

Kolmannet osapuolet

Aihekohtainen vaatimus

Topical Requirement

Käyttöopas



The Institute of
Internal Auditors

Sisältö

Johdanto aihekohtaisiin vaatimuksiin	2
Sovellettavuus, riski ja ammatillinen harkinta.....	2
Huomioon otettavaa	8
Hallinnossa huomioon otettavaa.....	8
Riskienhallinnassa huomioon otettavaa	9
Valvonnassa(kontrolleissa) huomioon otettavaa.....	11
Liite A. Käytännön soveltamisesimerkkejä.....	17
Liite B. Valinnainen dokumentointityökalu	19
Kolmansien osapuolten hallinnointi.....	19
Kolmansien osapuolten riskienhallinta	21
Kolmansien osapuolten valvonta.....	22

Johdanto aihekohtaisiin vaatimuksiin

Aihekohtaiset vaatimukset ovat olennainen osa Sisäisen tarkastuksen ammatillista viitekehystä (International Professional Practices Framework IPPF®) Kansainvälisten sisäisen tarkastuksen standardien ja Kansainvälisten ohjeiden kanssa. The Institute of Internal Auditors (IIA) edellyttää, että aihekohtaisia vaatimuksia käytetään yhdessä standardien kanssa, jotka määrittävät perustan vaadituille käytännöille. Tässä oppaassa on viittauksia standardeihin, joissa on yksityiskohtaisempia tietoja.

Aihekohtaiset vaatimukset määrittävät, miten sisäisten tarkastajien tulee käsitellä keskeisiä riskialueita. Tämä tukee sisäisen tarkastuksen laatua ja johdonmukaisuutta. Aihekohtaiset vaatimukset määrittävät perustason ja antavat relevantit kriteerit niihin liittyvien varmennuspalvelujen tekemiselle (Standardi 13.4 Arviointikriteerit). Aihekohtaisten vaatimusten noudattaminen on pakollista varmennuspalveluissa ja suositeltavaa neuvonantopalveluissa. Aihekohtaisten vaatimusten ei ole tarkoitus kattaa kaikkia mahdollisia näkökohtia, jotka tulisi ottaa huomioon varmennustoimeksiantoja toteutettaessa, vaan niiden tarkoituksena on pikemminkin määrittää minimivaatimukset, joiden avulla voidaan tehdä johdonmukainen ja luotettava arviointi kyseisestä aiheesta.

Aihekohtaiset vaatimukset liittyvät selkeästi IIA:n Kolmen linjan malliin ja Kansainvälisiin sisäisen tarkastuksen standardeihin. Hallinto-, riskienhallinta- ja valvontaprosessit ovat aihekohtaisten vaatimusten pääkomponentteja, jotka ovat yhdenmukaiset standardin 9.1 ”Hallinto-, riskienhallinta- ja valvontaprosessien ymmärtäminen” kanssa. Kolmen linjan mallin mukaan hallinto liittyy hallitukseen/hallintoelimeen, riskienhallinta liittyy toiseen linjaan ja valvontatoimenpiteet (kontrollit) tai -prosessit ensimmäiseen linjaan. Johto on edustettuna sekä ensimmäisessä että toisessa linjassa, ja sisäinen tarkastus on kuvattu kolmannessa linjassa riippumattomana ja objektiivisena varmennuksen antajana, joka raportoi hallitukselle/hallintoelimelle (Periaate 8 Hallituksen valvonta).

Sovellettavuus, riski ja ammatillinen harkinta

Aihekohtaisia vaatimuksia täytyy noudattaa silloin, kun sisäinen tarkastus tekee varmennustoimeksiantoja aiheista, joista on olemassa aihekohtainen vaatimus, tai kun muissa varmennustoimeksiannoissa tunnistetaan aihekohtaiseen vaatimukseen liittyviä näkökohtia.

Kuten standardeissa kuvataan, riskien arviointi on tärkeä osa sisäisen tarkastuksen johtajan suunnittelua. Sisäisen tarkastuksen suunnitelmaan sisällytettävien varmennustoimeksiantojen määrittäminen edellyttää organisaation strategioiden, tavoitteiden ja riskien arviointia vähintään vuosittain (Standardi 9.4 Sisäisen tarkastuksen suunnitelma). Suunnitellessaan yksittäisiä varmennustoimeksiantoja sisäisen tarkastuksen on arvioitava toimeksiantoon liittyvät riskit (Standardi 13.2 Toimeksiannon riskiarvio).

Kun aihekohtaisen vaatimuksen aihe tunnistetaan riskiperusteisen sisäisen tarkastuksen suunnitteluprosessin aikana ja se sisällytetään tarkastussuunnitelmaan, aihekohtaisessa vaatimuksessa esitetyt vaatimuksia on käytettävä tähän soveltuvien toimeksiantojen yhteydessä. Lisäksi, kun sisäiset tarkastajat toteuttavat toimeksiannon (joko suunnitelmaan kuuluvan tai siihen kuulumattoman) ja siihen tunnistetaan liittyvän aihekohtaisia vaatimuksia, aihekohtaisen vaatimuksen soveltuvuus on arvioitava osana toimeksiantoa. Mikäli pyydetään toimeksiantoa, joka ei alun perin sisältynyt suunnitelmaan ja joka sisältää aihekohtaiseen vaatimukseen liittyviä aiheita, aihekohtaisen vaatimuksen soveltuvuus on arvioitava.

Ammatillisella harkinnalla on keskeinen rooli aihekohtaista vaatimusta sovellettaessa. Riskiarviot ohjaavat sisäisen tarkastuksen johtajien päätöksiä siitä, mitkä toimeksiannot sisällytetään sisäisen tarkastuksen suunnitelmaan (Standardi 9.4). Lisäksi sisäiset tarkastajat käyttävät ammatillista harkintaa päättäessään, mitä näkökohtia kussakin toimeksiannossa käsitellään (Standardit 13.3 Toimeksiannon tavoitteet ja laajuus, 13.4 Arviointikriteerit ja 13.6 Työohjelma).

Todennusaineisto siitä, että kunkin aihekohtaisen vaatimuksen soveltuvuus on arvioitu, täytyy säilyttää, sisältäen perustelut sille, miksi jotain vaatimusta ei ole sovellettu. Aihekohtaisen vaatimuksen noudattaminen täytyy dokumentoida käyttämällä ammatillista harkintaa, kuten Standardissa 14.6 Toimeksiannon asiakirjat on kuvattu.

Vaikka aihekohtainen vaatimus määrittää perustason valvontaprosesseille, organisaatiot, jotka arvioivat aiheeseen liittyvän riskin erittäin korkeaksi, saattavat joutua arvioimaan myös muita näkökohtia.

Jos sisäisellä tarkastuksella ei ole vaadittavaa pätevyyttä toteuttaa toimeksiantoja, jotka liittyvät aihekohtaisiin vaatimuksiin, sisäisen tarkastuksen johtajan on määriteltävä, miten resurssit saadaan hankittua. Hallitukselle ja ylimmälle johdolle on ilmoitettava hyvissä ajoin rajoitusten vaikutuksista ja siitä, miten resurssien puute aiotaan korjata. Sisäisen tarkastuksen johtaja on viime kädessä vastuussa siitä, että sisäisen tarkastuksen toiminto toimii aihekohtaisten vaatimusten mukaisesti riippumatta siitä, miten resurssit hankitaan (Standardit 3.1 Ammatitaito, 7.2 Sisäisen tarkastuksen johtajan pätevyysvaatimukset, 8.2 Resurssit, 10.2 Henkilöresurssien hallinta).

Toteuttaminen, dokumentointi ja raportointi

Sisäisten tarkastajien on aihekohtaisia vaatimuksia soveltaessaan noudatettava myös Standardeja ja suoritettava työnsä Asiakokonaisuus V mukaisesti: Sisäisen tarkastuksen palvelujen toteuttaminen. Asiakokonaisuuden V standardeissa kuvataan toimeksiantojen suunnittelua (Periaate 13 Toimeksiannon tuloksellinen suunnittelu), toimeksiantojen toteuttamista (Periaate 14 Toimeksiannon toteuttaminen) ja toimeksiantojen tuloksista viestimistä (Periaate 15 Viestintä toimeksiannon tuloksista ja toimenpidesuunnitelmien seuranta).

Aihekohtaiset vaatimukset on suunniteltu tukemaan johdonmukaisia ja laadukkaita sisäisen tarkastuksen käytäntöjä. Paikalliset lait, asetukset, valvojien edellytykset ja muut ammatilliset viitekehykset voivat asettaa lisä- tai erityisvaatimuksia. Sisäisten tarkastajien on ymmärrettävä ja noudatettava lakeja ja/tai säädöksiä, jotka koskevat toimialaa ja alueita, joilla organisaatio toimii, sisältäen vaadittavien tietojen ilmoittaminen Standardin 1.3 Lainmukainen ja eettinen käyttäytyminen mukaisesti. Sisäiset tarkastajat ovat saattaneet jo sisällyttää nämä

lisävaatimukset tarkastusohjelmiin ja testausmenettelyihin, ja heidän tulisi sovittaa ne yhteen aihekohtaisen vaatimuksen kanssa varmistaakseen riittävän kattavuuden toimeksiannoissa.

Aihekohtaisen vaatimuksen huomioon ottaminen voidaan dokumentoida joko sisäisen tarkastuksen suunnitelmaan tai toimeksiannon työpapereihin tarkastajien ammatillisen harkinnan perusteella. Yksi tai useampi sisäisen tarkastuksen toimeksianto voi kattaa vaatimukset. Lisäksi kaikki vaatimukset eivät välttämättä ole sovellettavissa. Todennusaineisto siitä, että Aihekohtaisen vaatimuksen soveltuvuus on arvioitu, täytyy säilyttää, sisältäen perustelut sille, miksi jotain on jätetty soveltamatta.

Laadunvarmistus

Standardit edellyttävät, että sisäisen tarkastuksen johtaja kehittää, toteuttaa ja ylläpitää laadunvarmistus- ja kehittämisohjelmaa, joka kattaa kaikki sisäisen tarkastuksen osa-alueet (Standardi 8.3 Laatu). Tuloksista on tiedotettava hallitukselle ja ylimmälle johdolle. Viestinnässä on raportoitava sisäisen tarkastuksen toiminnon Standardien noudattamisesta ja tavoitteiden saavuttamisesta.

Aihekohtaisten vaatimusten noudattamista 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. Tämä liikesuhde voidaan vahvistaa sopimuksella tai muulla tavoin, jotta organisaatiolle voidaan tarjota tuotteita, palveluja, työvoimaa, tuotantoa tai tietoteknisiä ratkaisuja, kuten datan varastointia, käsittelyä ja ylläpitoa.

Termiä "kolmas osapuoli" voidaan käyttää eri tavoin toimialan tai muun asiayhteyden mukaan. Kullakin sisäisen tarkastuksen toiminnolla on mahdollisuus käyttää harkintavaltaansa Aihekohtaisen vaatimuksen soveltamisessa sen mukaan, miten ensisijainen organisaatio (kolmannen osapuolen kanssa sopimuksen tekevä organisaatio) määrittelee kolmannet osapuolet. Kolmansia osapuolia koskevassa Aihekohtaisessa vaatimuksessa ja käyttöoppaassa termillä "kolmas osapuoli" tarkoitetaan myyjiä, toimittajia, urakoitsijoita, alihankkijoita, ulkoistettuja palveluntarjoajia, muita toimijoita ja konsultteja. Termi "kolmas osapuoli" kattaa kaikki tällaiset järjestelyt, mukaan lukien kolmannen osapuolen ja sen alihankkijoiden väliset järjestelyt.

Tämä Aihekohtainen vaatimus ei kohdistu ensisijaisen organisaation epäsuoriin ulkoisiin suhteisiin, etuihin tai toimiin, kuten sääntelyviranomaisiin, asiamiehiin, välittäjiin, sijoittajiin, edunvalvojiin/hallituksen jäseniin, julkisiin palveluihin ja suureen yleisöön, tai sisäisiin suhteisiin, kuten työntekijöihin tai konsernin sisäisiin palveluntarjoajiin.

Termi "kolmas osapuoli" voidaan määritellä ja sitä voidaan käyttää eri tavoin toimialan tai asiayhteyden mukaan. Sisäisten tarkastajien tulisi käyttää ammatillista harkintaansa

Huomautus:

Aihekohtaisissa vaatimuksissa käytetään sisäisen tarkastuksen yleistä terminologiaa, joka on määritelty Kansainvälisissä sisäisen tarkastuksen standardeissa. Lukijoiden tulisi tutustua Standardien sanastossa oleviin termeihin ja määritelmiin.

soveltaessaan Aihekohtaista vaatimusta ensisijaisen organisaation määritelmään kolmansista osapuolista.

Organisaation kolmansien osapuolten hallintaan liittyvien prosessien tuloksellisuutta voidaan arvioida koko organisaation ja/tai yhden tai useamman yksittäisen sopimuksen tai liikesuhteen tasolla. Sisäisten tarkastajien tulisi soveltaa ylhäältä alaspäin suuntautuvaa lähestymistapaa, jotta he ymmärtäisivät organisaation kolmansiin osapuoliin liittyvät toimintaperiaatteet, menettelytavat, prosessit, puitteet ja elinkaaren. Sisäisten tarkastajien tulisi käyttää harkintaansa ymmärtääkseen kolmansien osapuolten riskeihin liittyviä nyansseja, jotka perustuvat toimialojen, organisaatioiden ja toimeksiantojen aiheiden erityispiirteisiin. Standardin 5.1 Tietojen käyttö mukaisesti sisäisten tarkastajien tulisi olla tietoisia ja noudattaa kaikkia toimintaperiaatteita ja menettelytapoja, jotka liittyvät kolmansien osapuolten tietoihin, joihin heillä on pääsy.

Aihekohtaista vaatimusta sovelletaan, kun sisäinen tarkastus toteuttaa varmennustoimeksiantoja kolmansista osapuolista ja/tai alihankintasuhteista, jotka sallitaan kolmannen osapuolen sopimuksessa ensisijaisen organisaation kanssa. Sisäisten tarkastajien tulisi priorisoida kolmannet ja muut alihankinnan osapuolet riskien perusteella, kuten jäljempänä riskienhallintaa koskevassa osassa kuvataan. Sisäisten tarkastajien täytyy soveltaa kaikkia vaatimuksia riskiarvioinnin mukaisesti. Poikkeukset on dokumentoitava.

Kolmannet osapuolet Aihekohtainen vaatimus ja käyttöopas viittaavat organisaation ja sen kolmansien osapuolten välisen liikesuhteen vaiheisiin, joita kutsutaan myös elinkaaren vaiheiksi: valinta, sopimuksen tekeminen, perehdytys, monitorointi ja liikesuhteen päättäminen. Kolmannet osapuolet Aihekohtaisessa vaatimuksessa ja käyttöoppaassa käytetään näitä vaiheita, vaikka joillakin toimialoilla on omat määritelmänsä elinkaarelle. Vaiheet ovat:

- Valinta: sisältää prosessit, joilla määritetään kolmannen osapuolen tarve, sen käyttöä koskeva suunnitelma ja valintaan liittyvät selvitykset. Lisäksi valinnassa tulisi arvioida mahdollisten ja valittujen kolmansien osapuolten riskit.
- Sopimuksen tekeminen: sisältää due diligence prosessit kolmannen osapuolen kanssa tehtävän oikeudellisen sopimuksen laatimiseen, neuvottelemiseen, hyväksymiseen ja täytäntöönpanoon.
- Perehdytys: alkaa, kun liikesuhteen sopimus allekirjoitetaan, ja se luo perustan sille, että kolmannet osapuolet täyttävät sopimuksen ehdot.
- Monitorointi: sisältää prosessit, jotka koskevat kolmannen osapuolen hallinnointia ja jatkuva valvontaa, kun sopimus on tehty ja hyväksytty. Lähestymistapa on yleensä systemaattinen ja riskiperusteinen, ja siinä tulisi ottaa huomioon jatkuva kehittäminen. Monitorointiin kuuluu myös voimassa olevien kolmansien osapuolten sopimusten uusiminen tarvittaessa.
- Liikesuhteen päättäminen: sisältää prosessit sopimusten päättämiseksi, riskien perusteella priorisoitujen kolmansien osapuolten irtautumissuunnitelman ylläpitämiseksi ja liikesuhteiden lopettamiseksi tarvittaessa. Prosessit perustuvat yleensä riskiperusteiseen lähestymistapaan, ja niihin voi sisältyä vahvistettu irtautumissuunnitelma.

Ensisijainen organisaatio vastaa edelleen tavoitteidensa saavuttamiseen liittyvistä riskeistä, vaikka se käyttäisi kolmatta osapuolta auttamaan sitä yhden tai useamman tavoitteen saavuttamisessa. Kolmansien osapuolten kanssa tehtävä yhteistyö voi vähentää joitakin organisaation prosessien toteuttamisesta aiheutuvia kustannuksia. Se voi kuitenkin aiheuttaa operatiivisia riskejä, koska ensisijaisella organisaatiolla on vähemmän näkymää ja valtaa kolmannen osapuolen valvonta(kontrolli)prosesseihin. Jos kolmas osapuoli ei toimi sopimuksen mukaisesti, toimii epäeettisellä tavalla tai sen liiketoiminta häiriintyy, ensisijaiseen organisaatioon voi kohdistua seuraamuksia.

Ensisijaisen organisaation täytyy tunnistaa, arvioida ja hallita riskejä asianmukaisten hallinto-, riskienhallinta- ja valvontaprosessien avulla. Kolmansiin osapuoliin liittyviä riskikategorioita ja esimerkkejä riskeistä ovat:

- Strategiset riskit, esimerkiksi kyky toteuttaa ensisijaisen organisaation missiota ja/tai ylätasen tavoitteita tai hallita fuusioiden ja yritysostojen vaikutuksia.
- Maineesen 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, kuten 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.

Sisäisten tarkastajien tulisi ottaa huomioon kaikki kolmannen osapuolen elinkaaren vaiheet arvioidessaan hallinto-, riskienhallinta- ja valvontaprosesseja koskevia vaatimuksia.

Kolmannet osapuolet Aihekohtaisen vaatimuksen vaatimukset on jaettu kolmeen osaan standardin 9.1 "Hallinto-, riskienhallinta- ja valvontaprosessien ymmärtäminen" mukaisesti:

- Hallinnointi - selkeästi määritellyt minimitavoitteet ja strategiat kolmansien osapuolten käyttämiseksi organisaation tavoitteiden, toimintaperiaatteiden ja menettelytapojen tukemiseen.

- Riskienhallinta - prosessit, joilla tunnistetaan, arvioidaan, hallitaan ja monitoroidaan kolmansien osapuolten käyttöön liittyviä riskejä, sisältäen prosessin, jolla vaaratilanteet eskaloidaan viipymättä.
- Valvontatoimenpiteet(kontrollit) - johdon määrittelemät, säännöllisesti arvioitavat valvontaprosessit, joiden tarkoituksena on mitigoida riskejä, kun käytetään kolmansia osapuolia.

Aihekohtaisen vaatimuksen ja tämän käyttöoppaan lisäksi sisäiset tarkastajat voivat halutessaan tutustua muihin kolmansia osapuolia koskeviin ammatillisiin ohjeisiin, kuten IPPF:n Kansainvälisiin ohjeisiin ja toimialakohtaisiin aineistoihin.

Huomioon otettavaa

Seuraavat huomiot voivat auttaa sisäisiä tarkastajia toteuttamaan Kolmannet osapuolet Aihekohtaisen vaatimuksen vaatimukset. Kussakin jäljempänä olevassa osiossa kuvataan Aihekohtaisen vaatimuksen vastaavat vaatimukset. Nämä ei-pakottavat huomiot ovat havainnollistavia, ja niiden tarkoituksena on antaa esimerkkejä siitä, miten vaatimuksia voidaan arvioida. Sisäisten tarkastajien tulisi käyttää ammatillista harkintaa päättäessään, mitä arviointeihin sisällytetään.

Hallinnossa huomioon otettavaa

Arvioidakseen, miten hallintoprosesseja, sisältäen hallituksen valvonnan, sovelletaan kolmansien osapuoliin liittyviin tavoitteisiin, sisäiset tarkastajat voivat käydä läpi todennusaineistoa seuraavista seikoista:

- A. Vahvistettu ja dokumentoitu riskiperusteinen lähestymistapa tai strategia kolmannen osapuolen käyttämisestä. Lähestymistapa käydään läpi säännöllisesti, ja siihen sisältyy:
 - Selkeästi määritelty standardoitu prosessi lähestymistavan toteuttamiseksi, joka on hyväksytty käytettäväksi organisaatiossa.
 - Budjetoidut resurssit kustannus-hyötyanalyysin perusteella, joka perustelee kolmannen osapuolen käytön sekä varmistaa yhdenmukaisuuden strategian kanssa ja resurssitehokkuuden.
 - Johdon arvio riskeistä ja valvontatoimenpiteistä(kontrolleista), sisältäen kolmansien osapuoliin liittyvien ongelmien käsittely.
 - Riittävät resurssit kolmansien osapuolten sopimusten tekemistä, hallinnointia ja monitorointia varten.
 - Sidosryhmien palautteen huomioiminen lähestymistavassa tai strategiassa.
- B. Toimintaperiaatteet, menettelytavat ja muut relevantit asiakirjat, joita käytetään kolmansien osapuolten liikesuhteiden määrittelyyn, arviointiin ja hallintaan koko elinkaaren ajan. Toimintaperiaatteet ja menettelytavat voivat sisältää:
 - Standardoituja työkaluja ja dokumenttipohjia, jotka tukevat keskeisiä hallinto-, riskienhallinta- ja valvonta(kontrolli)prosesseja.
 - Prosessit, joiden avulla toimintaperiaatteita ja menettelytapoja arvioidaan säännöllisesti, määritetään niiden riittävyys ja päivitetään niitä tarvittaessa.
 - Määritellyt kriteerit kolmansien osapuolten valinnalle, sopimusten tekemiselle, perehdytykselle, monitoroinnille ja liikesuhteen päättämiseksi.
 - Sovellettavien sääntelyvaatimusten tunnistamisen ja säännöllisen tarkastelun, jotta voidaan varmistaa niiden yhdenmukaisuus toimintaperiaatteiden ja menettelytapojen kanssa.



- Vertailuanalyysieja(benchmarking), joiden avulla tunnistetaan ja vertaillaan johtavia kolmannen osapuolen hallinnointikäytäntöjä.
- C. Määriteltyt roolit ja vastualueet, jotka tukevat kolmansiin osapuoliin liittyvien tavoitteiden saavuttamista. Muuta näyttöä voivat olla:
- Prosessit, joilla arvioidaan, ovatko kolmannen osapuolen arvot, eettiset periaatteet ja yhteiskuntavastuu yhdenmukaisia ensisijaisen organisaation periaatteiden kanssa. Prosessin tulisi sisältää toimintatavat, miten mahdollisiin eturistiriitoihin tai epäeettisiin käytäntöihin puututaan viipymättä.
 - Kolmansien osapuolten hallinnointitehtävissä toimivien säännöllinen koulutus ja heidän pätevyytensä säännöllinen arviointi.
 - Prosessi sen arvioimiseksi, onko koulutusta annettu koko organisaation tietoisuuden lisäämiseksi kolmansista osapuolista.
 - Roolit ja vastualueet on sovitettu yhteen Kolmen linjan mallin kanssa.
- D. Oikea-aikainen viestintä ja yhteistyö relevanttien sidosryhmien (esimerkiksi hallitus, ylin johto, hankinnat, liiketoiminnot, riskienhallinta, compliance, lakiasiat, tietotekniikka, tietoturva, henkilöstöhallinto ja muut) kanssa koko kolmannen osapuolen elinkaaren ajan, sisältäen:
- Tiedot kolmansien osapuolten riskeistä ja tiedossa olevista mahdollisista haavoittuvuuksista kokouspöytäkirjoissa, raporteissa tai sähköpostiviesteissä.
 - Kolmannen osapuolen hallinnointia koskeva tiedonvaihto ja yhteistyön edistäminen (esimerkiksi säännöllisin väliajoin järjestettävien laaja-alaisten kokousten avulla).

Riskienhallinnassa huomioon otettavaa

Arvioidakseen, miten riskienhallintaprosesseja sovelletaan kolmansiin osapuoliin liittyviin tavoitteisiin, sisäiset tarkastajat voivat tarkastella seuraavaa todennusaineistoa:

- A. Kolmansia osapuolia käyttäviä tahoja koskevat standardoidut ja kattavat riskienhallintaprosessit sisältävät määriteltyt roolit ja vastualueet, ja niissä käsitellään riittävästi organisaation kannalta keskeisiä riskejä:
- Kolmansien osapuolten riskien arviointiin ja hallintaan liittyvät prosessit sisältävät sen, miten keskeisiä riskejä:
 - Alun perin on tunnistettu ja raportoitu
 - Analysoidaan, jotta voidaan arvioida niiden vaikutus organisaation tavoitteiden saavuttamiseen
 - Mitigoidaan, sisältäen toimintasuunnitelmat riskin pienentämiseksi hyväksyttävälle tasolle.
 - Monitoroidaan, sisältäen mahdollisten haasteiden tunnistamisen ja käsittelyn, sekä suunnitelman jatkuvaa raportointia varten, kunnes haasteet on täysin ratkaistu.

- Prosessien noudattamista valvotaan ja korjaavia toimenpiteitä toteutetaan, jotta organisaation pitkän aikavälin tavoitteet tai strategia eivät vaarantuisi.
 - Riskienhallintakomitea tai muu ryhmä valvoo suoraan kolmansia osapuolia ja antaa tietoja hallitukselle. Komitealla on määritelty tarkoitus, ja se kokoontuu säännöllisesti. Todennusaineistoa voivat olla kokouspöytäkirjat.
- B.** Kolmansiin osapuoliin liittyvät riskit tunnistetaan ja arvioidaan säännöllisesti koko elinkaaren ajan. Riskiarviossa luokitellaan ja priorisoidaan kolmannet osapuolet. Riskienhallintatoimenpiteet luokitellaan ja priorisoidaan.
- Ensisijainen organisaatio ottaa kolmansien osapuolten riskiarviota laatiessaan huomioon muun muassa organisaation koon, maturiteetin ja käytettävien kolmansien osapuolten lukumäärän.
 - Riskiarvio on dokumentoitu, ja siinä tunnistetaan ominaisriskit ja jäännösriskit.
 - Organisaatio noudattaa due diligence prosessia riskiarvion tarkastelemiseksi ja päivittämiseksi.
 - Kriteerit on määritelty kolmansien osapuolten luokitteluun ja priorisoimiseksi riskien mukaisesti. Esimerkkejä tällaisista kriteereistä ovat:
 - Tarjotut palvelut ovat kriittisiä organisaation toiminnan kannalta.
 - Järjestelyn taloudellinen arvo on olennainen.
 - Liikesuhde on uusi, nopeasti solmittu ja/tai sen kesto on pitkä.
 - Mukana on useita ulkopuolisia osapuolia.
 - Kolmas osapuoli aikoo teettää työn osittain tai kokonaan alihankintana.
 - Organisaatio noudattaa yleisesti hyväksyttyjä käytäntöjä riskiarvioinnissa, sisältäen riskiarvion toteuttamisen mahdollisimman varhaisessa vaiheessa, yleensä kolmannen osapuolen valintavaiheessa tarjousta arvioitaessa, ennen perehdytystä.
 - Toimittajat täyttävät kyselylomakkeen, jonka avulla määritetään niiden riskiluokitus ja priorisointi ominaisriskien perusteella. Organisaatio varmistaa, että relevantti henkilöstö täyttää kyselylomakkeet ja sen, että ne tarkistetaan oikeellisuuden varmistamiseksi.
 - Organisaatio hankkii säännöllisesti tietoja kolmansien osapuolten riskienhallinnasta eri toiminta-alueilta, kuten tietotekniikasta, hankinnoista, kokonaisvaltaisesta riskienhallinnasta (ERM), henkilöstöhallinnosta, lakiasioista, compliancesta, liiketoiminnoista, laskentatoimesta ja rahoituksesta.
- C.** Riskienhallintatoimenpiteet, kuten riskien mitigointi, hyväksyminen, poistaminen ja jakaminen, tunnistetaan ja suhteutetaan riskien luokitteluun.
- Riskienhallintatoimenpiteet dokumentoidaan, ja niihin sisältyy kolmansien osapuolten valvontaympäristön tarkastelu.
 - Dokumentaatio siitä, että ensisijaisen organisaation riskinsietokyvyn ylittävien riskien hallintatoimenpiteiden asianmukaisuus tarkistetaan erityisesti silloin, kun



riskit hyväksytään. Toimenpiteet sisältävät myös mahdollisten eturistiriitojen käsittelyn kolmansien osapuolten kanssa.

- D. Prosessit kolmansien osapuolten riskien hallintaa ja eskalointia varten, sisältäen uhkan tai riskin tason arvioinnin, määrittämisen ja priorisoinnin. Tarkastelu voi sisältää seuraavien seikkojen tunnistamisen:
- Organisaation riskitasojen - kuten korkea, kohtalainen ja matala - määritelmät ja kuvaukset sekä kutakin riskiluokkaa koskevat eskalointimenettelyt.
 - Luettelo kolmansista osapuolista, jotka on priorisoitu tunnistettujen riskien mukaan, ja riskien mitigoinnin tilanne.
 - Sovellettavat lakeihin, sääntelyyn ja vaatimustenmukaisuuteen (compliance) liittyvät vaatimukset
 - Riskien vaikutukset, niin taloudelliset kuin muutkin vaikutukset (esimerkiksi maine)
 - Prosessit kolmansien osapuolten riskeistä tiedottamiseksi johdolle ja henkilökunnalle, sisältäen riskiprofiilin säännöllisen raportoinnin hallitukselle (tai muulle asianmukaiselle taholle). Viestinnän tulisi sisältää päivityksiä priorisoitujen kolmansien osapuolten kanssa havaittujen ongelmien korjaamisesta.
 - Prosessit, joilla riskien luokitusta ja priorisointia arvioidaan uudelleen, kun ensisijaisen organisaation riskinottohalukkuus ja riskinsietokyky muuttuvat.

Valvonnassa(kontrolleissa) huomioon otettavaa

Arvioidakseen, miten valvontaprosesseja sovelletaan liikesuhteissa kolmansien osapuolten kanssa, sisäiset tarkastajat voivat tarkastella seuraavaa todennusaineistoa:

- A. Kolmansien osapuolten hankintaa ja valintaa varten on käytössä asianmukainen due diligence -prosessi, joka sisältää dokumentoidun ja hyväksytyn liiketoimintasuunnitelman tai muun relevantin dokumentaation, jossa kuvataan ja perustellaan kolmannen osapuolen liikesuhteen tarve ja luonne.
- Liiketoimintasuunnitelma voi myös:
 - Käsitellä riskejä, jotka liittyvät kolmannen osapuolen kykyyn täyttää odotukset, ja riskien mahdollisia vaikutuksia organisaatioon.
 - Sisältää yksityiskohtaisen kustannus-hyötyanalyysin.
 - Vakiintuneita hankintaprosesseja - kuten tarjouskilpailuja, tarjouspyyntöjä ja suorahankintoja - noudatetaan. Prosessit sisältävät:
 - Kriteerit, jotka koskevat tärkeitä osa-alueita, kuten kyberturvallisuusmenettelyjen tarkastelua, pankkitietojen varmistamista ja taloudellisten taustatietojen selvittämistä sekä kolmannen osapuolen organisaatorakenteen, rikos- ja oikeushistorian, ajotietojen, poliittisen toiminnan ja rikolliseen toimintaan liittyvien yhteyksien tutkimista.
 - Hyvin määritellyt valintaperusteet, sisältäen aiemman suoriutumisen, referenssien, maineen ja sopimuskustannusten arvioinnin.



- Huolellisuus(due diligence) toimittajien asianmukaisen valinnan varmistamiseksi, kuten monialaisten työryhmien muodostaminen tarjousten arviointia varten. Puolueellisuusriskin mitigoimiseksi arviointiryhmien valvontatoimenpiteisiin(kontrolleihin) kuuluvat muun muassa ryhmien muodostamisen menettelytavat ja vaatimukset mahdollisten eturistiriitojen ilmoittamisesta.
- Huolelliset menetelmät kolmannen osapuolen valvontaympäristön arvioinnissa; esimerkiksi käynti paikan päällä tai tarkastelu, jonka kohteena ovat kolmannen osapuolen:
 - Järjestelmän ja organisaation valvontaa (SOC) koskevat raportit.
 - Taloudellinen vakaus.
 - Yhtiöjärjestys tai kaupparekisteriote ja ote yritys- ja yhteisötietojärjestelmästä.
 - Läpinäkyvyys keskeisen johdon ja keskeisten sidosryhmien päätöksenteossa.
 - Organisaatorakenne.
 - Toiminnan vakaus.
 - Kyberturvallisuusmenettelyt.
 - Relevanttien lakien, säädösten ja standardien noudattaminen.
 - Eettisyys.
 - Aikaisempi toiminta ensisijaisen organisaation kanssa.
 - Maine.
- Todennusaineisto siitä, että mahdolliset toimittajat (myyjät tai urakoitsijat) etenevät sopimuksentekovaiheeseen vasta sitten, kun relevantit due diligence selvitykset on toteutettu ja tulokset on analysoitu.

B. Sopimuksen tekemisen periaatteet ja menettelytavat on laadittu ja niitä noudatetaan.

- Sopimukset laaditaan yksiselitteisin ehdoin.
- Keskeiset riskit otetaan huomioon sopimuksen laatimisvaiheessa, ja niistä kirjataan asiaankuuluvat lausekkeet. Ratkaisua vaativista asioista keskustellaan tässä vaiheessa kolmannen osapuolen kanssa.
- Sopimusten olennaiset osat määritetään organisaation sopimuksen tekemisen periaatteiden ja menettelytapojen sekä kolmannen osapuolen prioriteetin perusteella. Olennaiset osat voivat sisältää:
 - Salassapitosopimukset (yksityisyyden suoja).
 - Irtisanomislausekkeet ja määritellyt parametrit tiedon käyttöoikeuksia varten.
 - Kyberturvallisuusvaatimukset, sisältäen vaatimukset, jotka koskevat pääsyä kaikkeen dataan ja sen jakamista, sekä raportointia vaaratilanteista tai loukkauksista tietyn määräajan kuluessa.



- Vaatimukset ilmoittaa ensisijaisen organisaation tietoihin vaikuttavista loukkauksista.
- Standardoitu prosessi kolmannen osapuolen tunnistetietojen varmentamiseksi, sisältäen täydellisen virallisen nimen, osoitteen, fyysisen sijainnin ja verkkosivuston varmentamisen. Vakiintunut käytäntö on käyttää tarkistuslistaa ja varmentaa tietojen oikeellisuus.
- Selkeästi määritellyt palvelutasosopimukset, joihin kirjataan odotetut tulokset ja kunkin osapuolen oikeudet, velvollisuudet, seuraamukset, palkkiot ja vastuut, sisältäen vastuun työvoimakustannusten maksamisesta (mukaan lukien alihankkijat).
- Tarkastusoikeutta koskeva lauseke, joka kattaa myös alihankkijat, tai vaatimus todennusaineistosta, että hyvämaineinen ja riippumaton varmennuksen antaja on tarkastanut osapuolet. Ilman tarkastusoikeutta koskevaa lauseketta sisäisen tarkastuksen mahdollisuudet saada tai antaa varmennusta voivat olla rajalliset.
- Ensisijaisella organisaatiolla on pääsy riippumattomien tarkastajien laatimiin kontrollien arviointiraportteihin, kuten esimerkiksi taloutta, vaatimustenmukaisuutta ja tietoturvaa koskeviin raportteihin (esim. ISAE ja SOC).
 - Mikäli luotetaan ulkoisten varmentajien työhön kolmannesta osapuolesta, asiakirjat tarkistetaan luotettavuuden varmistamiseksi.
 - SOC-raportteja käytetään tunnistamaan riittämättömät riskien- ja muutostenhallintaprosessit.
- Toimintaperiaatteissa ja menettelytavoissa käsitellään kaikkia tietyille organisaatioille tai sopimustyypeille olennaisia osatekijöitä:
 - Ympäristö- ja vastuullisuuslausekkeet.
 - Whistleblowing-menettelyt.
 - Suoritusarviointia koskevat vaatimukset.
 - Testattu liiketoiminnan jatkuvuussuunnitelma kolmansille osapuolille.
 - Tekoälyn käyttö palvelujen tarjoamisessa.
 - Kaikkien alihankintatöiden selkeä yksilöinti, kirjaaminen, ehdot ja laajuus.
 - Muutoksenhallintaprosessi, jossa kuvataan, miten sopimuskauden aikana tehtävät muutokset laajuuteen, ehtoihin tai toiminnallisiin vaatimuksiin (kuten teknologian muutoksiin tai sääntelyn päivityksiin) käsitellään.
 - Muutostilausten tai laskutusten määrää koskevat rajoitukset.
- Toimintaperiaatteet ja menettelytavat edellyttävät lopputuotteiden muodollista hyväksyntää ennen maksun suorittamista tai pidätetyn maksun vapauttamista.
- Kolmansien osapuolten edellytetään jakavan omat eettiset toimintaperiaatteensa tai ohjeensa ja/tai noudattavan ensisijaisen organisaation vastaavia periaatteita ja ohjeita.



- Mikäli sopimuksen laatii kolmas osapuoli, ensisijainen organisaatio on tehnyt oikeudellisen tarkastelun, ja keskeiset riskit on ymmärretty ja niitä tuetaan asianmukaisella riskienhallintastrategialla.
- C. Asianmukaiset sidosryhmät, mukaan lukien lakiasiat ja compliance, tarkastavat ja hyväksyvät viimeistellyt sopimukset, jotka tallennetaan turvallisesti ja siirretään sopimuksen vastuuhenkilölle tai hallinnoijalle.
 - Sopimus tai muu virallinen asiakirja, josta käy ilmi ulkoistettu liikesuhde ja kolmannen osapuolen velvollisuudet, sekä todennusaineisto kaikista vaadituista lain- ja vaatimustenmukaisuus(compliance)selvityksistä.
- D. Kaikista kolmansien osapuolten kanssa olevista liikesuhteista ylläpidetään tarkkaa, täydellistä ja ajantasaista luetteloa, esimerkiksi keskitetyssä sopimustenhallintajärjestelmässä.
 - Prosessi uusien kolmansien osapuolten sopimusten lisäämiseksi luetteloon tai järjestelmään.
 - Prosessi mahdollisten kolmansien osapuolten tietojen syöttämiseksi toimittajahallintajärjestelmään, sekä niiden poistamiseksi, mikäli sopimusta ei hyväksytä.
 - Prosessi, jolla kolmansien osapuolten sopimukset poistetaan luettelosta tai järjestelmästä.
 - Seurantajärjestelmä, jonka avulla voidaan dokumentoida toimittajien (urakoitsijoiden tai myyjien) kanssa esiintyvät ongelmat myöhempää käyttöä varten.
 - Tarkastusprosessi sen määrittämiseksi, onko kolmansien osapuolten tiedot dokumentoitu tarkasti ja täydellisesti.
- E. Dokumentoidut perehdytysprosessit laaditaan ja niitä noudatetaan, jotta kolmannet osapuolet voivat täyttää sopimuksen ehdot. Arviointeihin voi sisältyä seuraavien seikkojen tarkistaminen:
 - Vakioidut perehdytysprosessit varmistavat, että kaikki tarvittava dokumentaatio, koulutukset ja vaatimustenmukaisuuden selvitykset on toteutettu.
 - Kolmannen osapuolen järjestelmät ja prosessit voidaan integroida saumattomasti ensisijaisen organisaation teknologiaan.
 - Jaetut järjestelmät ovat yhteensopivia ja turvallisia. Todennusaineistoon voi sisältyä täydentäviä organisaatiotason käyttäjähallinnan valvontatoimenpiteitä osana SOC-raportointia.
 - Ensisijainen organisaatio arvioi kolmannen osapuolen liiketoiminnan jatkuvuussuunnitelmat, joilla varmistetaan palvelun jatkuminen hätätilanteissa. Mahdollisten häiriöiden varalta on laadittu varautumissuunnitelmat.
- F. Prosessit, joilla monitoroidaan jatkuvasti toimittajan suoritusta suhteessa sopimuksen tavoitteisiin, sisältäen keskeisten suoritusmittareiden arvioinnit.



- Monitorointiprosessit tukevat kolmannen osapuolen riskiarvioita, ja havaittuja kontrolliheikkouksia käydään läpi, eskaloidaan ja niihin puututaan tarvittaessa.
- Raportit tai havainnot prosesseista, teknologioista ja työkaluista, jotka on otettu käyttöön reaaliaikaista monitorointia varten.
- Prosessit, joilla varmistetaan, että maksut suoritetaan sopimusehtojen mukaisesti, esimerkiksi hankkeen aikataulujen, välitavoitteiden ja viestintävaatimusten täyttyessä. Maksut suoritetaan vain hyväksytyille toimittajille, jotka ovat suorittaneet perehdytysvaiheen ja jotka on kirjattu toimittajien maksujärjestelmään. Kun sopimuksessa on määritetty toteutettavat suoritteet, loppusuoritus maksetaan vasta, kun suoritteet on vahvistettu.
- Monitorointi kolmansien osapuolten sopimukseen liittyvien kustannusten kontrolloimiseksi, arvon varmistamiseksi ja sijoitetun pääoman tuoton määrittämiseksi. Kustannus-hyötyanalyysien tuloksia käytetään sopimusten uudelleen neuvotteluissa.
- Prosessit, joilla arvioidaan seuraamuksia, jos sopimukseen sisältyviä palvelutasosopimuksia ei noudateta. Seuraamusmaksut lasketaan ja veloitetaan silloin, kun ne syntyvät.
- Priorisoitujen kolmansien osapuolten riskiluokitus arvioidaan uudelleen määrääjain, kun sopimukseen tehdään muutoksia ja kun sopimus on lähellä päättymistä tai automaattista uusimista.
- Priorisoitujen kolmansien osapuolten tarkastukset, esimerkiksi paikan päällä tai neljännesvuosittain tehtävät liiketoimintatarkastukset kontrollien ja toiminnan integriteetin vahvistamiseksi.
- Jatkuva lisävalvontaa voidaan osoittaa seuraavilla tavoilla:
 - Kolmannen osapuolen taloudellista vakautta koskevat analyysit.
 - Kolmansiin osapuoliin kohdistuvien valitusten arviointi.
 - Johdon tarkastelut riippumattomien tarkastajien raporteista, esimerkiksi ISAE, SSAE, ISO-sertifioinnit sekä muista taloudellisista, tarkastus-, vaatimustenmukaisuus- ja tietoturvaraporteista joita kolmannet osapuolet toimittavat.
 - Johdon tarkastelut kolmannen osapuolen suorittamista liiketoiminnan resilienssitesteistä, sisältäen kaikki havaitut merkittävät ongelmat.
 - Edellytykset ja rajoitukset, jotka koskevat toimittajan tai sen alihankkijoiden käyttöä.
 - Kolmannen osapuolen eettisten arvojen, kulttuurin ja käyttäytymisen arvioinnit.
 - Vastaukset tiedotusvälineiden kyselyihin.
 - Arviot yksityisyyden suojaa ja kyberturvallisuutta koskevista menettelytavoista, joilla suojataan ensisijaisen organisaation datan ja tiedon varastointia ja siirtoa, sisältäen pitkälle kehittyneiden teknologioiden, kuten tekoälyn, käytön.
 - Organisaation tunnistamat mahdollisuudet suorituksen jatkuvaan parantamiseen ja sopimuksen tavoitteiden saavuttamiseen.



- Tehtävien eriyttämisen tarkastelu.
- G. Menettelyt, joilla käynnistetään korjaavat toimet havaittujen tilanteiden osalta, kun kolmas osapuoli ei täytä sopimuksen vaatimuksia tai jos kolmannen osapuolen toimet lisäävät riskiä ensisijaiselle organisaatiolle.
 - Menettelyt vaaratilanteiden eskaloimiseksi tilanteen vakavuuden ja kolmannen osapuolen prioriteetin perusteella.
 - Vaaratilanteen jälkitarkastelu, mukaan lukien juurisyiden analysointi.
- H. Prosessit, jotka hälyttävät sopimuksista, jotka lähestyvät voimassaolon päättymistä tai automaattista uusimista. Automaattisen uusimisen prosesseihin kuuluu seuraavien seikkojen tarkastelu:
 - Kolmannen osapuolen suoriutuminen.
 - Sopimuksen ehdot ja mahdolliset lisäykset.
 - Riskitekijät.
- I. Vahvistettua liikesuhteen päättämissuunnitelmaa noudatetaan sen varmistamiseksi, että aikataulua ja odotuksia koskevat sopimusvaatimukset otetaan asianmukaisesti huomioon, myös mahdollisten alihankkijoiden osalta.
 - Tarkistuslistat tai keskeisten sidosryhmien haastattelut sen varmistamiseksi, että turvaamistoimenpiteet ovat tehokkaita.
 - Kolmannen osapuolen hallussa olevat organisaatiotiedot tai data on palautettu tai tuhottu.
 - Kolmannen osapuolen pääsy organisaation dataan, järjestelmiin tai tiloihin on poistettu.
 - Ensisijaisen organisaation omaisuus, kuten laitteet, ohjelmistolisenssit, aineettomat oikeudet ja dokumentaatio, on palautettu.
 - Kun kolmas osapuoli irtisanotaan perustellusta syystä, lieventävät olosuhteet tai riskit yksilöidään ja saatetaan ylimmän johdon ja/tai hallituksen tietoon.
 - Kun priorisoidun kolmannen osapuolen sopimus irtisanotaan, osapuoli korvataan saman riskiarvion perusteella, ellei sopimus ole päättynyt tai sitä ei enää tarvita.



Liite A. Käytännön soveltamisesimerkkejä

Seuraavissa esimerkeissä kuvataan skenaarioita, joissa Kolmannet osapuolet Aihekohtaista vaatimusta voitaisiin soveltaa:

Esimerkki 1: Sisäisen tarkastuksen suunnitelmaan sisältyvään toimeksiantoon sisältyy palvelu tai tuotos, jonka tarjoaa tällä hetkellä kolmas osapuoli.

Kun sisäisen tarkastuksen toiminto saattaa päätökseen riskiperusteisen suunnitteluprosessinsa ja sisällyttää sisäisen tarkastuksen suunnitelmaan yhden tai useamman toimeksiannon, joka koskee palveluja tai tuotoksia, joita liikesuhteessa olevat kolmannet osapuolet tarjoavat tällä hetkellä, Aihekohtainen vaatimus on pakollinen.

Kaikkia Aihekohtaisen vaatimuksen vaatimuksia ei välttämättä sovelleta kaikissa toimeksiannoissa. Kun sisäiset tarkastajat käyttävät ammatillista harkintaansa ja päättävät, että yhtä tai useampaa Kolmannet osapuolet Aihekohtaisen vaatimuksen vaatimusta ei voida soveltaa ja että se tulisi sen vuoksi jättää toimeksiannon ulkopuolelle, sisäisten tarkastajien on dokumentoitava ja säilytettävä perustelut kyseisten vaatimusten poisjättämiselle. Tiettyjen vaatimusten poisjättämistä voidaan perustella esimerkiksi sillä, että sisäinen tarkastus on todennut, että organisaation riippuvuus kolmansista osapuolista liiketoimintakriittisissä palveluissa on vähäinen tai että kyseessä on vakiintunut suhde, jonka taloudellinen vaikutus on vähäinen.

Esimerkki 2: Kolmansiin osapuoliin liittyvät riskit tunnistetaan muun kuin kolmansia osapuolia tai sopimusten hallinnointia koskevan varmennustoimeksiannon yhteydessä.

Sisäiset tarkastajat saattavat havaita merkittävän kolmannen osapuolen riskin arvioidessaan prosessia, jonka ei alun perin katsottu liittyvän kolmansiin osapuoliin tai sopimusten hallinnointiin. Kun sisäiset tarkastajat esimerkiksi suunnittelevat toimeksiantoa datan tallentamisen arvioimiseksi, he saavat tietää, että pilvipalveluja hallinnoi kolmas osapuoli. Kolmannen osapuolen tarjoamiin palveluihin liittyvissä johdon haastatteluissa sisäiset tarkastajat tunnistavat kolmanteen osapuoleen liittyviä kyberturvallisuusriskejä.

Kun relevantit riskit on tunnistettu, sisäisten tarkastajien on tarkasteltava sekä Kolmannet osapuolet että Kyberturvallisuus Aihekohtaisia vaatimuksia ja määritettävä, mitkä vaatimukset ovat sovellettavissa. Sisäiset tarkastajat saattavat jättää kolmansien osapuolten hallinnointi- tai riskienhallintaprosessin toimeksiannon ulkopuolelle ja keskittyä tarkastettavien palvelujen kolmansien osapuolten valvontatoimenpiteisiin (kontrolleihin). Samaa ammatillista harkintaa sovelletaan myös Kyberturvallisuus Aihekohtaisen vaatimuksen soveltamiseen. Sisäisten tarkastajien täytyy dokumentoida toimeksiannon työpapereihin perustelut sille, miksi jotkut vaatimukset Kolmannet osapuolet tai Kyberturvallisuus Aihekohtaisista vaatimuksista on jätetty pois, ja säilytettävä asiakirjat.



Esimerkki 3: Tarvitaan kolmanteen osapuoleen liittyvä toimeksianto, joka ei alun perin sisältynyt sisäisen tarkastuksen suunnitelmaan.

Organisaatiossa ilmenee ongelma, johon liittyy priorisoitu kolmas osapuoli ja joka vaatii sisäisen tarkastuksen välitöntä huomiota. Ongelma liittyy kontrollivirheeseen. Sisäisen tarkastuksen johtajan tulisi olla tarvittaessa yhteydessä hallitukseen sisäisen tarkastuksen tarkastussuunnitelman ja resurssien uudelleen priorisoinnista. Sisäisen tarkastajan tulisi yhdessä tapaukseen liittyvän johdon kanssa määritellä toimeksiannon tavoitteet tilanteen arvioimiseksi ja suositusten antamiseksi tulevien tapausten estämiseksi. Sisäisen tarkastuksen johtajan tulisi tarkastella Aihekohtaista vaatimusta toimeksiannon laajuuden määrittämiseksi, määriteltävä sovellettavat vaatimukset ja vastaavasti dokumentoitava mahdolliset vaatimusten poisjättämiset.



Liite B. Valinnainen dokumentointityökalu

Sisäisten tarkastajien odotetaan käyttävän ammatillista harkintaansa määritellessään riskiarvioon perustuvien vaatimusten soveltuvuutta ja dokumentoivan asianmukaisesti tiettyjen vaatimusten poisjättäminen. Aihekohtainen vaatimus voidaan dokumentoida sisäisen tarkastuksen suunnitelmaan tai toimeksiannon työpapereihin sisäisen tarkastajan ammatillisen harkinnan perusteella. Yksi tai useampi sisäisen tarkastuksen toimeksianto voi kattaa vaatimukset. Lisäksi kaikki vaatimukset eivät välttämättä ole sovellettavissa. Jäljempänä oleva tulostettava lomake on yksi vaihtoehto dokumentoida Kolmannet osapuolet Aihekohtaisen vaatimuksen noudattaminen, mutta sen käyttö ei ole pakollista.

Kolmansien osapuolten hallinnointi

Vaatus	Toteutettu kattavuus tai poisjättämisen perustelut	Dokumentaation viite
A. Kolmannen osapuolen kanssa solmittavan liikesuhteen päättämiseksi laaditaan ja toteutetaan virallinen lähestymistapa, jota tarkastellaan säännöllisesti. Lähestymistapa sisältää asianmukaiset kriteerit, joilla määritellään ja arvioidaan tarvittavat ja käytettävissä olevat resurssit, jotta tavoitteet voidaan saavuttaa tarjoamalla tuote tai palvelu.		
B. Kolmansien osapuolten kanssa solmittavien liikesuhteiden ja riskien määrittelemiseksi, arvioimiseksi ja hallinnoimiseksi laaditaan toimintaperiaatteet ja menettelytavat kolmansien osapuolten koko elinkaaren ajaksi. Toimintaperiaatteet ja menettelytavat ovat yhdenmukaiset sovellettavien sääntelyvaatimusten kanssa, ja ne tarkistetaan ja päivitetään säännöllisesti valvontaympäristön vahvistamiseksi.		



Vaatus	Toteutettu kattavuus tai poisjättämisen perustelut	Dokumentaation viite
C. Organisaation kolmansien osapuolten hallinnointitehtävät ja - vastuut on määritelty, ja niissä määritellään yksityiskohtaisesti, kuka valitsee, ohjaa, hallinnoi, pitää yhteyttä ja valvoo kolmansia osapuolia sekä kenelle on tiedotettava kolmansiin osapuoliin liittyvästä toiminnasta. On olemassa prosessi, jolla varmistetaan, että kolmansiin osapuoliin liittyviin tehtäviin ja vastuualueisiin nimetyillä on asianmukainen pätevyys.		
D. Relevanttien sidosryhmien kanssa käytävää yhteydenpitoa varten on määritetty menettelyt, joihin sisältyy oikea-aikainen raportointi priorisoitujen kolmansien osapuolten suoriutumisesta, riskeistä ja vaatimustenmukaisuudesta (erityisesti lakien ja asetusten rikkomisesta). Kolmannet osapuolet priorisoidaan riskien perusteella. Relevantteja sidosryhmiä voivat olla muun muassa hallitus, ylin johto, hankinnat, liiketoiminnot, riskienhallinta, compliance, lakiasiat, tietotekniikka, tietoturva, henkilöstöhallinto ja muut.		

Kolmansien osapuolten riskienhallinta

Vaatus	Toteutettu kattavuus tai poisjättämisen perustelut	Dokumentaation viite
A. Kolmansien osapuolten ja niiden palvelujen riskienhallintaprosessit ovat standardoituja ja kattavia, ne sisältävät määritellyt roolit ja vastualueet ja käsittelevät riittävästi organisaation kannalta keskeisiä riskejä (kuten strategisia, maine, eettisiä, operatiivisia, taloudellisia, compliance, kyberturvallisuus, tietotekniikka, oikeudellisia, vastuullisuus ja geopolittisia riskejä). Prosessien noudattamista monitoroidaan ja poikkeamia korjaavat toimenpiteet toteutetaan.		
B. Kolmansiin osapuoliin liittyvät riskit tunnistetaan ja arvioidaan säännöllisesti koko elinkaaren ajan. Riskiarviota käytetään luokittelemaan ja priorisoimaan kolmansia osapuolia, sisältäen alihankkijat. Myös riskienhallintatoimet luokitellaan ja priorisoidaan. Riskiarviota tarkastellaan ja päivitetään säännöllisesti.		
C. Riskienhallintatoimenpiteet ovat riittäviä ja täsmällisiä, ja ne ovat oikeassa suhteessa riskiluokitukseen. Riskienhallintatoimenpiteet toteutetaan, tarkistetaan, hyväksytään, valvotaan, arvioidaan ja mukautetaan tarvittaessa.		



Vaatus	Toteutettu kattavuus tai poisjättämisen perustelut	Dokumentaation viite
D. Käytössä on menettelytavat, joilla hallitaan ja tarvittaessa eskaloidaan kolmansista osapuolista ilmeneviä ongelmia, varmistetaan vastuut tuloksista ja lisätään todennäköisyyttä saavuttaa sopimusten ehdot. Jos kolmas osapuoli ei reagoi eskaloituneisiin huolenaiheisiin, johdolla on käytössään prosessit, joiden avulla se voi arvioida jatkuvan liikesuhteen riskejä ja ryhtyä tarvittaessa lisätoimiin, korjaaviin toimenpiteisiin tai irtisanomiseen.		

Kolmansien osapuolten valvonta

Vaatus	Toteutettu kattavuus tai poisjättämisen perustelut	Dokumentaation viite
A. Kolmansien osapuolten hankintaa ja valintaa varten on käytössä due diligence -prosessi, sisältäen dokumentoidun ja hyväksytyn liiketoimintasuunnitelman tai muun asiaankuuluvan dokumentaation, jossa kuvataan ja perustellaan kolmannen osapuolen liikesuhteen tarve ja luonne.		
B. Sopimukset ja hyväksynät tehdään organisaation kolmansien osapuolten riskienhallintaperiaatteiden ja -menettelytapojen mukaisesti, ja tähän liittyen tehdään yhteistyötä organisaation asianmukaisten tahojen kanssa.		

Vaatus	Toteutettu kattavuus tai poisjättämisen perustelut	Dokumentaation viite
C. Kaikki asiaankuuluvat sidosryhmät, mukaan lukien lakiasiat ja compliance, tarkastavat ja hyväksyvät lopulliset sopimukset, molempien osapuolten valtuutetut henkilöt allekirjoittavat ne, ja sopimukset tallennetaan turvallisesti. Kullekin sopimukselle on määritelty sopimuksesta vastaava päällikkö tai hallinnoija.		
D. Kaikista kolmansien osapuolten kanssa olevista liikesuhteista ylläpidetään tarkkaa, täydellistä ja ajantasaista luetteloa, esimerkiksi keskitetyssä sopimustenhallintajärjestelmässä.		
E. Dokumentoidut perehdytysprosessit luodaan ja niitä noudatetaan, jotta kolmansien osapuolten on mahdollista täyttää sopimuksen ehdot.		
F. Käytössä on jatkuva valvontaprosessi, jonka avulla arvioidaan, toimivatko kolmannet osapuolet sopimuksen ehtojen mukaisesti koko elinkaaren ajan ja täyttävätkö kolmannet osapuolet sopimusvelvoitteensa. Prosessit sisältävät toimitettujen tietojen luotettavuuden tarkistamisen sekä suorituksen uudelleenarvioinnin määräajoin ja aina kun sopimus muuttuu.		
G. On laadittu menettelyt korjaavien toimenpiteiden käynnistämiseksi, mikäli kolmas osapuoli ei täytä odotuksia tai aiheuttaa lisääntyneen tai odottamattoman riskin. Menettelyihin kuuluu vaaratilanteiden eskalointi niiden vakavuuden perusteella, jälkitarkastelu ja juurisyiden analysointi.		
H. Sopimusten voimassaolon päättymis- ja uusimispäivämääriä monitoroidaan, ja uusimistoimiin ryhdytään tarvittaessa.		

Vaatus	Toteutettu kattavuus tai poisjättämisen perustelut	Dokumentaation viite
I. Toteutetaan ja noudatetaan vahvistettua liikesuhteen päättämissuunnitelmaa sen varmistamiseksi, että aikataulua ja odotuksia koskevat sopimusvaatimukset otetaan asianmukaisesti huomioon. Prosessit sisältävät muun muassa seuraavat ohjeet: • Kolmannen osapuolen irtisanominen. • Kolmannen osapuolen korvaaminen tarvittaessa. • Kolmannen osapuolen hallussa olevien arkaluonteisten tietojen siirtäminen, palauttaminen tai tuhoaminen. • Kolmannen osapuolen pääsyn poistaminen järjestelmästä, työkaluista ja tiloista.		



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.

Vastuuvapauslauseke

IIA julkaisee tämän asiakirjan tiedotus- ja koulutustarkoituksessa. Aineiston tarkoituksena ei ole antaa lopullisia vastauksia yksittäisiin olosuhteisiin, ja se on tarkoitettu vain ohjeeksi. IIA suosittelee hankkimaan riippumatonta asiantuntija-apua, joka liittyy suoraan tiettyyn tilanteeseen. IIA ei ota vastuuta siitä, että henkilö luottaa yksinomaan tähän aineistoon.

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

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