Küberturvalisus

Topical Requirement

Valdkondlik nõue

The Institute of
Internal Auditors

Küberturvalisuse valdkondlik nõue

Rahvusvahelise kutsetegevuse raampõhimõtted (International Professional Practices Framework®) koosnevad Ülemaailmsetest siseauditi standarditest (Global Internal Audit Standards™), valdkondlikest nõuetest ja ülemaailmsetest juhistest. Valdkondlikud nõuded on kohustuslikud ning neid tuleb kasutada koos Ülemaailmsete siseauditi standarditega, mis on nõutava praktika tunnustatud aluseks.

Valdkondlikud nõuded annavad siseaudiitoritele selged ootused, kehtestades konkreetsete riskiteemade auditeerimiseks miinimumnõuded. Organisatsiooni riskiprofiilist tingituna võib siseaudiitoritel olla vajalik kaaluda antud valdkonna täiendavaid aspekte.

Vastavus valdkondlikele nõuetele suurendab siseauditi teenuste osutamise järjepidevust ning parandab siseauditi teenuste ja tulemuste kvaliteeti ja usaldusväärsust. Viimaks, valdkondlikud nõuded edendavad siseauditi kutseala.

Siseaudiitorid peavad valdkondlikke nõudeid rakendama kooskõlas Ülemaailmsete siseauditi standarditega. Vastavus valdkondlikele nõuetele on kindlustandvate teenuste puhul kohustuslik ja nõuandvate teenuste puhul soovituslik.

Valdkondlik nõue on kohaldatav järgmistel juhtudel:

A. Siseauditi tööplaanis sisaldub selleteemaline töö.
B. Valdkondliku nõude teema asjakohasus tuvastatakse töö teostamisel.
C. Esitatakse selleteemaline töö ettepanek või tellimus (ei sisaldu esialgses siseauditi tööplaanis).

Iga valdkondlikus nõudes sisalduva nõude kohaldatavuse hindamine peab olema dokumenteeritud ning asjakohane tõendusmaterjal tuleb säilitada. Kõik üksikud nõuded ei pruugi iga töö puhul olla alati kohaldatavad; kui mingit üksikut nõuet ei kohaldata, tuleb põhjendus dokumenteerida ja säilitada. Valdkondlikele nõuetele vastavus on kohustuslik ja seda hinnatakse kvaliteedi hindamiste käigus.

Lisateave on leitav küberturvalisuse valdkondliku nõude kasutusjuhendist.

Küberturvalisus

Riiklik standardite ja tehnoloogia instituut (NIST) defineerib küberturvalisust lihtsalt kui "võimet turvata või kaitsta küberruumi kasutatavust küberrünnakute eest". Küberturvalisus on üldise infoturbe alamharu. Infoturvet määratleb NIST järgmiselt: "Teabe ja infosüsteemide kaitsmine volitamata juurdepääsu, kasutamise, avalikustamise, katkestuse, muutmise või hävitamise eest, et tagada konfidentsiaalsus, terviklus ja käideldavus."

Küberturvalisus vähendab riske, tugevdades üldist kontrollikeskkonda ja kaitstes organisatsiooni infovarasid volitamata juurdepääsu, katkestuse, muutmise või hävitamise eest. Küberrünnakud võivad põhjustada märkimisväärseid otseseid ja kaudseid mõjusid, sest arvutid, võrgud, programmid, andmed ja tundlik teave on enamiku organisatsioonide kriitilise tähtsusega osad.

Küberturvalisuse valitsemise, riskijuhtimise ja kontrolliprotsesside hindamine ja analüüs

Valdkondlik nõue annab järjepideva ja tervikliku lähenemisviisi küberturvalisuse valitsemise, riskijuhtimise ja kontrolliprotsesside kavandamise ja rakendamise hindamiseks. Nõuded määravad organisatsiooni küberturvalisuse hindamise miinimumnõuded.

VALITSEMINE: Küberturvalisuse valitsemise hindamine ja analüüs

Nõuded:

Siseaudiitorid peavad hindama organisatsiooni küberturvalisuse valitsemist, keskendudes järgmistele aspektidele:

- **A.** Ametlik küberturvalisuse strateegia ja eesmärgid on kehtestatud ning neid ajakohastatakse perioodiliselt. Küberturvalisuse eesmärkide täitmise kohta esitatakse kõrgemale juhtorganile perioodilisi ülevaateid, mis sisaldavad sealhulgas hinnangut strateegia elluviimiseks vajalike ressursside ja eelarve olemasolu kohta.
- **B.** Kontrollikeskkonna tugevdamiseks on kehtestatud küberturvalisusega seotud poliitikad ja protseduurid ning neid ajakohastatakse perioodiliselt.
- **C.** Küberturvalisuse eesmärkide saavutamiseks on määratud selged rollid ja vastutusvaldkonnad ning on kehtestatud protsess, mille abil hinnatakse perioodiliselt vastutavate isikute teadmisi, oskusi ja võimeid.
- **D.** Asjaomased huvirühmad osalevad küberturvalisuse keskkonnas esinevate nõrkuste ja tekkivate ohtude aruteludes ning tegelevad nende riskide maandamisega. Huvirühmade hulka kuuluvad tippjuhtkond, tegevjuhtkond, riskijuhtimine, personalijuhtimine, juriidiline osakond, vastavuskontroll, tarnijad/pakkujad ja muud seotud osapooled.

RISKIJUHTIMINE: Küberturvalisuse riskijuhtimise hindamine ja analüüs

Nõuded:

Siseaudiitorid peavad hindama organisatsiooni küberturvalisuse riskide juhtimist, keskendudes järgmistele aspektidele:

- **A.** Organisatsiooni riskihindamise ja -juhtimise protsessid hõlmavad küberturvalisuse ohtude tuvastamist, analüüsimist, maandamist ja pidevat jälgimist ning nende mõju hindamist strateegiliste eesmärkide saavutamisele.
- **B.** Küberturvalisuse riskijuhtimine on rakendatud kogu organisatsioonis ja see võib hõlmata järgmisi valdkondi: infotehnoloogia, ettevõtte riskijuhtimine,

personalijuhtimine, juriidilised küsimused, vastavuskontroll, organisatsiooni igapäevased protsessid, tarneahel, raamatupidamine, finantsjuhtimine ja muud seotud valdkonnad.

C. Küberturvalisuse riskijuhtimise protsessi eest on määratud kindel vastutaja. Määratud on isik või meeskond, kes jälgib perioodiliselt küberturvalisuse riskide juhtimist ning teeb selle kohta ülevaateid. Sealhulgas teavitab riskide maandamiseks vajalikest ressurssidest ja tuvastab uusi tekkivaid küberohtusid.

D. Organisatsioonis on kehtestatud protsess, mille abil saab kiiresti eskaleerida mis tahes küberturberiske (nii uusi kui ka varem tuvastatuid), mis ületavad aktsepteeritava taseme vastavalt organisatsiooni riskijuhtimise juhistele või kohaldatavatele õiguslikele ja regulatiivsetele nõuetele. Arvesse tuleb võtta küberturberiskide rahalist ja mitterahalist mõju.

E. Organisatsioonis on loodud protsess küberturberiskide teadlikkuse suurendamiseks juhtkonna ja töötajate seas. Juhtkond peab perioodiliselt üle vaatama probleemid, puudujäägid, nõrkused või kontrollimeetmete tõrked ning tagama nende õigeaegse raporteerimise ja kõrvaldamise.

F. Organisatsioonis on rakendatud küberturbeintsidentide haldamise ja taastamise protsessi, mis hõlmab tuvastamist, tõkestamist, taastamist ja intsidendijärgset analüüsi. Seda protsessi testitakse perioodiliselt.

KONTROLLID: Küberturvalisuse kontrolliprotsesside hindamine ja analüüs

Nõuded:

Siseaudiitorid peavad hindama organisatsiooni küberturvalisuse kontrolliprotsesse, keskendudes järgmistele aspektidele:

A. Organisatsioonis on kehtestatud protsess, millega tagatakse nii sisekontrolli kui ka tarnijapõhiste kontrollimeetmete rakendamine, et kaitsta organisatsiooni süsteemide ja andmete konfidentsiaalsust, terviklust ja käideldavust. Kontrollide tõhusust hinnatakse perioodiliselt, et tagada küberturbe eesmärkide täitmine ning probleemide kiire lahendamine.

B. Organisatsioonis on kehtestatud kompetentside halduse protsess, mis hõlmab koolitust küberturbe tegevustega seotud tehnilise pädevuse arendamiseks ja säilitamiseks. Seda protsessi vaadatakse perioodiliselt üle.

C. Organisatsioonis on loodud pidev jälgimis- ja aruandlusprotsess küberturbe ohtude ja nõrkuste tuvastamiseks ning küberturbe parandamise võimaluste määratlemiseks, prioriseerimiseks ja elluviimiseks.

D. Küberturvalisus on kaasatud IT-varade elutsükli kõikidesse etappidesse (valimine, kasutamine, hooldus ja kasutusest kõrvaldamine) ning kohaldub riistvarale, tarkvarale ja tarnijateenustele.

E. Organisatsioonis on rakendatud protsessid küberturvalisuse tugevdamiseks, sealhulgas süsteemide konfiguratsioonid, lõppkasutaja seadmete haldamine, krüpteerimine, turvapaikamine, kasutajate juurdepääsu haldamine ning käideldavuse

ja jõudluse monitoorimine. Küberturvalisuse nõuded on integreeritud tarkvara arendamisse (DevSecOps).

F. Võrguga seotud kontrollimeetmed on kehtestatud, sealhulgas võrgule juurdepääsu kontroll ja segmenteerimine; tulemüüride kasutamine ja paigutamine; piiratud ühendused sise- ja välisvõrkude vahel, virtuaalse privaatvõrgu (VPN) ja nullusaldusvõrgu(zero trust) (ZTNA) lahendused; asjade interneti (IoT) võrgukontrollid ning sissetungide tuvastus- ja ennetussüsteemid (IDS ja IPS).

G. Lõppseadme sidekanalite turvameetmed on kehtestatud selliste teenuste jaoks nagu e-post, internetibrauserid, videokonverentsid, sõnumside, sotsiaalmeedia, pilveteenused ja failijagamisprotokollid.

Veebruar 2025

The Institute of Internal Auditors

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