Trešā puse

Tematiskā prasība

Topical Requirement

Lietotāja rokasgrāmata

The Institute of
Internal Auditors

Saturs

Tematisko prasību pārskats

Tematiskās prasības ir būtisks Starptautiskās profesionālās prakses ietvara® (International Professional Practices Framework®) sastāvdaļa, kā arī Globālo iekšējā audita standartu™ (Global Internal Audit Standards™) un Globālo vadlīniju komponents. Iekšējo auditoru institūts pieprasa, lai Tematiskās prasības tiktu izmantotas kopā ar Standartiem, kas ir autoritatīvs nepieciešamās prakses pamats. Šajā rokasgrāmatā ir atsauces uz Standartiem, kas ir detalizētākas informācijas avots.

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

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

Piemērojamība, risks un profesionāls vērtējums

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

Kā aprakstīts Standartos, risku novērtēšana ir svarīga iekšējā audita vadītāja plānošanas daļa. Lai noteiktu, kādus pārliecības sniegšanas uzdevumus iekļaut iekšējā audita plānā, vismaz reizi gadā jānovērtē organizācijas stratēģijas, mērķi un riski (9.4. standarts "Iekšējā audita plāns"). Plānojot individuālus pārliecības sniegšanas uzdevumus, iekšējiem auditorem ir jāizvērtē ar uzdevumu saistītie riski (13.2. standarts "Riska novērtējums darba uzdevuma ietvaros").

Ja uz risku balstītā iekšējā audita plānošanas procesa laikā tiek identificēta tematiskā prasība un tā tiek iekļauta audita plānā, tad tematiskās prasības ir jāizmanto, lai novērtētu šo tēmu piemērojamo uzdevumu ietvaros. Turklāt, ja iekšējie auditori veic uzdevumu (plānā iekļautu vai neiekļautu) un parādās aktuālās prasības elementi, aktuālā prasība ir jāizvērtē, vai tā ir piemērojama kā daļa no uzdevuma. Visbeidzot, ja

tiek pieprasīts uzdevums, kas sākotnēji nebija iekļauts plānā un ietver šo tēmu, ir jāizvērtē, vai ir piemērojama tematiskā prasība.

Piemērojot tematisko prasību, būtiska nozīme ir profesionālam vērtējumam. Riska novērtējumi nosaka iekšējā audita vadītāju lēmumus par to, kādus uzdevumus iekļaut iekšējā audita plānā (9.4. standarts "Iekšējā audita plāns"). Turklāt iekšējie auditori izmanto profesionālu vērtējumu, lai noteiktu, kādi aspekti tiks aptverti katrā uzdevumā (13.3. standarts " Darba uzdevumu mērķi un apjoms ", 13.4. standarts "Vērtēšanas kritēriji" un 13.6. standarts "Darba programma").

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

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

Ja iekšējā audita struktūrvienībai nav vajadzīgās kompetences, lai veiktu uzdevumus par aktuālo prasību tēmu, iekšējā audita vadītājam ir jānosaka, kā iegūt resursus, un savlaicīgi jāinformē valde (padome) un augstākā līmeņa vadība par ierobežojumu ietekmi un par to, kā tiks risināts resursu trūkums. Iekšējā audita vadītājs saglabā galīgo atbildību par iekšējā audita funkcijas atbilstību Aktuālajām prasībām neatkarīgi no tā, kā tiek iegūti resursi (3.1. standarts "Kompetence", 7.2. "Iekšējā auditavadītāja kvalifikācija", 8.2. "Resursi", 10.2. " Personāla plānošana ").

Veiktspēja, dokumentācija un ziņošana

Piemērojot Tematiskās prasības, iekšējiem auditoriem arī jāievēro Standarti, veicot savu darbu saskaņā ar V sadaļu: Iekšējā audita pakalpojumu sniegšana. V sadaļas jomas standarti apraksta darba uzdevuma plānošanu (13. princips " Efektīva darba uzdevuma plānošana "), iesaistes veikšanu (14. princips " Darba uzdevumu veikšana ") un darba rezultātu paziņošanu (15. princips " Darba rezultātu paziņošana un rīcības plāna izpildes uzraudzība ").

Tematiskās prasības ir izstrādātas, lai atbalstītu konsekventu, augstas kvalitātes iekšējā audita praksi. Vietējie likumi, noteikumi, uzraudzības prasības un citas profesionāli atzītas sistēmas var noteikt papildu vai specifiskākas prasības. Iekšējiem auditorem ir jāizprot un jāievēro likumi un/vai noteikumi, kas attiecas uz nozari un jurisdikcijām, kurās darbojas organizācija, tostarp saskaņā ar 1.3. standartu " Uzvedības likumība un ētiskums ", kā arī saskaņā ar tiem jāatklāj nepieciešamā informācija. Iekšējie auditori, iespējams, jau ir iekļāvuši šīs papildu prasības audita programmās un pārbaudes procedūrās, un viņiem tās jāsaskaņo ar tematisko prasību, lai nodrošinātu atbilstošu segumu.

Tematiskās prasības ievērošanu var dokumentēt vai nu iekšējā audita plānā, vai uzdevuma darba dokumentos, pamatojoties uz auditoru profesionālo vērtējumu. Prasības var attiekties uz vienu vai vairākiem iekšējās audita uzdevumiem. Turklāt ne visas prasības var būt piemērojamas. Jāsaglabā pierādījumi par to, ka ir novērtēta tematiskās prasības piemērojamība, tostarp pamatojums, kurā paskaidroti visi izņēmumi.

Kvalitātes nodrošināšana

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

Atbilstība tematiskajām prasībām tiks novērtēta kvalitātes novērtējumos.

Trešā puse

Trešā puse ir ārēja persona, grupa vai organizācija, ar kuru organizācija ("galvenā organizācija") nodibina darījumu attiecības, lai iegūtu produktus vai pakalpojumus. Attiecības var tikt formalizētas, noslēdzot līgumu, vienošanos vai izmantojot citus līdzekļus, lai sniegtu organizācijai produktus, pakalpojumus, darbaspēku, ražošanu vai informācijas tehnoloģiju risinājumus, piemēram, datu uzglabāšanu, apstrādi un uzturēšanu.

> Piezīme
>
> Tematiskajās prasībās tiek izmantota vispārējā iekšējā audita terminoloģija, kas definēta Globālajos iekšējā audita standartos. Lasītājiem jāiepazīstas ar terminiem un definīcijām Standartu glosārijā.

Terminu "trešā puse" var lietot atšķirīgi atkarībā no nozares vai cita konteksta. Katrai iekšējā audita funkcijai ir rīcības brīvība izmantot savu spriedumu, piemērojot Tematisko prasību atbilstoši tam, kā galvenā organizācija (organizācija, kas noslēdz vienošanos ar trešo pusi) definē trešās puses. Tematiskajā prasībā un lietotāja rokasgrāmatā termins "trešā puse" attiecas uz pārdevējiem, piegādātājiem, darbuzņēmējiem, apakšuzņēmējiem, ārpakalpojumu sniedzējiem, citām aģentūrām un konsultantiem. Termins "trešā puse" ietver visas šādas vienošanās, tostarp vienošanās starp trešo pusi un tās apakšuzņēmējiem, kurus bieži dēvē par "pakārtotajiem" apakšuzņēmējiem, "ceturtajām pusēm", "piektajām pusēm" vai "N-tajām pusēm"

Šī tematiskā prasība neattiecas uz netiešām ārējām attiecībām, interesēm vai saistībām ar galveno organizāciju, piemēram, regulatoriem, aģentiem, brokeriem, investoriem, pilnvarniekiem/valdes (padomes) locekļiem, valsts dienestiem un sabiedrības locekļiem, vai iekšējām attiecībām, piemēram, darbiniekiem vai grupas iekšējiem pakalpojumu sniedzējiem.

Terminu "trešā puse" var definēt un lietot atšķirīgi atkarībā no nozares vai cita konteksta. Iekšējiem auditorem ir dota rīcības brīvība, un viņiem jāpaļaujas uz savu profesionālo vērtējumu, lai pielāgotu tematisko prasību galvenās organizācijas trešās puses definīcijai.

Organizācijas trešo pušu attiecību vadības procesu efektivitāti var novērtēt visā organizācijā un/vai viena vai vairāku atsevišķu līgumu, vienošanos vai attiecību līmenī. Iekšējiem auditoriem jāizmanto lejup ejoša pieeja, lai izprastu organizācijas trešo pušu politiku, procedūras, procesus, sistēmu un dzīves ciklu. Iekšējiem auditoriem ir jāizmanto spriedums, lai izprastu nianses trešo pušu riskos atkarībā no atsevišķām nozarēm, organizācijām un uzdevumu tēmām. Saskaņā ar 5.1. standartu "Informācijas lietošana" iekšējiem auditoriem jāzina un jāievēro visas politikas un procedūras, kas saistītas ar trešo pušu informāciju, kurai viņi var piekļūt.

Tematiskā prasība attiecas uz gadījumiem, kad iekšējā audita funkcija veic pārliecības sniegšanasa uzdevumus attiecībā uz trešajām pusēm un/vai jebkādām apakšuzņēmēju attiecībām, tostarp ceturtajām vai tālākām pakārtotajām attiecībām, ko pieļauj trešās puses līgums vai vienošanās ar galveno

organizāciju. Iekšējiem auditoriem jānosaka trešo un turpmāko pakārtoto pušu prioritātes, pamatojoties uz risku, kā aprakstīts turpmāk riska vadības sadaļā. Iekšējiem auditoriem jāpiemēro visas prasības, kā norādīts riska novērtējuma rezultātos, un izņēmumi jādokumentē.

Trešo pušu tematiskā prasība un lietotāja rokasgrāmata attiecas uz organizācijas attiecību ar trešajām pusēm posmiem, kas pazīstami arī kā dzīves cikla posmi: atlase, līgumu slēgšana, iekļaušana, uzraudzība un izslēgšana. Šie posmi tiks izmantoti trešo pušu tematisko prasību un lietotāja rokasgrāmatas vajadzībām, lai gan dažās nozarēs ir savas dzīves cikla versijas. Posmi ir šādi:

- Atlase: ietver procesus, lai noteiktu trešās puses nepieciešamību, tās izmantošanas plānu un pienācīgu rūpību atlases veikšanai. Turklāt atlasē jāiekļauj potenciālo un iesaistīto trešo pušu risku novērtējums.
- Līgumu slēgšana: ietver pienācīgas pārbaudes procesus, lai sagatavotu, apspriestu, apstiprinātu un īstenotu juridisku līgumu ar trešo pusi.
- Uzņemšana: sākas, kad tiek parakstīts līgums par attiecību uzsākšanu, un izveido pamatu, lai trešās puses varētu izpildīt līguma vai vienošanās noteikumus.
- Uzraudzība: ietver procesus, kas saistīti ar trešās puses vadību "darbības laikā" un nepārtrauktu uzraudzību pēc līguma noslēgšanas un apstiprināšanas. Šī pieeja parasti ir sistemātiska un balstīta uz risku, un tajā jāņem vērā nepārtraukta uzlabošana. Uzraudzība ietver spēkā esošo trešo pušu līgumu vai vienošanos atjaunošanu, ja nepieciešams.
- Izslēgšana: ietver procesus līgumu un vienošanos izbeigšanai, izejas stratēģijas uzturēšanai attiecībā uz trešajām pusēm, kas ir prioritizētas, pamatojoties uz risku, un attiecību pārtraukšanai, ja nepieciešams. Šajos procesos parasti izmanto uz risku balstītu pieeju, un tie var ietvert oficiālu izejas plānu.

Galvenā organizācija saglabā atbildību par riskiem, kas saistīti ar tās mērķu sasniegšanu, pat tad, ja tā iesaistās trešās puses darbā, lai palīdzētu tai sasniegt vienu vai vairākus mērķus. Iesaistot trešās puses, var samazināt dažas organizācijas izmaksas, kas saistītas ar procesu veikšanu. Tomēr tas var radīt operacionālos riskus, jo galvenajai organizācijai ir mazāka pārredzamība un tiesības attiecībā uz trešās puses kontroles procesiem. Ja trešā puse nepilda līgumā noteiktos pienākumus, piedalās neētiskā darbībā vai piedzīvo darbības traucējumus, galvenā organizācija var ciest no sekām.

Galvenajai organizācijai ir jāidentificē, jānovērtē un jāvada riski, izmantojot atbilstošus pārvaldības, riska vadības un kontroles procesus. Ar trešajām pusēm saistīto risku kategorijas un piemēri ietver:

- Stratēģiskas, piemēram, spēja īstenot organizācijas misiju un/vai augsta līmeņa mērķus vai vadīt apvienošanās un pārņemšanas ietekmi.
- Reputācijas, piemēram, kaitējums, kas nodarīts videi vai galveno organizāciju attiecībām un uzticībai ar klientiem, klientiem un ieinteresētajām pusēm.
- Ētiskas riski, piemēram, integritātes trūkumi, interešu konflikti, kukuļošana un korupcija.
- Darbības, piemēram, fiziskā un informācijas drošība, iekšējais risks, pakalpojumu traucējumi un mērķu nesasniegšana.
- Finanšu, piemēram, trešo pušu maksātnespēja un krāpšana.

- Atbilstība piemērojamajām vietējām, nacionālajām un starptautiskajām normatīvajām prasībām.
- Kiberdrošība un cita veida datu aizsardzība, piemēram, sensitīvu datu kompromitēšana un noplūde.
- Informācijas tehnoloģijas, piemēram, pakalpojumu trūkums kritisko operāciju atbalstam.
- Juridiskie riski, piemēram, interešu konflikti, strīdi un tiesvedība par līguma pārkāpumiem.
- Ilgtspējība, piemēram, vides, sociālā un pārvaldības. Piemēram, riski, kas saistīti ar organizācijas ietekmi uz vidi, un riski, kas attiecas uz organizācijas mijiedarbību ar kopienām.
- Ģeopolitiskie, piemēram, tirdzniecības strīdi/sankcijas un politiskā nestabilitāte.

Iekšējiem auditoriem, novērtējot pārvaldības, riska vadības un kontroles procesu prasības, jāņem vērā katrs trešās puses dzīves cikla posms.

Trešās puses tematiskās prasības ir sadalītas trīs iedaļās saskaņā ar 9.1. standartu "Pārvaldības, riska pārskaības un kontroles procesu izpēte":

- Pārvaldība - skaidri definēti pamatmērķi un stratēģijas trešo pušu izmantošanai, lai atbalstītu organizācijas mērķus, politiku un procedūras.
- Risku vadība - procesi, lai identificētu, analizētu, vadītu un uzraudzītu ar trešajām pusēm saistītos izmantošanas riskus, tostarp procesu, lai nekavējoties ziņotu par incidentiem.
- Kontroles - vadības noteikti, periodiski novērtēti kontroles procesi, lai samazinātu riskus, izmantojot trešās puses.

Papildus tematiskajām prasībām un šai lietotāja rokasgrāmatai iekšējie auditori var izmantot papildu profesionālās vadlīnijas par trešajām pusēm, piemēram, IPPF globālās vadlīnijas un nozarei specifiskus resursus.

Apsvērumi

Tālāk izklāstītie apsvērumi var palīdzēt iekšējiem auditoriem īstenot Trešo pušu tematiskās prasības. Turpmāk katrā iedaļā ar burtiem apzīmētie apgalvojumi atkārto vai pārfrāzē attiecīgās tematiskās prasības. Šie neobligātie apsvērumi ir ilustratīvi, lai sniegtu piemērus, kā novērtēt prasības. Iekšējiem auditoriem, nosakot, ko iekļaut novērtējumā, jāizmanto profesionāls vērtējums.

Pārvaldības apsvērumi

Lai novērtētu, kā pārvaldības procesi, tostarp valdes (padomes) pārraudzība, tiek piemēroti trešo pušu mērķiem, iekšējie auditori var pārbaudīt pierādījumus par:

A. Formalizētas un dokumentētas uz risku balstītas pieejas vai stratēģijas, lai noteiktu, vai izmantot trešo pusi. Šī pieeja tiek periodiski pārskatīta un ietver:

- Skaidri definētu un standartizētu procesu pieejas ieviešanai, ko organizācija ir apstiprinājusi izmantošanai.
- Budžetā paredzētie resursi, pamatojoties uz izmaksu un ieguvumu analīzi, lai pamatotu trešās puses iesaistīšanu, nodrošinot stratēģisko saskaņotību un resursu produktivitāte.
- Vadības veiktais risku un kontroles mehānismu novērtējums, tostarp to, kas attiecas uz jautājumiem, kuri saistīti ar trešām pusēm.
- Atbilstoši resursi, lai slēgtu līgumus ar trešām pusēm, vadītu un uzraudzītu to darbību.
- Ieinteresēto pušu atsauksmju integrēšana pieejā vai stratēģijā.

B. Politikas, procedūras un cita attiecīgā dokumentācija, ko izmanto, lai definētu, novērtētu un vadītu attiecības ar trešām pusēm visā dzīves ciklā. Politikas un procedūras var ietvert:

- Standartizētus rīkus un veidnes, lai atvieglotu galvenos pārvaldības, riska vadības un kontroles procesus.
- Procesus, lai periodiski novērtētu politikas un procedūras, noteiktu to atbilstību un vajadzības gadījumā tās atjauninātu.
- Izstrādātus kritērijus trešo pušu atlasei, līgumu slēgšanai, iekļaušanai, uzraudzībai un izslēgšanai.
- Piemērojamo normatīvo prasību identificēšanu un periodisku pārskatīšanu, lai nodrošinātu atbilstību politikām un procedūrām.
- Salīdzinošo novērtēšanu, kas veikta, lai noteiktu un salīdzinātu vadošās trešo pušu vadības prakses.

C. Definētas lomas un pienākumus, kas palīdz sasniegt trešo pušu mērķus. Papildu pierādījumi var ietvert:

- Procesus, lai novērtētu, vai trešās puses vērtības, ētika un korporatīvā sociālā atbildība atbilst galvenās organizācijas principiem. Šajā procesā jāietver, kā nekavējoties novērst iespējamus interešu konfliktus vai neētisku praksi.
- Regulāra trešās puses vadības funkciju veicēju personāla apmācība un periodiska viņu kompetences novērtēšana.
- Process, kas paredz izvērtēt, vai apmācības ir ieviestas ar mērķi veicināt vispārēju izpratni organizācijā par trešajām pusēm.
- Lomas un pienākumi ir saskaņoti ar trīs līniju modeli.

D. Savlaicīga saziņa un sadarbība ar attiecīgajām ieinteresētajām pusēm visā trešās puses dzīves ciklā (piemēram, ar valdi, augstāko vadību, iepirkumu, operācijām, riska vadību, atbilstību, juridiskajām, informācijas tehnoloģijām, informācijas drošību, cilvēkresursiem un citiem), kas ietver:

- Informācija par trešo pušu riskiem un zināmām iespējamām ievainojamām vietām sanāksmju protokolos, ziņojumos vai e-pasta ziņojumos.
- Informācijas apmaiņa par trešo pušu vadību un sadarbības veicināšana (piemēram, periodiskās starpfunkcionālās sanāksmēs).

Riska vadības apsvērumi

Lai novērtētu, kā riska vadības procesi tiek piemēroti trešo pušu mērķu sasniegšanai, iekšējie auditori var pārbaudīt pierādījumus par:

A. Standartizēti un visaptveroši riska vadības procesi trešo pušu pakalpojumu lietotājiem ietver definētas lomas un pienākumus un pietiekami pievēršas galvenajiem riskiem, kas attiecas uz organizāciju:

- Trešo pušu risku novērtēšanas un vadības procesi ietver to, kā galvenie riski:
  - Sākotnēji identificēts un ziņots
  - Analizēti, lai novērtētu to ietekmi uz spēju sasniegt organizācijas mērķus
  - Samazināts, tostarp rīcības plāni, lai samazinātu risku līdz pieņemamam līmenim.
  - Uzraudzība, tostarp agrīno brīdinājumu atklāšana un reaģēšana uz tiem, kā arī pastāvīgas ziņošanas plāns, līdz draudi ir pilnībā novērsti.
- Tiek uzraudzīta procesu ievērošana un koriģējošo pasākumu īstenošana, lai novērstu organizācijas ilgtermiņa mērķu vai stratēģijas apdraudējumu.
- Riska vadības komiteja vai cita grupa nodrošina tiešu trešo pušu uzraudzību un sniedz informāciju valdei (padomei). Komitejai ir noteikts mērķis, un tā regulāri rīko sanāksmes. Pierādījumi var ietvert sanāksmju protokoli.

B. Riski, kas saistīti ar trešām pusēm visā dzīves ciklā, tiek regulāri identificēti un novērtēti. Riska novērtējumā trešās puses tiek sarindotas un noteiktas to prioritātes. Reakcijas uz riskiem tiek sarindotas un prioritizētas.

- Izstrādājot trešo pušu riska novērtējumu, galvenā organizācija ņem vērā tādus faktorus kā tās lielums, gatavība un iesaistīto trešo pušu skaits.
- Riska novērtējums ir dokumentēts, un tajā ir identificēti raksturīgie un atlikušie riski.
- Organizācijā tiek ievērots uzticamības pārbaudes process, lai pārskatītu un atjauninātu riska novērtējumu.
- Tiek noteikti kritēriji, lai trešās puses sarindotu un noteiktu to prioritāti atbilstoši riskiem. Piemēri šādiem kritērijiem ietver:
  - Sniegtie pakalpojumi ir ļoti svarīgi organizācijas darbībai.
  - Vienošanās finansiālā vērtība ir būtiska.
  - Attiecības ir jaunas, noslēgtas ātri un/vai to ilgums ir ilgs
  - Ir iesaistītas vairākas ārējās puses.
  - Trešā puse plāno daļu vai visu darbu nodot apakšuzņēmējam.
- Organizācija ievēro vispārpieņemto riska novērtēšanas praksi, tostarp to, ka riska novērtējums jāveic pēc iespējas agrākā posmā, parasti tad, kad atlases posmā tiek analizēts priekšlikums, un pirms darba uzsākšanas.
- Pārdevēji aizpilda anketu, lai noteiktu savu riska klasifikāciju un prioritāti, pamatojoties uz raksturīgajiem riskiem. Organizācija nodrošina, ka anketas aizpilda attiecīgie darbinieki un ka tās tiek pārskatītas, lai nodrošinātu precizitāti.
- Organizācija periodiski saņem informāciju par trešo pušu riska vadību no tādām funkcionālajām jomām kā informācijas tehnoloģijas, iepirkumi, uzņēmuma riska vadība, cilvēkresursi, juridiskie jautājumi, atbilstība, darbības, grāmatvedība un finanses.

C. Tiek noteiktas riska reakcijas, piemēram, riska mazināšana, pieņemšana, novēršana un dalīšana, un tās ir samērīgas ar riska klasifikāciju.

- Atbildes uz riskiem tiek dokumentētas, un tajās tiek ņemta vērā trešās puses kontroles vide.
- Dokumentācija, kas apliecina, ka atbildes reakcijas uz riskiem, kas pārsniedz galvenās organizācijas pieļaujamo riska līmeni, tiek pārskatītas, lai noteiktu to atbilstību, jo īpaši, ja riski tiek pieņemti. Atbildes ietver atbildes, kas attiecas uz iespējamiem interešu konfliktiem ar trešām pusēm.

D. Trešo pušu risku vadības un eskalācijas procesi, tostarp veids, kā tiek novērtēts, piešķirts un noteikts apdraudējuma vai riska līmenis un prioritātes. Pārskatā var iekļaut sekojošu identificēšanu:

- Organizācijas riska līmeņu definīcijas un skaidrojumi, piemēram, augsts, vidējs un zems riska līmenis, un eskalācijas procedūras katrai riska kategorijai.
- Trešo pušu saraksts, kas prioritizētas pēc identificētajiem riskiem, un visu riska notikumu mazināšanas statuss
- Piemērojamās juridiskās, normatīvās un atbilstības prasības
- Risku ietekme, gan finansiāla, gan nefinansiāla (piemēram, reputācija)

- Procesi, kā vadība un darbinieki tiek informēti par trešo pušu riskiem, tostarp regulāra ziņošana valdei (padomei vai citai atbilstošai struktūrai) par riska profilu. Saziņā jāiekļauj jaunākā informācija par to, kā tiek novērstas visas problēmas, kas konstatētas saistībā ar prioritizētām trešām pusēm.
- Procesi, kas ļauj pārskatīt klasifikāciju un prioritāšu noteikšanu, kad mainās galvenās organizācijas vēlme uzņemties risku un riska tolerances līmeņi.

Kontroles apsvērumi

Lai novērtētu, kā kontroles procesi tiek piemēroti attiecībām ar trešajām pusēm, iekšējie auditori var pārbaudīt pierādījumus ka

A. Ir ieviests stingrs uzticamības pārbaudes process trešo pušu meklēšanai un atlasei, un ir dokumentēta un apstiprināta uzņēmējdarbības analīze vai cita attiecīga dokumentācija, kurā aprakstīta un pamatota vajadzība pēc attiecībām ar trešo pusi un to raksturs.

- Biznesa analīze var arī:
  - Pievērsiet uzmanību riskiem, kas saistīti ar trešās puses spēju attaisnot cerības, un iespējamai ietekmei uz organizāciju.
  - Ietveriet detalizētu izmaksu un ieguvumu analīzi.
- Tiek ievēroti iedibinātie iepirkuma procesi, piemēram, konkursi, piedāvājumu pieprasījumi un vienīgais iepirkums. Procesi ietver:
  - Svarīgu aspektu kritēriji, piemēram, kiberdrošības protokolu pārskatīšana, bankas datu pārbaude, finanšu fona pārbaude, trešās puses organizatoriskās struktūras, sodāmības un juridisko ierakstu, autovadītāja apliecību, politisko aktivitāšu un saistību ar noziedzīgām darbībām izpēte.
  - Precīzi definēti atlases kritēriji, tostarp iepriekšējās darbības, atsauksmju, reputācijas un līguma izmaksu novērtēšana.
  - Pienācīga rūpība, lai nodrošinātu atbilstošu piegādātāju atlasi, piemēram, starpfunkcionālu komandu veidošana, lai pārskatītu priekšlikumus. Lai samazinātu neobjektivitātes risku, pārbaužu grupu kontrole ietver grupas izveides procedūras un prasības par iespējamo interešu konfliktu atklāšanu.
  - Pienācīga rūpība, novērtējot trešās puses kontroles vidi, piemēram, apmeklējot objektu vai pārskatot trešās puses:
    - Sistēmas un organizācijas kontroles (SOC) ziņojumi.
    - Finanšu stabilitāte.
    - Dibināšanas statūti vai apliecība par labu stāvokli.
    - Galvenās vadības un ieinteresēto pušu lēmumu pieņemšanas pārredzamība.
    - Organizatoriskā struktūra.
    - Darbības stabilitāte.
    - Kiberdrošības protokoli.

- Atbilstība attiecīgajiem likumiem, noteikumiem un standartiem.
- Ētika.
- Vēsture ar galveno organizāciju.
- Reputācija.

  - Pierādījumi, ka potenciālie pārdevēji vai līgumslēdzēji pāriet uz līguma slēgšanas posmu tikai pēc tam, kad ir veikti attiecīgie uzticamības pārbaudes procesi un analizēti rezultāti.

B. Tiek izstrādātas un ievērotas līgumu slēgšanas politikas un procedūras.

- Līgumi tiek rakstīti ar nepārprotamiem noteikumiem.
- Galvenie riski tiek ņemti vērā līguma sagatavošanas posmā, un tiek iekļauti attiecīgie punkti. Šajā posmā ar trešo pusi tiek sazināti jautājumi, kurus nepieciešams atrisināt.
- Līgumu būtiskie elementi tiek noteikti, pamatojoties uz organizācijas līgumu slēgšanas politiku un procedūrām un trešās puses prioritātes līmeni. Elementi var ietvert:
  - Konfidencialitātes neizpaušanas (privātuma) līgumi.
  - Izbeigšanas klauzulas un definēti datu piekļuves parametri.
  - Kiberdrošības prasības, tostarp prasības par piekļuvi visiem datiem un dalīšanos ar tiem, kā arī ziņošanu par incidentiem vai pārkāpumiem noteiktā termiņā.
  - Prasības attiecībā uz paziņojumiem par pārkāpumu, kas ietekmē galvenās organizācijas datus.
  - Standartizēts process trešo pušu identifikācijas pārbaudei, tostarp pilns juridiskais nosaukums, adrese, fiziskā(-ās) atrašanās vieta(-as) un tīmekļa vietne. Standarta prakse ir identifikācijas procesā izmantot kontrolsarakstu un pārbaudīt informācijas precizitāti.
  - Skaidri definēti pakalpojumu līmeņa līgumi, kuros norādīti gala rezultāti un katras puses tiesības, pienākumi, sodi, atlīdzība un atbildība, tostarp atbildība par darbaspēka izmaksu segšanu (tostarp pakārtotiem apakšuzņēmējiem).
  - Noteikums par tiesībām veikt iekšējo auditu, kas ietver pakārtotos apakšuzņēmējus, vai prasība iesniegt pierādījumus, ka cienījams, neatkarīgs pārliecības sniedzējs ir veicis pušu auditu. Ja līgmā nav iekļautas tiesības veikt auditu, iekšējā audita funkcijas spēja iegūt vai sniegt pārliecību var būt ierobežota.
- Galvenajai organizācijai ir pieejami neatkarīgo auditoru kontroles novērtējuma ziņojumi, piemēram, par finanšu, atbilstības un datu drošības jautājumiem, piemēram, Starptautiskais standarts par pārliecības sniegšanas uzdevumiem vai SOC ziņojumi.
  - Ja paļaujas uz trešās puses ārējo ticamības apliecinājumu sniedzēju darbu, dokumenti tiek pārskatīti, lai pārliecinātos par to ticamību.
  - SOC ziņojumi tiek izmantoti, lai identificētu neatbilstošus riska un izmaiņu vadības procesus.
- Politikas un procedūras attiecas uz visiem komponentiem, kas ir būtiski konkrētām organizācijām vai līgumu veidiem:
  - Vides aizsardzības un ilgtspējas klauzulas.

- Trauksmes celšanas protokoli
- Prasības attiecībā uz veiktspējas mērījumu novērtējumiem.
- Pārbaudīts trešo pušu darbības nepārtrauktības plāns.
- Mākslīgā intelekta izmantošana pakalpojumu sniegšanā.
- Skaidra apakšuzņēmēja darba identifikācija, atklāšana, noteikumi un apjoms.
- Izmaiņu vadības process, kurā izklāstīts, kā rīkoties, lai līguma darbības laikā veiktu izmaiņas darbības jomā, noteikumos vai darbības prasībās (piemēram, izmaiņas tehnoloģijās vai regulējuma atjauninājumos).
- Ierobežojumi attiecībā uz izmaiņu pasūtījumu skaitu vai summām, par kurām var tikt izrakstīts rēķins.

- Saskaņā ar politiku un procedūrām pirms maksājuma veikšanas vai jebkāda ieturējuma atbrīvošanas ir nepieciešama formāla galaproduktu pieņemšana.
- Trešajām pusēm ir jādalās ar savu ētikas politiku vai rīcības kodeksu un/vai jāievēro galvenās organizācijas ētikas politika vai rīcības kodekss.
- Ja līgumu nodrošina trešā puse, galvenā organizācija ir veikusi juridisko pārbaudi, un galvenie riski ir izprasti un pamatoti ar piemērotu riska mazināšanas stratēģiju.

C. Pabeigtos līgumus vai nolīgumus pārskata un apstiprina attiecīgās ieinteresētās puses, tostarp juridiskās un atbilstības nodrošināšanas speciālisti, tie tiek droši uzglabāti un piešķirti atbildīgajam līguma vadītājam vai administratoram.

- Līgums vai cits oficiāls dokuments, kas apliecina ārpakalpojuma attiecības un trešās puses saistības, kā arī pierādījumi par visām nepieciešamajām juridiskajām un atbilstības pārbaudēm.

D. Tiek uzturēts precīzs, pilnīgs un aktuāls visu trešo pušu attiecību saraksts, piemēram, centralizētā līgumu vadības sistēmā.

- Process, kā sarakstā vai sistēmā pievienot jaunus trešo pušu līgumus vai vienošanās.
- Process, kā ievadīt potenciālās trešās puses pārdevēju sistēmā un izņemt tās, ja līgums netiek apstiprināts.
- Process, kā no saraksta vai sistēmas dzēst trešo pušu līgumus vai vienošanās.
- Izsekošanas sistēma, lai dokumentētu problēmas ar konkrētiem darbuzņēmējiem vai piegādātājiem turpmākai atsaucei.
- Pārskatīšanas process, lai noteiktu, vai trešo pušu kopums ir precīzs un pilnīgs.

E. Tiek izveidoti un ievēroti dokumentēti ievades procesi, lai trešās puses varētu izpildīt līguma vai vienošanās noteikumus. Pārskatos var pārbaudīt, vai:

- Standartizētas darbā uzsākšanas procedūras nodrošina, ka tiek veikta visa nepieciešamā dokumentācija, apmācība un atbilstības pārbaudes.
- Trešās puses sistēmas un procesi var viegli integrēties ar galvenās organizācijas tehnoloģijām.

- Koplietojamās sistēmas ir saderīgas un drošas. Pierādījumi var ietvert papildu lietotāja struktūras kontroles, kas ir daļa no SOC ziņojumiem.
- Galvenā organizācija novērtē trešās puses darbības nepārtrauktības plānus, kas nodrošina pakalpojumu nepārtrauktību ārkārtas situācijās. Ir iekļauti ārkārtas rīcības plāni, lai novērstu iespējamus traucējumus.

F. Procesi, kas paredzēti pastāvīgai pārdevēja darbības rezultātu uzraudzībai attiecībā uz līguma vai nolīguma mērķiem, tostarp galveno darbības rādītāju novērtēšana.

- Uzraudzības procesi sniedz informāciju trešās puses riska novērtējumam, un konstatētie kontroles trūkumi tiek pārskatīti, aktualizēti un vajadzības gadījumā novērsti.
- Ziņojumi vai novērojumi par procesiem, tehnoloģijām un rīkiem, kas izveidoti, lai vadītu uzraudzību reāllaikā.
- Procesi, kas nodrošina, ka maksājumi tiek veikti saskaņā ar līguma vai vienošanās noteikumiem, piemēram, projekta termiņu, starpposma mērķu un saziņas prasību ievērošanu. Maksājumi tiek veikti tikai apstiprinātiem līgumslēdzējiem, kuri ir pabeiguši ievades posmu un ir ievadīti pārdevēju maksājumu sistēmā. Ja līgumā ir norādīti nodevumi, galīgie maksājumi tiek veikti tikai tad, kad tie ir pārbaudīti.
- Uzraudzība, lai kontrolētu ar trešo pušu līgumiem saistītās izmaksas, lai nodrošinātu vērtību un noteiktu ieguldījumu atdevi. Izmaksu un ieguvumu analīzes rezultāti tiek izmantoti, lai pārskatītu līgumus.
- Sodu noteikšanas procesi par līgumā vai nolīgumā iekļauto pakalpojumu līmeņa nolīgumu neievērošanu. Sankcijas tiek aprēķinātas un iekasētas to rašanās brīdī.
- Uz risku balstīta prioritāro trešo pušu ranžēšana tiek periodiski pārskatīta, ja līgumā tiek veiktas izmaiņas un ja līguma termiņš tuvojas beigām vai automātiskai atjaunošanai.
- Prioritāri izvērtēto trešo pušu pārskati, piemēram, apmeklējumi klātienē vai ceturkšņa biznesa pārskati, lai pārbaudītu kontroles mehānismus un darbības integritāti.
- Papildu pastāvīgās uzraudzības pierādījumi var ietvert:
  - Trešās puses finansiālās stabilitātes analīze.
  - Trešo pušu darbības izvērtējums, balstoties uz saņemtajām sūdzībām
  - Vadības veiktas neatkarīgu auditoru ziņojumu, piemēram, Starptautisko standartu par apliecinājuma darba uzdevumiem, Pārskatu par apliecinājuma uzdevumu standartiem, trešo pušu sniegto finanšu, audita, atbilstības un datu drošības ziņojumu pārbaudes; ISO sertifikācija.
  - Vadības izvērtējums par trešās puses veiktajiem biznesa noturības testiem, tai skaitā jebkuriem nozīmīgiem konstatētajiem jautājumiem.
  - Apakšuzņēmēju vai pakārtoto pušu izmantošanas nosacījumi un ierobežojumi.
  - Trešo pušu ētisko vērtību, kultūras un uzvedības novērtējums.
  - Atbildes uz plašsaziņas līdzekļu pieprasījumiem.

- Privātuma un kiberdrošības protokolu novērtēšana, lai aizsargātu galvenās organizācijas datu un informācijas glabāšanu un pārsūtīšanu, tostarp progresīvu tehnoloģiju, piemēram, mākslīgā intelekta, izmantošanu.
- Organizācijas iespējas nepārtraukti uzlabot darbības rezultātus un sasniegt līguma vai vienošanās mērķus.
- Pienākumu nošķiršanas pārskatīšana.

G. Protokoli, lai sāktu koriģējošus pasākumus konstatēto incidentu gadījumā, ja trešā puse neievēro līguma vai vienošanās prasības vai ja trešās puses darbības palielina risku galvenajai organizācijai.

- Incidentu eskalācijas protokoli, pamatojoties uz incidenta nopietnību un trešās puses prioritāti.
- Pārskats pēc negadījuma, tostarp pamatcēloņu analīze.

H. Procesi, lai nodrošinātu brīdinājumus par līgumiem un līgumiem, kuru termiņš tuvojas beigām vai automātiskai atjaunošanai. Automātiskās atjaunošanas procesi ietver pārskatīšanu:

- Trešās puses darbība.
- Līguma vai vienošanās noteikumi un jebkuri papildinājumi.
- Riska faktori.

I. Tiek ieviests un ievērots formalizēts ārpakalpojumu plāns, lai nodrošinātu, ka tiek atbilstoši ievērotas līguma prasības attiecībā uz termiņiem un gaidām, tostarp attiecībā uz visiem pakārtotajiem apakšuzņēmējiem.

- Kontrolsaraksti vai intervijas ar galvenajām ieinteresētajām pusēm, lai pārliecinātos par drošības pasākumu efektivitāti.
- Organizācijas informācija vai dati, kas atrodas trešās puses glabāšanā, ir atdoti vai iznīcināti.
- Trešajai pusei ir anulēta piekļuve organizācijas datiem, sistēmām vai iekārtām.
- Ir atgriezti galvenās organizācijas aktīvi, piemēram, ierīces, programmatūras licences, intelektuālais īpašums un dokumentācija.
- Ja darba attiecības ar trešo pusi tiek pārtrauktas attaisnota iemesla dēļ, attaisnojošie apstākļi vai riski tiek identificēti, un par tiem tiek informēta augstākā līmeņa vadība un/vai valde (padome).
- Ja tiek izbeigts prioritizētas trešās puses līgums, šī puse tiek aizstāta, pamatojoties uz to pašu riska novērtējumu, ja vien līgums nav pabeigts vai vairs nav vajadzīgs.

A pielikums. Praktiskā pielietojuma piemēri

Turpmākajos piemēros ir aprakstīti scenāriji, kuros būtu piemērojama trešās puses tematiskā prasība:

1. piemērs: Iekšējās audita uzdevumā, kas iekļauts iekšējās audita plānā, ir iekļauts pakalpojums vai darbības rezultāts, ko pašlaik sniedz trešā puse.

Ja iekšējā audita funkcija pabeidz uz risku balstītu plānošanas procesu un iekšējā audita plānā iekļauj vienu vai vairākus uzdevumus par pakalpojumiem vai darbības rezultātiem, kurus pašlaik sniedz trešās puses saskaņā ar līgumu vai vienošanos, ir obligāti jāievēro tematiskā prasība.

Ne visas Tematiskās prasības var attiekties uz katru uzdevumu. Ja iekšējie auditori piemēro profesionālu spriedumu un nosaka, ka viena vai vairākas Trešās puses tematiskās prasības nav piemērojamas un tāpēc ir jāizslēdz no uzdevuma, iekšējiem auditoriem jādokumentē un jāsaglabā pamatojums šo prasību izslēgšanai. Piemēram, dažu prasību izslēgšanas pamatojums varētu būt tāds, ka iekšējā audita funkcija ir noteikusi, ka organizācijas paļaušanās uz trešajām pusēm attiecībā uz kritiski svarīgiem pakalpojumiem ir neliela vai ka tās ir iedibinātas attiecības ar mazu finansiālo ietekmi.

2. piemērs: Trešo pušu riski tiek identificēti, veicot pārliecības sniegšanas uzdevumu par tēmu, kas nav trešās puses vai līgumu vadība.

Iekšējie auditori var identificēt būtisku trešās puses risku, novērtējot procesu, kas sākotnēji nav noteikts kā saistīts ar trešām pusēm vai līgumu vadību. Piemēram, plānojot datu glabāšanas novērtēšanas uzdevumu, iekšējie auditori uzzina, ka mākoņpakalpojumi tiek mitināti ar trešās puses starpniecību. Intervijās ar trešās puses sniegto pakalpojumu vadību iekšējie auditori identificē kiberdrošības riskus, kas saistīti ar trešo pusi.

Kad attiecīgie riski ir identificēti, iekšējiem auditoriem jāpārskata gan Trešo pušu, gan kiberdrošības tematiskās prasības un jānosaka, kuras prasības ir piemērojamas. Auditori var neiekļaut trešās puses pārvaldības procesu vai trešās puses riska vadības procesu uzdevuma tvērumā un koncentrēties uz trešo pušu kontrolēm attiecībā uz revidējamiem pakalpojumiem. Tas pats profesionālais vērtējums attiecas uz kiberdrošības tematiskās prasības piemērošanu. Auditoriem uzdevuma darba dokumentos jādokumentē pamatojums, kāpēc nav iekļautas trešās puses vai kiberdrošības tematisko prasības, un dokumentācija jāsaglabā.

3. piemērs: Nepieciešams trešās puses uzdevums, kas sākotnēji nebija iekļauts iekšējāaudita plānā.

Organizācijā rodas jautājums, kas saistīts ar prioritāri noteiktu trešo pusi, kam nepieciešama tūlītēja iekšējā audita funkcijas uzmanība. Problēma bija saistīta ar kontroles kļūmi. Iekšējā audita vadītājam ir jāsazinās ar valdi par prioritāšu maiņu iekšējā audita funkcijas audita plānā un resursos, lai pielāgotos šai nepieciešamībai. Auditoram ir jāsadarbojas ar ietekmēto vadību, lai izstrādātu uzdevuma mērķus situācijas novērtēšanai un sniegtu ieteikumus, lai novērstu turpmākus gadījumus. Iekšējā audita vadītājam jāpārskata Tematiskās prasības, lai noteiktu uzdevuma darbības jomu, noteiktu, kuras prasības ir piemērojamas, un attiecīgi jādokumentē visi izņēmumi.

B pielikums. Neobligātais dokumentācijas rīks

No iekšējiem auditoriem tiek sagaidīts profesionāls vērtējums, lai noteiktu prasību piemērojamību, pamatojoties uz riska novērtējumu, un pienācīgi dokumentētu dažu prasību nepiemērošanu. Tematisko prasību var dokumentēt iekšējā audita plānā vai uzdevuma darba dokumentos, pamatojoties uz auditora profesionālo vērtējumu. Prasības var attiekties uz vienu vai vairākiem iekšējā audita uzdevumiem. Turklāt ne visas prasības var būt piemērojamas. Tālāk sniegtā veidlapa, ko var izdrukāt, ir viena no iespējām, kā dokumentēt atbilstību Trešās puses aktuālajai prasībai, taču tās izmantošana nav obligāta.

Trešo pušu pārvaldība

Prasība	Izpildītais segums vai izslēgšanas pamatojums	Atsauce uz dokumentāciju
A. Lai noteiktu, vai slēgt līgumu ar trešo pusi, tiek izstrādāta, īstenota un periodiski pārskatīta oficiāla pieeja. Šī pieeja ietver atbilstošus kritērijus, lai noteiktu un novērtētu nepieciešamos un pieejamos resursus, kas nepieciešami mērķu sasniegšanai, nodrošinot produktu vai pakalpojumu.		
B. Ir izstrādātas politikas un procedūras, lai definētu, novērtētu un vadītu attiecības un riskus ar trešām pusēm visā trešo pušu dzīves ciklā. Politikas un procedūras ir saskaņotas ar piemērojamām normatīvajām prasībām un tiek periodiski pārskatītas un atjauninātas, lai stiprinātu kontroles vidi.		
C. Ir definētas organizācijas trešo pušu vadības funkcijas un pienākumi, detalizēti norādot, kas izvēlas, vada, vada, sazinās un uzrauga trešās puses un kam jābūt informētam par trešo pušu darbībām. Pastāv process, lai nodrošinātu, ka personām, kurām uzticētas trešo pušu funkcijas un pienākumi, ir atbilstoša kompetence.		

Prasība	Izpildītais segums vai izslēgšanas pamatojums	Atsauce uz dokumentāciju
D. Ir definēti protokoli saziņai ar attiecīgajām ieinteresētajām pusēm, un tie ietver savlaicīgu ziņošanu par prioritāro trešo pušu darbības, risku un atbilstības (jo īpaši likumu un noteikumu pārkāpumu) statusu. Trešo pušu prioritāte tiek noteikta, pamatojoties uz risku. Attiecīgās ieinteresētās puses var būt valde (padome), augstākā līmeņa vadība, iepirkuma, operatīvās darbības, riska vadības, atbilstības, juridiskās, informācijas tehnoloģiju, informācijas drošības, cilvēkresursu un citas.		

Trešo pušu riska vadība

Prasība	Izpildītais segums vai izslēgšanas pamatojums	Atsauce uz dokumentāciju
A. Trešo pušu un to pakalpojumu riska vadības procesi ir standartizēti un visaptveroši, tajos ir noteiktas lomas un pienākumi, un tajos ir pietiekami ņemti vērā galvenie ar organizāciju saistītie riski (piemēram, stratēģiskie, reputācijas, ētiskie, darbības, finanšu, atbilstības, kiberdrošības, informācijas tehnoloģiju, juridiskie, ilgtspējības un ģeopolitiskie riski). Procesu ievērošana tiek uzraudzīta, un jebkuru noviržu gadījumā tiek īstenoti koriģējoši pasākumi.		
B. Riski, kas saistīti ar trešām pusēm visā dzīves ciklā, tiek regulāri identificēti un novērtēti. Riska novērtējumu izmanto, lai sarindotu un noteiktu prioritātes trešajām pusēm, tostarp tām, kas atrodas tālāk pa straumi. Riska risinājumi ir arī sarindoti un prioritizēti. Riska novērtējums tiek pārskatīts un periodiski atjaunināts.		

Prasība	Izpildītais segums vai izslēgšanas pamatojums	Atsauce uz dokumentāciju
C. Atbildes uz riskiem ir atbilstošas un precīzas, samērojamas ar klasifikāciju. Reaģēšana uz riskiem tiek īstenota, pārskatīta, apstiprināta, uzraudzīta, novērtēta un pēc vajadzības koriģēta.		
D. Ir ieviesti procesi, lai vadītu un vajadzības gadījumā risinātu jautājumus, kas rodas no trešām pusēm, nodrošinot pārskatāmību par gala rezultātiem un palielinot līgumu vai citu vienošanos noteikumu izpildes iespējamību. Ja trešā puse nereaģē uz izteiktajām bažām, ir ieviesti procesi, kas ļauj vadībai novērtēt pastāvīgo darījumu attiecību riskus un, ja nepieciešams, veikt turpmākus pasākumus, novērst trūkumus vai izbeigt attiecības.		

Trešo pušu vadības ierīces

Prasība	Izpildītais segums vai izslēgšanas pamatojums	Atsauce uz dokumentāciju
A. Ir ieviests stingrs uzticamības pārbaudes process trešo pušu meklēšanai un atlasei, un ir dokumentēta un apstiprināta uzņēmējdarbības analīze vai cits attiecīgs dokuments, kurā aprakstīta un pamatota vajadzība pēc attiecībām ar trešo pusi un to raksturs.		
B. Līgumu slēgšana un apstiprināšana tiek veikta saskaņā ar organizācijas trešo pušu riska vadības politiku un procedūrām un ietver sadarbību starp attiecīgajām organizācijas struktūrvienībām.		
C. Galīgos līgumus vai vienošanās pārskata un apstiprina visas attiecīgās ieinteresētās puses, tostarp juridiskās un atbilstības nodrošināšanas speciālisti, un tos paraksta abu pušu pilnvarotas personas, un tie tiek droši uzglabāti. Par katru līgumu ir atbildīgs līguma vadītājs vai administrators.		

Prasība	Izpildītais segums vai izslēgšanas pamatojums	Atsauce uz dokumentāciju
D. Tiek uzturēts precīzs, pilnīgs un aktuāls visu trešo pušu attiecību saraksts, piemēram, centralizētā līgumu vadības sistēmā.		
E. Tiek izveidoti un ievēroti dokumentēti ievadprocesi, lai radītu pamatu trešām pusēm izpildīt līguma vai vienošanās noteikumus.		
F. Pastāvīgi tiek veikti uzraudzības procesi, lai novērtētu, vai trešās puses visā dzīves cikla laikā darbojas saskaņā ar līguma vai vienošanās noteikumiem un vai trešās puses pilda savas līgumsaistības. Šie procesi ietver sniegtās informācijas ticamības pārbaudi, kā arī periodisku darbības veiktspējas rezultātu atkārtotu novērtēšanu un katru reizi, kad mainās līgums.		
G. Ir izstrādāti protokoli, lai uzsāktu koriģējošus pasākumus, ja trešā puse neatbilst gaidītajam vai rada paaugstinātu vai neparedzētu risku. Protokolos ietilpst incidentu eskalācija atkarībā no to nopietnības, pēcincidentu pārskatīšana un incidentu pamatcēloņu analīze.		
H. Tiek uzraudzīti līgumu beigu un atjaunošanas datumi, un, ja nepieciešams, tiek veikti atjaunošanas pasākumi.		
I. Tiek ieviests un ievērots formalizēts darbinieku izlaišanas no darba plāns, lai nodrošinātu, ka tiek atbilstoši ievērotas līguma prasības attiecībā uz termiņiem un gaidām. Procesi ietver, kā: • Izbeigt trešās puses darbību. • Ja nepieciešams, nomainiet trešo pusi. • Pārdot glabāšanu un atgriezt vai iznīcināt organizācijas sensitīvos datus, kas glabājas pie trešās puses. • Atcelt trešās puses piekļuvi sistēmām, rīkiem un iekārtām.		

Par Iekšējo auditoru institūtu

IIA ir starptautiska profesionāla asociācija, kas apvieno vairāk nekā 265 000 biedru visā pasaulē un ir piešķīrusi vairāk nekā 200 000 sertificēta iekšējā auditora (CIA®) sertifikātu visā pasaulē. IIA ir dibināta 1941. gadā un visā pasaulē ir atzīta par iekšējā audita profesijas līderi standartu, sertifikācijas, izglītības, pētniecības un tehnisko vadlīniju jomā. Lai uzzinātu vairāk, apmeklējiet theiia.org.

Atruna

IIA publicē šo dokumentu informatīviem un izglītojošiem mērķiem. Šis materiāls nav paredzēts, lai sniegtu galīgas atbildes uz konkrētiem individuāliem apstākļiem, un tādēļ to var izmantot tikai kā ceļvedi. IIA iesaka meklēt neatkarīgu ekspertu konsultācijas, kas tieši attiecas uz jebkuru konkrētu situāciju. IIA neuzņemas nekādu atbildību par to, ka kāds paļaujas tikai uz šo materiālu.

Autortiesības

2025. gada septembris

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