Küberturvalisus

Topical Requirement

Valdkondlik nõue

Kasutusjuhend

The Institute of
Internal Auditors

Sisu

Ülevaade valdkondlikest nõuetest **2**

Kohaldatavus, risk ja ametialane hinnang 2

Kaalutlused 5

Lisa A. Praktilised rakendusnäited **10**

Lisa B. Raamistikega kaardistamine **12**

Lisa C. Vabatahtlik dokumenteerimisvahend **17**

Ülevaade valdkondlikest nõuetest

Valdkondlikud nõuded on Rahvusvahelise kutsetegevuse raampõhimõtete (International Professional Practices Framework®) oluline osa koos Ülemaailmsete siseauditi standardite (Global Internal Audit Standards™) ja ülemaailmsete juhistega. Rahvusvaheline Siseaudiitorite Instituut eeldab, et valdkondlikke nõudeid kasutataks koos Ülemaailmsete siseauditi standarditega, mis moodustavad kohustusliku praktika tunnustatud aluse. Juhendis on toodud läbivalt viited standarditele, pakkudes põhjalikumat teavet.

Valdkondlikud nõuded määratlevad, kuidas siseaudiitorid käsitlevad levinud riskivaldkondi, edendades seeläbi kutseala kvaliteeti ja järjepidevust. Valdkondlikud nõuded loovad aluse ja pakuvad asjakohased kriteeriumid valdkonnaga seotud kindlustandvate teenuste läbiviimisel (standard 13.4 Hindamiskriteeriumid). Vastavus valdkondlikele nõuetele on kindlustandvate teenuste puhul kohustuslik ja nõuandvate teenuste puhul soovituslik. Valdkondlikud nõuded ei ole mõeldud hõlmama kõiki võimalikke aspekte, mida tuleks kindlustandvate teenuste läbiviimisel arvesse võtta, vaid kehtestavad miinimumnõuded, et tagada valdkonna ühtne ja usaldusväärne hindamine.

Valdkondlikud nõuded on selgelt seotud IIA kolme liini mudeli ja Ülemaailmsete siseauditi standarditega. Valitsemine, riskijuhtimine ja kontrolliprotsessid on valdkondlike nõuete põhikomponendid, mis on kooskõlas standardiga 9.1 Valitsemis-, riskijuhtimis- ja kontrolliprotsesside mõistmine. Kolme liini mudeli kontekstis on valitsemine seotud kõrgema juhtorganiga, riskijuhtimine teise liiniga ja kontrollid või kontrolliprotsessid on seotud esimese liiniga. Kui juhtkond on esindatud nii esimeses kui ka teises liinis, siis siseauditi funktsioon tegutseb kolmandas liinis kui sõltumatu ja objektiivne kindluse andja, kes annab aru kõrgemale juhtorganile (põhimõte 8 Kõrgema juhtorgani järelevalve).

Kohaldatavus, risk ja ametialane hinnang

Valdkondlikke nõudeid tuleb järgida, kui siseauditi funktsioon osutab kindlustandvaid töid teemadel, mille kohta on olemas valdkondlik nõue, või kui muid kindlustandvaid teenuseid osutades tuvastatakse valdkondliku nõude järgimist vajavaid aspekte.

Nagu standardites kirjeldatud, on riskide hindamine siseauditi juhi planeerimisprotsessis oluline osa. Selleks, et määrata kindlaks, milliseid kindlustandvaid töid siseauditi tööplaani lisada, tuleb vähemalt kord aastas hinnata organisatsiooni strateegiaid, eesmärke ja riske (standard 9.4 Siseauditi tööplaan). Üksikute kindlustandvate tööde kavandamisel peavad siseaudiitorid hindama konkreetse tööga seotud riske (standard 13.2 Töö riskide hindamine).

Kui valdkondliku nõudega kaetud teema tuvastatakse siseauditi riskipõhises planeerimisprotsessis ja see lisatakse siseauditi tööplaani, tuleb seda teemat hinnata vastavalt valdkondliku nõude nõuetele kõigis asjakohastes töödes. Lisaks sellele, kui siseaudiitorid viivad läbi töövõttu (olenemata sellest, kas see sisaldub algses siseauditi tööplaanis või mitte) ja valdkondliku nõude elemendid ilmnevad töö käigus, tuleb valdkondliku nõude kohaldatavust hinnata töövõtu osana. Lõpuks, kui tellitakse töö, mida algselt plaanis ei olnud, kuid mis hõlmab valdkondliku nõude teemat, tuleb hinnata valdkondliku nõude kohaldatavust. Ametialane hinnang mängib võtmerolli valdkondlike nõuete kohaldamisel. Riskide hindamised mõjutavad siseauditi juhtide otsuseid selle kohta, milliseid tööülesandeid siseauditi tööplaani lisada (standard 9.4 Siseauditi tööplaan). Lisaks kasutavad siseaudiitorid ametialast hinnangut et kindlaks määrata, milliseid aspekte iga töövõtu raames käsitletakse (standardid 13.3 Töö eesmärgid ja ulatus, 13.4 Hindamiskriteeriumid ja 13.6 Tööprogramm). Lisas A "Praktilised rakendusnäited" kirjeldatakse, kuidas siseaudiitorid määravad kindlaks, kas valdkondlik nõue on kohaldatav.

Iga valdkondlikus nõudes sisalduva nõude kohaldatavuse hindamise tõendusmaterjal tuleb säilitada, sealhulgas põhjendus iga nõude välistamise kohta. Valdkondliku nõude järgimine tuleb dokumenteerida, kasutades audiitori ametialast hinnangut, nagu on kirjeldatud standardis 14.6 Töö dokumenteerimine.

Kuigi küberturvalisuse valdkondlik nõue pakub kontrolliprotsesside miinimumtaseme, võivad organisatsioonid, kes hindavad küberriski väga kõrgeks, vajada täiendavate aspektide hindamist.

Kui siseauditi juht jõuab järeldusele, et siseauditi üksusel ei ole vajalikke teadmisi, et viia läbi töid teemal, mille kohta on välja antud valdkondlikud nõuded, võib töö sisse osta (standardid 3.1 Pädevus, 7.2 Siseauditi juhi kvalifikatsioon, 10.2 Personalijuhtimine). Siiski ei vabasta sisseostmine siseauditi funktsiooni vastutusest valdkondlike nõuete järgimise osas. Siseauditi juht vastutab lõplikult selle eest, et nõuetele vastavus oleks tagatud. Lisaks, kui siseauditi juht leiab, et siseauditi ressursid on ebapiisavad, peab siseauditi juht teavitama kõrgeimat juhtorganit ebapiisavate ressursside mõjust ja sellest, kuidas ressursside puudujäägid lahendatakse (standard 8.2 Ressursid).

Tulemuslikkus, dokumenteerimine ja aruandlus

Valdkondlike nõuete rakendamisel peavad siseaudiitorid samuti vastama standarditele, tehes oma tööd kooskõlas V valdkonnaga "Siseauditi läbiviimine". V valdkonna standardid kirjeldavad tööde planeerimist (põhimõte 13 Tööde mõjus planeerimine), tööde teostamist (põhimõte 14 Töö teostamine) ja tööde tulemuste edastamist (põhimõte 15 Töö tulemustest teavitamine ja tegevuskavade seire).

Valdkondliku nõude täitmist võib vastavalt siseaudiitori ametialasele hinnangule dokumenteerida kas töö kavas või tööpaberites. Nõuded võivad olla kaetud ühes või mitmes siseauditi töös. Samas, kõik nõuded ei pruugi alati olla kohaldatavad. Tuleb säilitada tõendid selle kohta, et valdkondlike nõuete kohaldatavust hinnati, sealhulgas põhjendused, mis selgitavad võimalikke välistusi.

Lisas C esitatud vabatahtlikku töövahendit võib võtta aluseks ja kasutada siseaudiitorite töö dokumenteerimiseks.

Kvaliteedi tagamine

Standardid nõuavad, et siseauditi juht töötaks välja, rakendaks ja säilitaks kvaliteedi tagamise ja parandamise programmi, mis hõlmab siseauditi funktsiooni kõiki aspekte (standard 8.3 Kvaliteet). Tulemustest tuleb teavitada kõrgemat juhtorganit ja tippjuhtkonda. Teabevahetus peab kajastama siseauditi funktsiooni vastavusest standarditele ja tulemuseesmärkide saavutamisest.

Kvaliteedi hindamisel hinnatakse vastavust valdkondlikele nõuetele. Kvaliteediülevaatuse ettevalmistamiseks võivad siseaudiitorid kasutada Lisas C esitatud töövahendit.

Küberturvalisus

Küberturvalisus on lai teema, mis on seotud iga organisatsiooni enamiku tehnoloogiliste aspektidega. Lisaks infotehnoloogiale on küberturvalisus tavaliselt osa ka äriprotsessidest, mistõttu siseaudiitorid peavad hindama küberriskide olemasolu kindlustandvate töövõttude planeerimisel, ulatuse määratlemisel ja läbiviimisel

USA kaubandusministeeriumi juurde kuuluv riiklik standardite ja tehnoloogia instituut (NIST) defineerib küberturvalisust lihtsalt kui "võimet turvata või kaitsta küberruumi kasutatavust küberrünnakute eest". Küberturvalisuse valdkondlik nõue keskendub välise perimeetri kaitsele, millega organisatsioonid kindlustavad volitamata kasutajate ja pahatahtlike küberohtudega seotud riskide vähendamise. Küberturvalisus on üldise infoturbe alamharu. NIST määratleb infoturvet kui "teabe ja infosüsteemide kaitset volitamata juurdepääsu, kasutamise, avalikustamise, katkestuse, muutmise või hävitamise eest, et tagada konfidentsiaalsus, terviklus ja käideldavus".

Küberturvalisuse valdkondlikus nõudes sisalduvad nõuded hõlmavad järgmist:

- Valitsemine - selgelt määratletud küberturvalisuse põhieesmärgid ja strateegiad, mis toetavad organisatsiooni eesmärke, poliitikaid ja protseduure.
- Riskijuhtimine - protsessid küberohtude tuvastamiseks, analüüsimiseks, haldamiseks ja jälgimiseks, sealhulgas protsess küberriskide kiireks eskaleerimiseks.
- Kontrolliprotseduurid - juhtkonna kehtestatud ja perioodiliselt hinnatavad kontrolliprotsessid küberriski maandamiseks.

Kaalutlused

Siseaudiitorid võivad kasutada järgmisi kaalutlusi, et aidata neil hinnata küberturvalisuse valdkondlikke nõudeid. Kaalutlused on näitlikud ega ole kohustuslikud. Siseaudiitorid peaksid oma hindamise ulatuse määramisel tuginema ametialasele hinnangule.

Valitsemisalased kaalutlused

Selleks, et hinnata, kuidas valitsemisprotsesse rakendatakse küberturvalisuse eesmärkide saavutamiseks, võivad siseaudiitorid üle vaadata järgmised aspektid:

A. Ametlik, dokumenteeritud küberturvalisuse strateegiline plaan ja eesmärgid, sealhulgas tõendid selle kohta, et kõrgem juhtorgan vaatab korrapäraselt (tavaliselt kord kvartalis) läbi küberturvalisuse ajakohastatud andmed, mida esitab infoturbefunktsiooni juht, näiteks infoturbejuht (CISO). Tõendid võivad sisaldada aruandeid järgmistest valdkondadest:
    - Strateegiliste eesmärkide saavutamise jälgimine.
    - Eelarvevajadused küberturvalisuse eesmärkide ja ülesannete toetamiseks.
    - Keskendumine riskidele ja sisekontrollidele, sealhulgas parandusmeetmete edusammudele.
    - Peamised tulemusnäitajad (KPI) edu mõõtmiseks.
    - Vajalikud inimressursid küberturvalisuse personali värbamiseks, koolitamiseks ja arendamiseks.
B. Küberturvalisuse protsesside haldamiseks kasutatavad poliitikad, protseduurid ja muud asjakohased dokumendid, sealhulgas:
    - Poliitikad, mis vaadatakse üle ja ajakohastatakse vähemalt kord aastas. Uued tekkivad küberriskid võivad tingida sagedasemaid ülevaatusi ja muudatusi.
    - Protsess, mille abil hinnatakse, kas poliitikad ja protseduurid on küberturvalisuse toetamiseks piisavad.
    - Laialdaselt kasutatavad raamistikud (NIST, COBIT jt) küberturvalisuse protsesside ja sisekontrollide tugevdamiseks.
C. Küberturbe eesmärkide saavutamist toetavad rollid ja vastutusvaldkonnad, sealhulgas struktuur, mis tagab, et küberturvalisuse funktsioon allub organisatsiooni tasandil piisava nähtavusega üksusele, et tagada organisatsiooni tugi.
    - Protsess, mille abil hinnatakse perioodiliselt küberturvalisuse rollides tegutsevate töötajate teadmisi, oskusi ja võimeid.
D. Tõendid koostööst asjakohaste huvirühmadega (nt tippjuhtkond, operatiivjuhtimine, riskijuhtimine, personalijuhtimine, juriidiline osakond, vastavuskontroll, strateegilised tarnijad ja teised), sealhulgas teabevahetus olemasolevate ja tekkivate küberriskide ning teadaolevate võimalike nõrkuste teemal. Tõendusmaterjalid teabevahetuse kohta võivad hõlmata koosolekute protokolle, aruandeid või e-kirju.

Riskijuhtimise kaalutlused

Et hinnata, kuidas riskijuhtimise protsesse rakendatakse küberturvalisuse eesmärkide saavutamiseks, võivad siseaudiitorid üle vaadata järgmised aspektid:

A. Kuidas organisatsioon hindab ja haldab küberturberiske, sealhulgas kuidas ohte ja nõrkusi:
   - Algselt tuvastatakse ja raporteeritakse.
   - Analüüsitakse, et hinnata riski mõju organisatsiooni eesmärkide saavutamisele.
   - Maandatakse, sealhulgas tegevuskavad, mis aitavad viia riski vastuvõetavale tasemele.
   - Jälgitakse, sealhulgas pidev aruandlus, kuni ohud on täielikult kõrvaldatud.

B. Kuidas organisatsioon saab perioodilist tagasisidet küberturvalisuse riskijuhtimise osas erinevatelt valdkondadelt, näiteks infotehnoloogia, ettevõtte riskijuhtimine, personalijuhtimine, juriidiline osakond, vastavuskontroll, operatiivjuhtimine, raamatupidamine ja finantsjuhtimine. Teabe saamiseks võib kasutada valdkonnaülest küberturvalisuse töörühma või IT-juhtimiskomiteed.

C. Kuidas organisatsioon on määranud küberturvalisuse riskijuhtimise protsessi eest vastutava isiku või meeskonna.
   - Vastutav(ad) isik(ud) peaks regulaarselt (kord kvartalis, kord kuus või vastavalt vajadusele) edastama kogu organisatsioonile teavet ajakohastatud küberturvalisuse riskide kohta. Vajadusel peaks nad andma ülevaate ka riskide maandamiseks vajalikest ressurssidest.

D. Millised on organisatsioonis küberturberiskide eskaleerimisprotsessid, sealhulgas see, kuidas ohu või riski taset hinnatakse, määratakse ja prioriseeritakse. Ülevaade võib hõlmata järgmiste asjaolude kindlakstegemist:
   - Organisatsiooni määratletud riskitasemed - näiteks kõrge, mõõdukas ja madal - koos iga taseme üksikasjaliku selgituse ning vastava eskaleerimisprotseduuriga.
   - Loetelu hetkel tuvastatud küberturberiskidest ja iga riskijuhtumi leevendamise staatus.
   - Kohaldatavad õiguslikud, regulatiivsed ja vastavusnõuded.
   - Nii finantsilised kui ka mittefinantsilised (nt mainega seotud) riskimõjud.

E. Kuidas organisatsioonis on korraldatud küberturberiskide edastamise protsess juhtkonnale ja töötajatele, mis hõlmab järgmist:
   - Regulaarsed (vähemalt kord aastas) töötajate küberturvalisuse alased koolitused (näiteks etteteatamata, simuleeritud andmepüügirünnakud, et testida ja jälgida organisatsiooni teadlikkust).
   - Olemasolevate küberturvalisuse probleemide parendusmeetmete ajakohastatud ülevaade koos eeldatava lõpukuupäevaga.

- Mittevastavuse jälgimine, mis hõlmab aruandlust kõrgemale juhtorganile ja tippjuhtkonnale.
- Ohtude ümberhindamine, kui organisatsiooni riskivalmidus ja riskitaluvus muutuvad.

F. Kuidas organisatsioonis on korraldatud protsessid intsidentidele reageerimiseks ja taastamiseks, mis hõlmavad järgmist:

- Dokumenteeritud plaan, mida vaadatakse üle ja ajakohastatakse vastavalt organisatsiooni tegevuse muutusele. Plaan peaks sisaldama järgmist:
  - Kuidas intsidente tuvastatakse ja kuidas neist teatatakse.
  - Kuidas intsidente hallatakse, et vältida edasist kahju.
  - Kuidas organisatsioon taastub ja reageerib, et tegevust jätkata.
  - Kuidas intsidenti analüüsitakse, et teha kindlaks saadud õppetunnid ja kuidas vältida sarnaseid sündmusi tulevikus.
- Perioodiline (vähemalt kord aastas) testimine (tabletop-harjutus) ja tulemuste esitamine tippjuhtkonnale ja asjaomastele huvirühmadele. Testimise tulemusena võidakse koostada plaanid parendustegevusteks.

Kontrolliprotsessi kaalutlused

Et hinnata, kuidas kontrolliprotsesse rakendatakse küberturvalisuse eesmärkide saavutamiseks, võivad siseaudiitorid üle vaadata järgmised aspektid:

A. Juhtkonna lähenemine tõhusa küberturvalisuse sisekontrollikeskkonna loomiseks, sealhulgas:
   - Organisatsiooni riskihindamise protsessi alusel vajalike sisekontrollide hindamine ja rakendamine, et maandada suurenenud riske ja kaitsta tundlikke, kriitilisi, isiklikke või konfidentsiaalseid andmeid.
   - Peamiste küberturvalisuse kontrollide toimimiseks ressursivajaduste kindlaksmääramine.
   - Tarnijapõhiste kontrollide arvestamine kontrollikeskkonna osana, sealhulgas teenusepakkujate SOC (Service Organization Control) aruannete läbivaatamine enne ärisuhte alustamist ja kogu koostööperioodi jooksul.
   - Perioodiline testimine, et tagada küberturvalisuse kontrollide toimimine viisil, mis maandab riske ja toetab küberturvalisuse eesmärkide saavutamist.
   - Protsess kontrolliprotseduuride puuduste kõrvaldamiseks või siseauditi funktsiooni või teiste kindlusandjate läbiviidud hindamiste (näiteks sissetungitestide) tulemuste käsitlemiseks.

B. Organisatsiooni talendijuhtimise protsess küberturvalisuse spetsialistide värbamiseks ja koolitamiseks, sealhulgas kuidas organisatsioon märkab võimalusi küberturvalisuse

spetsialistide pädevuse suurendamiseks, et toetada tehnilisi teadmisi ja parandada organisatsiooni teadlikkust esilekerkivatest probleemidest.

- Näideteks on koolitustel osalemine, teadmiste jagamise gruppidesse kaasamine ning erialase täiendõppe läbimine, sealhulgas küberturvalisusega seotud sertifikaatide omandamine.

C. Juhtkonna protsess küberturvalisuse uute ohtude ja nõrkuste pidevaks tuvastamiseks, prioriseerimiseks, jälgimiseks ja raporteerimiseks, keskendudes igapäevastele toimingutele. Ülevaatus võib hõlmata protsesside olemasolu ohtude ja nõrkuste hindamiseks, mis on seotud uute või esilekerkivate tehnoloogiatega, näiteks tehisintellekti kasutamine.

D. Juhtkonna protsessid ja kontrollimeetmed, mis on kehtestatud IT-vara haldamiseks ja kaitsmiseks kogu elutsükli jooksul, sealhulgas riistvara, tarkvara ja tarnijateenuste valiku, kasutamise, hoolduse ja kasutuselt kõrvaldamise osas. Riistvara hõlmab servereid, võrguseadmeid (näiteks ruuterid või tulemüürid), lauaarvuteid, sülearvuteid, mobiiltelefone, tahvelarvuteid ja välisseadmeid. Tarkvara hõlmab operatsioonisüsteeme (nt Windows), ettevõtte ressursside planeerimise tarkvara, rakendusi, viirusetõrjeprogramme ja muud. Riist- ja tarkvaraga seotud kaalutlused võivad hõlmata järgmist:

- Organisatsiooni kasutatav krüpteerimine, viirusetõrjetarkvara, mobiilseadmete haldus, keerukate paroolide nõuded, virtuaalne privaatvõrk (VPN)/ nullusaldusvõrgustik (ZTN) autentimiseks ja püsivara perioodiline uuendamine.
- Varahalduspротsess, mis tagab, et ettevõtte väljastatud riistvara on väljastamise hetkel asjakohase turvakonfiguratsiooniga ja et varade kasutuselt eemaldamisel hävitatakse need nõuetekohaselt. Andmebaasidega seotud kontrollimeetmed, mis hõlmavad kasutajate ja administraatorite juurdepääsuõiguste piiramist, krüpteerimise kasutamist, andmebaaside varundamist ja testimist ning tugevate võrguturbe kontrollimeetmete olemasolu.
- Küberturbeohtude ja nõrkuste arvestamine süsteemi arenduse elutsüklis (SDLC).
- Arenduse, turvalisuse ja operatsioonide (DevSecOps) lähenemisviis, millega integreeritakse küberturvalisus tarkvaraarendusse, et tuvastada nõrkused ennetavalt.

E. Protsessid, mida kasutatakse küberturvalisuse tugevdamiseks, sealhulgas:

- Turvasätete konfigureerimine küberturberiski minimeerimiseks.
- Mobiilseadme haldamine (sealhulgas e-posti ja rakenduste kasutamine) on seadistatud küberturberiskide maandamiseks ning võimaldab kaugjuhtimist juhuks, kui kasutaja seade on ohustatud.
- Krüpteerimise kasutamine andmete „hoiustamisel“ (*at rest*) (näiteks kõvakettale salvestatud andmed) või andmete „edastamisel“ (*in transit*) (näiteks e-kirjade krüpteerimine edastamisel).

- Serverite või tarkvara (näiteks operatsioonisüsteemi) uuendamine uusimate turvapaikadega.
- Kasutaja juurdepääsu haldamine, näiteks mitmefaktorilise autentimise (MFA) ja unikaalsete kasutajatunnuste kasutamine koos keerukate paroolidega, mis aeguvad perioodiliselt.
- Kontrollimeetmed, mis võimaldavad hinnata süsteemi saadavust ja ressursside kasutamist ning analüüsida võimalikke küberturbeprobleeme, mis võivad mõjutada süsteemi jõudlust.
- Küberturvalisuse integreerimine tarkvaraarenduse elukaare protsessi (SDLC-sse), et tuvastada ja kõrvaldada küberturvalisuse nõrkused enne tarkvara tootmisse viimist.

F. Võrguga seotud kontrollimeetmed, mis kindlustavad organisatsiooni perimeetri, sealhulgas kuidas organisatsioon kasutab:
   - Võrgu segmenteerimist.
   - Tulemüüre.
   - Kasutaja juurdepääsu kontrolle.
   - Piiranguid nii välis- kui ka siseühendustele.
   - Asjade internetti ümbritsevaid kontrolle ühendatud võrkude puhul.
   - Sissetungi avastamise/ennetamise süsteeme, et ennetada, avastada ja taastuda küberrünnakutest.

G. Kontrollid, mis ümbritsevad lõppseadme sidekanalite turvameetmeid, mida kohaldatakse selliste teenuste suhtes nagu e-post, internetibrauserid, videokonverentsid, sõnumirakendused (Zoom, MS Teams ja muud), sotsiaalmeedia, pilveteenused ja failijagamisprotokollid. Kontrollimeetmed võivad hõlmata teatud faililaiendite (nt .exe failid) kasutamise piiramist ja mitmefaktorilist autentimist failide jagamisel.

Lisa A. Praktilised rakendusnäited

Järgnevad näited kirjeldavad olukordi, kus küberturvalisuse valdkondlik nõue oleks kohaldatav:

Näide 1: Küberturvalisuse teema on asjakohane siseauditi tööplaanis sisalduvas siseauditi töövõtus.

Kui siseauditi funktsioon viib läbi riskipõhise planeerimisprotsessi ja lisab siseauditi tööplaani ühe või mitu küberturvalisusega seotud tööd, on valdkondlike nõuete järgimine selliste tööde läbiviimisel kohustuslik. Vastavuse saavutamiseks võib nõudeid rakendada ühes või mitmes siseauditi tööplaanis sisalduvad töös.

Küberturvalisus on lai teema ja mitte kõik valdkondlikus nõudes toodud nõuded ei pruugi olla kohaldatavad iga töövõtu puhul. Kui siseaudiitorid rakendavad ametialast hinnangut ja otsustavad, et üks või mitu küberturvalisuse valdkondlikus nõudes sisalduvat nõuet ei ole konkreetse töö jaoks asjakohased ning tuleks välja jätta, peavad nad dokumenteerima ja säilitama põhjenduse nende nõuete välistamiseks. Mõne nõude väljajätmise põhjendus võib olla näiteks see, et siseauditi funktsioon täidab erinevaid küberturbeülesandeid rotatsiooni korras või on otsustanud, et konkreetse töö puhul on vastava riski olulisus madal.

Näide 2: Küberturberiskid tuvastatakse auditi käigus, mis ei keskendu küberturvalisusele.

Siseaudiitorid võivad tuvastada küberturvalisuse riske, kui nad hindavad protsessi, mis ei ole otseselt seotud küberturvalisusega. Näiteks võivad siseaudiitorid hinnata ostuarvete menetlust töö raames, mille fookus ei ole küberturvalisusel, ning ka planeerimisetapis ei pruugita küberturberiske töö ulatusse kaasata. Kuid pärast esmast protsessi ülevaatust võivad siseaudiitorid jõuda järeldusele, et küberturberiskid tuleks siiski arvesse võtta – näiteks juhul, kui tuvastatakse veebipõhise ostutellimuse esitamisega seotud küberturbeohud (standard 13.2 Töö riskide hindamine).

Kui asjakohased riskid on kindlaks tehtud, peavad siseaudiitorid vaatama läbi küberturvalisuse valdkondlikud nõuded ja tegema kindlaks, millised nõuded on kohaldatavad. Selles näites võivad nad välistada küberturvalisuse valitsemise või küberturvalisuse riskijuhtimise protsessi. Kõik välistatud küberturvalisuse valdkondlikus nõudes sisalduvad nõuded tuleb dokumenteerida auditi töödokumentides koos põhjendusega ning dokumentatsioon tuleb säilitada.

Näide 3: Algselt siseauditi tööplaani mittekuuluv küberturvalisuse audititöö tellitakse eraldi.

Huvirühmad, näiteks kõrgem juhtorgan, tippjuhtkond või reguleeriv asutus, võivad paluda siseaudiitoritel viia läbi küberturvalisuse hindamisi väljaspool esialgset siseauditi tööplaani. Näiteks kui organisatsioon satub küberrünnaku sihtmärgiks, võib kõrgem juhtorgan tellida

siseauditilt töö, et hinnata küberturvalisuse kontrollimeetmete tõhusust. Sellisel juhul on valdkondlik nõue kohaldatav, kõik nõuded tuleb läbi vaadata ning kõik välistatud nõuded peavad olema dokumenteeritud ja põhjendatud.

Lisa B. Raamistikega kaardistamine

Organisatsioonil võivad olla oma küberturvalisuse meetmed, mis põhinevad sellistel riskijuhtimise ja valitsemise raamistikel nagu COBIT või NIST. Siseaudiitorid võivad olla juba välja töötanud auditiprogrammid ja testimise protseduurid, mis põhinevad nendel raamistikel. Siseaudiitorid peaksid sobitama oma kavandatud küberturvalisuse kontrollide testimised valdkondlike nõudega, et tagada piisav katvus. Allolevas tabelis on seostatud küberturvalisuse valdkondlikud nõuded kolme üldkasutatava raamistikuga: NIST Cybersecurity Framework 2.0, COBIT 2019 ja NIST 800-53. Kaardistus põhineb nendel raamistikel, kuna need on kergesti ja tasuta kättesaadavad.

	Raamistiku viited		
Valitsemise nõuded	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
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 vajalikke ressursside ja eelarve olemasolu kohta.	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. Kontrollikeskkonna tugevdamiseks on kehtestatud küberturvalisusega seotud poliitikad ja protseduurid ning neid ajakohastatakse perioodiliselt.	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. Küberturvalisuse eesmärkide saavutamiseks on määratud selged rollid ja vastutusvaldkonnad ning on kehtestatud protsess, mille abil hinnatakse perioodiliselt vastutavate isikute teadmisi, oskusi ja võimeid.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

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.	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
Riskijuhtimise nõuded	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Organisatsiooni riskihindamise ja -juhtimise protsessid hõlmavad küberturvalisuse ohtude tuvastamist, analüüsimist, maandamist ja pidevat jälgimist ning nende mõju hindamist strateegiliste eesmärkide saavutamisele.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
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.	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. Küberturvalisuse riskijuhtimise protsessi eest on määratud kindel vastutaja. Määratud on isik või meeskond, kes jälgib ja raporteerib perioodiliselt küberturvalisuse riskide juhtimise kohta. Sealhulgas teavitab riskide maandamiseks vajalikest ressurssidest ja tuvastab uusi tekkivaid küberohtusid.	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. 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.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
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.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Organisatsioon on rakendanud küberturbeintsidentide haldamise ja taastamise protsessi, mis hõlmab tuvastamist, tõkestamist, taastamist ja intsidendijärgset analüüsi. Seda protsessi testitakse perioodiliselt.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Kontrolliprotsessi nõuded	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Organisatsioonis on kehtestatud protsess, millega tagatakse nii sise- 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.	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. Organisatsioonis on kehtestatud kompetentside halduse protsess, mis hõlmab koolitust küberturbe tegevustega seotud tehnilise pädevuse arendamiseks ja säilitamiseks. Seda protsessi vaadatakse perioodiliselt üle.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Organisatsioonis on loodud pidev jälgimis- ja aruandlusprotsess küberturbe ohtude ja nõrkuste tuvastamiseks ning küberturbe parandamise võimaluste määratlemiseks, prioriseerimiseks ja elluviimiseks.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Küberturvalisus on kaasatud IT-varade elutsükli kõikidesse etappidesse (valimine, kasutamine, hooldus ja kasutusest kõrvaldamine) ning kohaldub riistvarale, tarkvarale ja tarnijateenustele.	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. 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).	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. 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).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02

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

Lisa C. Vabatahtlik dokumenteerimisvahend

Siseaudiitoritelt oodatakse ametialase hinnangu kasutamist, et riskipõhiselt määrata kindlaks valdkondlike nõuete kohaldatavus ning asjakohaselt dokumenteerida teatud nõuetest kõrvalekaldumised. Valdkondlike nõuete kohaldatavuse analüüsi võib dokumenteerida auditi kavas või tööpaberites, sõltuvalt audiitori ametialasest hinnangust. Üks või mitu siseauditi tööd võivad hõlmata valdkondlikke nõudeid. Samas, kõik nõuded ei pruugi alati olla kohaldatavad. Allolev prinditav vorm on üks võimalus küberturvalisuse valdkondlike nõuete järgimise dokumenteerimiseks, kuid selle kasutamine ei ole kohustuslik.

Küberturvalisus - valitsemine

Nõue	Teostatud ulatus või välistamise põhjendus	Dokumentatsiooni viide
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.		

Küberturvalisus - riskijuhtimine

Nõue	Teostatud ulatus või välistamise põhjendus	Dokumentatsiooni viide
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.		

Nõue	Teostatud ulatus või välistamise põhjendus	Dokumentatsiooni viide
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 rakendanud küberturbeintsidentide haldamise ja taastamise protsessi, mis hõlmab tuvastamist, tõkestamist, taastamist ja intsidendijärgset analüüsi. Seda protsessi testitakse perioodiliselt.		

Küberturvalisus - kontrolliprotsessid

Nõue	Teostatud ulatus või välistamise põhjendus	Dokumentatsiooni viide
A. Organisatsioonis on kehtestatud protsess, millega tagatakse nii sise- 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.		

Nõue	Teostatud ulatus või välistamise põhjendus	Dokumentatsiooni viide
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.		

Rahvusvahelisest Siseaudiitorite Instituudist

Rahvusvaheline Siseaudiitorite Instituut (The IIA) on rahvusvaheline kutseühing, mis teenindab enam kui 255 000 liiget kogu maailmas ja on väljastanud üle 200 000 sertifitseeritud siseaudiitori® (CIA®) sertifikaadi kogu maailmas. 1941. aastal asutatud IIA on kogu maailmas tunnustatud kui siseauditi kutseala liider standardite, sertifikaatide, hariduse, uurimistöö ja tehniliste juhiste vallas. Lisateavet leiate veebilehelt www.theiia.org.

Vastutusnõue

IIA avaldab käesoleva dokumendi teavitamise ja harimise eesmärgil. Käesolev materjal ei ole mõeldud selleks, et anda lõplikke vastuseid konkreetsetele üksikjuhtumitele ja on mõeldud kasutamiseks ainult juhisena. IIA soovitab pöörduda sõltumatu eksperdi poole, kes on otseselt seotud iga konkreetse olukorraga. IIA ei võta vastutust selle eest, e keegi tugineb ainult sellele materjalile.

Autoriõigus

© 2025 The Institute of Internal Auditors, Inc. Kõik õigused kaitstud. Reprodutseerimise loa saamiseks võtke palun ühendust aadressil copyright@theiia.org.

Veebruar 2025

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