugų ir rezultatų kokybę bei patikimumą. Galiausiai teminiai reikalavimai tobulina vidaus audito profesiją.

Vidaus auditoriai privalo taikyti teminius reikalavimus pagal Pasaulinius vidaus audito standartus. Atitiktis teminiams reikalavimams yra privaloma teikiant užtikrinimo paslaugas ir rekomenduojama teikiant konsultavimo paslaugas.

Teminis reikalavimas taikomas, kai audito tema yra viena iš šių:

- A. Vidaus audito plano užduoties objektas.
- B. Nustatyta atliekant užduotį.
- C. Užduoties pagal užklausą objektas, neįtrauktas į pradinį vidaus audito planą.

Įrodymai, kad buvo įvertintas kiekvienas teminis reikalavimas privalo būti dokumentuojami ir saugomi. Ne visi atskiri reikalavimai gali būti taikomi kiekvienai užduočiai; jei reikalavimai netaikomi, privalo būti dokumentuotas ir išsaugotas pagrindimas. Atitiktis teminiam reikalavimui yra privaloma ir bus vertinama atliekant kokybės vertinimus.

[Daugiau informacijos rasite Kibernetinio saugumo teminio reikalavimo naudotojo vadove.](#)

Kibernetinis saugumas

Nacionalinis standartų ir technologijų institutas (NIST) kibernetinį saugumą apibrėžia taip: "Gebėjimas apsaugoti arba apginti kibernetinės erdvės naudojimą nuo kibernetinių atakų." Kibernetinis saugumas yra visa apimančio informacijos saugumo pogrupis, kurį NIST



apibrėžia taip: "Informacijos ir informacinių sistemų apsauga nuo neteisėtos prieigos, naudojimo, atskleidimo, sutrikdymo, pakeitimo ar sunaikinimo, siekiant užtikrinti konfidencialumą, vientisumą ir prieinamumą."

Kibernetinis saugumas mažina riziką stiprindamas bendrą kontrolės aplinką ir apsaugodamas organizacijos informacinį turtą nuo neteisėtos prieigos, sutrikdymo, pakeitimo ar sunaikinimo. Kibernetinės atakos gali sukelti tiesioginį ir netiesioginį poveikį, kuris dažnai būna didelis, nes kompiuteriai, tinklai, programos, duomenys ir jautri informacija yra svarbiausi daugelio organizacijų komponentai.

Kibernetinio saugumo valdysenos, rizikos valdymo ir kontrolės procesų vertinimas ir įvertinimas

Šiame teminiame reikalavime pateikiamas nuoseklus ir išsamus požiūris į kibernetinio saugumo valdysenos, rizikos valdymo ir kontrolės procesų kūrimo ir įgyvendinimo vertinimą. Šie reikalavimai yra minimalus bazinis kibernetinio saugumo vertinimo organizacijoje pagrindas.

VALDYSENA: Kibernetinio saugumo valdysenos vertinimas ir įvertinimas

Reikalavimai:

Vidaus auditoriai privalo įvertinti šiuos dalykus, susijusius su organizacijos kibernetinio saugumo valdysena:

- A.** Nustatyta ir periodiškai atnaujinama oficiali kibernetinio saugumo strategija ir tikslai. Apie kibernetinio saugumo tikslų įgyvendinimo atnaujinimus, įskaitant kibernetinio saugumo strategijai paremti skirtus išteklius ir biudžeto lėšas, periodiškai pranešama ir juos peržiūri valdyba.
- B.** Siekiant sustiprinti kontrolės aplinką, nustatyta ir periodiškai atnaujinama su kibernetiniu saugumu susijusi politika ir procedūros.
- C.** Nustatytos kibernetinio saugumo tikslus padedančios įgyvendinti funkcijos ir pareigos, taip pat nustatytas procesas, pagal kurį periodiškai vertinamos šias funkcijas atliekančių asmenų žinios, įgūdžiai ir gebėjimai.
- D.** Atitinkamos suinteresuotosios šalys įtraukiamos aptarti esamas kibernetinio saugumo aplinkos silpnąsias vietas ir kylančias grėsmes bei imtis veiksmų. Suinteresuotosios šalys apima vyresniąją vadovybę, operacijas, rizikos valdymą, žmogiškuosius išteklius, teisinius ir atitikties užtikrinimo klausimus, tiekėjus ir kt.

RIZIKOS VALDYMAS: Kibernetinio saugumo rizikos valdymo vertinimas ir įvertinimas

Reikalavimai:

Vidaus auditoriai privalo įvertinti šiuos dalykus, susijusius su organizacijos kibernetinio saugumo rizikos valdymu:



- A. Organizacijos rizikos vertinimo ir valdymo procesai apima kibernetinio saugumo grėsmių ir jų poveikio strateginių tikslų įgyvendinimui nustatymą, analizę, mažinimą ir stebėseną.
- B. Kibernetinio saugumo rizikos valdymas atliekamas visoje organizacijoje ir gali apimti šias sritis: informacinių technologijų, įmonės rizikos valdymo, žmogiškųjų išteklių, teisės, atitikties, operacijų, tiekimo grandinės, apskaitos, finansų ir kitas.
- C. Nustatyta atskaitomybė ir atsakomybė už kibernetinio saugumo rizikos valdymą. Nustatomas asmuo arba komanda, kurie periodiškai stebi ir teikia ataskaitas, kaip valdoma kibernetinio saugumo rizika, įskaitant išteklius, reikalingus rizikai mažinti ir naujoms kibernetinio saugumo grėsmėms nustatyti.
- D. Nustatytas procesas, skirtas greitai eskaluoti bet kokią kibernetinio saugumo riziką (kylančią ar anksčiau nustatytą), kuri pasiekia nepriimtina lygį pagal organizacijos nustatytas rizikos valdymo gaires arba taikomus teisinius ir reguliavimo reikalavimus. Turėtų atsižvelgti į finansinį ir nefinansinį kibernetinio saugumo rizikos poveikį.
- E. Nustatytas procesas, pagal kurį vadovybė ir darbuotojai informuojami apie kibernetinio saugumo riziką, o vadovybė periodiškai peržiūri problemas, spragas, trūkumus arba kontroliuoja savalaikiai pateiktus trūkumus ir jų šalinimą.
- F. Organizacijoje įdiegtas kibernetinio saugumo incidentų valdymo procesas, apimantis aptikimą, suvaldymą, atkūrimą ir analizę po incidento. Kibernetinio saugumo incidentų valdymo procesas periodiškai testuojamas.

KONTROLĖ: Kibernetinio saugumo kontrolės procesų vertinimas ir įvertinimas

Reikalavimai:

Vidaus auditoriai privalo įvertinti toliau išvardytus dalykus, susijusius su organizacijos kibernetinio saugumo kontrolės procesais:

- A. Nustatytas procesas, kuriuo siekiama užtikrinti, kad būtų įdiegtos tiek vidaus, tiek tiekėjų kontrolės priemonės, skirtos organizacijos sistemų ir duomenų konfidencialumui, vientisumui ir prieinamumui apsaugoti. Periodiškai atliekami vertinimai, siekiant nustatyti, ar kontrolės priemonės veikia taip, kad būtų skatinama siekti organizacijos kibernetinio saugumo tikslų ir greitai spręsti problemas.
- B. Nustatytas talentų valdymo procesas, apimantis mokymus, skirtus techninei kompetencijai, susijusiai su kibernetinio saugumo operacijomis, ugdyti ir palaikyti. Šis procesas periodiškai peržiūrimas.
- C. Nustatytas procesas, skirtas nuolat stebėti ir pranešti apie kylančias kibernetinio saugumo grėsmes ir pažeidžiamumus, taip pat prioretizuoti ir įgyvendinti kibernetinio saugumo operacijų gerinimo galimybes.
- D. Kibernetinis saugumas įtraukiamas į viso IT turto, įskaitant techninę ir programinę įrangą bei tiekėjų paslaugas, gyvavimo ciklo valdymą (parinkimą, naudojimą, priežiūrą ir eksploatavimo nutraukimą).



- E. Nustatyti kibernetinio saugumo stiprinimo procesai, įskaitant konfigūravimą, galutinių naudotojų įrenginių administravimą, šifravimą, spragų taisymą, naudotojų prieigos valdymą ir prieinamumo bei našumo stebėjimą. Kibernetinio saugumo aspektai įtraukiami į programinės įrangos kūrimą (DevSecOps).
- F. Nustatytos su tinklu susijusios kontrolės priemonės, pavyzdžiui, tinklo prieigos kontrolė ir segmentavimas; saugasienių naudojimas ir išdėstymas; ribotas prisijungimas iš išorinių tinklų ir prie jų; virtualus privatus tinklas (VPN) / nulinio pasitikėjimo tinklo prieiga (ZTNA); daiktų interneto (IoT) tinklo kontrolė ir įsilaužimo aptikimo / prevencijos sistemos (IDS ir IPS).
- G. Nustatytos galinio ryšio taškų, tokių kaip el. paštas, interneto naršyklės, vaizdo konferencijos, pranešimų siuntimas, socialinė žiniasklaida, debesijos ir dalijimosi failais protokolai, saugumo kontrolės. .

Apie Vidaus auditorių institutą

Vidaus auditorių institutas (IIA) yra tarptautinė profesinė asociacija, vienijanti daugiau nei 255 000 narių visame pasaulyje ir suteikusi daugiau nei 200 000 sertifikuotų vidaus auditorių (CIA®) pažymėjimų visame pasaulyje. Įkurtas 1941 m., IIA visame pasaulyje pripažįstamas kaip vidaus audito profesijos lyderis standartų, sertifikavimo, švietimo, mokslinių tyrimų ir techninių rekomendacijų srityje. Daugiau informacijos rasite svetainėje www.theiia.org.

Autorinės teisės

© 2025 Vidaus auditorių institutas, Inc. Visos teisės saugomos. Dėl leidimo dauginti kreipkitės adresu@theiia.org.

2025 m. vasaris



The Institute of
Internal Auditors

Pasaulinė būstinė

1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, JAV
Telefonas: +1-407-937-1111
Faksas: +1-407-937-1101

