Kiberdrošība

Topical Requirement

Aktuāla prasība

The Institute of
Internal Auditors

Kiberdrošības tematiskā prasība

Starptautisko profesionālās prakses ietvarstruktūru (International Professional Practices Framework®) veido Vispārējie iekšējā audita standarti (Global Internal Audit Standards™), Tematiskās prasības un Vispārējās vadlīnijas. Tematiskās prasības ir obligātas, un tās ir jāizmanto kopā ar Standartiem, kas ir autoritatīvs nepieciešamās prakses pamats.

Tematiskās prasības sniedz skaidras gaidas iekšējiem auditoriem, nosakot minimālo bāzes līmeni konkrētu riska tematu revīzijai. Organizācijas riska profils var prasīt, lai iekšējie auditori ņemtu vērā papildu tēmas aspektus.

Atbilstība tematiskajām prasībām palielinās iekšējā audita pakalpojumu sniegšanas konsekvenci un uzlabos iekšējā audita pakalpojumu un rezultātu kvalitāti un uzticamību. Visbeidzot, Aktuālās prasības paaugstina iekšējā audita profesijas prestižu.

Iekšējiem auditoriem jāpiemēro Tematiskās prasības saskaņā ar Globālajiem iekšējā audita standartiem. Atbilstība Aktuālajām prasībām ir obligāta apliecinājuma pakalpojumiem un ieteicama konsultāciju pakalpojumiem.

Tematiskā prasība ir piemērojama, ja tēma ir viena no šādām:

A. Iekšējā audita plāna uzdevuma priekšmets.
B. Identificēts, veicot uzdevumu.
C. Uzdevuma pieprasījuma priekšmets, kas nav iekļauts sākotnējā iekšējā audita plānā.

Ir jādokumentē un jāsaglabā pierādījumi par to, ka katras tematiskās prasības piemērojamība ir novērtēta. Ne visas atsevišķās prasības var būt piemērojamas katrā uzdevumā; ja prasības netiek piemērotas, ir jādokumentē un jāsaglabā pamatojums. Atbilstība tematiskajai prasībai ir obligāta, un tā tiks novērtēta kvalitātes novērtējuma laikā.

Lai iegūtu vairāk informācijas, skatiet Kiberdrošības tematisko prasību lietotāja rokasgrāmatu.

Kiberdrošība

Nacionālais standartu un tehnoloģiju institūts (NIST) kiberdrošību definē vienkārši kā "spēju aizsargāt vai aizstāvēt kibertelpas izmantošanu no kiberuzbrukumiem". Kiberdrošība ir visaptverošas informācijas drošības apakšgrupa, ko NIST definē kā "informācijas un informācijas sistēmu aizsardzību pret nesankcionētu piekļuvi, izmantošanu, izpaušanu, traucēšanu, pārveidošanu vai iznīcināšanu, lai nodrošinātu konfidencialitāti, integritāti un pieejamību".

Kiberdrošība samazina risku, stiprinot vispārējo kontroles vidi un aizsargājot organizācijas informācijas aktīvus no nesankcionētas piekļuves, traucējumiem, izmaiņām vai iznīcināšanas. Kiberuzbrukumi var radīt tiešu un netiešu ietekmi, kas bieži vien ir būtiska, jo datori, tīkli, programmas, dati un sensitīva informācija ir kritiski svarīgi lielākās daļas organizāciju komponenti.

Kiberdrošības pārvaldības, riska pārvaldības un kontroles procesu novērtēšana un izvērtēšana

Šī tematiskā prasība nodrošina konsekventu, visaptverošu pieeju kiberdrošības pārvaldības, riska pārvaldības un kontroles procesu izstrādes un īstenošanas novērtēšanai. Prasības ir minimālais pamats kiberdrošības novērtēšanai organizācijā.

PĀRVALDĪBA: Kiberdrošības pārvaldības novērtēšana un izvērtēšana

Prasības:

Iekšējiem revidentiem saistībā ar organizācijas kiberdrošības pārvaldību jānovērtē šādi aspekti:

A. Tiek izstrādāta un periodiski atjaunināta oficiāla kiberdrošības stratēģija un mērķi. Atjauninājumi par kiberdrošības mērķu sasniegšanu tiek periodiski paziņoti un izskatīti valdē, tostarp par resursiem un budžeta apsvērumiem kiberdrošības stratēģijas atbalstam.
B. Lai stiprinātu kontroles vidi, tiek izstrādātas un periodiski atjauninātas ar kiberdrošību saistītās politikas un procedūras.
C. Ir noteiktas lomas un pienākumi, kas atbalsta kiberdrošības mērķus, un ir izveidots process, lai periodiski novērtētu to personu zināšanas, prasmes un spējas, kuras pilda šīs lomas.
D. Attiecīgās ieinteresētās personas tiek iesaistītas, lai apspriestu esošās neaizsargātības un jaunos draudus kiberdrošības vidē un rīkotos saistībā ar tiem. Ieinteresēto pušu vidū ir augstākā līmeņa vadība, operatīvās darbības, riska vadība, cilvēkresursi, juridiskie jautājumi, atbilstība, piegādātāji un citi.

RISKU PĀRVALDĪBA: Kiberdrošības riska pārvaldības novērtēšana un izvērtēšana

Prasības:

Iekšējiem revidentiem saistībā ar organizācijas kiberdrošības riska pārvaldību ir jānovērtē šādi aspekti:

A. Organizācijas riska novērtēšanas un riska pārvaldības procesi ietver kiberdrošības draudu un to ietekmes uz stratēģisko mērķu sasniegšanu identificēšanu, analīzi, mazināšanu un uzraudzību.
B. Kiberdrošības riska pārvaldība tiek veikta visā organizācijā, un tā var ietvert šādas jomas: informācijas tehnoloģijas, uzņēmuma riska pārvaldību, cilvēkresursus,

juridisko jomu, atbilstību, operatīvo darbību, piegādes ķēdi, grāmatvedību, finanses un citas.

C. Ir noteikta atbildība un pienākumi par kiberdrošības riska pārvaldību. Ir noteikta persona vai komanda, kas periodiski uzrauga un ziņo, kā tiek pārvaldīti kiberdrošības riski, tostarp resursi, kas nepieciešami risku mazināšanai un jaunu kiberdrošības draudu identificēšanai.

D. Ir izveidots process, lai ātri eskalētu jebkuru kiberdrošības risku (jaunu vai iepriekš identificētu), kas sasniedz nepieņemamu līmeni saskaņā ar organizācijas noteiktajām riska pārvaldības vadlīnijām vai piemērojamajām juridiskajām un normatīvajām prasībām. Jāņem vērā kiberdrošības riska finansiālā un nefinansiālā ietekme.

E. Ir izveidots process, lai informētu vadību un darbiniekus par kiberdrošības riskiem un lai vadība periodiski pārskatītu problēmas, nepilnības, trūkumus vai kontroles kļūmes, savlaicīgi ziņojot par tām un novēršot trūkumus.

F. Organizācijā ir ieviests kiberdrošības incidentu reaģēšanas un atjaunošanas process, kas ietver atklāšanu, ierobežošanu, atjaunošanu un pēcincidentu analīzi. Incidentu reaģēšanas un atjaunošanas process tiek periodiski testēts.

KONTROLES: Kiberdrošības kontroles procesu novērtēšana un izvērtēšana

Prasības:

Iekšējiem revidentiem saistībā ar organizācijas kiberdrošības kontroles procesiem ir jānovērtē šādi aspekti:

A. Ir izveidots process, lai nodrošinātu gan iekšējās kontroles, gan piegādātāju kontroles, lai aizsargātu organizācijas sistēmu un datu konfidencialitāti, integritāti un pieejamību. Periodiski tiek veikti novērtējumi, lai noteiktu, vai kontroles darbojas tā, lai veicinātu organizācijas kiberdrošības mērķu sasniegšanu un ātru problēmu risināšanu.

B. Ir izveidots talantu pārvaldības process, kas ietver apmācību, lai attīstītu un uzturētu tehniskās kompetences, kas saistītas ar kiberdrošības operācijām. Process tiek periodiski pārskatīts.

C. Ir izveidots process, lai nepārtraukti uzraudzītu un ziņotu par jauniem kiberdrošības apdraudējumiem un ievainojamībām, kā arī identificētu, noteiktu prioritātes un īstenotu iespējas uzlabot kiberdrošības darbības.

D. Kiberdrošība ir iekļauta visu IT aktīvu, tostarp aparatūras, programmatūras un piegādātāju pakalpojumu, dzīves cikla pārvaldībā (atlase, lietošana, uzturēšana un ekspluatācijas pārtraukšana).

E. Ir izveidoti procesi kiberdrošības stiprināšanai, tostarp konfigurācijas, galalietotāju ierīču administrēšanas, šifrēšanas, labošanas, lietotāju piekļuves pārvaldības, kā arī pieejamības un veiktspējas uzraudzības procesi. Kiberdrošības apsvērumi ir iekļauti programmatūras izstrādē (DevSecOps).

F. Tiek ieviestas ar tīklu saistītas kontroles, piemēram, tīkla piekļuves kontrole un segmentācija, ugunsmūru izmantošana un izvietošana, ierobežoti savienojumi no

ārējiem tīkliem un uz tiem, virtuālais privātais tīkls (VPN) / piekļuve nulles uzticamības tīklam (ZTNA), lietu interneta (IoT) tīkla kontrole un ielaušanās atklāšanas/novēršanas sistēmas (IDS un IPS).

G. Tādi pakalpojumi kā e-pasts, interneta pārlūkprogrammas, videokonferences, ziņapmaiņa, sociālie mediji, mākoņi un failu koplietošanas protokoli tiek nodrošināti ar galapunktu komunikācijas drošības kontroli.

Par Iekšējo auditoru institūtu

Iekšējo auditoru institūts (IIA) ir starptautiska profesionāla asociācija, kas apvieno vairāk nekā 255 000 biedru visā pasaulē un ir piešķīrusi vairāk nekā 200 000 sertificēta iekšējā auditora® (CIA®) sertifikātu visā pasaulē. IIA ir dibināta 1941. gadā un visā pasaulē ir atzīta par iekšējā audita profesijas līderi standartu, sertifikācijas, izglītības, pētniecības un tehnisko vadlīniju jomā. Lai iegūtu vairāk informācijas, apmeklējiet www.theiia.org.

Autortiesības

2025. gada februāris

The Institute of Internal Auditors

Globālā galvenā mītne
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, ASV
Tālrunis: +1-407-937-1111
Fakss: +1-407-937-1101