Third-Party

Valdkondlik nõue

Topical Requirement

The Institute of
Internal Auditors

Kolmanda osapool valdkondlik nõue

Rahvusvahelised kutsetegevuse raampõhimõtted (The 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 esitavad siseaudiitoritele selged ootused, kehtestades konkreetsete riskivaldkondade 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. Lõpetuseks edendavad valdkondlikud nõuded siseauditi kutseala.

Siseaudiitorid peavad valdkondlikke nõudeid rakendama kooskõlas Ülemaailmsete siseauditi standarditega. Vastavus valdkondlikele nõuetele on kindlustandvate tööde puhul kohustuslik ja nõuandvate tööde puhul soovituslik. Valdkondlik nõue on kohaldatav järgmistel juhtudel:

1. Siseauditi tööplaanis sisaldub selleteemaline töö.
2. Valdkondliku nõude teema asjakohasus tuvastatakse töö teostamisel.
3. Esitatakse selleteemaline töö ettepanek või tellimus, mis ei olnud 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.

Kolmandad osapooled

Kolmas osapool on väline üksikisik, grupp või üksus, kellega organisatsioon ("põhiorganisatsioon") loob ärisuhte toodete või teenuste saamiseks. Suhte võib vormistada lepingu, kokkuleppe või muul kujul. Käesolevas valdkondlikus nõudes kasutatakse mõistet "kolmas osapool", mis viitab müüjatele, tarnijatele, töövõtjatele, alltöövõtjatele, allhankijatele, sisseostetud teenusepakkujatele, teistele asutustele ja konsultantidele. Mõiste hõlmab kolmanda osapoole ja tema alltöövõtjate vahelisi lepinguid.

Antud valdkondlikku nõuet kohaldatakse, kui siseauditi funktsioon täidab kindlustandvaid ülesandeid kolmandate isikute ja/või alltöövõtjate suhtes, sealhulgas neljandas või järgmises etapis, mis on lubatud kolmanda osapoole lepingu või kokkuleppega põhiorganisatsiooniga. Siseaudiitorid peaksid seadma kolmandad ja edasised osapooled riskipõhiselt tähtsuse

järjekorda, nagu on kirjeldatud allpool riskijuhtimise osas. Siseaudiitorid peavad kohaldama kõiki nõudeid, nagu on näidatud riskihindamise tulemustes, ning erandid tuleb dokumenteerida.

Käesolev valdkondlik nõue ei käsitle kaudseid väliseid suhteid, huvisid või osalusi põhiorganisatsiooniga, näiteks reguleerivaid asutusi, agente, usaldusisikuid/juhatuse liikmeid, ega ka organisatsioonisiseseid suhteid, näiteks töötajaid.

Mõiste "kolmas isik" võib olla määratletud ja seda võib kasutada erinevalt, sõltuvalt tööstusharust või muust kontekstist. Siseaudiitoritele on tagatud paindlikkus ja nad peaksid tuginema oma kutsealasele hinnangule, et kohandada valdkondlikku nõuet vastavalt põhiorganisatsiooni kolmanda osapoole määratlusega.

Põhiorganisatsioon (kolmanda osapoolega lepingu sõlminud organisatsioon) vastutab oma eesmärkide saavutamisega seotud riskide eest isegi siis, kui ta kaasab kolmanda osapoole, kes aitab tal saavutada ühte või mitut eesmärki. Töö kolmandate osapooltega toob kaasa riske, mida tuleb tuvastada, hinnata ja juhtida asjakohaste juhtimis-, riskijuhtimis- ja kontrolliprotsesside kaudu, nagu on kirjeldatud käesolevas valdkondlikus nõudes. Kui kolmas osapool ei täida lepingut, osaleb ebaeetilistes tegevustes või tal esineb äritegevuse häireid, võib põhiorganisatsioon selle tagajärjel kannatada. Kolmandate osapooltega seotud riskide kategooriad ja näited hõlmavad muuhulgas järgmist:

- Strateegilised riskid, näiteks võimet täita põhiorganisatsiooni missiooni ja/või kõrgetasemelisi eesmärke või juhtida ühinemiste ja ülevõtmiste mõjusid.
- Maineriskid, näiteks keskkonnale tekitatud kahju või põhiorganisatsiooni suhete ja usalduse kahjustamine klientide, tarbijate ja teiste sidusrühmadega.
- Eetilised riskid, näiteks aususe puudumine, huvide konfliktid, altkäemaksud ja korruptsioon.
- Operatiivsed riskid, näiteks füüsilise ja infoturbe, siseringi risk, teenusekatkestused ja eesmärkide mittetäitmine.
- Finantsrisk, näiteks kolmanda osapoole maksejõuetus ja pettus.
- Vastavusriskid, näiteks mittevastavus kehtivatele kohalikele, riiklikele ja rahvusvahelistele regulatiivsetele nõuetele.
- Küberturvalisus ja andmekaitse riskid, näiteks tundlike andmete ohustamine ja lekkimine.
- Infotehnoloogia riskid, näiteks kriitiliste toimingute toetamiseks vajalike IT-teenuste puudumine.
- Õiguslikud riskid, näiteks huvide konfliktid, vaidlused ja lepingurikkumistest tulenevad kohtuvaidlused.
- Jätkusuutlikkuse riskid, näiteks keskkonna-, sotsiaalsed ja valitsemise alased (ESG) riskid. Näidetena võib tuua riskid, mis on seotud organisatsiooni mõjuga looduskeskkonnale, ja riskid, mis puudutavad organisatsiooni suhtlust kogukondadega.
- Geopoliitilised riskid, näiteks kaubandusvaidlused/ sanktsioonid ja poliitiline ebastabiilsus.

Kolmanda osapoole elutsükkel koosneb valimisest, lepingute sõlmimisest, kasutuselevõtust, jälgimisest ja suhte lõpetamisest. Siseaudiitorid peaksid neid etappe arvesse võtma, hinnates valitsemise-, riskijuhtimise ja kontrolliprotsesside nõuete asjakohasust ja piisavust.

Kolmanda osapoole valitsemise, riskijuhtimise ja kontrolliprotsesside hindamine ja analüüs

Käesolev valdkondlik nõue annab järjepideva ja tervikliku lähenemisviisi kolmanda osapoole valitsemise, riskijuhtimise ja kontrolliprotsesside kavandamise ja rakendamise hindamiseks. Need nõuded kujutavad endast hindamise minimaalset baasnõuete taset.

VALITSEMINE

Nõuded:

Siseaudiitorid peavad hindama järgmisi põhiorganisatsiooni kolmandate osapoolte valitsemise aspekte, sealhulgas kõrgema juhtorgani järelevalvet:

A. Organisatsioonis on kehtestatud, rakendatud ja perioodiliselt üle vaadatav ametlik lähenemine, mille aluselt otsustatakse, kas sõlmida leping kolmanda osapoolega. Lähenemine hõlmab asjakohaseid kriteeriume, et määratleda ja hinnata ressursse, mis on vajalikud ja kättesaadavad eesmärkide saavutamiseks toote või teenuse osutamise kaudu.

B. Kehtestatud on sisekorrad, et määratleda, hinnata ja hallata kolmanda osapoole suhteid ja riske kogu elutsükli jooksul. Sisekorrad on kooskõlas kohaldatavate regulatiivsete nõuetega ning neid vaadatakse korrapäraselt läbi ja ajakohastatakse kontrollikeskkonna tugevdamiseks.

C. Organisatsiooni kolmanda osapoole haldamise rollid ja vastutused on selgelt määratletud, sealhulgas täpsustades, kes vastutab kolmandate osapoolte valimise, suunamise, juhtimise, nendega suhtlemise ja järelevalve eest ning keda tuleb kolmanda osapoole tegevusest teavitada. Kehtib protsess, millega tagatakse, et kolmanda osapoolele määratud rollid ja vastutusalad vastavad nende pädevustele.

D. Määratletud on suhtlusprotokollid asjaomaste huvirühmadega, mis hõlmavad õigeaegset aruandlust prioriteetsete kolmandate osapoolte tulemuslikkuse, riskide ja vastavuse kohta (sh seaduste ja regulatsioonide rikkumised). Kolmandad osapooled seatakse riskide alusel tähtsuse järjekorda. Asjakohased huvirühmad võivad hõlmata kõrgemat juhtorganit, tippjuhtkonda, hangete, tegevuse, riskijuhtimise, vastavuse, õigusvaldkonna, infotehnoloogia, infoturbe, personalijuhtimise ja teiste valdkondade esindajaid.

RISKIJUHTIMINE

Nõuded:

Siseaudiitorid peavad hindama järgmisi organisatsiooni kolmanda osapoole riskijuhtimise aspekte.

A. Kolmandate osapoolte ja nende teenuste riskijuhtimise protsessid on standardiseeritud ja terviklikud, hõlmavad selgelt määratletud rolle ja vastutusi ning käsitlevad piisavalt organisatsiooni jaoks olulisi põhiriske (näiteks strateegilisi, mainega seotud, eetilisi, tegevus-, finants-, vastavus-, küberturbe-, infotehnoloogia-, õigus-, kestlikkuse ja geopoliitilisi riske). Protsesside kinnipidamist järgitakse ja tuvastatud kõrvalekallete korral rakendatakse parandusmeetmeid.

B. Kolmandate osapooltega seotud riskid tuvastatakse ja hinnatakse korrapäraselt kogu elutsükli jooksul. Riskihindamise tulemusi kasutatakse kolmandate osapoolte järjestamiseks ja prioriseerimiseks, sealhulgas ka ahela järgmistes etappides olevate osapoolte puhul. Ka riskidele reageerimise meetmed järjestatakse ja seatakse prioriteetsuse järjekorda. Riskihindamine vaadatakse perioodiliselt üle ja ajakohastatakse.

C. Riskidele reageerimise meetmed on piisavad ja asjakohased, vastavuses riski taseme ja prioriteetsusega. Riskidele reageerimise meetmeid rakendatakse, vaadatakse läbi, kiidetakse heaks, jälgitakse, hinnatakse ja vajaduse korral kohandatakse.

D. Kehtestatud on protsessid kolmandate osapooltest tulenevate probleemide haldamiseks ja vajaduse korral eskaleerimiseks, tagades vastutuse tulemuste eest ning suurendades lepingute või muude kokkulepete tingimuste täitmise tõenäosust. Kui kolmas osapool ei reageeri eskaleeritud probleemidele, on olemas protsessid, mis võimaldavad juhtkonnal hinnata jätkuva ärisuhtega seotud riske ning vajaduse korral võtta täiendavaid meetmeid, rakendada parandusmeetmeid või lõpetada koostöö, kui see on õigustatud.

KONTROLLID

Nõuded:

Siseaudiitorid peavad hindama järgmisi kontrolle nende kolmandate osapoolte puhul, kes on riskipõhiselt prioriseeritud. Hindamine peab hõlmama juhtkonna protsesse organisatsiooni kolmandate osapoolte pidevaks hindamiseks ja järelevalveks.

A. Kehtib tugev hoolsusmeetmete (*due diligence*) protsess kolmandate osapoolte leidmiseks ja valikuks, mille aluseks on dokumenteeritud ja heaks kiidetud äriline põhjendus või muu asjakohane dokument, mis kirjeldab ja põhjendab kolmanda osapoolega suhte vajadust ja olemust.

B. Lepingute sõlmimine ja heakskiitmine toimub vastavalt organisatsiooni kolmanda osapoole riskijuhtimise põhimõtetele ja sisekordadele ning hõlmab koostööd organisatsiooni asjakohaste üksuste vahel.

C. Lõplikud lepingud või kokkulepped vaadatakse läbi ja kiidetakse heaks kõigi asjaomaste huvirühmade poolt (sh õigusteenistus ja vastavuskontroll)l, need allkirjastatakse mõlema poole volitatud isikute poolt ning säilitatakse turvaliselt. Igale lepingule on määratud lepinguomanik või temaga võrdsustatud vastutav isik.

D. Kõikide kolmandate osapoolte vaheliste suhete täpne, täielik ja ajakohane loetelu säilitatakse, näiteks tsentraliseeritud lepingute haldussüsteemis.

E. Kolmandate osapoolte kasutuselevõtu protsess on dokumenteeritud ja seda järgitakse, et luua alus kolmandate osapoolte lepingu või kokkuleppe tingimuste täitmiseks

F. On olemas pidev järelevalveprotsess, mille abil hinnatakse kogu elutsükli vältel, kas kolmandad osapooled tegutsevad vastavalt lepingu või kokkuleppe tingimustele ning täidavad oma lepingulisi kohustusi. Protsessid hõlmavad esitatud teabe usaldusväärsuse kontrollimist ning tulemuslikkuse ümberhindamist perioodiliselt ja alati, kui kokkulepet muudetakse.

G. Kehtestatud on protokollid parandusmeetmete algatamiseks, kui kolmas osapool ei vasta ootustele või kujutab endast suurenenud või ootamatut riski. Protokollid hõlmavad

intsidentide eskaleerimist vastavalt nende tõsidusele, intsidentide järgset ülevaatuste läbiviimist ja algpõhjuste analüüsi.

H. Lepingute lõppemise ja uuendamise kuupäevi jälgitakse ning vajaduse korral rakendatakse õigeaegselt uuendamisega seotud tegevusi.

I. Kolmandate osapoolte suhte lõpetamise plaani rakendatakse ja järgitakse, et tagada lepingunõuete (sh ajastus ja ootused) nõuetekohane täitmine. Protsessid hõlmavad järgmist:

   - Kolmanda osapoolega lepingu lõpetamine.
   - Kolmanda osapoole asendamine vajadusel.
   - Vastutuse ümbermääramine ning kolmanda osapoole juures hoitavate organisatsiooni tundlike andmete tagastamine või hävitamine.
   - Kolmanda osapoole juurdepääsude tühistamine organisatsiooni süsteemides, vahendites ja ehitistes.

Rahvusvahelisest Siseaudiitorite Instituudist

IIA on rahvusvaheline kutseühing, mis teenindab üle maailma enam kui 265 000 liiget ja on väljastanud üle 200 000 sertifitseeritud siseaudiitori® (CIA®) sertifikaadi kogu maailmas. 1941. aastal asutatud IIA on tunnustatud kui siseauditi kutseala liider standardite, sertifitseerimise, hariduse, teadusuuringute ja tehniliste juhiste valdkonnas kogu maailmas. Lisateavet leiate veebilehelt theiia.org.

Autoriõigus

September 2025

The Institute of Internal Auditors

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