

Kolmas osapool

Valdkondlik nõue

Kasutusjuhend

Topical Requirement



The Institute of
Internal Auditors

Sisu

Ülevaade valdkondlikest nõuetest.....	2
Kohaldatavus, risk ja kutsealane otsustus.....	2
Kaalutlused.....	7
Valitsemisalased kaalutlused	7
Riskijuhtimisega seotud kaalutlused	8
Kontrollidega seotud kaalutlused.....	10
Lisa A. Praktilised näited	16
Lisa B. Vabatahtlik dokumenteerimise tööriist	18
Kolmanda osapoole valitsemine	18
Kolmanda osapoole riskijuhtimine	20
Kolmanda osapoole kontroll	21

Ülevaade valdkondlikest nõuetest

Valdkondlikud nõuded on Rahvusvaheliste 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 kasutatakse 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 tööde läbiviimisel (standard 13.4 Hindamiskriteeriumid). Vastavus valdkondlikele nõuetele on kindlustandvate tööde puhul kohustuslik ja nõuandvate tööde puhul soovituslik. Valdkondlikud nõuded ei ole mõeldud hõlmama kõiki võimalikke aspekte, mida tuleks kindlustandvate tööde 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 kutsealane otsustus

Valdkondlikke nõudeid tuleb järgida, kui siseauditi funktsioon osutab kindlustandvaid töid teemadel, mille kohta on olemas valdkondlik nõue, või kui muid kindlustandvaid töid tehes 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 tööplaani). 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 töö (olenemata sellest, kas see sisaldub algses siseauditi tööplaanis või mitte) ja valdkondliku

nõude elemendid ilmnevad töö käigus, tuleb valdkondliku nõude kohaldatavust hinnata töö osana. Lõpuks, kui tellitakse töö, mida algselt plaanis ei olnud, kuid mis hõlmab valdkondliku nõude teemat, tuleb hinnata valdkondliku nõude kohaldatavust.

Kutsealane otsustus mängib võtmerolli valdkondlike nõuete kohaldamisel. Riskihinnangute alusel otsustavad siseauditi juhid, milliseid tööülesandeid siseauditi tööplaani lisada (standard 9.4). Lisaks kasutavad siseaudiitorid kutsealast otsustust, et kindlaks määrata, milliseid aspekte iga töö raames käsitletakse (standardid 13.3 Töö eesmärgid ja ulatus, 13.4 Hindamiskriteeriumid ja 13.6 Tööprogramm).

Iga valdkondlikus nõudes sisalduva nõude kohaldatavuse hindamise tõendusmaterjal tuleb säilitada, sealhulgas põhjendus iga nõude välistamise kohta. Valdkondlikule nõudele vastavus tuleb dokumenteerida, kasutades audiitorite kutsealast otsustust, nagu on kirjeldatud standardis 14.6 "Töö dokumenteerimine".

Kuigi Kolmandate osapoolte valdkondlik nõue annab kontrolliprotsesside põhijooned, mida tuleb arvesse võtta, võivad organisatsioonid, kes hindavad antud riskiteemat väga kõrgeks, vajada täiendavate aspektide hindamist.

Kui siseauditi üksusel ei ole nõutavat pädevust, et teostada tööülesandeid mõne valdkondliku nõude teemaga seoses, peab siseauditi juht kindlaks määrama, kuidas hankida ressursse, ning teavitama õigeaegselt juhatust ja kõrgemat juhtorganit piirangute mõjust ja sellest, kuidas ressursside puudujäägid kõrvaldatakse. Siseauditi juht kannab lõplikku vastutust selle eest, et siseauditi funktsioon vastab valdkondlikele nõuetele, sõltumata sellest, kuidas ressursid on saadud (standardid 3.1 Pädevus, 7.2 Auditi juhi kvalifikatsioon, 8.2 Ressursid, 10.2 Personalijuhtimine).

Tulemuslikkus, dokumenteerimine ja aruandlus

Valdkondlike nõuete kohaldamisel 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).

Valdkondlikud nõuded on loodud järjepidevate ja kvaliteetsete siseauditi praktikate toetamiseks. Kohalikud seadused, määrused, järelevalvelasend ootused ja muud kutsealaselt tunnustatud raamistikud võivad kehtestada täiendavaid või spetsiifilisemaid nõudeid. Siseaudiitorid peavad mõistma ja järgima seadusi ja/või määrusi, mis on seotud selle tööstusharu ja jurisdiktsiooniga, kus organisatsioon tegutseb, sealhulgas avalikustama nõutava teabe vastavalt standardile 1.3 "Õiguspärane ja eetiline käitumine". Siseaudiitorid võivad olla juba integreerinud need lisanõuded auditiprogrammidesse ja testimisprotseduuridesse ning peaksid neid võrdlema valdkondlike nõuetega, et tagada piisav katvus.

Valdkondliku nõude täitmist võib vastavalt siseaudiitori kutsealasele otsustusele dokumenteerida kas siseauditi tööplaanis 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.

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.

Kolmas osapool

Kolmas osapool on väline isik, grupp või üksus, kellega organisatsioon ("põhiorganisatsioon") loob ärisuhte toodete või teenuste saamiseks. Suhted võivad olla vormistatud lepingu, kokkuleppe või muul kujul, et pakkuda organisatsioonile tooteid, teenuseid, tööjõudu, tootmist või infotehnoloogilisi lahendusi, näiteks andmete säilitamist, töötlemist ja hooldust.

Mõistet "kolmas osapool" võidakse määratleda ja kasutada erinevalt, sõltuvalt tööstusharust või muust kontekstist. Igal siseauditi funktsioonil on paindlikkus kasutada oma otsustusõigust valdkondliku nõude kohaldamisel vastavalt sellele, kuidas põhiorganisatsioon (organisatsioon, kes sõlmib kolmanda osapoolega lepingu) kolmandaid osapooli määratleb. Kolmanda osapoole valdkondlikus nõudes ja kasutusjuhendis tähendab mõiste "kolmas osapool" müüjaid, tarnijaid, töövõtjaid, alltöövõtjaid, sisseostetud teenusepakkujaid, muid asutusi ja konsultante. Mõiste "kolmas osapool" hõlmab kõiki selliseid kokkuleppeid, sealhulgas kolmanda osapoole ja tema alltöövõtjate vahelisi kokkuleppeid, mida sageli nimetatakse "alltöövõtjateks", "neljandateks osapoolteks", "viiendateks osapoolteks" või üldisemalt "n-nda taseme osapoolteks".

Käesolev valdkondlik nõue ei käsitle kaudseid väliseid suhteid, huvisid või seotusi põhiorganisatsiooniga, näiteks regulaatorite, esindajate, maaklerite, investorite, usaldusisikute/juhatuse liikmete, avalike teenuste ja üldsusega, ega sisemisi suhteid, näiteks töötajate või kontsernisiseste teenusepakkujatega.

Mõiste "kolmas osapool" võib olla määratletud ja seda võib kasutada erinevalt, sõltuvalt tööstusharust või muudest kontekstidest. Siseaudiitoritele on tagatud paindlikkus ja nad peaksid tuginema oma kutsealasele otsustusvõimele, et kohendada valdkondlikku nõuet põhiorganisatsiooni kolmanda osapoole määratlusega.

Organisatsiooni protsesside tõhusust oma suhete haldamisel kolmanda osapoolega võib hinnata kogu organisatsioonis ja/või ühe või mitme üksiku lepingu, kokkuleppe või suhte tasandil. Siseaudiitorid peaksid kasutama ülalt-alla lähenemisviisi, et arendada arusaamist organisatsiooni kolmanda osapoole poliitikatest, protseduuridest, protsessidest, raamistikust ja elutsüklist. Siseaudiitorid peaksid kasutama kutsealast otsustust, et mõista kolmanda osapoole riskide nüansse, lähtudes konkreetsetest tööstusharudest, organisatsioonidest ja tööde teemadest. Kooskõlas standardiga 5.1 "Informatsiooni kasutamine" peaksid siseaudiitorid olema teadlikud ja

Märkus

Valdkondlikud nõuded kasutavad üldist siseauditi terminoloogiat, mis on määratletud Ülemaailmsetes siseauditi standardites. Lugejad peaksid tutvuma standardite sõnastikus esitatud mõistete ja määratlustega.

järgima kõiki poliitikaid ja protseduure, mis on seotud kolmanda osapoole teabega, millele nad võivad juurdepääsu saada.

Käesolevat valdkondlikku nõuet kohaldatakse, kui siseauditi funktsioon täidab kindlustandvaid ülesandeid kolmandate osapoolte ja/või alltöövõtjate suhtes, sealhulgas neljandas või järgmises järgus, mis on lubatud kolmanda isiku 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 vastavalt riskihindamise tulemustele, ning kõik erandid tuleb dokumenteerida.

Kolmanda osapoole valdkondlik nõue ja kasutusjuhend viitavad organisatsiooni ja tema kolmandate osapoolte vaheliste suhete etappidele, mida nimetatakse ka elutsükli etappideks: valimine, lepingute sõlmimine, kasutuselevõtmine, järelevalve ja suhte lõpetamine. Neid etappe kasutatakse kolmanda osapoole valdkondlike nõuete ja kasutusjuhendi puhul ka siis, kui mõnes tegevusvaldkonnas kasutatakse elutsükli kohta teistsuguseid käsitlusi. Elutsükli etapid on järgmised:

- Valimine: hõlmab protsesse, mille abil määratakse kindlaks vajadus kolmanda osapoole järele, kavandatakse selle kasutamine ning viiakse läbi valikuga seotud hoolsusmeetmed (*due diligence*). Lisaks peaks valik hõlmama võimalike ja kaasatud kolmandate osapoolte riskide hindamist.
- Lepingute sõlmimine: hõlmab hoolsusmeetmete protsesse kolmanda osapoolega sõlmitava lepingu või muu õigusliku kokkuleppe koostamiseks, läbirääkimisteks, heakskiitmiseks ja rakendamiseks.
- Kasutuselevõtt: algab lepingu allkirjastamisel suhte alustamiseks ning loob aluse sellele, et kolmandad osapooled saaksid täita lepingu või kokkuleppe tingimusi.
- Järelevalve: hõlmab nn „aktiivse elutsükli“ juhtimist ja kolmanda osapoole pidevat jälgimist pärast lepingu sõlmimist ja heakskiitmist. Lähenedisviis on tavaliselt süstemaatiline ja riskipõhine ning peaks arvestama pideva parendamisega. Järelevalve hõlmab ka vajaduse korral kolmanda osapoolega sõlmitud lepingute või kokkulepete uuendamist.
- Suhte lõpetamine: hõlmab lepingute ja kokkulepete lõpetamise protsesse, riskipõhiselt prioriseeritud kolmandate osapoolte väljumisstrateegia haldamist ja vajaduse korral suhete lõpetamist. Protsessid kasutavad tavaliselt riskipõhist lähenedisviisi ja võivad hõlmata ametlikku väljumisplaani (*exit plan*).

Põhiorganisatsioon vastutab oma eesmärkide saavutamise seotud riskide eest isegi siis, kui ta kaasab kolmanda osapoole, kes aitab tal saavutada ühte või mitut eesmärki. Kolmandate osapoolte kaasamine võib vähendada mõningaid organisatsiooni kulusid, mis on seotud protsesside läbiviimisega. See võib aga tekitada tegevusriske, sest põhiorganisatsioonil on vähem nähtavust ja volitusi kolmanda osapoole kontrolliprotsesside üle. Kui kolmas osapool ei täida lepingut, osaleb ebaeetilistes tegevustes või või kogeb ärikatkestusi, võib see tuua põhiorganisatsioonile negatiivseid tagajärgi.

Põhiorganisatsioon peab tuvastama, hindama ja juhtima riske asjakohaste valitsemise-, riskijuhtimis- ja kontrolliprotsesside kaudu. Kolmandate osapooltega seotud riskide kategooriad ja näited hõlmavad muuhulgas järgmist:

- Strateegilised riskid, näiteks organisatsiooni võime täita oma missiooni ja/või kõrgetasemelisi eesmäärke või hallata ühinemiste ja omandamiste mõju.
- Maineriskid, näiteks keskkonnakahjustustest tulenev kahju või kahju põhiorganisatsiooni suhetele ja usaldusele klientide, tarbijate ning huvirühmadega.
- Eetilised riskid, näiteks aususe puudumine, huvide konfliktid, altkäemaksud ja korruptsioon.
- Tegevusriskid, näiteks füüsilise ja infoturbe puudujäägid, siseringirisk, teenusekatkestused ja eesmärkide mittesaavutamine.
- Finantsriskid, näiteks kolmanda osapoole maksejõuetus ja pettus.
- Vastavusriskid, näiteks mittevastavus kehtivatele kohalikele, riiklikele ja rahvusvahelistele regulatiivsetele nõuetele.
- Küberturvalisus ja muud andmekaitse riskid, näiteks tundlike andmete ohustamine ja lekkimine.
- Infotehnoloogilised riskid, näiteks kriitiliste tegevuste toetamiseks vajalike IT-teenuste puudumine.
- Õiguslikud riskid, näiteks huvide konfliktid, vaidlused ja kohtuvaidlused lepingu rikkumise korral.
- Jätkusuutlikkuse riskid, näiteks keskkonna-, sotsiaalsed ja valitsemisalased (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.

Siseaudiitorid peaksid valitsemis-, riskijuhtimis- ja kontrolliprotsesside nõuete hindamisel arvestama kolmanda osapoole elutsükli kõiki etappe.

Kolmanda osapoole valdkondlikud nõuded on jaotatud kolme ossa vastavalt standardile 9.1 "Valitsemis-, riskijuhtimis- ja kontrolliprotsesside mõistmine":

- Valitsemine - selgelt määratletud põhieesmärgid ja strateegiad kolmandate osapoolte kasutamiseks organisatsiooni eesmärkide, poliitikate ja protseduuride toetamiseks.
- Riskijuhtimine - protsessid kolmandate osapoolte kasutamisega seotud riskide tuvastamiseks, analüüsimiseks, juhtimiseks ja jälgimiseks, sealhulgas protsess intsidentide kiireks eskaleerimiseks.
- Kontrollid - juhtkonna poolt kehtestatud ja perioodiliselt hinnatud kontrolliprotsessid, et maandada riske kolmandate osapoolte kasutamisel.

Lisaks valdkondlikele nõuetele ja käesolevale kasutusjuhendile võivad siseaudiitorid soovida tutvuda täiendavate kutsealaste juhenditega kolmandate osapoolte kohta, näiteks Rahvusvahelistest kutsetegevuse raampõhimõtte (IPPF) ülemaailmsete juhenditega ja tegevusvaldkonna spetsiifiliste ressurssidega.

Kaalutlused

Järgmised kaalutlused võivad aidata siseaudiitoritel rakendada kolmanda osapoole valdkondlikke nõudeid. Iga alljärgneva jaotise tähega tähistatud väiteid esitavad vastava valdkondliku nõude nõudeid uuesti või parafraseerivad neid. Need mittekohustuslikud kaalutlused on illustratiivsed, et anda näiteid nõuete hindamise võimaluste kohta. Siseaudiitorid peaksid kasutama kutsealast otsustust, kui nad hindavad, mida oma otsustes arvesse võtta.

Valitsemisalased kaalutlused

Selleks, et hinnata, kuidas valitsemisprotsesse, sealhulgas kõrgema juhtorgani järelevalvet, rakendatakse kolmanda osapoole eesmärkide suhtes, võivad siseaudiitorid vaadata läbi tõendusmaterjali järgmistest aspektidest:

- A. Formaliseeritud ja dokumenteeritud riskipõhine lähenemine või strateegia otsustamiseks, kas kasutada kolmandat osapoolt. Lähenemine vaadatakse perioodiliselt läbi ja see hõlmab järgmist:
 - Selgelt määratletud ja standardiseeritud protsess lähenemisviisi rakendamiseks, mis on organisatsiooni poolt kasutamiseks heaks kiidetud.
 - Eelarvestatud ressursid, mis põhinevad kulude-tulude analüüsil, et põhjendada kolmanda osapoole kaasamist, tagades strateegilise kooskõla ja ressursi tõhusa kasutuse.
 - Juhtkonna hinnang riskidele ja kontrollidele, sealhulgas neile, mis käsitlevad kolmandate osapooltega seotud probleeme.
 - Piisavad ressursid kolmanda osapoollega lepingu sõlmimiseks, selle haldamiseks ja tulemuslikkuse jälgimiseks.
 - Huvirühmade tagasiside integreerimine lähenemisviisi või strateegiasse.
- B. Põhimõtted, protseduurid ja muud asjakohased dokumendid, mida kasutatakse kolmanda osapoole suhete määratlemiseks, hindamiseks ja haldamiseks kogu elutsükli jooksul. Põhimõtted ja protseduurid võivad hõlmata järgmist:
 - Standardiseeritud tööriistad ja mallid, et hõlbustada peamisi valitsemis-, riskijuhtimis- ja kontrolliprotsesse.
 - Protsessid põhimõtete ja protseduuride perioodiliseks hindamiseks, nende piisavuse kindlakstegemiseks ning vajaduse korral ajakohastamiseks.
 - Kehtestatud kriteeriumid kolmandate osapoolte valimiseks, lepingute sõlmimiseks, kasutuselevõtuks, järelevalveks ja suhte lõpetamiseks.
 - Kohaldatavate regulatiivsete nõuete tuvastamine ja perioodiline läbivaatamine, et tagada põhimõtete ja protseduuride vastavus.

- Võrdlusanalüüsid, mille eesmärk on tuvastada ja võrrelda parimaid praktikaid kolmanda osapoole haldamisel.
- C. Selgelt määratletud rollid ja vastutused, mis toetavad kolmanda osapoolega seotud eesmärkide saavutamist. Täiendavad tõendid võivad hõlmata järgmist:
 - Protsessid, mille abil hinnatakse, kas kolmanda osapoole väärtused, eetika ja ettevõtte sotsiaalne vastutus on kooskõlas põhiorganisatsiooni põhimõtetega. Protsess peaks hõlmama seda, kuidas võimalikke huvide konflikte või ebaeetilisi tavasid kiiresti käsitleda.
 - Regulaarne koolitus töötajatele, kes täidavad kolmanda osapoole haldamisega seotud rolle, ning nende pädevuste perioodiline hindamine.
 - Protsess, millega hinnatakse, kas läbiviidud koolitused toovad kaasa organisatsiooni teadlikkuse tõstmise kolmandatest osapooltest.
 - Rollid ja vastutused on kooskõlas kolme liini mudeliga.
- D. Õigeaegne suhtlus ja koostöö asjakohaste huvirühmadega kogu kolmanda osapoole elutsükli jooksul (näiteks kõrgem juhtorgan, tippjuhtkond, hangete üksus, operatiivüksused, riskijuhtimine, vastavuskontroll, õigusteenistus, infotehnoloogia, infoturve, personaliosakond jt), mis hõlmab järgmist:
 - Teave kolmanda osapoole riskide ja teadaolevate võimalike haavatavuste kohta, mis on kajastatud koosolekute protokollides, aruannetes või e-kirjades.
 - Teabevahetus kolmanda osapoole haldamise kohta ja koostöö edendamine (näiteks regulaarsete valdkonnaüleste kohtumiste kaudu).

Riskijuhtimisega seotud kaalutlused

Selle hindamiseks, kuidas riskijuhtimise protsesse rakendatakse kolmanda osapoolega seotud eesmärkidele, võivad siseaudiitorid vaadata üle tõendid selle kohta, et:

- A. Kolmanda osapoole teenuste kasutaja standardiseeritud ja terviklikud riskijuhtimise protsessid hõlmavad määratletud rolle ja vastutusi ning käsitlevad piisavalt organisatsiooni jaoks olulisi põhiriske:
 - Kolmanda osapoole riskide hindamise ja haldamise protsessid hõlmavad kuidas peamisi riske:
 - algselt tuvastatakse ja raporteeritakse.
 - analüüsitakse, et hinnata nende mõju organisatsiooni eesmärkide saavutamise võimele.
 - maandatakse, sealhulgas tegevuskavadega vähendatakse risk vastuvõetavale tasemele.
 - monitooritakse, sealhulgas varajaste hoiatusmärkide tuvastamine ja neile reageerimine ning olemas on pidev aruandlus kuni ohtude täieliku kõrvaldamiseni.

- Jälgitakse protsessidest kinnipidamist ja kõrvalekallete korral parandusmeetmete rakendamist, et vältida organisatsiooni pikaajaliste eesmärkide või strateegia kahjustamist.
 - Riskijuhtimise komitee või muu üksus teostab kolmandate osapoolte üle otsest järelevalvet ning annab sisendi kõrgemale juhtorganile. Komiteel on selgelt määratletud eesmärk ja ta kohtub regulaarselt. Tõendusmaterjaliks võivad olla koosolekute protokollid.
- B.** Kolmandate osapooltega seotud riske tuvastatakse ja hinnatakse korrapäraselt kogu elutsükli jooksul. Riskihindamise tulemusel järjestatakse ja prioriseeritakse kolmandad osapooled. Samuti järjestatakse ja seatakse prioriteetsuse järjekorda riskidele reageerimise meetmed.
- Põhiorganisatsioon võtab kolmanda osapoole riskihindamise väljatöötamisel arvesse selliseid tegureid nagu tema suurus, küpsusaste ja kaasatud kolmandate osapoolte arv.
 - Riskihindamine on dokumenteeritud ja selles on kindlaks määratud loomuomased ja jääkriskid.
 - Organisatsioon järgib riskihindamise läbivaatamisel ja ajakohastamisel hoolsusmeetmete protsessi.
 - Kehtestatud on kriteeriumid kolmandate osapoolte järjestamiseks ja prioriseerimiseks vastavalt riskitasemele. Sellised kriteeriumid on näiteks järgmised:
 - Osutatavad teenused on organisatsiooni tegevuse jaoks kriitilise tähtsusega.
 - Kokkuleppe rahaline väärtus on oluline.
 - Suhe on uus, kiiresti sõlmitud ja/või selle kestus on pikk.
 - Sellega on seotud mitmed välised osapooled.
 - Kolmas osapool kavatseb töö teostamiseks kasutada osaliselt või täielikult alltöövõttu.
 - Organisatsioon järgib üldtunnustatud riskihindamise tavasid, sealhulgas põhimõtet, et riskihindamine viiakse läbi võimalikult varajases etapis, tavaliselt siis, kui pakkumist analüüsitakse valikufaasis, ja enne kolmanda osapoole kasutuselevõtmist.
 - Tarnijad täidavad küsimustiku, et määrata kindlaks nende riskide järjestus ja prioriteetsus loomumaste riskide põhjal. Organisatsioon tagab, et küsimustikud täidetakse asjakohaste töötajate poolt ja need vaadatakse üle, et tagada nende täpsus.
 - Organisatsioon kogub regulaarselt sisendit kolmanda osapoole riskijuhtimise kohta erinevatelt üksustelt, nagu infotehnoloogia, hankefunktsioon, ettevõtte riskijuhtimine, personalijuhtimine, õigusteenistus, vastavuskontroll, operatsioonid, raamatupidamine ja finantsüksus.
- C.** Riskidele reageerimise meetmed, nagu riskide maandamine, aktsepteerimine, kõrvaldamine ja jagamine, on kindlaks määratud ja vastavuses riskihinnangule.

- Riskidele reageerimise meetmed on dokumenteeritud ja see hõlmab ka kolmandate osapoolte kontrollikeskkonna arvestamist.
 - Olemas on dokumentatsioon, mis kinnitab, et organisatsiooni riskitaluvust ületavate riskide (eriti juhul, kui riskid aktsepteeritakse) käsitlemine on üle vaadatud ja hinnatud asjakohaseks. Reageerimismeetmed hõlmavad ka kolmandate osapooltega seotud võimalike huvide konfliktide käsitlemist.
- D.** Kehtivad protsessid kolmanda osapoole riskide haldamiseks ja eskaleerimiseks, sealhulgas see, kuidas ohu või riski taset hinnatakse, määratakse ja prioriseeritakse. Ülevaade võib muuhulgas hõlmata järgmiste asjaolude kindlakstegemist:
- Organisatsiooni riskitasemete määratlused ja selgitused (näiteks kõrge, mõõdukas ja madal risk) ning iga riskikategooria eskaleerimisprotseduurid.
 - Riskide alusel prioriseeritud kolmandate osapoolte loetelu ning riskisündmuste maandamise staatus.
 - Kohaldatavad õiguslikud, regulatiivsed ja vastavusnõuded.
 - Riskide mõjud, nii finantsiline kui ka mittefinantsiline (näiteks mainekahju).
 - Kehtivad protsessid kolmanda osapoolega seotud riskide kommunikeerimiseks juhtkonnale ja töötajatele, sealhulgas riskiprofiili regulaarne aruandlus kõrgemale juhtorganile (või muule asjakohasele organile). Kommunikatsioon peaks sisaldama ajakohastatud teavet prioriteetsete kolmandate osapooltega seotud probleemide kõrvaldamise seisu kohta.
 - Olemas on protsessid kolmandate osapoolte riskitaseme ja prioriteetsuse ümberhindamiseks, kui põhiorganisatsiooni riskiisu ja riskitaluvuse tasemed muutuvad.

Kontrollidega seotud kaalutlused

Selleks, et hinnata, kuidas kontrolliprotsesse rakendatakse kolmanda osapoolega seotud suhtes, võivad siseaudiitorid kontrollida tõendeid, et:

- A.** Kolmandate osapoolte leidmiseks ja valimiseks on kehtestatud tugev hoolsuskohustuse täitmise protsess, mis sisaldab dokumenteeritud ja heakskiidetud ärilist põhjendust või muud asjakohast dokumentatsiooni, mis kirjeldab ja põhjendab kolmanda osapoolega suhte vajadust ja olemust.
- Äriline põhjendus võib ka:
 - Käsitleda riske, mis võivad mõjutada kolmanda osapoole võimet täita ootusi, ning nende võimalikku mõju organisatsioonile.
 - Sisaldada üksikasjalikku kulude-tulude analüüsi.
 - Järgitakse kehtestatud hankemenetlust, näiteks konkurentsipõhine hankemenetlus, pakkumiskutse ja otseost. Protsesside hulka kuuluvad:
 - Oluliste aspektide hindamise kriteeriume, näiteks küberturbe protokollide läbivaatamine, pangarekvisiitide kontrollimine, finantstausta kontrollimine ning kolmanda osapoole organisatsioonilise struktuuri, kriminaal- ja kohturegistrite,

sõidukijuhtimise ajalooga seotud andmete, poliitilise tegevuse ja võimalike kuritegelike sidemete uurimine.

- Selgelt määratletud valikukriteeriumid, sealhulgas varasemate tulemuslikkuse, soovitude, maine ja lepinguliste kulude hindamiseks.
- Hoolsuskohustuse täitmine, et tagada tarnijate asjakohane valik, näiteks moodustades valdkondade üleseid meeskondi pakkumiste hindamiseks. Kallutatuse riski maandamiseks on ülevaatusmeeskondadele kehtestatud kontrollid, sealhulgas meeskondade moodustamise protseduurid ja nõuded võimalike huvide konfliktide avalikustamiseks.
- Hoolsusmeetmed kolmanda osapoole kontrollikeskkonna hindamisel; näiteks kohapealse külastuse läbiviimine või kolmanda osapoole järgmiste aspektide läbivaatamine:
 - Süsteemi ja organisatsiooni kontrolli (SOC) aruanded.
 - Finantsstabiilsus.
 - Asutamisleping või tegevusluba.
 - Võtmejuhtkonna ja huvigruppide otsustusprotsessi läbipaistvus.
 - Organisatsiooniline struktuur.
 - Operatiivne stabiilsus.
 - Küberturvalisuse protokollid.
 - Vastavus asjakohastele seadustele, määrustele ja standarditele.
 - Eetika.
 - Varasem koostöökogemus põhiorganisatsiooniga.
 - Maine.
- Olemas on tõendid selle kohta, et potentsiaalsed tarnijad või töövõtjad liiguvad elutsükli lepingu sõlmimise etappi alles pärast asjakohaste hoolsusmeetmete läbiviimist ning tulemuste analüüsimist.

B. Lepingute sõlmimistega seotud põhimõtted ja protseduurid on kehtestatud ja neid järgitakse.

- Lepingud on sõnastatud üheselt mõistetavalt.
- Lepingu koostamise etapis võetakse arvesse peamisi riske ja lisatakse asjakohased klauslid. Lahendamist vajavad küsimused kommunikeeritakse kolmanda osapoolega juba selles etapis.
- Lepingute olulised elemendid määratakse kindlaks vastavalt organisatsiooni lepingute sõlmimise põhimõtetele ja protseduuridele ning kolmanda osapoole prioriteetsuse tasemest lähtuvalt. Elementide hulka võivad kuuluda:
 - Konfidentsiaalsuse- ja andmekaitseklauslid.
 - Lepingu lõpetamisklauslid ja selgelt määratletud andmetele juurdepääsu parameetrid.

- Küberturbe nõuded, sealhulgas nõuded, mis käsitlevad juurdepääsu kõikidele andmetele ja nende jagamist ning vahejuhtumitest või rikkumistest teatamist kindlaksmääratud aja jooksul.
 - Nõuded, mis on seotud põhiorganisatsiooni andmeid mõjutava rikkumise teatamisega.
 - Standardiseeritud protsess kolmanda isiku tuvastamiseks, sealhulgas tema täieliku juriidilise nime, aadressi, füüsilise asukoha (füüsilised asukohad) ja veebilehe. Tavapärane on kasutada identifitseerimisprotsessi ajal kontroll-lehte ja kontrollida teabe õigsust.
 - Selgelt määratletud teenusetaseme lepingud (SLAd), milles määratakse kindlaks oodatavad tulemused ning iga osapooli õigused, kohustused, trahvid, hüved ja vastutused, sealhulgas vastutus tööjõukulude tasumise eest (sh alltöövõtjatele).
 - Auditeerimisõiguse klausel, mis hõlmab alltöövõtjaid või nõuet tõendada, et usaldusväärne sõltumatu teenusepakkuja on osapooli auditeerinud. Ilma auditeerimisõiguse klauslita võib siseauditi funktsiooni võime saada või anda kindlust olla piiratud.
- Põhiorganisatsioonil on juurdepääs sõltumatute audiitorite kontrollihindamise aruannetele, näiteks finants-, vastavus- ja andmeturbe aruannetele, nagu kindlustandvate tööde rahvusvahelise standardi aruanded või SOC-aruanded.
 - Kui tuginetakse välise kolmanda osapool kindlustandvale tööle, vaadatakse dokumendid läbi, et tagada usaldusväärsus.
 - Süsteemi ja organisatsiooni kontrolli (SOC) aruandeid kasutatakse ebapiisavate riski- ja muutuste juhtimise protsesside tuvastamiseks.
- Põhimõtted ja protseduurid käsitlevad kõiki komponente, mis on konkreetsete organisatsioonide või lepingutüüpide jaoks olulised:
 - Keskkonna- ja jätkusuutlikkuse klauslid.
 - Vilepühumise põhimõtted.
 - Nõuded tulemusnäitajate hindamisele.
 - Testitud talitluspidevuse plaanid kolmandate isikute jaoks.
 - Tehisintellekti kasutamine teenuste osutamisel.
 - Kõikide allhanketööde selge määratlemine, avalikustamine, nende tingimused ja ulatus.
 - Muudatuste haldamise protsess, milles kirjeldatakse, kuidas käsitleda lepingu kehtivusaja jooksul toimuvaid muudatusi selle ulatuses, tingimustes või tegevusnõuetes (näiteks muudatused tehnoloogias või uuendused regulatsioonides).
 - Piirangud lepingumuudatuste arvus või summas, mida võib arveldada.
- Põhimõtted ja protseduurid nõuavad lõpptoodete ametlikku vastuvõtmist enne makse tegemist või mis tahes kinnipeetud summa vabastamist.

- Kolmandatelt osapooltelt nõutakse oma eetikapoliitika või käitumiskodeksi jagamist ja/või põhiorganisatsiooni vastavate nõuete järgimist.
 - Kui lepingu esitab kolmas osapool, on põhi organisatsioon teinud sellele õigusliku ülevaatuses ning on tuvastanud peamised riskid ja paika pannud sobiva riskimaandamisestrategia.
- C. Lõplikud lepingud või kokkulepped vaatavad läbi ja kiidavad heaks asjakohased huvirühmad, sealhulgas õigus- ja vastavusfunktsioon, neid säilitatakse turvaliselt ning vastutus määratakse lepinguomanikule või selle halduritele.
- Leping või muu ametlik dokument, mis kinnitab allhanke suhte olemasolu ja kolmanda osapoole kohustusi, ning tõendid nõutavate õigus- ja vastavusfunktsiooni kontrollide kohta.
- D. Kõikide kolmandate osapoolte vaheliste suhete täpne, täielik ja ajakohane loetelu säilitatakse, näiteks tsentraliseeritud lepinguhaldussüsteemis.
- Protsess uute kolmandate osapoolte lepingute või kokkulepete lisamiseks loetellu või süsteemi.
 - Protsess võimalike kolmandate osapoolte sisestamiseks tarnijate süsteemi ja nende eemaldamiseks, kui lepingut heaks ei kiideta.
 - Protsess kolmanda osapoole lepingute või kokkulepete eemaldamiseks süsteemist.
 - Jälgimissüsteem, et dokumenteerida konkreetsete töövõtjate või tarnijatega seotud probleemid edaspidiseks.
 - Ülevaatusprotsess veendumaks, et kolmandate osapoolte loetelu on täpne ja täielik.
- E. Tarnijate kasutuselevõtuprotsessid on dokumenteeritud ja neid järgitakse, et võimaldada kolmandatel osapooltel täita lepingu või kokkuleppe tingimusi. Ülevaatused võivad hõlmata kontrolli selle üle, kas:
- Standardiseeritud kasutuselevõtuprotseduurid tagavad, et kogu vajalik dokumentatsioon, koolitused ja vastavusülevaatused on lõpule viidud.
 - Kolmandate osapoolte süsteemid ja protsessid saab sujuvalt integreerida põhiorganisatsiooni tehnoloogiaga.
 - Jagatud süsteemid on ühilduvad ja turvalised. Tõendusmaterjalid võivad hõlmata täiendavaid kasutajaüksuse kontrole süsteemi ja organisatsiooni kontrolli (SOC) aruandluse osana.
 - Põhiorganisatsioon hindab kolmanda osapoole talitluspidevuse plaane, mis tagavad teenuse jätkumise hädaolukordades. Võimalike häirete lahendamiseks on olemas varuplaanid.
- F. Protsessid tarnijate tulemuslikkuse pidevaks jälgimiseks võrreldes lepingu või kokkuleppe eesmärkidega, sealhulgas põhitulemusnäitajate hindamine.
- Järelevalveprotsessid annavad sisendi kolmanda osapoole riskihindamisele ning tuvastatud kontrollinõrkused vaadatakse läbi, eskaleeritakse ja vajaduse korral käsitletakse neid.

- Aruanded või tehtud tähelepanekud protsesside, tehnoloogiate ja tööriistade kohta, mis on loodud reaalajas monitoorimiseks.
 - Protsessid tagamaks, et maksed tehakse vastavalt lepingu või kokkuleppe tingimustele, näiteks projekti ajakava, vaheetappide ja teavitamiskooste täitmisel. Makseid tehakse ainult heakskiidetud töövõtjatele, kes on läbinud kogu tarnijate kasutuselevõtu protsessi ja on sisestatud tarnijate maksesüsteemi. Kui lepingus on määratletud üleantavad tulemused, tehakse lõppmaksed alles pärast nende kontrollimist.
 - Kolmanda osapoole lepingutega seotud kulude kontroll, et tagada soovitud lisandväärtus ja hinnata investeringu tasuvus. Kulu-tulu analüüsi tulemusi kasutatakse lepingute uuesti läbirääkimiseks.
 - Protsessid trahvide hindamiseks lepingus või kokkuleppes sätestatud teenustaseme kokkulepete rikkumise korral. Trahvid arvutatakse ja nõutakse sisse nende tekkimisel.
 - Prioriseeritud kolmandate osapoolte riskipõhist järjestust hinnatakse perioodiliselt ümber, kui lepingus tehakse muudatusi ja kui leping on lõppemise või automaatse uuendamise lähedal.
 - Prioriteetsete kolmandate osapoolte ülevaated, näiteks kohapealsed kontrollid või kvartaalsed ärilised ülevaated, et kinnitada kontrollide ja tegevuse terviklikkust.
 - Täiendava pideva jälgimise tõendid võivad hõlmata järgmist:
 - Kolmanda osapoole finantsstabiilsuse analüüsid.
 - Kolmandate osapoolte vastu esitatud kaebuste hindamised.
 - Juhtkonna ülevaated sõltumatu audiitori aruannetest, näiteks kindlustandvate tööde rahvusvahelise standardi (International Standard on Assurance Engagements), tõendusandvate tööde standardite (Statements on Standards for Attestation Engagements), finants-, auditi-, vastavus- ja andmeturbe aruannete ning kolmandate osapoolte esitatud ISO-sertifikaatide kohta.
 - Juhtkonna ülevaated kolmanda osapoole läbiviidud talitluspidevuse (*business resilience*) testidest, sealhulgas kõigist tuvastatud olulistest probleemidest.
 - Alltöövõtjate kasutamise tingimused ja piirangud.
 - Kolmanda osapoole eetiliste väärtuste, kultuuri ja käitumise hindamised.
 - Vastused meedia päringutele.
 - Privaatsuse ja küberturvalisuse protokollide hindamised, et kaitsta põhiorganisatsiooni andmete ja teabe säilitamist ja edastamist, sealhulgas kõrgtehnoloogia, näiteks tehisintellekti kasutamist.
 - Organisatsiooni tuvastatud võimalused tulemuslikkuse pidevaks parandamiseks ja lepingu või kokkuleppe eesmärkide täitmiseks.
 - Ülesannete lahususe läbivaatamine.
- G. Protokollid parandusmeetmete algatamiseks tuvastatud intsidentide korral, kui kolmas osapool ei täida lepingu või kokkuleppe nõudeid või kui kolmanda osapoole tegevus suurendab põhiorganisatsiooni riski.

- Protokollid intsidentide eskaleerimiseks vastavalt intsidendi tõsidusele ja kolmanda osapoole prioriteetsusele.
 - Intsidendijärgne läbivaatus, sealhulgas algpõhjuste analüüs.
- H. Protsessid, mis annavad hoiatusi lepingute ja kokkulepete lõppemise või automaatse pikenemise kohta. Automaatse pikenemise protsessid hõlmavad järgmise ülevaatamist:
- Kolmanda osapoole tulemuslikkus.
 - Lepingu või kokkuleppe tingimused ja kõik lisad.
 - Riskitegurid.
- I. Ametlikku tarnijasuhete lõpetamise plaani rakendatakse ja järgitakse, et tagada lepingutingimuste, sealhulgas ajastuse ja ootuste, nõuetekohane täitmine, samuti kõigi allapoole delegeeritud alltöövõtjate puhul.
- Kontroll-lehed või intervjuud peamiste huvirühmadega, et tagada turvameetmete tõhusus.
 - Kolmanda osapoole valduses olnud organisatsiooni teave või andmed on tagastatud või hävitatud.
 - Kolmanda osapoole juurdepääs organisatsiooni andmetele, süsteemidele või ruumidele on tühistatud.
 - Põhiorganisatsiooni varad, nagu seadmed, tarkvaralitsentsid, intellektuaalomand ja dokumentatsioon, on tagastatud.
 - Kui kolmanda osapoole leping lõpetatakse mõjuval põhjusel, tuvastatakse erandlikud asjaolud või riskid ja edastatakse need tippjuhtkonnale ja/või kõrgemale juhtorganile.
 - Kui prioriteetse kolmanda osapoole leping lõpetatakse, asendatakse see osapool sama riskihinnangu alusel, välja arvatud juhul, kui leping on täidetud või seda ei ole enam vaja.

Lisa A. Praktilised näited

Järgnevad näited kirjeldavad olukordi, mille puhul kohaldatakse Kolmanda osapoole valdkondlikku nõuet:

Näide 1: Siseauditi tööplaanis sisalduv siseauditi töö hõlmab teenust või väljundit, mida pakub praegu kolmas osapool.

Kui siseauditi funktsioon viib lõpule oma riskipõhise planeerimisprotsessi ja lisab siseauditi tööplaani ühe või mitu sellist teenust või väljundit, mida praegu osutavad lepingu või kokkuleppe alusel kolmandad osapooled, on valdkondliku nõude rakendamine kohustuslik.

Kõik valdkondliku nõude nõuded ei pruugi olla kohaldatavad iga töö puhul. Kui siseaudiitorid rakendavad kutsealast otsustust ja otsustavad, et üks või mitu kolmanda osapoole valdkondliku nõude nõuet ei ole kohaldatavad ja seetõttu tuleks need tööst välja jätta, peavad siseaudiitorid selle dokumenteerima ja säilitama nende nõuete väljajätmise põhjenduse. Näiteks võib teatavate nõuete väljajätmise põhjuseks olla see, et siseauditi funktsioon on kindlaks teinud, et organisatsiooni sõltuvus kolmandatest isikutest missioonikriitiliste teenuste osutamisel on väike või et tegemist on väljakujunenud suhtega, millel on väike finantsmõju.

Näide 2: Kolmanda osapoole riskid tuvastatakse kindlustandva töö käigus teemal, mis ei puuduta kolmandaid osapooli ega lepingute haldamist.

Siseaudiitorid võivad tuvastada märkimisväärse kolmanda osapoolega seotud riski, hinnates protsessi, mida algselt ei peetud kolmandate osapoolte või lepingute haldamisega seotud olevaks. Näiteks andmete säilitamise hindamise töö planeerimisel saavad siseaudiitorid teada, et pilveteenuseid haldab kolmas osapool. Intervjuude käigus kolmanda osapoole pakutavate teenuste juhtkonnaga tuvastavad siseaudiitorid kolmanda osapoolega seotud küberturbe riskid.

Pärast asjakohaste riskide tuvastamist peavad siseaudiitorid läbi vaatama nii kolmanda osapoole kui ka küberturbe valdkondlikud nõuded ning määrama kindlaks, millised nõuded on kohaldatavad. Audiitorid võivad töö ulatusest välja jätta kolmanda osapoole valitsemisprotsessi või kolmanda osapoole riskijuhtimise protsessi ja keskenduda auditeeritavate teenuste üle teostatavale kolmanda osapoole kontrollile. Sama kutsealane otsustus kehtib ka küberturvalisuse valdkondliku nõude kohaldamisel. Audiitorid peavad dokumenteerima tööde dokumentides põhjendused, miks kolmanda osapoole või küberturvalisuse valdkondlike nõuete mis tahes nõuded on välja jäetud ning säilitama selle dokumentatsiooni.

Näide 3: Vajalikuks osutub kolmanda osapoolega seotud töö, mida ei olnud algselt siseauditi tööplaani lisatud.

Organisatsioonis tekib probleem, mis on seotud prioriteetse kolmanda osapoolega ja mis nõuab siseauditi funktsiooni viivitamatut tähelepanu. Probleem hõlmas kontrolli mittetoimimist. Siseauditi juht peaks suhtlema kõrgema juhtorganiga siseauditi tööplaani ja ressursside

ümberrangustamisest, et tekkinud vajadust arvesse võtta. Audiitor peaks tegema koostööd sellest mõjutatud juhtkonnaga, et töötada välja töö eesmärgid olukorra hindamiseks ja soovitude tegemiseks tulevaste juhtumite ennetamiseks. Siseauditi juht peaks läbi vaatama antud valdkondlikud nõuded, et määrata töö ulatus, otsustada, millised nõuded kehtivad ja dokumenteerida kõik välistused.

Lisa B. Vabatahtlik dokumenteerimise tööriist

Siseaudiitoritelt eeldatakse kutsealase otsustuse kasutamist, et määrata riskihindamise alusel nõuete kohaldatavus ning dokumenteerida asjakohaselt teatud nõuete välistamised. Valdkondlike nõuete kohaldatavuse analüüsi võib dokumenteerida siseauditi tööplaanis või töö tööpaberites, sõltuvalt audiitori kutsealasest otsustusest. Üks või mitu siseauditi töö võivad hõlmata valdkondlikke nõudeid. Samas, kõik nõuded ei pruugi alati olla kohaldatavad. Allolev prinditav vorm pakub ühe võimaluse kolmanda osapoole valdkondliku nõudega vastavuse dokumenteerimiseks, kuid selle kasutamine ei ole kohustuslik.

Kolmanda osapoole valitsemine

Nõue	Kaetud ulatus või välistamise põhjendus	Viide dokumentatsioonile
A. Kehtestatud on ametlik lähenemisviis, mida rakendatakse ja vaadatakse perioodiliselt üle, et otsustada, kas sõlmida leping kolmanda osapoolega. Lähenemisviis sisaldab asjakohaseid kriteeriume eesmärkide saavutamiseks vajalike ja olemasolevate ressursside määratlemiseks ja hindamiseks toote või teenuse pakkumise kaudu.		
B. Kehtestatud on põhimõtted ja protseduurid kolmanda osapoolega seotud suhete ja riskide määratlemiseks, hindamiseks ja haldamiseks kogu kolmanda osapoole elutsükli vältel. Põhimõtted ja protseduurid kontrollikeskkonna tugevdamiseks on kooskõlas kohaldatavate regulatiivsete nõuetega ning neid vaadatakse korrapäraselt üle ja ajakohastatakse.		

Nõue	Kaetud ulatus või välistamise põhjendus	Viide dokumentatsioonile
C. Organisatsiooni kolmanda osapoole haldamise rollid ja vastutused on määratletud, kirjeldades, kes kolmandaid osapooli valib, juhib, haldab, nendega suhtleb ja neid jälgib ning keda tuleb kolmanda osapoole tegevusest teavitada. Olemas on protsess tagamaks, et kolmanda osapoolega seotud rollidesse ja vastutusaladesse määratud isikutel on asjakohased pädevused.		
D. Asjakohaste huvirühmadega suhtlemise protokollid on määratletud ja hõlmavad õigeaegset aruandlust prioriteetsete kolmandate osapoolte tulemuslikkuse, riskide ja vastavuse seisundi kohta, sealhulgas seaduste ja regulatsioonide rikkumiste kohta. Kolmandad osapooled on riskipõhiselt prioriseeritud. Asjakohased huvirühmad võivad hõlmata kõrgemat juhtorganit (nõukogu), tippjuhtkonda, hangete, operatsioonide, riskijuhtimise, vastavuse, õigusvaldkonna, infotehnoloogia, infoturbe, personalijuhtimise ja teiste valdkondade esindajaid.		

Kolmanda osapoolte riskijuhtimine

Nõue	Kaetud ulatus või välistamise põhjendus	Viide dokumentatsioonile
A. Kolmandate osapoolte ja nende teenuste riskijuhtimise protsessid on standardiseeritud ja terviklikud, sisaldavad määratletud rolle ja vastutusi ning käsitlevad piisavalt organisatsiooni jaoks olulisi põhiriske (näiteks strateegilisi, maine-, eetika-, tegevus-, finants-, vastavus-, küberturbe-, infotehnoloogia-, õigus-, kestlikkuse- ja geopoliitilisi riske). Protsessidest kinnipidamist jälgitakse ning kõrvalekallete korral rakendatakse parandusmeetmeid.		
B. Kolmandate osapooltega seotud riske tuvastatakse ja hinnatakse regulaarselt kogu elutsükli jooksul. Riskihinnangut kasutatakse kolmandate osapoolte, sealhulgas allapoole delegeeritud osapoolte järjestamiseks ja prioriseerimiseks. Riskidele reageerimise meetmed on samuti tähtsuse järjekorda seatud. Riskihindamine vaadatakse perioodiliselt üle ja ajakohastatakse.		
C. Riskidele reageerimise meetmed on piisavad, täpsed ning vastavad pingereale. Riskidele reageerimise meetmeid rakendatakse, vaadatakse läbi, kiidetakse heaks, jälgitakse, hinnatakse ja kohandatakse vastavalt vajadusele.		

Nõue	Kaetud ulatus või välistamise põhjendus	Viide dokumentatsioonile
D. Olemas on protsessid kolmandate osapooltega seotud probleemide haldamiseks ja vajaduse korral eskaleerimiseks, tagades vastutuse tulemuste eest ning suurendades tõenäosust, et lepingute või muude kokkulepete tingimused saavutatakse. Kui kolmas osapool ei reageeri eskaleeritud probleemidele, on juhtkonnal olemas protsessid jätkuva ärisuhete riskide hindamiseks ning vajaduse korral edasiste meetmete, parenduste või lepingu lõpetamise algatamiseks.		

Kolmanda osapoole kontroll

Nõue	Kaetud ulatus või välistamise põhjendus	Viide dokumentatsioonile
A. Kolmandate osapoolte leidmiseks ja valikuks on olemas põhjalik hoolsuskontrolli protsess koos dokumenteeritud ja heaks kiidetud ärilise põhjenduse või muu asjakohase dokumendiga, mis kirjeldab ja põhjendab kolmanda osapoolega suhte vajadust ja olemust.		
B. Lepingute sõlmimine ja heakskiitmine toimub vastavalt organisatsiooni kolmanda osapoole riskijuhtimise põhimõtetele ja protseduuridele ning hõlmab koostööd organisatsiooni asjakohaste osade vahel.		
C. Lõplikud lepingud või kokkulepped vaadatakse läbi ja kiidetakse heaks kõigi asjaomaste huvigruppide poolt, sealhulgas õigus- ja vastavusfunktsioon, need allkirjastatakse mõlema poole volitatud isikute poolt ning neid säilitatakse turvaliselt. Iga lepingu jaoks määratakse vastutav lepinguomanik või haldur.		

Nõue	Kaetud ulatus või välistamise põhjendus	Viide dokumentatsioonile
D. Kõigist kolmandate osapoolte suhetest peetakse täpset, täielikku ja ajakohast nimekirja, näiteks tsentraliseeritud lepinguhaldussüsteemis.		
E. Dokumenteeritud tarnijate kasutuselevõtuprotsessid on kehtestatud ja neid järgitakse, et luua alus kolmandatele osapooltele lepingu või kokkuleppe tingimuste täitmiseks.		
F. Olemas on pideva jälgimise protsessid hindamaks, kas kolmandad osapooled tegutsevad kogu elutsükli jooksul lepingu või kokkuleppe tingimuste kohaselt ning kas nad täidavad oma lepingulisi kohustusi. Protsessid hõlmavad esitatud teabe usaldusväärsuse kontrollimist ning tulemuslikkuse ümberhindamist perioodiliselt ja alati, kui kokkulepe muutub.		
G. Kehtestatud on protokollid parandusmeetmete algatamiseks, kui kolmas osapool ei vasta ootustele või kujutab endast suurenenud või ootamatut riski. Protokollid hõlmavad juhtumite eskaleerimist raskusastme alusel, intsidentide järgseid ülevaatusi ning intsidentide algpõhjuste analüüsi.		
H. Lepingute lõppemise ja pikendamise kuupäevi jälgitakse ning vajaduse korral rakendatakse pikendamisega seotud meetmeid.		

Nõue	Kaetud ulatus või välistamise põhjendus	Viide dokumentatsioonile
I. Rakendatakse ja järgitakse ametlikku tarnijasuhete lõpetamise plaani, et tagada lepingutingimuste, sealhulgas ajastuse ja ootuste, piisav käsitlemine. Protsessid hõlmavad seda, kuidas: • lõpetada suhe kolmanda osapoolega, • vajaduse korral asendada kolmas osapool, • määrata ümber vastutus ning tagastada või hävitada kolmanda osapoole juures hoitavad organisatsiooni tundlikud andmed, • tühistada kolmanda osapoole juurdepääs süsteemidele, vahenditele ja ruumidele.		

Rahvusvahelisest Siseaudiitorite Instituudist

Rahvusvaheline Siseaudiitorite Instituut (The IIA) on rahvusvaheline kutseühing, mis teenindab enam kui 265 000 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, sertifitseerimise, hariduse, teadusuuringute ja tehniliste juhiste vallas. Lisateaveteleiate veebilehelt theiia.org.

Vastutusunõue

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

Autoriõigus

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

September 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