Trečioji šalis

Teminis reikalavimas

Topical Requirements

Naudotojo vadovas

The Institute of
Internal Auditors

Turinys

Teminių reikalavimų apžvalga

Teminiai reikalavimai yra esminė Tarptautinės profesinės praktikos sistemos („Professional Practices Framework®“) sudedamoji dalis kartu su Pasauliniais vidaus audito standartais („Global Internal Audit Standards™“) ir Visuotinėmis gairėmis. Vidaus auditorių institutas reikalauja, kad Teminiai reikalavimai būtų taikomi kartu su Standartais, kurie suteikia autoritetingą pagrindą reikalaujamai praktikai. Šiame vadove pateikiamos nuorodos į Standartus kaip išsamesnės informacijos šaltinį.

Teminiai reikalavimai įformina, kaip vidaus auditoriai sprendžia dažniausiai pasitaikančias rizikos sritis, siekiant skatinti kokybę ir nuoseklumą profesijoje. Teminiai reikalavimai nustato pagrindinius reikalavimus ir pateikia atitinkamus kriterijus, pagal kuriuos teikiamos užtikrinimo paslaugos, susijusios su Teminio reikalavimo objektu (13.4 standartas „Vertinimo kriterijai“). Atitiktis Teminiams reikalavimams yra privaloma teikiant užtikrinimo paslaugas ir rekomenduojama įvertinti teikiant konsultavimo paslaugas. Teminiais reikalavimais nesiekiama aprėpti visų galimų aspektų, į kuriuos reikėtų atsižvelgti atliekant užtikrinimo užduotis; jais veikiau siekiama nustatyti minimalius reikalavimus, kad būtų galima nuosekliai ir patikimai įvertinti temą.

Teminiai reikalavimai aiškiai susieti su VAI (IIA) Trijų linijų modeliu ir Pasauliniais vidaus audito standartais. Valdysenos, rizikos valdymo ir kontrolės procesai yra pagrindinės Teminių reikalavimų, atitinkančių 9.1 standartą „Valdysenos, rizikos valdymo ir kontrolės procesų supratimas“, sudedamosios dalys. Remiantis Trijų linijų modeliu, valdysena yra susijusi su valdyba / valdymo organu, rizikos valdymas – su antrąja linija, o kontrolės arba kontrolės procesai – su pirmąja linija. Nors vadovybė atstovaujama tiek pirmojoje, tiek antrojoje linijose, vidaus audito funkcija vaizduojama trečiojoje linijoje kaip nepriklausomas ir objektyvus užtikrinimo teikėjas, atsiskaitantis valdybai ir (arba) valdymo organui (8 principas „Valdybos vykdoma priežiūra“).

Taikomumas, rizika ir profesinis vertinimas

Teminių reikalavimų privaloma laikytis, kai vidaus audito funkcijos atlieka užtikrinimo užduotis, susijusias su temomis, kurioms taikomas Teminis reikalavimas, arba kai Teminio reikalavimo aspektai nustatomi kitose užtikrinimo užduotyse.

Kaip aprašyta Standartuose, rizikų įvertinimas yra svarbi vidaus audito vadovo planavimo dalis. Nustatant, kokias užtikrinimo užduotis įtraukti į vidaus audito planą, reikia bent kartą per metus įvertinti organizacijos strategijas, tikslus ir rizikas (9.4 standartas „Vidaus audito planas“). Planuodami individualias užtikrinimo užduotis, vidaus auditoriai turi įvertinti su užduotimi susijusias rizikas (13.2 standartas „Užduoties rizikos vertinimas“).

Kai Teminio reikalavimo tema nustatoma per rizika pagrįsto vidaus audito planavimo procesą ir įtraukiama į audito planą, tuomet Teminiame reikalavime išdėstyti reikalavimai privalo būti naudojami temai įvertinti taikomų užduočių metu. Be to, kai vidaus auditoriai atlieka užduotį (įtrauktą arba neįtrauktą į planą) ir iškyla Teminio reikalavimo elementai, privaloma įvertinti Teminio reikalavimo taikymą atliekant užduotį.

Galiausiai, jei prašoma atlikti užduotį, kuri iš pradžių nebuvo įtraukta į planą, bet apima temą, privaloma įvertinti Teminio reikalavimo taikymą.

Taikant Teminį reikalavimą svarbiausias vaidmuo tenka profesiniam vertinimui. Rizikos vertinimai lemia vidaus audito vadovų sprendimus, kokias užduotis įtraukti į vidaus audito planą (9.4 standartas). Be to, vidaus auditoriai, remdamiesi profesiniu vertinimu, nustato, kokie aspektai bus nagrinėjami kiekvienos užduoties metu (13.3 standartas „Užduoties tikslai ir apimtis“, 13.4 standartas „Vertinimo kriterijai“ ir 13.6 standartas „Darbo programa“).

Turi būti išsaugomi įrodymai, kad buvo įvertintas kiekvieno Teminio reikalavimo pritaikomumas, įskaitant pagrindimą, paaiškinantį bet kokių reikalavimų netaikymą. Atitiktis Teminiam reikalavimui turi būti dokumentuojama remiantis auditorių profesiniu vertinimu, kaip aprašyta 14.6 standarte „Užduoties dokumentai“.

Nors Teminis reikalavimas pateikia pagrindinius kontrolės procesus, į kuriuos reikia atsižvelgti, organizacijoms, kurios rizikos temą vertina kaip labai didelę, gali tekti įvertinti papildomus aspektus.

Jei vidaus audito funkcija neturi reikiamos kompetencijos atlikti užduotis Teminio reikalavimo tema, vidaus audito vadovas turi nustatyti, kaip gauti reikalingų išteklių, ir laiku pranešti valdybai bei vyresniajai vadovybei apie apribojimų poveikį ir kaip bus sprendžiamas išteklių trūkumo klausimas. Vidaus audito vadovas prisiima galutinę atsakomybę už vidaus audito funkcijos atitikties Teminiams reikalavimams užtikrinimą, nepriklausomai nuo to, kokiu būdu gaunami ištekliai (3.1 standartas „Kompetencija“, 7.2 standartas „Vidaus audito vadovo kvalifikacija“, 8.2 standartas „Ištekliai“, 10.2 standartas „Žmogiškųjų išteklių valdymas“).

Vykdymas, dokumentavimas ir ataskaitų teikimas

Taikydami Teminius reikalavimus, vidaus auditoriai taip pat privalo laikytis Standartų ir savo darbą atlikti pagal V sritį: Vidaus audito paslaugų teikimas. V srities standartuose aprašomas užduočių planavimas (13 principas „Veiksmingai planuoti užduotis“), užduočių vykdymas (14 principas „Atlikti užduoties darbą“) ir užduočių rezultatų komunikavimas (15 principas „Pranešti apie užduoties rezultatus ir vykdyti veiksmų planų stebėseną“).

Teminiai reikalavimai yra skirti nuosekliai ir kokybiškai vidaus audito praktikai palaikyti. Vietos įstatymai, reglamentai, priežiūros institucijų lūkesčiai ir kitos profesiniu požiūriu pripažintos sistemos gali nustatyti papildomus ar konkretesnius reikalavimus. Vidaus auditoriai turi suprasti ir laikytis įstatymų ir (arba) kitų teisės aktų, susijusių su tuo sektoriumi ir jurisdikcijomis, kuriose veikia organizacija, įskaitant informacijos atskleidimą, kaip reikalaujama pagal 1.3 standartą „Teisinis ir etiškas elgesys“. Vidaus auditoriai šiuos papildomus reikalavimus jau gali būti įtraukę į audito programas ir testavimo procedūras, todėl, siekdami užtikrinti tinkamą jų aprėptį, turėtų juos suderinti su Teminiu reikalavimu.

Teminio reikalavimo aprėptis gali būti dokumentuojama vidaus audito plane arba užduoties dokumentuose, remiantis auditorių profesiniu vertinimu. Reikalavimus gali apimti viena ar kelios vidaus audito užduotys. Be to, ne visi reikalavimai gali būti taikytini. Turi būti išsaugoti įrodymai, kad buvo įvertintas Teminio reikalavimo pritaikomumas, įskaitant bet kokių išimčių pagrindimą.

Kokybės užtikrinimas

Standartuose reikalaujama, kad vidaus audito vadovas parengtų, įgyvendintų ir palaikytų kokybės užtikrinimo ir tobulinimo programą, apimančią visus vidaus audito funkcijos aspektus (8.3 standartas „Kokybė“). Rezultatai privalo būti pateikti valdybai ir vyresniajai vadovybei. Komunikacijoje turi būti pateikiama informacija apie vidaus audito funkcijos atitiktį Standartams ir veiklos tikslų pasiekimą.

Atitiktis Teminiams reikalavimams bus vertinama atliekant kokybės vertinimus.

Trečioji šalis

Trečioji šalis – tai išorinis asmuo, grupė ar subjektas, su kuriuo organizacija (toliau – pagrindinė organizacija) užmezga verslo santykius, siekdama įsigyti produktų ar paslaugų. Santykiai gali būti įforminti sutartimi, susitarimu ar kitomis formomis, siekiant organizacijai teikti produktus, paslaugas, darbo jėgą, gamybą ar informacinių technologijų sprendimus, pavyzdžiui, duomenų saugojimą, apdorojimą ir priežiūrą.

> Pastaba
>
> Teminiuose reikalavimuose vartojama bendroji vidaus audito terminologija, kaip apibrėžta Pasauliniuose vidaus audito standartuose. Skaitytojai turėtų remtis Standartų žodyno sąvokomis ir apibrėžimais.

Sąvoka „trečioji šalis“ gali būti vartojama skirtingai, atsižvelgiant į sektorių ar kitas aplinkybes. Kiekviena vidaus audito funkcija gali lanksčiai spręsti, kaip taikyti šį Teminį reikalavimą, atsižvelgdama į tai, kaip pagrindinė organizacija (organizacija, sudaranti susitarimą su trečiąja šalimi) apibrėžia trečiąsias šalis. Trečiosios šalies Teminiame reikalavime ir naudotojo vadove sąvoka „trečioji šalis“ reiškia pardavėjus, tiekėjus, rangovus, subrangovus, užsakomųjų paslaugų teikėjus, kitas agentūras ir konsultantus. Sąvoka „trečioji šalis“ apima visus tokius susitarimus, įskaitant susitarimus tarp trečiosios šalies ir jos subrangovų, dažnai vadinamų „tolesnės grandies“ subrangovais, „ketvirtosiomis šalimis“, „penktosiomis šalimis“ arba „N-osiomis šalimis“.

Šis Teminis reikalavimas nėra skirtas spręsti netiesioginiams išoriniams santykiams, interesams ar ryšiams su pagrindine organizacija (pvz., su reguliavimo institucijomis, agentais, tarpininkais, investuotojais, patikėtiniais ir (arba) valdybos nariais, viešosiomis tarnybomis ir plačiosios visuomenės nariais) arba vidiniams santykiams (pvz., su darbuotojais ar grupės vidaus paslaugų teikėjais).

Sąvoka „trečioji šalis“ gali būti apibrėžiama ir vartojama skirtingai, atsižvelgiant į sektorių ar kitas aplinkybes. Vidaus auditoriams suteikiamas lankstumas ir jie turėtų remtis savo profesiniu vertinimu, kad pritaikytų Teminį reikalavimą prie pagrindinės organizacijos trečiosios šalies apibrėžimo.

Organizacijos santykių su trečiosiomis šalimis valdymo procesų veiksmingumą galima vertinti visoje organizacijoje ir (arba) vienos ar kelių atskirų sutarčių, susitarimų ar santykių lygmeniu. Vidaus auditoriai turėtų taikyti metodą „iš viršaus į apačią“, kad geriau suprastų organizacijos trečiųjų šalių politikas, procedūras, procesus, sistemą ir gyvavimo ciklą. Vidaus auditoriai turėtų vadovautis savo nuožiūra, kad suprastų trečiųjų šalių rizikos niuansus, atsižvelgiant į atskirus sektorius, organizacijas ir užduočių temas. Pagal 5.1 standartą „Informacijos naudojimas“ vidaus auditoriai turėtų žinoti ir laikytis bet kokių politikų ir procedūrų, susijusių su trečiųjų šalių informacija, kurios jiems yra prieinamos.

Teminis reikalavimas taikomas, kai vidaus audito funkcija atlieka užtikrinimo užduotis trečiosioms šalims ir (arba) bet kokiems subrangos santykiams, įskaitant ketvirtąsias ar tolesnes grandis, kurias leidžia trečiosios šalies sutartis ar susitarimas su pagrindine organizacija. Vidaus auditoriai turėtų teikti

pirmenybę trečiosioms ir tolesnėms grandies šalims, atsižvelgdami į riziką, kaip aprašyta tolesniame rizikos valdymo skyriuje. Vidaus auditoriai privalo taikyti visus reikalavimus, kaip nurodyta rizikos vertinimo rezultatuose, o išimtys turi būti dokumentuotos.

Trečiosios šalies Teminiame reikalavime ir naudotojo vadove nurodomi organizacijos santykių su trečiosiomis šalimis etapai, dar vadinami gyvavimo ciklo etapais: atranka, sutarčių sudarymas, integracija, stebėsena ir santykių nutraukimas. Šie etapai bus naudojami Trečiosios šalies Teminio reikalavimo ir naudotojo vadovo tikslais, nors kai kurios pramonės šakos turi savo gyvavimo ciklo versijas. Etapai:

- Atranka: apima procesus, skirtus trečiosios šalies poreikiui nustatyti, jos naudojimo planą ir išsamų atrankos patikrinimą. Be to, atliekant atranką reikėtų įvertinti potencialių ir dalyvaujančių trečiųjų šalių riziką.
- Sutarčių sudarymas: apima išsamaus patikrinimo procesus, skirtus teisinio susitarimo su trečiąja šalimi rengimui, deryboms, tvirtinimui ir įgyvendinimui.
- Integracija: prasideda, kai pasirašoma sutartis, kuria pradedami santykiai, ir sukuria pagrindą trečiosioms šalims laikytis sutarties ar susitarimo sąlygų.
- Stebėsena: apima trečiosios šalies valdymo „gyvavimo laikotarpiu“ ir nuolatinės trečiosios šalies stebėsenos procesus po to, kai sutartis sudaryta ir patvirtinta. Šis metodas paprastai yra sistemingas ir pagrįstas rizika, todėl reikėtų atsižvelgti į nuolatinį tobulinimą. Stebėsena apima galiojančių sutarčių ar susitarimų su trečiosiomis šalimis atnaujinimą, kai tai būtina.
- Santykių nutraukimas: apima sutarčių ir susitarimų nutraukimo procesus, pasitraukimo strategijos palaikymą trečiosioms šalims, kurioms buvo nustatyta prioritetinė rizika, ir santykių nutraukimą, kai tai būtina. Procesai paprastai grindžiami rizika pagrįstu požiūriu ir gali apimti oficialų pasitraukimo planą.

Pagrindinė organizacija lieka atsakinga už riziką, susijusią su jos tikslų įgyvendinimu, net jei ji pasitelkia trečiąją šalį, kad ši padėtų jai pasiekti vieną ar daugiau tikslų. Bendradarbiavimas su trečiosiomis šalimis gali sumažinti kai kurias organizacijos išlaidas, susijusias su procesų vykdymu. Tačiau dėl to gali kilti operacinė rizika, nes pagrindinė organizacija turi mažiau galimybių matyti trečiosios šalies kontrolės procesus ir mažiau įgaliojimų juos kontroliuoti. Jei trečioji šalis nevykdo sutartyje numatytų įsipareigojimų, dalyvauja neetiškoje veikloje arba patiria verslo sutrikimų, pagrindinė organizacija gali patirti pasekmių.

Pagrindinė organizacija privalo nustatyti, įvertinti ir valdyti riziką taikydama tinkamus valdysenos, rizikos valdymo ir kontrolės procesus. Su trečiosiomis šalimis susijusios rizikos kategorijos ir pavyzdžiai:

- Strateginė rizika, pavyzdžiui, gebėjimas įgyvendinti organizacijos misiją ir (arba) strateginius tikslus arba valdyti susijungimų ir įsigijimų poveikį.
- Reputacinė rizika, pavyzdžiui, žala, padaryta aplinkai arba pagrindinės organizacijos santykiams ir pasitikėjimui su klientais, vartotojais ir suinteresuotosiomis šalimis.
- Etinė rizika, pavyzdžiui, sąžiningumo trūkumai, interesų konfliktai, kyšiai ir korupcija.
- Operacinė rizika, pavyzdžiui, fizinis ir informacijos saugumas, vidinė rizika, paslaugų sutrikimai ir tikslų nepasiekimas.
- Finansinė rizika, pavyzdžiui, trečiųjų šalių nemokumas ir sukčiavimas.

- Atitikties rizika taikomiems vietiniams, nacionaliniams ir tarptautiniams teisiniams (teisės aktų) reikalavimams.
- Kibernetinio saugumo ir duomenų apsaugos rizika, pavyzdžiui, jautrių duomenų pažeidimas ir nutekėjimas.
- Informacinių technologijų rizika, pavyzdžiui, paslaugų, skirtų kritinėms operacijoms palaikyti, trūkumas.
- Teisinė rizika, pavyzdžiui, interesų konfliktai, ginčai ir bylinėjimasis dėl sutarties pažeidimų.
- Tvarumo rizika, pavyzdžiui, aplinkosaugos, socialinė ir valdysenos. Pavyzdžiai apima riziką, susijusią su organizacijos poveikiu gamtinei aplinkai, ir riziką, susijusią su organizacijos sąveika su bendruomenėmis.
- Geopolitinė rizika, pavyzdžiui, prekybiniai ginčai ir (arba) sankcijos bei politinis nestabilumas.

Vidaus auditoriai turėtų atsižvelgti į šiuos etapus vertindami valdysenos, rizikos valdymo ir kontrolės procesų reikalavimus.

Reikalavimai trečiosioms šalims Teminiuose reikalavimuose yra suskirstyti į tris dalis pagal 9.1 standartą „Valdysenos, rizikos valdymo ir kontrolės procesų supratimas“.

- Valdysena – aiškiai apibrėžti baziniai tikslai ir strategijos, kaip pasitelkti trečiąsias šalis organizacijos tikslams, politikoms ir procedūroms įgyvendinti.
- Rizikos valdymas – procesai, skirti nustatyti, analizuoti, valdyti ir stebėti riziką, susijusią su trečiųjų šalių pasitelkimu, įskaitant greito incidentų eskalavimo procesą.
- Kontrolė – vadovybės nustatyti, periodiškai vertinami kontrolės procesai, skirti rizikai sumažinti, kai naudojamasi trečiųjų šalių paslaugomis.

Be Teminio reikalavimo ir šio naudotojo vadovo, vidaus auditoriai gali norėti pasinaudoti papildomomis profesinėmis gairėmis dėl trečiųjų šalių, pavyzdžiui, Tarptautine profesinės praktikos sistema (TPPS), Visuotinėmis gairėmis ir konkretaus sektoriaus šaltiniais.

Aspektai

Toliau išdėstyti aspektai gali padėti vidaus auditoriams įgyvendinti Trečiųjų šalių Teminio reikalavimo nuostatas. Kiekviename toliau pateiktame skyriuje raidėmis pažymėti teiginiai pakartoja arba perfrazuoja atitinkamus Teminio reikalavimo punktus. Šie neprivalomi aspektai yra iliustratyvūs ir pateikiami kaip pavyzdžiai, kaip galima įvertinti reikalavimus. Nustatydami, ką įtraukti į savo vertinimus, vidaus auditoriai turėtų vadovautis profesiniu sprendimu.

Valdysenos aspektai

Siekiant įvertinti, kaip valdysenos procesai, įskaitant valdybos priežiūrą, yra taikomi trečiųjų šalių tikslams, vidaus auditoriai gali peržiūrėti šiuos įrodymus:

A. Formalizuotą ir dokumentuotą, rizika pagrįstą požiūrį arba strategiją, skirtą nustatyti, ar naudotis trečiosios šalies paslaugomis. Šis metodas periodiškai peržiūrimas ir apima:

- Aiškiai apibrėžtas ir standartizuotas procesas, skirtas požiūriui įgyvendinti, kurį patvirtino organizacija.
- Biudžeto ištekliai, pagrįsti sąnaudų ir naudos analize, siekiant pateisinti trečiosios šalies pasitelkimą, užtikrinant strateginį suderinamumą ir išteklių efektyvumą.
- Vadovybės atliekamas rizikos ir kontrolės priemonių, įskaitant tas, kuriomis sprendžiami su trečiosiomis šalimis susiję klausimai, vertinimas.
- Pakankami ištekliai sutartims su trečiosiomis šalimis sudaryti, valdyti ir stebėti jų veiklą.
- Suinteresuotųjų šalių atsiliepimų integravimas į požiūrį ar strategiją.

B. Politikoms, procedūroms ir kitiems susijusiems dokumentams, naudojamiems nustatant, vertinant ir valdant santykius su trečiosiomis šalimis per visą gyvavimo ciklą. Politikos ir procedūros gali apimti:

- Standartizuotos priemonės ir šablonai, palengvinantys pagrindinius valdysenos, rizikos valdymo ir kontrolės procesus.
- Procesai, skirti periodiškai vertinti politikas ir procedūras, nustatyti jų tinkamumą ir prireikus jas atnaujinti.
- Nustatyti trečiųjų šalių atrankos, sutarčių sudarymo, įdarbinimo, stebėsenos ir santykių nutraukimo kriterijai.
- Taikomų reguliavimo reikalavimų nustatymas ir periodinė peržiūra, siekiant juos suderinti su politikomis ir procedūromis.
- Lyginamoji analizė, atliekama siekiant nustatyti ir palyginti pažangiausias trečiųjų šalių valdymo praktikas.

C. Apibrėžti vaidmenys ir atsakomybės, padedantys siekti trečiosios šalies tikslų. Kiti galimi įrodymai:

- Procesai, skirti įvertinti, ar trečiosios šalies vertybės, etika ir įmonės socialinė atsakomybė atitinka pagrindinės organizacijos principus. Šiame procese turėtų būti numatyta, kaip nedelsiant spręsti galimų interesų konfliktų ar neetiškos praktikos klausimus.
- Reguliarus darbuotojų, einančių trečiųjų šalių vadovų pareigas, mokymas ir periodinis jų kompetencijos vertinimas.
- Procesas, skirtas įvertinti, ar buvo įdiegti mokymai, skirti visos organizacijos informuotumui apie trečiąsias šalis didinti.
- Vaidmenys ir atsakomybės yra suderinti su Trijų linijų modeliu.

D. Savalaikis bendravimas ir bendradarbiavimas su atitinkamomis suinteresuotosiomis šalimis per visą trečiosios šalies gyvavimo ciklą (pavyzdžiui, valdyba, vyresniąja vadovybe, viešųjų pirkimų, operacijų, rizikos valdymo, atitikties, teisės, informacinių technologijų, informacinės saugos, žmogiškųjų išteklių ir kitų sričių specialistais), kuris apima:

- Informaciją apie trečiųjų šalių riziką ir žinomus galimus pažeidžiamumus posėdžių protokoluose, ataskaitose ar el. laiškuose.
- Keitimąsi informacija apie trečiųjų šalių valdymą ir bendradarbiavimo skatinimą (pvz., periodiškai rengiami tarpfunkciniai susitikimai).

Rizikos valdymo aspektai

Siekdami įvertinti, kaip rizikos valdymo procesai taikomi trečiosios šalies tikslams, vidaus auditoriai gali peržiūrėti įrodymus, kad:

A. Standartizuoti ir išsamūs rizikos valdymo procesai trečiųjų šalių paslaugų naudotojams apima apibrėžtus vaidmenis ir atsakomybes bei pakankamai atsižvelgia į pagrindines organizacijai aktualias rizikas:

- Trečiųjų šalių rizikos vertinimo ir valdymo procesai apima tai, kai pagrindinės rizikos yra:
  - Iš pradžių nustatomos ir apie jas pranešama.
  - Analizuojamos siekiant įvertinti jų poveikį gebėjimui pasiekti organizacijos tikslus.
  - Sumažintos, įskaitant veiksmų planus, skirtus rizikoms sumažinti iki priimtino lygio.
  - Stebimos, įskaitant išankstinių perspėjimų aptikimą ir reagavimą į juos bei nuolatinio pranešimo planą, kol grėsmės bus visiškai pašalintos.
- Stebima, kaip laikomasi procesų, ir įgyvendinami bet kokių nukrypimų korekciniai veiksmai, kad nebūtų pakenkta ilgalaikiams organizacijos tikslams ar strategijai.
- Rizikos valdymo komitetas ar kita grupė tiesiogiai prižiūri trečiąsias šalis ir teikia informaciją valdybai. Komitetas turi apibrėžtą tikslą ir reguliariai renkasi į posėdžius. Įrodymai gali būti posėdžių protokolai.

B. Su trečiosiomis šalimis susijusios rizikos per visą gyvavimo ciklą yra nustatomos ir reguliariai vertinamos. Atliekant rizikos vertinimą, trečiosios šalys yra reitinguojamos ir prioritetizuojamos. Reagavimo į riziką būdai yra reitinguojami ir prioritetizuojami.

- Rengdama trečiųjų šalių rizikos vertinimą, pagrindinė organizacija atsižvelgia į tokius veiksnius kaip jos dydis, brandumas ir pasitelktų trečiųjų šalių skaičius.
- Rizikos vertinimas yra dokumentuojamas ir jame nustatoma prigimtinė ir likutinė rizika.
- Organizacijoje taikomas išsamus patikrinimo procesas, kurio metu peržiūrimas ir atnaujinamas rizikos vertinimas.
- Nustatomi kriterijai, pagal kuriuos trečiosios šalys klasifikuojamos ir skirstomos pagal riziką. Tokių kriterijų pavyzdžiai:
  - Teikiamos paslaugos yra labai svarbios organizacijos veiklai.
  - Susitarimo finansinė vertė yra reikšminga.
  - Santykiai yra nauji, užmegzti skubotai ir (arba) jų trukmė yra ilga.
  - Dalyvauja kelios išorės šalys.
  - Trečioji šalis planuoja dalį arba visus darbus perduoti subrangovams.
- Organizacija laikosi visuotinai pripažintos rizikos vertinimo praktikos, įskaitant tai, kad rizikos vertinimas turi būti atliekamas kuo ankstesniame etape, paprastai tada, kai pasiūlymas analizuojamas atrankos etape, ir prieš integraciją.
- Pardavėjai užpildo klausimyną, kad būtų nustatytas jų rizikos reitingas ir prioritetas pagal prigimtinę riziką. Organizacija užtikrina, kad klausimynus užpildytų atitinkami darbuotojai ir kad jie būtų peržiūrėti, užtikrinant tikslumą.
- Organizacija periodiškai gauna informaciją apie trečiųjų šalių rizikos valdymą iš funkcinių sričių, pavyzdžiui, informacinių technologijų, viešųjų pirkimų, įmonės rizikos valdymo, žmogiškųjų išteklių, teisės, atitikties, operacijų, apskaitos ir finansų.

C. Nustatomi rizikos valdymo būdai, pavyzdžiui, rizikos mažinimas, priėmimas, atsisakymas ir perleidimas, kurie atitinka rizikos klasifikaciją.

- Reagavimas į riziką yra dokumentuojamas ir apima trečiosios šalies kontrolės aplinkos įvertinimą.
- Dokumentai, patvirtinantys, kad reagavimas į riziką, kuri viršija pagrindinės organizacijos rizikos toleranciją, yra peržiūrimas, ar jis yra tinkamas, ypač kai rizika yra priimtina. Tarp atsakymų yra ir atsakymai dėl galimų interesų konfliktų su trečiosiomis šalimis.

D. Trečiųjų šalių rizikos valdymo ir eskalavimo procesai, įskaitant tai, kaip vertinamas, priskiriamas ir nustatomas grėsmės ar rizikos lygis ir prioritetai. Peržiūra gali apimti:

- Organizacijos rizikos lygių (pavyzdžiui, aukšto, vidutinio ir žemo) apibrėžimai ir paaiškinimai bei kiekvienos rizikos kategorijos eskalavimo procedūros.
- Trečiųjų šalių sąrašas pagal nustatytą riziką ir visų rizikos įvykių sušvelninimo statusas
- Taikomi teisiniai, reguliavimo ir atitikties reikalavimai

- Finansinės ir nefinansinės rizikos poveikis (pvz., reputacijai).
- Trečiųjų šalių rizikos perdavimo vadovybei ir darbuotojams procesai, įskaitant reguliarias ataskaitas apie rizikos pobūdį valdybai (arba kitam atitinkamam organui). Į pranešimus turėtų būti įtraukiama atnaujinta informacija apie bet kokių problemų, susijusių su trečiosiomis šalimis, kurioms suteiktas prioritetas, šalinimą.
- Procesai, skirti iš naujo įvertinti reitingavimą ir prioritetų nustatymą, kai pasikeičia pagrindinės organizacijos rizikos apetitas ir rizikos tolerancijos lygis.

Kontrolės aspektai

Siekdami įvertinti, kaip kontrolės procesai taikomi trečiųjų šalių santykiams, vidaus auditoriai gali peržiūrėti įrodymus, kad:

A. Yra įdiegtas patikimas išsamaus patikrinimo procesas trečiųjų šalių paieškai ir atrankai, kartu su dokumentuotu ir patvirtintu verslo pagrindimu ar kita atitinkama dokumentacija, kurioje apibūdinamas ir pagrindžiamas santykių su trečiąja šalimi poreikis bei pobūdis.

- Verslo pagrindimas taip pat gali:
  - Atsižvelgti į rizikas, susijusias su trečiosios šalies gebėjimu pateisinti lūkesčius, ir galimą poveikį organizacijai.
  - Apimti išsamią sąnaudų ir naudos analizę.
- Laikytis nustatytų tiekimo procesų, tokių kaip konkurencinių pasiūlymų teikimas, pasiūlymų užklausos ir vienintelio tiekėjo pasirinkimas. Šie procesai apima:
  - Kriterijus svarbiems aspektams, tokiems kaip kibernetinio saugumo protokolų peržiūra, banko duomenų tikrinimas, finansinės praeities tikrinimas, trečiosios šalies organizacinės struktūros, teistumo ir teisinių įrašų, vairavimo įrašų, politinės veiklos ir ryšių su nusikalstama veikla tyrimas.
  - Gerai apibrėžtus atrankos kriterijus, įskaitant ankstesnės veiklos, rekomendacijų, reputacijos ir sutarties išlaidų vertinimą.
  - Išsamų patikrinimą, siekiant užtikrinti tinkamą tiekėjų parinkimą, pavyzdžiui, sudarant tarpfunkcines komandas pasiūlymams peržiūrėti. Siekiant sumažinti šališkumo riziką, komandų peržiūrai skirtos kontrolės priemonės apima komandos sudarymo procedūras ir galimų interesų konfliktų atskleidimo reikalavimus.
  - Išsamų patikrinimą vertinant trečiosios šalies kontrolės aplinką, pavyzdžiui, apsilankymą vietoje arba trečiosios šalies dokumentų peržiūrą:
    - Sistemos ir organizacijos kontrolės (angl. SOC) ataskaitos.
    - Finansinis stabilumas.
    - Steigimo dokumentai arba geros reputacijos pažymėjimas.
    - Pagrindinės vadovybės ir suinteresuotųjų šalių sprendimų priėmimo skaidrumas.
    - Organizacinė struktūra.
    - Veiklos stabilumas.

- Kibernetinio saugumo protokolai.
- Atitiktis atitinkamiems įstatymams, reglamentams ir standartams.
- Etika.
- Ankstesnė bendradarbiavimo istorija su pagrindine organizacija.
- Reputacija.

  - Įrodymus, kad potencialūs tiekėjai ar rangovai pereina į sutarties sudarymo etapą tik po to, kai atliekami išsamaus patikrinimo procesai ir yra išanalizuojami jų rezultatai.

B. Sutarčių sudarymo politika ir procedūros yra nustatytos ir jų laikomasi.

- Sutartys rašomos nedviprasmiškai.
- Rengiant sutartį atsižvelgiama į pagrindines rizikas ir įtraukiamos atitinkamos sąlygos. Šio etapo metu su trečiąja šalimi komunikuojami klausimai, kuriuos reikia išspręsti.
- Esminiai sutarčių elementai nustatomi remiantis organizacijos sutarčių sudarymo politika ir procedūromis bei trečiosios šalies prioriteto lygiu. Elementai gali apimti:
  - Neatskleidimo (privatumo) susitarimus.
  - Nutraukimo sąlygas ir apibrėžtus duomenų prieigos parametrus.
  - Kibernetinio saugumo reikalavimus, įskaitant prieigos prie visų duomenų ir dalijimosi jais bei pranešimo apie incidentus ar pažeidimus per nustatytą laikotarpį reikalavimus.
  - Reikalavimus, taikomus pranešimams apie pažeidimą, turintį įtakos pagrindinės organizacijos duomenims.
  - Standartizuotą trečiosios šalies tapatybės patvirtinimo procesą, įskaitant visą juridinį pavadinimą, adresą, fizinę (-es) vietą (-as) ir interneto svetainę. Įprasta praktika yra naudoti kontrolinį sąrašą identifikavimo proceso metu ir peržiūrėti informacijos tikslumą.
  - Aiškiai apibrėžti paslaugų lygio susitarimai, kuriose nurodomi laukiami rezultatai ir kiekvienos šalies teisės, įsipareigojimai, nuobaudos, atlygis ir atsakomybė, įskaitant atsakomybę už darbo sąnaudų apmokėjimą (įskaitant subrangovus).
  - Nuostata dėl teisės atlikti auditą, apimanti tolesnius subrangovus, arba reikalavimas pateikti įrodymus, kad patikimas nepriklausomas užtikrinimo paslaugų teikėjas atliko šalių auditą. Nesant teisės atlikti auditą nuostatos, vidaus audito funkcijos gebėjimas gauti ar suteikti užtikrinimą gali būti ribotas.
- Pagrindinė organizacija turi prieigą prie nepriklausomų auditorių kontrolės vertinimo ataskaitų, pavyzdžiui, finansinių, atitikties ir duomenų saugumo ataskaitų, tokių kaip Tarptautiniai užtikrinimo užduočių standartai arba SOC ataskaitos.
  - Jei remiamasi trečiosios šalies išorės patikinimo paslaugų teikėjų darbu, dokumentai peržiūrimi siekiant užtikrinti patikimumą.
  - SOC ataskaitos naudojamos netinkamiems rizikos ir pokyčių valdymo procesams nustatyti.

- Politikos ir procedūros apima visus komponentus, būtinus konkrečioms organizacijoms arba sutarčių tipams:
  - Aplinkosaugos ir tvarumo sąlygos.
  - Pranešimų apie pažeidimus protokolai.
  - Veiklos rezultatų vertinimo reikalavimai.
  - Patikrintas trečiųjų šalių veiklos tęstinumo planas.
  - Dirbtinio intelekto naudojimas teikiant paslaugas.
  - Aiškus visų tolesnių subrangos darbų identifikavimas, atskleidimas, sąlygos ir apimtis.
  - Pakeitimų valdymo procesas, kuriame aprašoma, kaip sutarties galiojimo laikotarpiu tvarkytis su apimties, sąlygų ar veiklos reikalavimų pakeitimais (pvz., technologijų ar teisės aktų atnaujinimais).
  - Pakeitimų užsakymų arba sumų, kurias galima apmokestinti, skaičiaus apribojimas.
- Politikos ir procedūros reikalauja oficialaus galutinių produktų priėmimo prieš atliekant mokėjimą arba grąžinant bet kokį užstatą.
- Trečiosios šalys privalo pasidalyti savo etikos politika ar elgesio kodeksu ir (arba) laikytis pagrindinės organizacijos taisyklių.
- Jei sutartį pateikia trečioji šalis, pagrindinė organizacija yra atlikusi teisinę peržiūrą, o pagrindinės rizikos yra suprastos ir pagrįstos tinkama rizikos mažinimo strategija.

C. Galutinai suderintos sutartys ar susitarimai yra peržiūrimi ir patvirtinami atitinkamų suinteresuotųjų šalių, įskaitant asmenis atsakingus už teisę ir atitiktį, saugiai saugomi ir priskiriami už juos atsakingam sutarčių vadovui ar administratoriui.

- Sutartis ar kitas oficialus dokumentas, kuriuo patvirtinami užsakomųjų paslaugų santykiai ir trečiosios šalies įsipareigojimai, taip pat įrodymai apie bet kokias privalomas teisines ir atitikties peržiūras.

D. Yra tvarkomas tikslus, išsamus ir atnaujintas visų trečiųjų šalių santykių sąrašas, pavyzdžiui, centralizuotoje sutarčių valdymo sistemoje.

- Naujų trečiųjų šalių sutarčių ar susitarimų įtraukimo į sąrašą ar sistemą procesas.
- Galimų trečiųjų šalių įtraukimo į tiekėjų sistemą ir jų pašalinimo, jei sutartis nepatvirtinama, procesas.
- Trečiųjų šalių sutarčių ar susitarimų pašalinimo iš sąrašo ar sistemos procesas.
- Sekimo sistema, skirta dokumentuoti problemas, susijusias su konkrečiais rangovais ar tiekėjais, kad būtų galima jomis remtis ateityje.
- Peržiūros procesas, skirtas nustatyti, ar trečiųjų šalių duomenų visuma yra tiksli ir išsami.

E. Nustatomi ir vykdomi dokumentuoti integracijos procesai, kad trečiosios šalys galėtų įvykdyti sutarties ar susitarimo sąlygas. Peržiūros gali apimti patikrinimą, ar:

- Standartizuotos integracijos procedūros užtikrina, kad būtų parengti visi būtini dokumentai, atlikti mokymai ir atitikties patikrinimai.
- Trečiosios šalies sistemos ir procesai gali būti sklandžiai integruoti su pagrindinės organizacijos technologijomis.
- Bendrai naudojamos sistemos yra suderinamos ir saugios. Įrodymai gali apimti papildomas naudotojo subjekto kontrolės priemones, kurios yra SOC ataskaitų dalis.
- Pagrindinė organizacija įvertina trečiosios šalies veiklos tęstinumo planus, kuriais užtikrinama, kad paslaugos būtų teikiamos ir ekstremalių situacijų metu. Įtraukti nenumatytų atvejų planai, skirti galimiems sutrikimams šalinti.

F. Procesai, skirti nuolatinei tiekėjo veiklos, susijusios su sutarties ar susitarimo tikslais, stebėsenai, įskaitant pagrindinių veiklos rodiklių vertinimą.

- Stebėsenos procesai informuoja apie trečiosios šalies rizikos vertinimą, o nustatyti kontrolės trūkumai peržiūrimi, perduodami ir prireikus šalinami.
- Ataskaitos arba pastebėjimai apie procesus, technologijas ir priemones, sukurtas stebėsenai valdyti realiuoju laiku.
- Procesai, skirti užtikrinti, kad mokėjimai būtų atliekami pagal sutarties ar susitarimo sąlygas, pavyzdžiui, laikantis projekto terminų, etapų ir komunikacijos reikalavimų. Mokėjimai atliekami tik patvirtintiems rangovams, kurie yra užbaigę integracijos etapą ir buvo įtraukti į tiekėjų mokėjimo sistemą. Kai sutartyje nurodomi rezultatai, galutiniai mokėjimai atliekami tik tada, kai rezultatai patikrinami.
- Vykdoma stebėsena siekiant kontroliuoti su trečiųjų šalių susitarimais susijusias išlaidas, kad būtų užtikrinta vertė ir nustatyta investicijų grąža. Išlaidų ir naudos analizės rezultatai naudojami iš naujo derantis dėl sutarčių.
- Procesai, skirti baudoms už bet kokių paslaugų lygio susitarimų, numatytų sutartyje ar susitarime, nesilaikymą vertinti. Baudos apskaičiuojamos ir taikomos, joms atsiradus.
- Rizika pagrįstas prioritetinis trečiųjų šalių reitingavimas yra periodiškai pervertinamas, kai keičiasi sutartis ir kai artėja sutarties galiojimo pabaiga arba automatinis pratęsimas.
- Prioritetinių trečiųjų šalių peržiūros, pavyzdžiui vietoje arba kas ketvirtį atliekamos verslo peržiūros, siekiant patvirtinti kontrolės priemones ir veiklos vientisumą.
- Papildomos nuolatinės stebėsenos įrodymai gali būti šie:
  - Trečiosios šalies finansinio stabilumo analizė.
  - Skundų dėl trečiųjų šalių vertinimas.
  - Vadovybės atliekamos nepriklausomų auditorių ataskaitų, tokių kaip Tarptautinis užtikrinimo užduočių standartas, Atestavimo užduočių standartų pareiškimai, trečiųjų šalių teikiamų finansinių, audito, atitikties, ir duomenų saugumo ataskaitų peržiūros; ISO sertifikatai.
  - Vadovybės atliktos trečiosios šalies atliktų verslo atsparumo testų peržiūros, įskaitant visas nustatytas reikšmingas problemas.

- Subrangos arba tolesnių šalių pasitelkimo sąlygos ir apribojimai.
- Trečiųjų šalių etinių vertybių, kultūros ir elgesio vertinimas.
- Atsakymai į žiniasklaidos užklausas.
- Privatumo ir kibernetinio saugumo protokolų, skirtų apsaugoti pagrindinės organizacijos duomenų ir informacijos saugojimą ir perdavimą, įskaitant pažangių technologijų pavyzdžiui, dirbtinio intelekto naudojimą, vertinimas.
- Organizacijos galimybių nuolat gerinti veiklos rezultatus ir siekti sutarties ar susitarimo tikslų identifikavimas.
- Pareigų atskyrimo peržiūra.

G. Protokolai, skirti taisomiesiems veiksmams dėl nustatytų incidentų inicijuoti, kai trečioji šalis nesilaiko sutarties ar susitarimo reikalavimų arba jei trečiosios šalies veiksmai didina riziką pagrindinei organizacijai.

- Incidentų eskalavimo protokolai, pagrįsti incidento rimtumu ir trečiosios šalies prioritetu.
- Peržiūra po incidento, įskaitant pagrindinių priežasčių analizę.

H. Procesai, skirti įspėjimams apie artėjančią sutarčių ir susitarimų galiojimo pabaigą arba automatinį atnaujinimo teikti. Automatinio atnaujinimo procesai apima peržiūrą:

- Trečiosios šalies veiklos rezultatai.
- Sutarties ar susitarimo sąlygos ir visi priedai.
- Rizikos veiksniai.

I. Įdiegiamas ir vykdomas formalus sutarties nutraukimo planas, siekiant užtikrinti, kad būtų tinkamai įvykdytos sutarties sąlygos, susijusius su terminais ir lūkesčiais, įskaitant visus tolesnius subrangovus.

- Kontroliniai sąrašai arba pokalbiai su pagrindiniais suinteresuotaisiais subjektais, siekiant užtikrinti saugumo priemonių veiksmingumą.
- Trečiosios šalies saugoma organizacinė informacija ar duomenys buvo grąžinti arba sunaikinti.
- Trečiosios šalies prieiga prie organizacijos duomenų, sistemų ar įrenginių buvo panaikinta.
- Buvo grąžintas pagrindinės organizacijos turtas, pavyzdžiui, įrenginiai, programinės įrangos licencijos, intelektinė nuosavybė ir dokumentai.
- Kai trečioji šalis nutraukia sutartį dėl pagrįstos priežasties, nustatomos lengvinančios aplinkybės arba rizika ir apie tai pranešama vyresniajai vadovybei ir (arba) valdybai.
- Nutraukus sutartį su prioritetine trečiąja šalimi, ji pakeičiama remiantis tuo pačiu rizikos vertinimu, išskyrus atvejus, kai sutartis baigta vykdyti arba nebereikalinga.

A priedas. Praktinio taikymo pavyzdžiai

Toliau pateiktuose pavyzdžiuose aprašyti scenarijai, kai būtų taikomas trečiosios šalies Teminis reikalavimas:

1 pavyzdys: Vidaus audito plane numatyta vidaus audito užduotis apima paslaugą ar rezultatą, kurį šiuo metu teikia trečioji šalis.

Kai vidaus audito funkcija užbaigia rizika pagrįstą planavimo procesą ir į vidaus audito planą įtraukia vieną ar daugiau užduočių, susijusių su paslaugomis ar rezultatais, kuriuos šiuo metu pagal sutartį ar susitarimą teikia trečiosios šalys, yra privaloma laikytis Teminio reikalavimo.

Ne kiekviena Teminio reikalavimo nuostata gali būti taikoma kiekvienai užduočiai. Kai vidaus auditoriai, vadovaudamiesi profesiniu sprendimu, nustato, kad viena ar daugiau Trečiosios šalies Teminio reikalavimo nuostatos nėra taikomos ir todėl neturėtų būti įtrauktos į užduotį, vidaus auditoriai turi dokumentuoti ir išsaugoti šių nuostatų neįtraukimo pagrindimą. Pavyzdžiui, tam tikrų nuostatų neįtraukimas gali būti pagrįstas tuo, kad vidaus audito funkcija nustatė, jog organizacijos priklausomybė nuo trečiųjų šalių teikiant kritines paslaugas yra nedidelė arba tai yra nusistovėję santykiai, turintys nedidelį finansinį poveikį.

2 pavyzdys: Trečiųjų šalių rizika nustatoma atliekant užtikrinimo užduotį kita tema nei trečiosios šalys ar sutarčių valdymas.

Vidaus auditoriai gali nustatyti reikšmingą trečiųjų šalių riziką vertindami procesą, kuris iš pradžių nebuvo nustatytas kaip susijęs su trečiosiomis šalimis ar sutarčių valdymu. Pavyzdžiui, planuodami duomenų saugojimo vertinimo užduotį, vidaus auditoriai sužino, kad debesijos paslaugas teikia trečioji šalis. Per pokalbius su trečiosios šalies teikiamų paslaugų vadovybe vidaus auditoriai nustato su trečiąja šalimi susijusią kibernetinio saugumo riziką.

Nustačius atitinkamas rizikas, vidaus auditoriai turi peržiūrėti Trečiosios šalies ir Kibernetinio saugumo Teminius reikalavimus ir nustatyti, kurie reikalavimai taikytini. Auditoriai gali neįtraukti trečiosios šalies valdysenos proceso arba trečiosios šalies rizikos valdymo proceso į užduoties apimtį ir sutelkti dėmesį į audituojamų paslaugų trečiosios šalies kontrolę. Tas pats profesinis sprendimas taikomas ir taikant kibernetinio saugumo teminį reikalavimą. Auditoriai privalo į užduoties darbo dokumentus įtraukti pagrindimą, kodėl nebuvo taikomos Trečiosios šalies arba Kibernetinio saugumo teminių reikalavimų nuostatos, ir išsaugoti šią dokumentaciją.

3 pavyzdys: Reikalingas trečiosios šalies įtraukimas, kuris iš pradžių nebuvo įtrauktas į vidaus audito planą.

Organizacijoje iškyla problema, susijusi su prioritetine trečiąja šalimi, kuri nedelsiant reikalauja vidaus audito funkcijos dėmesio. Problema buvo susijusi su kontrolės nesuveikimu. Vidaus audito vadovas turėtų bendrauti su valdyba dėl vidaus audito funkcijos audito plano ir išteklių prioritetų perskirstymo, kad būtų patenkintas poreikis. Auditorius turėtų bendradarbiauti su poveikį patyrusia vadovybe ir parengti užduoties tikslus, kad įvertintų situaciją ir pateiktų rekomendacijas, kaip užkirsti kelią to kiems atvejams ateityje. Vidaus audito vadovas turėtų peržiūrėti Teminį reikalavimą, kad apibrėžtų užduoties apimtį, nustatytų, kurie reikalavimai taikomi, ir atitinkamai dokumentuotų visas išimtis.

B priedas. Papildoma dokumentavimo priemonė

Tikimasi, kad vidaus auditoriai vadovausis profesiniu sprendimu, nustatydami reikalavimų taikymą, pagrįstą rizikos vertinimu, ir tinkamai dokumentuos tam tikrų reikalavimų išimtis. Teminis reikalavimas gali būti dokumentuojamas vidaus audito plane arba užduoties darbo dokumentuose, remiantis auditoriaus profesiniu sprendimu. Viena ar kelios vidaus audito užduotys gali apimti reikalavimus. Be to, ne visi reikalavimai gali būti taikomi. Žemiau pateikiama spausdinama forma, kaip vienas iš būdų dokumentuoti atitiktį Trečiosios šalies Teminiam reikalavimui, tačiau jos naudojimas nėra privalomas.

Trečiosios šalies valdysena

Reikalavimas	Įvykdyta apimtis arba pašalinimo pagrindimas	Dokumentacijos nuoroda
A. Nustatomas, įgyvendinamas ir periodiškai peržiūrimas oficialus metodas, pagal kurį sprendžiama, ar sudaryti sutartį su trečiąja šalimi. Šis metodas apima tinkamus kriterijus, skirtus apibrėžti ir įvertinti išteklius, būtinus ir prieinamus tikslams pasiekti, teikiant produktą ar paslaugą.		
B. Nustatomos politikos ir procedūros, skirtos apibrėžti, įvertinti ir valdyti santykius bei riziką su trečiosiomis šalimis per visą trečiosios šalies gyvavimo ciklą. Politikos ir procedūros yra suderintos su taikomais teisės aktų reikalavimais ir periodiškai peržiūrimos bei atnaujinamos siekiant sustiprinti kontrolės aplinką.		
C. Apibrėžti organizacijos trečiųjų šalių valdymo vaidmenis ir atsakomybes, išsamiai nurodant, kas atrenka, vadovauja, valdo, bendrauja su trečiosiomis šalimis ir jas stebi, ir kas turi būti informuojamas apie trečiųjų šalių veiklą. Egzistuoja procesas, užtikrinantis, kad asmenys, kuriems priskirti trečiųjų šalių vaidmenys ir atsakomybės, turėtų atitinkamas kompetencijas.		

Reikalavimas	Įvykdyta apimtis arba pašalinimo pagrindimas	Dokumentacijos nuoroda
D. Nustatyti bendravimo su atitinkamomis suinteresuotosiomis šalimis protokolai, į kuriuos įtrauktos savalaikės ataskaitos apie prioritetinių trečiųjų šalių veiklos, rizikos ir atitikties (ypač įstatymų ir kitų teisės aktų pažeidimų) būklę. Trečiosios šalys prioritetizuojamos atsižvelgiant į riziką. Atitinkamos suinteresuotosios šalys gali būti valdyba, vyresnioji vadovybė, pirkimų, operacijų, rizikos valdymo, atitikties, teisės, informacinių technologijų, informacinės saugos, žmogiškųjų išteklių ir kitų sričių specialistai.		

Trečiųjų šalių rizikos valdymas

Reikalavimas	Įvykdyta apimtis arba pašalinimo pagrindimas	Dokumentacijos nuoroda
A. Trečiųjų šalių ir jų teikiamų paslaugų rizikos valdymo procesai yra standartizuoti ir išsamūs, apima apibrėžtus vaidmenis ir atsakomybę ir pakankamai atsižvelgia į pagrindines organizacijai aktualias rizikas (pavyzdžiui, strateginę, reputacinę, etinę, operacinę, finansinę, atitikties, kibernetinio saugumo, informacinių technologijų, teisinę, tvarumo ir geopolitinę). Stebima, kaip laikomasi procesų, o esant nukrypimams įgyvendinami korekciniai veiksmai.		
B. Su trečiosiomis šalimis susijusios rizikos per visą gyvavimo ciklą yra nustatomos ir reguliariai vertinamos. Rizikos vertinimas naudojamas trečiųjų šalių, įskaitant ir tolesnius subrangovus, reitingavimui ir prioritetizavimui. Reagavimo į riziką būdai yra taip pat reitinguojami ir nustatomi jų prioritetai. Rizikos vertinimas periodiškai peržiūrimas ir atnaujinamas.		

Reikalavimas	Įvykdyta apimtis arba pašalinimo pagrindimas	Dokumentacijos nuoroda
C. Atsakymai į riziką yra tinkami ir tikslūs, atitinkantys reitingą. Atsakymai į riziką įgyvendinami, peržiūrimi, patvirtinami, stebimi, vertinami ir prireikus koreguojami.		
D. Yra įdiegti procesai, skirti valdyti ir, jei reikia, eskaluoti problemas, kylančias iš trečiųjų šalių, užtikrinant atsakomybę už rezultatus ir didinant sutarčių ar kitų susitarimų sąlygų įvykdymo tikimybę. Jei trečioji šalis nereaguoja į eskaluojamus susirūpinimus, taikomi procesai, skirti vadovybei įvertinti turimų verslo santykių riziką ir imtis tolesnių veiksmų, korekcinių priemonių arba nutraukti santykius, jei tai yra pagrįsta.		

Trečiųjų šalių kontrolė

Reikalavimas	Įvykdytas apimtis arba pašalinimo pagrindimas	Dokumentacijos nuoroda
A. Taikomas patikimas išsamaus patikrinimo procesas trečiųjų šalių paieškai ir atrankai, kartu su dokumentuotu ir patvirtintu verslo pagrindimu ar kita atitinkama dokumentacija, apibūdinančia ir pagrindžiančia poreikį bei santykių su trečiąja šalimi pobūdį.		
B. Sutarčių sudarymas ir tvirtinimas atliekami pagal organizacijos trečiųjų šalių rizikos valdymo politikas ir procedūras, įskaitant bendradarbiavimą tarp atitinkamų organizacijos padalinių.		
C. Galutines sutartis ar susitarimus peržiūri ir patvirtina visos susijusios suinteresuotosios šalys, įskaitant atsakingus už teisę ir atitiktį, pasirašo abiejų šalių įgalioti asmenys ir jie saugiai saugomi. Už kiekvieną sutartį yra atsakingas sutarties vadovas arba administratorius.		

Reikalavimas	Įvykdytas apimtis arba pašalinimo pagrindimas	Dokumentacijos nuoroda
D. Palaikomas tikslus, išsamus ir aktualus visų santykių su trečiosiomis šalimis sąrašas, pavyzdžiui, centralizuotoje sutarčių valdymo sistemoje.		
E. Nustatomi ir vykdomi dokumentuoti integracijos procesai, skirti sudaryti sąlygas trečiosioms šalims įvykdyti sutarties ar susitarimo sąlygas.		
F. Vykdomi nuolatinės stebėsenos procesai, kuriais siekiama įvertinti, ar trečiosios šalys per visą gyvavimo ciklą vykdo sutarties ar susitarimo sąlygas ir ar trečiosios šalys vykdo savo sutartinius įsipareigojimus. Šie procesai apima pateiktos informacijos patikimumo tikrinimą ir periodinį veiklos rezultatų pervertinimą bei pervertinimą kaskart pasikeitus susitarimui.		
G. Nustatyti protokolai, pagal kuriuos inicijuojami korekciniai veiksmai, jei trečioji šalis nepateisina lūkesčių arba kelia padidintą ar netikėtą riziką. Protokolai apima incidentų eskalavimą pagal jų sunkumą, peržiūrų po incidentų atlikimą ir pagrindinių incidentų priežasčių analizę.		
H. Stebimos sutarčių galiojimo ir atnaujinimo datos, ir prireikus imamasi atnaujinimo veiksmų.		
I. Įdiegiamas ir vykdomas formalus sutarties nutraukimo planas, siekiant užtikrinti, kad sutarties reikalavimai, susiję su terminais ir lūkesčiais, būtų tinkamai įvykdyti. Procesai apima, kaip: • Nutraukti trečiosios šalies veiklą. • Esant poreikiui, pakeisti trečiąją šalį. • Perskirstyti saugojimą ir grąžinti arba sunaikinti organizacijos jautrius duomenis, saugomus trečiosios šalies. • Panaikinti trečiosios šalies prieigą prie sistemų, įrankių ir įrenginių.		

Apie Vidaus auditorių institutą

Vidaus auditorių institutas (VAI) yra tarptautinė profesinė asociacija, vienijanti daugiau nei 265 000 narių visame pasaulyje ir suteikusi daugiau nei 200 000 sertifikuotų vidaus auditorių (CIA®) sertifikatų visame pasaulyje. Įkurtas 1941 m., VAI (IIA) visame pasaulyje pripažįstamas kaip vidaus audito profesijos lyderis standartų, sertifikavimo, švietimo, mokslinių tyrimų ir techninių rekomendacijų srityje. Daugiau informacijos rasite svetainėje theiia.org.

Atsakomybės apribojimas

VAI (IIA) šį dokumentą skelbia informaciniais ir švietimo tikslais. Šioje medžiagoje nesiekiama pateikti galutinių atsakymų konkrečiomis individualiomis aplinkybėmis, todėl ja galima naudotis tik kaip vadovu. VAI (IIA) rekomenduoja kreiptis į nepriklausomus ekspertus dėl konsultacijų, tiesiogiai susijusių su konkrečia situacija. VAI (IIA) neprisiima jokios atsakomybės už asmenis, kurie pasikliauja tik šia medžiaga.

Autorinės teisės

2025 m. rugsėjis

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