Kiberdrošība

Aktuāla prasība

Lietotāja rokasgrāmata

The Institute of
Internal Auditors

Saturs

Tematisko prasību pārskats

Tematiskās prasības ir būtiska Starptautiskās profesionālās prakses ietvarstruktūras (International Professional Practices Framework®) sastāvdaļa, kā arī Globālie iekšējā audita standarti (Global Internal Audit Standards™) un Globālās vadlīnijas. Iekšējo auditoru institūts pieprasa, lai Aktuālās prasības tiktu izmantotas kopā ar Globālajiem iekšējā audita standartiem, kas ir autoritatīvs nepieciešamās prakses pamats. Šajā rokasgrāmatā ir atsauces uz Standartiem kā uz detalizētākas informācijas avotu.

Tematiskās prasības formalizē to, kā iekšējie auditori risina dominējošās riska jomas, lai veicinātu kvalitāti un konsekvenci profesijā. Tematiskās prasības nosaka pamatu un sniedz atbilstošus kritērijus, lai sniegtu apliecinājuma pakalpojumus, kas saistīti ar tematiskās prasības priekšmetu (13.4. standarts "Vērtēšanas kritēriji"). Atbilstība Aktuālajām prasībām ir obligāta apliecinājuma pakalpojumiem un ieteicama novērtēšanai konsultāciju pakalpojumu laikā. Tematiskās prasības nav paredzētas, lai aptvertu visus iespējamos aspektus, kas būtu jāņem vērā, veicot apliecinājuma uzdevumus; drīzāk tās ir paredzētas, lai nodrošinātu prasību minimālo kopumu, kas ļautu veikt konsekventu un uzticamu tēmas novērtējumu.

Tematiskās prasības ir skaidri saistītas ar IIA Trīs līniju modeli un Globālajiem iekšējā audita standartiem. Pārvaldība, riska pārvaldība un kontroles procesi ir galvenie tematisko prasību komponenti, kas atbilst 9.1. standartam "Pārvaldības, riska pārvaldības un kontroles procesu izpratne". Atsaucoties uz Trīs līniju modeli, pārvaldība ir saistīta ar valdi/vadības struktūru, riska pārvaldība - ar otro līniju, bet kontrole vai kontroles procesi - ar pirmo līniju. Lai gan vadība ir pārstāvēta gan pirmajā, gan otrajā līnijā, iekšējā audita funkcija ir attēlota trešajā līnijā kā neatkarīgs un objektīvs pārliecības sniedzējs, kas atskaitās valdei/vadības struktūrai (8. princips "Pārrauga valde").

Piemērojamība, risks un profesionāls vērtējums

Tematiskās prasības ir jāievēro, ja iekšējā audita funkcijas veic apliecinājuma uzdevumus par tēmām, par kurām pastāv tematiskās prasības, vai ja tematiskās prasības aspekti ir identificēti citos apliecinājuma uzdevumos.

Kā aprakstīts Standartos, riska novērtēšana ir svarīga revīzijas vadītāja plānošanas daļa. Lai noteiktu, kādus apliecinājuma uzdevumus iekļaut iekšējā audita plānā, vismaz reizi gadā ir jāizvērtē organizācijas stratēģijas, mērķi un riski (9.4. standarts "Iekšējā audita plāns"). Plānojot atsevišķus apliecinājuma uzdevumus, iekšējiem revidentiem jānovērtē ar uzdevumu saistītie riski (13.2. standarts "Uzdevuma riska novērtējums").

Ja uz risku balstītā iekšējā audita plānošanas procesa laikā tiek identificēta tematiskā prasība un tā tiek iekļauta audita plānā, tad tematiskās prasības ir jāizmanto, lai novērtētu šo

tēmu piemērojamo uzdevumu ietvaros. Turklāt, ja iekšējie auditori veic uzdevumu (kas iekļauts vai nav iekļauts plānā) un aktuālās prasības elementi parādās, tad aktuālā prasība ir jāizvērtē, lai to piemērotu kā daļu no uzdevuma. Visbeidzot, ja tiek pieprasīts uzdevums, kas sākotnēji nebija iekļauts plānā un ietver šo tēmu, jāizvērtē, vai tematiskā prasība ir piemērojama.

Piemērojot tematisko prasību, būtiska nozīme ir profesionālam vērtējumam. Riska novērtējumi nosaka revīzijas vadītāju lēmumus par to, kādus uzdevumus iekļaut iekšējā audita plānā (9.4. standarts "Iekšējā audita plāns"). Turklāt iekšējie auditori izmanto profesionālu vērtējumu, lai noteiktu, kādi aspekti tiks aptverti katrā uzdevumā (13.3. standarts "Uzdevuma mērķi un darbības joma", 13.4. standarts "Vērtēšanas kritēriji" un 13.6. standarts "Darba programma"). A pielikumā "Praktiskās piemērošanas piemēri" aprakstīts, kā iekšējie auditori nosaka, vai ir piemērojama Tematiskā prasība.

Jāsaglabā pierādījumi par to, ka katras tematiskās prasības piemērojamība ir izvērtēta, tostarp pamatojums, kas izskaidro, kāpēc kāda prasība nav iekļauta. Atbilstība tematiskajai prasībai jādokumentē, izmantojot revidenta profesionālo vērtējumu, kā aprakstīts 14.6. standartā "Uzdevuma dokumentācija".

Lai gan kiberdrošības tematiskā prasība sniedz kontroles procesu pamatprincipus, kas jāņem vērā, organizācijām, kuras novērtē kiberdrošības risku kā ļoti augstu, var būt nepieciešams novērtēt papildu aspektus.

Ja revīzijas vadītājs konstatē, ka iekšējā audita struktūrvienībai nav vajadzīgo zināšanu, lai veiktu revīzijas uzdevumus par aktuālo prasību tēmu, revīzijas uzdevumu var uzticēt ārpakalpojumu sniedzējam (3.1. standarts "Kompetence", 7.2. standarts "Revīzijas vadītāja kvalifikācija", 10.2. standarts "Cilvēkresursu vadība"). Pat tad ārpakalpojuma nodošana neatbrīvo iekšējās revīzijas funkciju no atbildības par atbilstību Tematiskajām prasībām. Galīgo atbildību par atbilstības nodrošināšanu saglabā revīzijas vadītājs. Turklāt, ja galvenais revīzijas vadītājs konstatē, ka iekšējā audita resursi ir nepietiekami, galvenajam revīzijas vadītājam jāinformē valde par nepietiekamo resursu ietekmi un par to, kā tiks risināts resursu trūkums (8.2. standarts Resursi).

Veiktspēja, dokumentācija un ziņošana

Piemērojot Tematiskās prasības, arī iekšējiem auditoriem ir jāievēro Standarti, veicot savu darbu saskaņā ar V jomu: Iekšējā audita pakalpojumu sniegšana. V jomas standarti apraksta uzdevumu plānošanu (13. princips "Efektīvi plānot uzdevumus"), uzdevumu veikšanu (14. princips "Veikt uzdevumus") un uzdevumu rezultātu paziņošanu (15. princips "Paziņot uzdevumu rezultātus un uzraudzīt rīcības plānus").

Tematiskās prasības ievērošanu var dokumentēt vai nu iekšējā audita plānā, vai uzdevuma darba dokumentos, pamatojoties uz revidentu profesionālo vērtējumu. Prasības var aptvert viens vai vairāki iekšējās revīzijas uzdevumi. Turklāt ne visas prasības var būt piemērojamas. Ir jāsaglabā pierādījumi, ka ir novērtēta tematiskās prasības piemērojamība, tostarp pamatojums, kas paskaidro visus izņēmumus.

C papildinājumā sniegto izvēles rīku var izmantot kā atsauci un dokumentēt iekšējo auditoru veikto darbu.

Kvalitātes nodrošināšana

Standarti nosaka, ka revīzijas vadītājam jāizstrādā, jāīsteno un jāuztur kvalitātes nodrošināšanas un uzlabošanas programma, kas aptver visus iekšējā audita funkcijas aspektus (8.3. standarts "Kvalitāte"). Par rezultātiem jāinformē valde un augstākā vadība. Paziņojumos jāziņo par iekšējā audita funkcijas atbilstību standartiem un darbības mērķu sasniegšanu.

Atbilstība tematiskajām prasībām tiks novērtēta kvalitātes novērtējumos. Lai sagatavotos kvalitātes novērtējumam, iekšējie auditori var izmantot C papildinājumā sniegto rīku.

Kiberdrošība

Kiberdrošība ir plaša tēma, kas saistīta ar lielāko daļu jebkuras organizācijas tehnoloģisko aspektu. Papildus informācijas tehnoloģijām kiberdrošība parasti ir uzņēmējdarbības procesu daļa, tāpēc iekšējiem revidentiem, plānojot, nosakot darbības jomu un veicot apliecinājuma uzdevumus, ir nepieciešams novērtēt ar kiberdrošību saistītos riskus.

Nacionālais standartu un tehnoloģiju institūts (NIST), kas ir daļa no ASV Tirdzniecības departamenta, kiberdrošību definē vienkārši kā "spēju aizsargāt vai aizstāvēt kibertelpas izmantošanu no kiberuzbrukumiem". Kiberdrošības tematiskā prasība koncentrējas uz ārējo perimetru, ko organizācijas nodrošina, lai mazinātu risku, ko rada neautorizēti lietotāji un ļaunprātīgi kiberdraudi. 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".

Kiberdrošības tematiskās prasības prasības ietver:

- Pārvaldība - skaidri definēti pamata kiberdrošības mērķi un stratēģijas, kas atbalsta organizācijas mērķus, politiku un procedūras.
- Risku pārvaldība - procesi, lai identificētu, analizētu, pārvaldītu un uzraudzītu kiberapdraudējumus, tostarp process, kas ļauj nekavējoties paziņot par kiberriskiem.
- Kontroles - vadības noteikti, periodiski novērtēti kontroles procesi kiberriska mazināšanai.

Apsvērumi

Iekšējie auditori var izmantot šādus apsvērumus, lai palīdzētu novērtēt kiberdrošības tematiskās prasības. Šie apsvērumi, kuros ir savstarpējas atsauces uz prasībām, ir ilustratīvi, bet nav obligāti. Iekšējiem revidentiem, nosakot, ko iekļaut novērtējumā, jāpaļaujas uz profesionālu vērtējumu.

Pārvaldības apsvērumi

Lai novērtētu, kā pārvaldības procesi tiek piemēroti kiberdrošības mērķiem, iekšējie auditori var pārbaudīt:

A. Formalizēts, dokumentēts kiberdrošības stratēģiskais plāns un mērķi, tostarp pierādījumi, ka valde periodiski (parasti reizi ceturksnī) pārskata kiberdrošības atjauninājumus, ko sniedz informācijas drošības funkcijas vadītājs, piemēram, galvenais informācijas drošības speciālists (CISO). Pierādījumi var ietvert ziņojumus par:
   - stratēģisko mērķu sasniegšanas uzraudzība.
   - Kiberdrošības mērķu un uzdevumu atbalstam nepieciešamais budžets.
   - Koncentrējieties uz riskiem un iekšējās kontroles mehānismiem, tostarp novēršanas progresu.
   - Galvenie darbības rādītāji (KPI), lai novērtētu panākumus.
   - Cilvēkresursi, kas nepieciešami, lai pieņemtu darbā, apmācītu un attīstītu kiberdrošības personālu.

B. Kiberdrošības procesu pārvaldībai izmantotās politikas, procedūras un cita attiecīgā dokumentācija, tostarp:
   - politikas, kas tiek pārskatītas un atjauninātas vismaz reizi gadā. Jaunu kiberrisku dēļ pārskatīšana un atjaunināšana var būt nepieciešama biežāk.
   - process, lai noteiktu, vai politikas un procedūras ir pietiekamas kiberdrošības operāciju atbalstam.
   - plaši pieņemtas sistēmas (NIST, COBIT un citas), lai stiprinātu kiberdrošības procesus un iekšējās kontroles mehānismus.

C. Kiberdrošības mērķu sasniegšanu veicinošas lomas un pienākumi, tostarp struktūra, kas nodrošina, ka kiberdrošības funkcija ir pakļauta tādam organizācijas līmenim, kuram ir pietiekama pārskatāmība, lai panāktu organizatorisko atbalstu.
   - procesu, lai periodiski novērtētu to darbinieku zināšanas, prasmes un iemaņas, kuri pilda kiberdrošības funkcijas.

D. Pierādījumi par sadarbību ar attiecīgajām ieinteresētajām personām (piemēram, augstāko vadību, operatīvajām darbībām, riska pārvaldību, cilvēkresursiem, juridisko dienestu, atbilstības nodrošināšanu, stratēģiskajiem piegādātājiem un citiem), tostarp saziņu par esošajiem un jaunajiem kiberriskiem un zināmajām potenciālajām

ievainojamībām. Saziņas pierādījumi var ietvert sanāksmju protokolus, ziņojumus vai e-pasta vēstules.

Riska pārvaldības apsvērumi

Lai novērtētu, kā riska pārvaldības procesi tiek piemēroti kiberdrošības mērķiem, iekšējie auditori var pārbaudīt:

A. Kā organizācija novērtē un pārvalda kiberdrošības riskus, tostarp kā tiek novērsti draudi un ievainojamības:
   - Sākotnēji identificēts un ziņots.
   - Analizē, lai novērtētu risku organizācijas mērķu sasniegšanai.
   - Samazināts, tostarp rīcības plāni, lai samazinātu risku līdz pieņemamam līmenim.
   - Uzraudzība, tostarp plāns pastāvīgai ziņošanai, līdz draudi ir pilnībā novērsti.

B. Kā organizācija periodiski saņem informāciju par kiberdrošības riska pārvaldību no tādām funkcionālajām jomām kā informācijas tehnoloģijas, uzņēmuma riska pārvaldība, cilvēkresursi, juridiskās, atbilstības, darbības, grāmatvedības un finanšu jomas. Informācijas iegūšanai var izmantot starpfunkcionālu kiberdrošības komandu vai IT vadības komiteju.

C. Kā organizācija ir piešķīrusi atbildību par kiberdrošības riska pārvaldību kādai personai vai komandai.
   - Atbildīgajai(-ām) personai(-ām) periodiski (reizi ceturksnī, mēnesī vai pēc vajadzības) jāinformē par kiberdrošības riska atjauninājumiem visā organizācijā, un tajā var būt iekļautas arī resursu prasības riska mazināšanas stratēģijām.

D. Kiberdrošības risku eskalācijas procesi, tostarp tas, kā tiek novērtēts, piešķirts un noteikts apdraudējuma vai riska līmenis. Pārskats var ietvert:
   - Organizācijas noteiktie riska līmeņi, piemēram, augsts, vidējs un zems, ar detalizētiem skaidrojumiem par katru riska līmeni un eskalācijas procedūrām katrai riska kategorijai.
   - Pašlaik identificēto kiberdrošības risku saraksts un katra riska gadījuma mazināšanas statuss.
   - Piemērojamās juridiskās, normatīvās un atbilstības prasības.
   - Gan finanšu, gan nefinanšu (piemēram, reputācijas) riska ietekme.

E. Kiberdrošības risku paziņošanas process vadībai un darbiniekiem, kas ietver:
   - periodiskas (vismaz reizi gadā) darbinieku kiberdrošības apmācības, piemēram, nepieteiktas, simulētas pikšķerēšanas kampaņas, lai pārbaudītu un uzraudzītu organizācijas informētību.

- atjaunināta informācija par esošo kiberdrošības problēmu novēršanu, norādot paredzamos pabeigšanas termiņus.
- neatbilstību uzraudzība, kas ietver jaunāko informāciju valdei un augstākajai vadībai.
- Draudu atkārtota novērtēšana, kad mainās organizācijas vēlme uzņemties risku un riska tolerance.

F. Procesi, ko organizācija ir ieviesusi attiecībā uz reaģēšanu uz incidentiem un to novēršanu, tostarp:

- Dokumentēts plāns, kas tiek pārskatīts un atjaunināts, jo organizācijas darbība laika gaitā mainās. Plānā jāiekļauj:
  - Incidentu atklāšana un ziņošana par tiem.
  - Kā incidenti tiek novērsti, lai novērstu turpmākus bojājumus.
  - Kā organizācija atgūsies un reaģēs, lai atsāktu darbību.
  - Kā tiks veikta incidenta analīze, lai noteiktu gūto pieredzi un to, kā novērst līdzīgus notikumus nākotnē.
- Periodiska (vismaz reizi gadā) testēšana (galda pārbaude) un rezultātu paziņošana augstākajai vadībai un attiecīgajām ieinteresētajām personām. Testēšanas rezultātā var tikt izstrādāti rīcības plāni.

Kontroles procesa apsvērumi

Lai novērtētu, kā kontroles procesi tiek piemēroti kiberdrošības mērķiem, iekšējie auditori var pārbaudīt:

A. Vadības pieeja efektīvas kiberdrošības iekšējās kontroles vides izveidei, tostarp:
- Organizācijas riska novērtēšanas procesā novērtēt un ieviest iekšējās kontroles mehānismus, kas nepieciešami, lai mazinātu paaugstinātus riskus un aizsargātu sensitīvus, kritiskus, personiskus vai konfidenciālus datus, pamatojoties uz organizācijas riska novērtēšanas procesu.
- Resursu prasību noteikšana, lai uzturētu galvenās kiberdrošības kontroles.
- Kontroles, kas balstās uz pārdevējiem, uzskatīšana par kontroles vides daļu, kas ietver pārdevēju pakalpojumu organizācijas kontroles (SOC) ziņojumu pārskatīšanu pirms darījumu attiecību uzsākšanas un attiecību laikā.
- Periodiska pārbaude, vai kiberdrošības kontroles darbojas tā, lai mazinātu riskus un palīdzētu sasniegt kiberdrošības mērķus.
- Iekšējās kontroles trūkumu novēršanas process vai iekšējās revīzijas funkcijas vai citu ticamības nodrošināšanas pakalpojumu sniedzēju veikto novērtējumu (piemēram, iekļūšanas testu) konstatējumu novēršana.

B. Organizācijas talantu pārvaldības process kiberdrošības speciālistu pieņemšanai darbā un apmācībai, tostarp tas, kā organizācija identificē iespējas palielināt

kiberdrošības speciālistu spējas, lai atbalstītu tehniskās zināšanas un uzlabotu organizācijas informētību par jauniem jautājumiem.

- Kā piemērus var minēt dalību apmācībās, iesaistīšanos zināšanu apmaiņas grupās un profesionālās tālākizglītības turpināšanu, kas ietver ar kiberdrošību saistītu sertifikātu iegūšanu.

C. Vadības process, kurā pastāvīgi identificē, nosaka prioritātes, uzrauga un ziņo par jauniem kiberdrošības apdraudējumiem un ievainojamībām, kas ir vērsts uz ikdienas darbībām. Pārskatā var iekļaut, ka ir izveidoti procesi, lai novērtētu draudus un ievainojamības, kas saistītas ar jaunām vai jaunām tehnoloģijām, piemēram, mākslīgā intelekta izmantošanu.

D. Vadības procesi un kontroles mehānismi, kas izveidoti, lai pārvaldītu un aizsargātu IT aktīvus visā to dzīves ciklā, tostarp aparatūras, programmatūras un piegādātāju pakalpojumu izvēli, lietošanu, uzturēšanu un ekspluatācijas pārtraukšanu. Aparatūra ietver serverus, tīkla iekārtas (piemēram, maršrutētājus vai ugunsmūrus), galddatorus, klēpjdatorus, mobilos tālruņus, planšetdatorus un perifērijas ierīces. Programmatūra ietver operētājsistēmas (piemēram, Windows), uzņēmuma resursu plānošanas programmatūru, lietojumprogrammas, antivīrusu programmas un citas. Aparatūras un programmatūras apsvērumi var ietvert:

- Organizācija izmanto šifrēšanu, pretvīrusu programmatūru, mobilo ierīču pārvaldību, sarežģītas paroles prasības, virtuālo privāto tīklu (VPN)/nulles uzticamības tīklu (ZTN) autentifikācijai un periodisku programmaparatūras atjaunināšanu.
- Aktīvu pārvaldības process, kas nodrošina, ka uzņēmuma izsniegtajai aparatūrai ir atbilstoša drošības konfigurācija, to izsniedzot, un pareiza iznīcināšana, kad aktīvi tiek izņemti no lietošanas.
- Ar datubāzēm saistītas kontroles, kas ietver lietotāju un administratoru piekļuves ierobežošanu, šifrēšanas nodrošināšanu, datu bāzu dublēšanu un testēšanu, kā arī stingras tīkla drošības kontroles.
- Kā kiberdrošības draudi vai ievainojamības tiek ņemti vērā sistēmas izstrādes dzīves ciklā (SDLC).
- Izstrādes, drošības un operāciju (DevSecOps) pieeja, ko izmanto, lai nodrošinātu, ka programmatūras izstrādes process ietver kiberdrošību un proaktīvi identificē ievainojamības.

E. Kiberdrošības stiprināšanai izmantotie procesi, tostarp:

- Drošības iestatījumu konfigurēšana, lai samazinātu kiberdrošības risku.
- Mobilo ierīču administrēšana (tostarp e-pasta un lietojumprogrammu lietošana) ir konfigurēta tā, lai mazinātu kiberdrošības riskus un varētu attālināti pārvaldīt, ja lietotāja ierīce ir apdraudēta.
- Šifrēšanas izmantošana datiem "miera stāvoklī", piemēram, informācijai, kas glabājas cietajā diskā, vai datiem "tranzītā", piemēram, e-pasta vēstuļu šifrēšanai.

- Serveru vai programmatūras (piemēram, operētājsistēmas) labošana, izmantojot jaunākās drošības versijas.
- Lietotāju piekļuves pārvaldība, piemēram, izmantojot daudzfaktoru autentifikāciju (MFA) un unikālus lietotāja ID ar sarežģītām parolēm, kuru derīguma termiņš periodiski beidzas.
- ieviestās uzraudzības kontroles, lai noteiktu, vai pieejamība un resursu izmantošana darbojas atbilstoši, ļaujot pārskatīt un analizēt iespējamās kiberdrošības problēmas, kas apdraud veiktspēju.
- Kiberdrošības integrēšana SDLC, lai identificētu un novērstu kiberdrošības ievainojamības pirms programmatūras nodošanas ražošanā.

F. Ar tīklu saistītās kontroles, kas nodrošina organizācijas perimetru, tostarp to, kā organizācija izmanto:
   - Tīkla segmentācija.
   - Ugunsmūri.
   - Lietotāja piekļuves kontrole.
   - Ierobežojumi gan ārējiem, gan iekšējiem savienojumiem.
   - Kontroles, kas saistītas ar lietu internetu (IoT) savstarpēji savienotiem tīkliem.
   - ielaušanās atklāšanas/novēršanas sistēmas, lai novērstu, atklātu un atjaunotu kiberdrošības uzbrukumus.

G. Kontroles, kas saistītas ar galapunktu komunikācijas drošības kontrolēm, kuras piemērojamas tādiem pakalpojumiem kā e-pasts, interneta pārlūkprogrammas, videokonferences, ziņapmaiņa (Zoom, MS Teams un citi), sociālie mediji, mākoņi un failu koplietošanas protokoli. Kontroles var ietvert noteiktu failu paplašinājumu (piemēram, .exe failu) izmantošanas ierobežošanu un daudzfaktoru autentifikāciju failu koplietošanai.

A pielikums. Praktiskā pielietojuma piemēri

Turpmākajos piemēros aprakstīti scenāriji, kuros būtu piemērojama kiberdrošības tematiskā prasība:

1. piemērs: Kiberdrošība ir noteikta iekšējās revīzijas uzdevumam, kas iekļauts iekšējās revīzijas plānā.

Ja iekšējā audita funkcija pabeidz uz risku balstītu plānošanas procesu un iekšējā audita plānā iekļauj vienu vai vairākus uzdevumus par kiberdrošību, tad, veicot šādus uzdevumus, ir obligāti jāievēro tematiskā prasība. Atbilstību var panākt, iekļaujot prasības vienā vai vairākos uzdevumos iekšējā audita plānā.

Kiberdrošība ir plaša tēma, un ne visas tematiskās prasības var attiekties uz katru uzdevumu. Ja iekšējie auditori piemēro profesionālu vērtējumu un nosaka, ka viena vai vairākas kiberdrošības tematiskās prasības prasības nav piemērojamas un tāpēc nav iekļaujamas uzdevumā, iekšējiem auditoriem jādokumentē un jāsaglabā pamatojums šo prasību izslēgšanai. Piemēram, dažu prasību izslēgšanas pamatojums varētu būt tāds, ka iekšējā audita funkcija veic dažādus kiberdrošības uzdevumus rotācijas kārtībā vai ir noteikusi, ka riska nozīmīgums konkrētajā uzdevumā ir neliels.

2. piemērs: Kiberdrošības riski tiek identificēti revīzijas uzdevuma laikā, kas nav vērsts uz kiberdrošību.

Iekšējie auditori var identificēt kiberdrošības riskus, novērtējot procesu, kas nav tieši saistīts ar kiberdrošību. Piemēram, iekšējie auditori var novērtēt kreditoru parādu procesu uzdevumā, kas nav vērsts uz kiberdrošību, un, plānojot uzdevumu, neidentificēt kiberdrošības riskus kā tādus, kas ietilpst uzdevuma darbības jomā. Tomēr pēc sākotnējās izpētes veikšanas iekšējie auditori konstatē, ka šādiem riskiem ir jābūt uzdevuma darbības jomā; piemēram, viņi identificē kiberdrošības riskus, kas saistīti ar sākotnējā pirkuma pasūtījuma pieprasījuma iesniegšanu internetā (13.2. standarts "Uzdevuma riska novērtējums").

Kad attiecīgie riski ir identificēti, iekšējiem auditoriem jāpārskata kiberdrošības tematiskā prasība un jānosaka, kuras prasības ir piemērojamas. Šajā piemērā viņi varētu izslēgt kiberdrošības pārvaldības procesu vai kiberdrošības risku pārvaldības procesu. Viņiem uzdevuma darba dokumentos jādokumentē pamatojums, kāpēc izslēgtas citas kiberdrošības tematiskās prasības, un dokumentācija jāsaglabā.

3. piemērs: tiek pieprasīts kiberdrošības uzdevums, kas sākotnēji nebija iekļauts iekšējā audita plānā.

Ieinteresētās puses, piemēram, valde, vadība vai regulators, var lūgt iekšējos auditorus veikt kiberdrošības novērtējumus ārpus sākotnējā revīzijas plāna. Piemēram, ja organizācijas ir kļuvušas par kiberuzbrukuma mērķi, valde var pieprasīt, lai iekšējais auditors novērtē kiberdrošības kontroles mehānismus. Tematiskā prasība ir piemērojama, prasības ir jānovērtē un visi izņēmumi jādokumentē.

B pielikums. Kartēšana ar ietvarstruktūrām

Organizācijai var būt savi kiberdrošības pasākumi, izmantojot riska pārvaldības un vadības sistēmas, piemēram, COBIT vai NIST. Iekšējie auditori, iespējams, jau ir izstrādājuši revīzijas programmas un testēšanas procedūras, pamatojoties uz šīm sistēmām. Iekšējiem auditoriem būtu jāsaskaņo plānotā kiberdrošības kontroles testēšana ar Tematisko prasību, lai nodrošinātu atbilstošu aptvērumu. Turpmāk dotajā tabulā ir attēlotas kiberdrošības tematiskās prasības un trīs plaši izmantotie ietvari: NIST kiberdrošības ietvarstruktūra 2.0, COBIT 2019 un NIST 800-53. Šie ietvari ir attēloti, jo tie ir viegli pieejami bez maksas.

Pārvaldības prasības	Pamatprincipi Atsauces		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Tiek izstrādāta un periodiski atjaunināta oficiāla kiberdrošības stratēģija un mērķi. Periodiski tiek paziņoti atjauninājumi par kiberdrošības mērķu sasniegšanu, un valde tos pārskata, tostarp resursus un budžeta apsvērumus kiberdrošības stratēģijas atbalstam.	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. Ar kiberdrošību saistītā politika un procedūras ir izstrādātas, periodiski atjauninātas un stiprina kontroles vidi.	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. Ir noteiktas lomas un pienākumi, kas atbalsta kiberdrošības mērķu sasniegšanu, un pastāv process, lai periodiski novērtētu šo lomu izpildītāju zināšanas, prasmes un iemaņas.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Attiecīgās ieinteresētās personas tiek iesaistītas, lai apspriestu un risinātu esošās ievainojamības un jaunos draudus kiberdrošības vidē. Ieinteresētās personas ietver augstākā līmeņa vadību, darbības, riska pārvaldību, cilvēkresursus, juridisko jomu, atbilstību, piegādātājus un citus.	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
Riska pārvaldības prasības	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Organizācijas riska novērtēšanas un riska pārvaldības procesi ietver kiberdrošības draudu un to ietekmes uz stratēģisko mērķu sasniegšanu identificēšanu, analīzi, mazināšanu un uzraudzību.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Kiberdrošības riska pārvaldība tiek veikta visā organizācijā, kas var ietvert šādas jomas: informācijas tehnoloģijas, uzņēmuma riska pārvaldība, cilvēkresursi, juridiskās, atbilstības, darbības, piegādes ķēdes, grāmatvedība, finanses un citas.	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. Ir noteikta atbildība un pienākumi par kiberdrošības risku pārvaldību, un ir noteikta persona vai komanda, kas periodiski uzrauga un ziņo, kā tiek pārvaldīti kiberdrošības riski, tostarp resursi, kas nepieciešami riska mazināšanai un jaunu kiberdrošības draudu identificēšanai.	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. Ir izveidots process, lai ātri eskalētu jebkuru kiberdrošības risku (jaunu vai iepriekš identificētu), kas sasniedz nepieņemamu līmeni, pamatojoties uz organizācijas noteiktajām riska pārvaldības pamatnostādnēm vai lai ievērotu piemērojamās juridiskās un normatīvās prasības. Jāņem vērā gan kiberdrošības riska finansiālā, gan nefinansiālā ietekme.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Ir izveidots process, lai informētu vadību un darbiniekus par kiberdrošības riskiem un lai vadība periodiski pārskatītu problēmas, nepilnības, trūkumus vai kontroles kļūmes, ziņotu par tām un veiktu to novēršanu.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Organizācija ir ieviesusi kiberdrošības incidentu reaģēšanas un atjaunošanas procesu, kas ietver atklāšanu, ierobežošanu, atjaunošanu un pēcincidentu analīzi. Incidentu reaģēšanas un atjaunošanas process tiek periodiski testēts.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Kontroles procesa prasības	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Ir izveidots process, kas nodrošina gan iekšējās kontroles, gan piegādātāju kontroles, lai aizsargātu organizācijas sistēmu un datu konfidencialitāti, integritāti un pieejamību. Kontroles tiek periodiski novērtētas, lai noteiktu, vai tās darbojas tā, lai veicinātu organizācijas kiberdrošības mērķu sasniegšanu un savlaicīgu problēmu risināšanu.	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. Kiberdrošības operācijām ir izveidots un periodiski pārskatīts talantu pārvaldības process, kas ietver apmācību iespējas, lai attīstītu un uzturētu tehniskās kompetences.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04

C. Ir izveidots process, lai nepārtraukti uzraudzītu un ziņotu par jauniem kiberdrošības apdraudējumiem un ievainojamībām, kā arī lai identificētu, noteiktu prioritātes un īstenotu iespējas uzlabot kiberdrošības darbības.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Kiberdrošība ir iekļauta visu IT aktīvu, tostarp aparatūras, programmatūras un piegādātāju pakalpojumu, dzīves cikla pārvaldībā (atlase, lietošana, uzturēšana un ekspluatācijas pārtraukšana).	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. Ir izveidoti procesi kiberdrošības veicināšanai, tostarp konfigurācijas, galalietotāju ierīču administrēšanas, šifrēšanas, labošanas, lietotāju piekļuves pārvaldības, kā arī pieejamības un veiktspējas uzraudzības procesi. Kiberdrošības apsvērumi ir iekļauti programmatūras izstrādē (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. Ir ieviestas ar tīklu saistītas kontroles, piemēram, piekļuves kontrole un segmentācija, ugunsmūru izmantošana un izvietošana, ierobežoti savienojumi no ārējiem tīkliem un uz tiem, virtuālais privātais tīkls (VPN)/notaļ uzticama piekļuve tīklam (ZTNA), lietiskā interneta (IoT) tīkla kontroles, kā arī ielaušanās atklāšanas/novēršanas sistēmas (IDS un IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
G. Ir izveidotas galapunktu saziņas drošības pārbaudes attiecībā uz tādiem pakalpojumiem kā e-pasts, interneta pārlūkprogrammas, videokonferences, ziņapmaiņa, sociālie mediji, mākoņdatošana un failu koplietošanas protokoli.	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 papildinājums. Papildu dokumentācijas rīks

No iekšējiem revidentiem tiek sagaidīts profesionāls vērtējums, lai noteiktu prasību piemērojamību, pamatojoties uz riska novērtējumu, un pienācīgi dokumentētu dažu prasību nepiemērošanu. Aktuālo prasību var dokumentēt iekšējā audita plānā vai uzdevuma darba dokumentos, pamatojoties uz revidenta profesionālo spriedumu. Prasības var attiekties uz vienu vai vairākiem iekšējā audita uzdevumiem. Turklāt ne visas prasības var būt piemērojamas. Zemāk dotajā izdrukājamā veidlapā ir sniegta viena no iespējām, kā dokumentēt atbilstību kiberdrošības tematiskajai prasībai, taču tās izmantošana nav obligāta.

Kiberdrošība - pārvaldība

Prasība	Izpildītais segums vai izslēgšanas pamatojums	Atsauce uz dokumentāciju
A. Tiek izstrādāta un periodiski atjaunināta oficiāla kiberdrošības stratēģija un mērķi. Periodiski tiek paziņoti atjauninājumi par kiberdrošības mērķu sasniegšanu, un valde tos pārskata, tostarp resursus un budžeta apsvērumus kiberdrošības stratēģijas atbalstam.		
B. Ar kiberdrošību saistītā politika un procedūras ir izstrādātas, periodiski atjauninātas un stiprina kontroles vidi.		
C. Ir noteiktas lomas un pienākumi, kas atbalsta kiberdrošības mērķus, un pastāv process, lai periodiski novērtētu to personu zināšanas, prasmes un iemaņas, kuras pilda šīs lomas.		
D. Attiecīgās ieinteresētās personas tiek iesaistītas, lai apspriestu un risinātu esošās ievainojamības un jaunos draudus kiberdrošības vidē. Ieinteresētās personas ietver augstākā līmeņa vadību, darbības, riska pārvaldību, cilvēkresursus, juridisko jomu, atbilstību, piegādātājus un citus.		

Kiberdrošība - riska pārvaldība

Prasība	Izpildītais segums vai izslēgšanas pamatojums	Atsauce uz dokumentāciju
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 pārvaldība, cilvēkresursi, juridiskās, atbilstības, darbības, piegādes ķēdes, grāmatvedība, finanses un citas.		
C. Ir noteikta atbildība un pienākumi par kiberdrošības riska pārvaldību. Ir noteikta persona vai komanda, kas periodiski uzrauga un ziņo par to, kā tiek pārvaldīti kiberdrošības riski, tostarp par resursiem, 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 pamatnostādnēm vai piemērojamām 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 un novēršot trūkumus.		

Prasība	Izpildītais segums vai izslēgšanas pamatojums	Atsauce uz dokumentāciju
F. Organizācija ir ieviesusi kiberdrošības incidentu reaģēšanas un seku novēršanas procesu, tostarp atklāšanas, ierobežošanas, seku novēršanas un pēcincidentu analīzes procesu. Incidentu reaģēšanas un atjaunošanas process tiek periodiski testēts.		

Kiberdrošība - kontroles procesi

Prasība	Izpildītais segums vai izslēgšanas pamatojums	Atsauce uz dokumentāciju
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 saistībā 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.		

Prasība	Izpildītais segums vai izslēgšanas pamatojums	Atsauce uz dokumentāciju
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 veicināšanai, 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. Ir ieviestas ar tīklu saistītas kontroles, piemēram, piekļuves kontrole un segmentācija, ugunsmūru izmantošana un izvietošana, ierobežoti savienojumi no ārējiem tīkliem un uz tiem, virtuālais privātais tīkls (VPN)/notaļ uzticama piekļuve tīklam (ZTNA), lietu interneta (IoT) tīkla kontrole un ielaušanās atklāšanas/novēršanas sistēmas (IDS un IPS).		
G. Ir izveidotas galapunktu saziņas drošības pārbaudes tādiem pakalpojumiem kā e-pasts, interneta pārlūkprogrammas, videokonferences, ziņapmaiņa, sociālie mediji, mākoņdatošana un failu koplietošanas protokoli.		

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. Sīkāka informācija www.theiia.org.

Atruna

IIA publicē šo dokumentu informatīviem un izglītojošiem mērķiem. Šis materiāls nav paredzēts, lai sniegtu galīgas atbildes uz konkrētiem individuāliem apstākļiem, un tāpēc tas ir paredzēts tikai kā ceļvedis. IIA iesaka meklēt neatkarīga eksperta padomu, kas tieši attiecas uz jebkuru konkrētu situāciju. IIA neuzņemas nekādu atbildību par to, ka kāds paļaujas tikai uz šo materiālu.

Autortiesības

2025. gada februāris

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