

Kolmannet osapuolet

Aihekohtainen vaatimus

Topical Requirement



The Institute of
Internal Auditors

Kolmannet osapuolet Aihekohtainen vaatimus

Sisäisen tarkastuksen ammatillinen viitekehys (International Professional Practices Framework® - IPPF) koostuu Kansainvälisistä sisäisen tarkastuksen standardeista™ (Global Internal Audit Standards™), Aihekohtaisista vaatimuksista ja Kansainvälisistä ohjeista. Aihekohtaiset vaatimukset ovat pakollisia, ja niitä on käytettävä yhdessä Standardien kanssa, jotka määrittävät perustan vaadituille käytännöille.

Aihekohtaiset vaatimukset määrittävät sisäisille tarkastajille minimitason tiettyjen riskiaiheiden tarkastamiselle. Organisaation riskiprofiili voi edellyttää, että sisäiset tarkastajat tarkastelevat myös aiheeseen liittyviä muita näkökohtia.

Aihekohtaisten vaatimusten noudattaminen lisää sisäisen tarkastuksen palvelujen johdonmukaisuutta ja parantaa sisäisen tarkastuksen palvelujen ja tulosten laatua ja luotettavuutta. Ennen kaikkea aihekohtaiset vaatimukset vahvistavat sisäisen tarkastuksen ammattikuntaa.

Sisäisten tarkastajien täytyy soveltaa aihekohtaisia vaatimuksia Kansainvälisten sisäisen tarkastuksen standardien mukaisesti. Aihekohtaisten vaatimusten noudattaminen on pakollista varmennuspalvelujen osalta ja suositeltavaa neuvonantopalvelujen osalta. Aihekohtaista vaatimusta sovelletaan seuraavasti:

1. Aihe sisältyy sisäisen tarkastuksen suunnitelmaan kuuluvaan toimeksiantoon.
2. Aihe tunnistetaan toimeksiantoa toteutettaessa.
3. Aihe sisältyy erikseen pyydettyyn toimeksiantoon, joka ei kuulu alkuperäiseen sisäisen tarkastuksen suunnitelmaan.

Aihekohtaiseen vaatimukseen sisältyvien vaatimusten soveltuvuus on arvioitava, tämä arviointi on dokumentoitava ja säilytettävä. Kaikki yksittäiset vaatimukset eivät välttämättä sovellu jokaiseen toimeksiantoon; jos vaatimuksia ei sovelleta, perustelut on dokumentoitava ja säilytettävä. Aihekohtaisten vaatimusten noudattaminen on pakollista, ja sitä arvioidaan laadunarvioinneissa.

Kolmannet osapuolet

Kolmas osapuoli on ulkopuolinen henkilö, ryhmä tai yhteisö, johon organisaatio ("ensisijainen organisaatio") on liikesuhteessa ja jolta organisaatio hankkii tuotteita tai palveluja. Liikesuhde voidaan vahvistaa sopimuksella tai muulla tavoin. Tässä Aihekohtaisessa vaatimuksessa termillä "kolmas osapuoli" tarkoitetaan myyjiä, toimittajia, urakoitsijoita, alihankkijoita, ulkoisia palveluntarjoajia, muita toimijoita ja konsultteja. Termi kattaa kolmannen osapuolen ja sen alihankkijoiden väliset sopimukset.



Aihekohtaista vaatimusta sovelletaan, kun sisäinen tarkastus tekee varmennustoimeksiantoja kolmansiin osapuoliin ja/tai muihin alihankintasuhteisiin, jotka sallitaan kolmannen osapuolen sopimuksessa ensisijaisen organisaation kanssa. Sisäisten tarkastajien tulisi priorisoida kolmannet osapuolet ja muut alihankkijat riskiarvion perusteella, kuten jäljempänä riskienhallintaa koskevassa osiossa kuvataan. Sisäisten tarkastajien täytyy soveltaa kaikkia vaatimuksia riskiarvioinnin mukaisesti. Poikkeukset on dokumentoitava.

Tämä Aihekohtainen vaatimus ei kohdistu ensisijaisen organisaation epäsuoriin ulkoisiin suhteisiin, intresseihin tai toimiin, kuten sääntelyviranomaisiin, asiamiehiin, edunvalvojiin/hallituksen jäseniin, tai sisäisiin suhteisiin, kuten työntekijöihin.

Termi "kolmas osapuoli" voidaan määritellä ja käyttää eri tavoin toimialakohtaisesti tai asiayhteyden mukaan. Sisäisten tarkastajien tulisi käyttää ammatillista harkintaansa soveltaessaan Aihekohtaista vaatimusta ensisijaisen organisaation määritelmään kolmansista osapuolista.

Ensisijainen organisaatio (kolmannen osapuolen kanssa sopimuksen tekävä organisaatio) säilyttää vastuun tavoitteidensa saavuttamiseen liittyvistä riskeistä, vaikka se käyttäisi kolmatta osapuolta auttamaan sitä yhden tai useamman tavoitteen saavuttamisessa. Työskentely kolmansien osapuolten kanssa tuo mukanaan riskejä, jotka on tunnistettava, arvioitava ja hallittava asianmukaisilla hallinnointi-, riskienhallinta- ja valvontaprosesseilla, kuten tässä Aihekohtaisessa vaatimuksessa esitetään. Jos kolmas osapuoli ei toimi sopimuksen mukaisesti, toimii epäeettisellä tavalla tai sen liiketoiminta häiriintyy, ensisijaiseen organisaatioon voi kohdistua seuraamuksia. Kolmansiin osapuoliin liittyviä riskikategorioita ja esimerkkejä riskeistä ovat:

- Strategiset riskit, esimerkiksi kyky toteuttaa ensisijaisen organisaation missiota ja/tai saavuttaa ylätasoa tavoitteita tai hallita fuusioiden ja yritysostojen vaikutuksia.
- Maineeseen liittyvät riskit, esimerkiksi ympäristölle tai ensisijaisen organisaation asiakas- ja sidosryhmäsuhteille sekä luottamukselle aiheutuneet vahingot.
- Eettiset riskit, esimerkiksi integriteetin puute, eturistiriidat, lahjukset ja korruptio.
- Operatiiviset riskit, esimerkiksi fyysiseen turvallisuuteen ja tietoturvaan liittyvät riskit, sisäpiiririskit, palveluhäiriöt ja riski, että tavoitteita ei saavuteta.
- Taloudelliset riskit, esimerkiksi kolmannen osapuolen maksukyvyttömyys ja väärinkäytökset.
- Sovellettavien paikallisten, kansallisten ja kansainvälisten sääntelyvaatimusten noudattamiseen liittyvät riskit.
- Kyberturvallisuus- ja tietosuojariskit, esimerkiksi arkaluonteisten tietojen vaarantuminen ja vuotaminen.
- Tietotekniikkariskit, esimerkiksi kriittisiä toimintoja tukevien palvelujen puute.
- Oikeudelliset riskit, esimerkiksi eturistiriidat, riita-asiat ja sopimusrikkomuksiin liittyvät oikeudenkäynnit.
- Vastuullisuusriskit, sisältäen ympäristö-, sosiaaliset ja hallinnolliset riskit. Esimerkkeinä voidaan mainita riskit, jotka liittyvät organisaation ympäristövaikutuksiin ja organisaation vuorovaikutukseen yhteisöjen kanssa.



- Geopoliittiset riskit, kuten kauppakiistat/pakotteet ja poliittinen epävakaus.

Kolmannen osapuolen elinkaari koostuu valinnasta, sopimuksen tekemisestä, perehdytyksestä, monitoroinnista ja liikesuhteen päättämisestä. Sisäisten tarkastajien tulisi ottaa nämä vaiheet huomioon arvioidessaan hallinnointi-, riskienhallinta- ja valvontaprosesseja (kontrolliprosesseja) koskevia vaatimuksia.



Kolmannen osapuolen hallinnointi-, riskienhallinta- ja valvontaprosessien arviointi.

Tämä Aihekohtainen vaatimus antaa johdonmukaisen ja kattavan lähestymistavan kolmansien osapuolten hallinnointi-, riskienhallinta- ja valvontaprosessien suunnittelun ja toteutuksen arviointiin. Vaatimukset määrittävät arvioinnin minimitason.

HALLINTO

Vaatimukset:

Sisäisten tarkastajien tulee arvioida seuraavia asioita, jotka liittyvät ensisijaisen organisaation kolmansien osapuolten hallinnointiin, sisältäen hallituksen valvonnan:

- A. Kolmansien osapuolten kanssa on määritetty virallinen toimintatapa sen selvittämiseksi, ryhdytäänkö liikesuhteeseen. Määritettyä toimintatapaa noudatetaan ja se käydään läpi säännöllisesti. Toimintatapa sisältää asianmukaiset kriteerit, joilla määritetään ja arvioidaan tarvittavat ja käytettävissä olevat resurssit, jotta tavoitteet voidaan saavuttaa kolmannen osapuolen tarjoamalla tuotteella tai palvelulla.
- B. Kolmansien osapuolten kanssa solmittavien liikesuhteiden ja riskien määrittelemiseksi, arvioimiseksi ja hallinnoimiseksi laaditaan toimintaperiaatteet ja menettelytavat koko liikesuhteen elinkaaren ajaksi. Toimintaperiaatteet ja menettelytavat ovat yhdenmukaiset sovellettavien sääntelyvaatimusten kanssa, ja niitä tarkistetaan ja päivitetään säännöllisesti valvonta(kontrolli)ympäristön vahvistamiseksi.
- C. Organisaation kolmansien osapuolten hallinnointitehtävät ja -vastuut on määritetty, ja niissä määritetään yksityiskohtaisesti, kuka valitsee, ohjaa, hallinnoi, valvoo ja pitää yhteyttä kolmansien osapuolten kanssa, sekä kenen on saatava tietoa kolmansiin osapuoliin liittyvästä toiminnasta. On olemassa prosessi, jolla varmistetaan, että kolmansiin osapuoliin liittyviin tehtäviin ja vastuisiin nimetyillä henkilöillä on asianmukainen pätevyys.
- D. Relevanttien sidosryhmien kanssa käytävää yhteydenpitoa varten on määritetty menettelytavat, joihin sisältyy oikea-aikainen raportointi priorisoitujen kolmansien osapuolten suoriutumisesta, riskeistä ja vaatimusten noudattamisesta (erityisesti liittyen lakien ja asetusten rikkomiseen). Kolmannet osapuolet priorisoidaan riskiperusteisesti. Relevantteja sidosryhmiä voivat olla muun muassa hallitus, ylin johto, hankintatoimi, liiketoiminnot, riskienhallinta, compliance -toiminto, lakiosasto, tietohallinto, henkilöstöhallinto ja muut.

RISKIENHALLINTA

Vaatimukset:

Sisäisten tarkastajien on arvioitava seuraavia organisaation kolmansien osapuolten riskienhallintaan liittyviä asioita.

- A. Kolmansiin osapuoliin ja niiden palveluihin liittyvät riskienhallintaprosessit ovat standardoituja ja kattavia, ne sisältävät määritellyt roolit ja vastuualueet ja käsittelevät riittävästi organisaation kannalta keskeisiä riskejä (esimerkiksi strategiset, maine-,



eettiset, operatiiviset, taloudelliset, compliance-, kyberturvallisuus-, tietotekniikka-, oikeudelliset, vastuullisuus- ja geopolittiset riskit). Prosessien noudattamista monitoroidaan ja tarvittavat korjaavat toimenpiteet toteutetaan.

- B. Kolmansiin osapuoliin liittyvät riskit tunnistetaan ja arvioidaan säännöllisesti koko liikesuhteen elinkaaren ajan. Riskiarviota käytetään luokittelemaan ja priorisoimaan kolmansia osapuolia, mukaan lukien toimitusketjussa alempana olevat osapuolet. Myös riskienhallintatoimenpiteet luokitellaan ja priorisoidaan. Riskiarviota käydään läpi ja päivitetään säännöllisesti.
- C. Riskienhallintatoimenpiteet ovat riittäviä ja täsmällisiä, ja ne ovat oikeassa suhteessa riskiluokitukseen. Riskienhallintatoimenpiteitä toteutetaan, käydään läpi, hyväksytään, monitoroidaan, arvioidaan ja mukautetaan tarvittaessa.
- D. On olemassa prosessit, joilla hallitaan ja tarvittaessa eskaloidaan kolmansiin osapuoliin liittyviä ongelmia. Näillä prosesseilla varmistetaan vastuu tuloksista ja lisätään todennäköisyyttä saavuttaa sopimusten ehdot. Jos kolmas osapuoli ei reagoi eskaloituihin huolenaiheisiin, johdolla on käytössään prosessit, joiden avulla se voi arvioida liikesuhteen riskejä ja tehdä tarvittaessa lisätoimia, korjaavia toimenpiteitä tai päättää sopimus.

VALVONTATOIMENPITEET (KONTROLLIT)

Vaatimukset:

Sisäisten tarkastajien täytyy arvioida seuraavat kolmansien osapuolten valvontatoimenpiteet, jotka on priorisoitu riskiperusteisesti. Arvioinnin täytyy sisältää johdon prosessit organisaation kolmansien osapuolten jatkuvaa arviointia ja monitorointia varten.

- A. Hankintaa ja kolmansien osapuolten valintaa varten on olemassa vahva due diligence -prosessi, johon liittyy dokumentoitu ja hyväksytty liiketoiminnallinen peruste tai muu relevantti asiakirja, jossa perustellaan liikesuhteen tarve kolmanteen osapuoleen ja kuvataan liikesuhteen luonne.
- B. Sopimukset laaditaan ja hyväksytetään organisaation kolmansia osapuolia koskevien riskienhallintaperiaatteiden ja -menettelytapojen mukaisesti, ja tässä prosessissa tehdään yhteistyötä organisaation asiaankuuluvien tahojen välillä.
- C. Kaikki relevantit sidosryhmät, mukaan lukien lakiosasto ja compliance -toiminto, tarkastavat ja hyväksyvät lopulliset sopimukset. Molempien osapuolten valtuutetut henkilöt allekirjoittavat sopimukset, ja ne tallennetaan turvallisesti. Kullekin sopimukselle nimetään sopimuksen valvoja tai hallinnoija.
- D. Kaikista kolmansista osapuolista ylläpidetään tarkkaa, täydellistä ja ajantasaista luetteloa esimerkiksi keskitetyssä sopimustenhallintajärjestelmässä.
- E. Kolmansille osapuolille on laadittu perehdytysprosessit ja niitä noudatetaan. Tämä luo pohjan sille, että kolmannet osapuolet voivat täyttää sopimuksen ehdot.
- F. On olemassa jatkuva monitorointiprosessi, jonka avulla arvioidaan, toimivatko kolmannet osapuolet sopimuksen ehtojen mukaisesti koko liikesuhteen elinkaaren ajan ja täyttävätkö ne sopimusvelvoitteensa. Prosessi sisältää saadun tiedon luotettavuuden varmistamisen sekä suorituksen arvioinnin säännöllisesti ja aina kun sopimus muuttuu.
- G. Jos kolmas osapuoli ei täytä odotuksia tai aiheuttaa kohonneen tai odottamattoman riskin, menettelyt korjaavien toimenpiteiden käynnistämiseksi on määritetty.



Menettelyihin kuuluvat poikkeamien eskalointi niiden vakavuuden perusteella, jälkiseuranta ja juurisyiden analysointi.

- H. Sopimusten voimassaolon päättymis- ja uusimispäivämääriä seurataan, ja sopimukset uusitaan tarvittaessa.
- I. Liikesuhteen päättämiselle on laadittu muodollinen suunnitelma, jota noudatetaan, jotta sopimuksen aikatauluja ja odotuksia koskevat vaatimukset tulevat asianmukaisesti huomioiduiksi. Suunnitelma sisältää muun muassa seuraavat ohjeet:
 - Kolmannen osapuolen liikesuhteen päättäminen.
 - Kolmannen osapuolen korvaaminen tarvittaessa.
 - Kolmannen osapuolen tallentamien organisaation arkaluonteisten tietojen hallinnan siirto ja palautus tai tuhoaminen.
 - Kolmannen osapuolen pääsyn estäminen järjestelmiin, työkaluihin ja tiloihin.

Sisäisten tarkastajien instituutti

IIA on kansainvälinen ammattijärjestö, joka palvelee yli 265 000 jäsentä maailmanlaajuisesti ja on myöntänyt yli 200 000 Certified Internal Auditor® (CIA®) -sertifikaattia maailmanlaajuisesti. Vuonna 1941 perustettu IIA tunnustetaan kaikkialla maailmassa sisäisen tarkastuksen alan johtavaksi standardien, sertifiointien, koulutuksen, tutkimuksen ja teknisen ohjauksen järjestäjäksi. Lisätietoja on osoitteessa theiia.org.

Tekijänoikeus

© 2025 The Institute of Internal Auditors, Inc. Kaikki oikeudet pidätetään. Lupaa jäljentämiseen voi pyytää osoitteesta copyright@theiia.org.

Syyskuu 2025



The Institute of
Internal Auditors

Kansainvälinen päämaja

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

