Kyberturvallisuus

Aihekohtainen vaatimus

Topical Requirement

Käyttöopas

The Institute of
Internal Auditors

Sisältö

Yleiskatsaus aihekohtaisiin vaatimuksiin

Aihekohtaiset vaatimukset ovat olennainen osa International Professional Practices Framework (IPPF)® -viitekehystä yhdessä Kansainvälisten sisäisen tarkastuksen standardien™ (Global Internal Audit Standards™) ja Kansainvälisten ohjeiden kanssa. Sisäisen tarkastuksen instituutti edellyttää, että aihekohtaisia vaatimuksia käytetään yhdessä Kansainvälisten sisäisen tarkastuksen standardien kanssa, jotka antavat määräävän perustan vaadituille käytännöille. Viittauksia standardeihin on kaikkialla tässä oppaassa yksityiskohtaisempien tietojen lähteenä.

Aihekohtaisilla vaatimuksilla vahvistetaan se, miten sisäiset tarkastajat käsittelevät keskeisiä riskialueita laadun ja johdonmukaisuuden edistämiseksi ammattikunnassa. Aihekohtaiset vaatimukset määrittävät minimitason ja relevantit kriteerit aiheeseen liittyvien varmennuspalvelujen suorittamiselle (Standardi 13.4 Arviointikriteerit). Aihekohtaisten vaatimusten noudattaminen on pakollista varmennuspalveluissa ja sen noudattamista suositellaan arvioitavaksi neuvonantopalveluissa. Aihekohtaisten vaatimusten ei ole tarkoitus kattaa kaikkia mahdollisia näkökohtia, jotka tulisi ottaa huomioon varmennustoimeksiantoja suoritettaessa, 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 kontrolli(valvonta)prosessit ovat Aihekohtaisten vaatimusten pääkomponentteja. Ne ovat yhdenmukaiset Standardin 9.1 Hallinto-, riskienhallinta- ja valvontaprosessien ymmärtäminen kanssa. Kolmen linjan mallin mukaan hallinto liittyy hallitukseen/hallintoelimeen, riskienhallinta liittyy toiseen linjaan ja kontrollit tai valvontaprosessit ensimmäiseen linjaan. Johto on edustettuna sekä ensimmäisessä että toisessa linjassa. 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 Aihekohtaisen vaatimuksen näkökohtia.

Kuten standardeissa todetaan, 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 sisäisten tarkastajien täytyy arvioida toimeksiannon relevantit riskit (Standardi 13.2 Toimeksiannon riskiarvio).

Kun Aihekohtaisen vaatimuksen aihe tunnistetaan riskiperusteisen sisäisen tarkastuksen suunnitteluprosessin aikana ja se sisällytetään tarkastussuunnitelmaan, Aihekohtaisessa vaatimuksessa esitettyjä vaatimuksia täytyy käyttää aiheen arvioinnissa sovellettavien toimeksiantojen yhteydessä. Lisäksi kun sisäiset tarkastajat tekevät toimeksiannon (joko suunnitelman sisältämänä tai siihen kuulumattomana) ja Aihekohtaisen vaatimuksen osatekijät(elementit) nousevat esiin, Aihekohtaisen vaatimuksen soveltuvuus täytyy arvioida osana toimeksiantoa. Jos pyydetään toimeksiantoa, joka ei alun perin sisältynyt suunnitelmaan ja joka sisältää kyseisen aiheen, Aihekohtaisen vaatimuksen soveltuvuus täytyy arvioida.

Ammatillisella harkinnalla on keskeinen rooli Aihekohtaista vaatimusta sovellettaessa. Riskiarviot ohjaavat sisäisen tarkastuksen johtajien päätöksiä siitä, mitkä toimeksiannot sisällytetään sisäisen tarkastuksen suunnitelmaan (Standardi 9.4 Sisäisen tarkastuksen suunnitelma). 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). Liitteessä A "Käytännön sovellusesimerkkejä" kuvataan, miten sisäiset tarkastajat määrittävät, sovelletaanko Aihekohtaista vaatimusta.

Todisteet siitä, että kunkin Aihekohtaisen vaatimuksen soveltuvuus on arvioitu, mukaan lukien perustelut, joilla selitetään, miksi jotakin vaatimusta ei ole sovellettu, on säilytettävä. Aihekohtaisen vaatimuksen noudattaminen täytyy dokumentoida käyttämällä sisäisen tarkastajan ammatillista harkintaa, kuten Standardissa 14.6 Toimeksiannon asiakirjat on kuvattu.

Vaikka kyberturvallisuutta koskeva Aihekohtainen vaatimus määrittää huomioitavan minimitason valvontaprosesseille, organisaatiot, jotka arvioivat kyberriskin erittäin suureksi, saattavat joutua arvioimaan myös muita näkökohtia.

Jos sisäisen tarkastuksen johtaja toteaa, että sisäisen tarkastuksen yksiköllä ei ole tarvittavaa tietämystä tarkastustoimeksiantojen tekemiseen Aihekohtaisen vaatimuksen mukaisesti, toimeksiannon tekeminen voidaan ulkoistaa (Standardit 3.1 Ammattitaito, 7.2 Sisäisen tarkastuksen johtajan pätevyysvaatimukset, 10.2 Henkilöresurssien hallinta). Ulkoistaminen ei tällöinkään vapauta sisäistä tarkastusta vastuusta noudattaa Aihekohtaisia vaatimuksia. Sisäisen tarkastuksen johtaja on edelleen viime kädessä vastuussa vaatimusten toteuttamisesta. Jos sisäisen tarkastuksen johtaja toteaa, että sisäisen tarkastuksen resurssit ovat riittämättömät, sisäisen tarkastuksen johtajan on ilmoitettava hallitukselle resurssien riittämättömyyden vaikutuksista ja siitä, miten resurssien puute aiotaan korjata (Standardi 8.2 Resurssit).

Toteuttaminen, dokumentointi ja raportointi

Sisäisen tarkastajan täytyy Aihekohtaisia vaatimuksia soveltaessaan noudattaa myös standardeja ja hänen on tehtävä työnsä Asiakokonaisuus V "Sisäisen tarkastuksen toteuttaminen" mukaisesti. Asiakokonaisuus V:n standardeissa kuvataan toimeksiantojen

suunnittelua (Periaate 13 Toimeksiannon tuloksellinen suunnittelu), toimeksiantojen toteuttamista (Periaate 14 Toimeksiannon toteuttaminen) ja toimeksiantojen tuloksista tiedottamista (Periaate 15 Viestintä toimeksiannon tuloksista ja toimenpidesuunnitelmien seuranta).

Aihekohtaisen vaatimuksen noudattaminen voidaan dokumentoida joko sisäisen tarkastuksen suunnitelmaan tai toimeksiannon työpapereihin sisäisten tarkastajien ammatillisen harkinnan perusteella. Yksi tai useampi sisäisen tarkastuksen toimeksianto voi kattaa vaatimukset. Lisäksi kaikki yksittäiset vaatimukset eivät välttämättä ole sovellettavissa. Todisteet siitä, että Aihekohtaisen vaatimuksen soveltuvuus on arvioitu, mukaan lukien perustelut mahdollisten yksittäisten vaatimusten poisjättämisten osalta, on säilytettävä.

Liitteessä C olevaa valinnaista työkalua voidaan käyttää viitteenä ja sisäisten tarkastajien toteuttaman työn dokumentointiin.

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 standardienmukaisuudesta ja tulostavoitteiden saavuttamisesta.

Aihekohtaisten vaatimusten noudattamista arvioidaan laadunarvioinneissa Sisäiset tarkastajat voivat käyttää laatuarvion valmisteluun liitteessä C olevaa työkalua.

Kyberturvallisuus

Kyberturvallisuus on laaja aihe, joka liittyy organisaatioiden useimpiin teknisiin näkökohtiin. Tietotekniikan lisäksi kyberturvallisuus on yleisesti osa liiketoimintaprosesseja, mikä edellyttää, että sisäiset tarkastajat arvioivat kyberriskejä suunnitellessaan, määritellessään ja suorittaessaan varmennustoimeksiantoja.

Yhdysvaltain kauppaministeriön alainen National Institute of Standards and Technology (NIST) määrittelee kyberturvallisuuden yksinkertaisesti seuraavasti: "Kyky suojella tai puolustaa kyberavaruuden käyttöä kyberhyökkäyksiltä". Kyberturvallisuuden Aihekohtainen vaatimus keskittyy ulkoiseen kehään, jonka organisaatiot turvaavat luvattomien käyttäjien ja pahantahtoisten kyberuhkien aiheuttamien riskien vähentämiseksi. Kyberturvallisuus on osa yleistä tietoturvaa, jonka NIST määrittelee seuraavasti: "Tietojen ja tietojärjestelmien suojaaminen luvattomalta pääsyltä, käytöltä, paljastamiselta, häirinnältä, muuttamiselta tai tuhoamiselta luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi."

Kyberturvallisuutta koskevan Aihekohtaisen vaatimuksen vaatimuksiin kuuluvat:

- Hallinnointi - selkeästi määritellyt minimitason kyberturvallisuustavoitteet ja -strategiat, jotka tukevat organisaation tavoitteita, käytäntöjä ja menettelyjä.

- Riskienhallinta - prosessit kyberuhkien tunnistamiseksi, analysoimiseksi, hallitsemiseksi ja seuraamiseksi, mukaan lukien prosessi kyberriskien nopeaa eskalointia varten.
- Kontrollit - johdon vahvistamat, säännöllisesti arvioitavat valvontaprosessit kyberriskien vähentämiseksi.

Näkökohtia

Sisäiset tarkastajat voivat käyttää seuraavia näkökohtia kyberturvallisuutta koskevan Aihekohtaisen vaatimuksen yksittäisten vaatimusten arvioinnin apuna. Nämä näkökohdat, joissa on ristiinviittaus yksittäisiin vaatimuksiin, ovat havainnollistavia mutta eivät pakollisia. Sisäisten tarkastajien tulisi käyttää ammatillista harkintaa päättäessään, mitä he sisällyttävät arviointeihinsa.

Hallintoa koskevia näkökohtia

Arvioidakseen, miten hallintoprosesseja sovelletaan kyberturvallisuustavoitteisiin, sisäiset tarkastajat voivat käydä läpi:

A. Vahvistettua, dokumentoitua kyberturvallisuuden strategista suunnitelmaa ja tavoitteita, mukaan lukien todisteet siitä, että hallitus käy läpi säännöllisesti (yleensä neljännesvuosittain) tietoturvatoiminnon johtajan, kuten tietoturvajohtajan(CISO), toimittamia kyberturvallisuutta koskevia päivityksiä. Näyttöön voi sisältyä raportointi seuraavista asioista:
   - Strategisten tavoitteiden saavuttamisen seuranta.
   - Budjetti kyberturvallisuuden päämäärien ja tavoitteiden tukemiseksi.
   - Keskittyminen riskeihin ja sisäiseen valvontaan (kontrolleihin), mukaan lukien korjausten edistyminen.
   - Keskeiset suorituskykymittarit (KPI) menestyksen mittaamiseksi.
   - Henkilöresurssit, joita tarvitaan kyberturvallisuushenkilöstön palkkaamiseen, kouluttamiseen ja kehittämiseen.

B. Toimintaperiaatteet, menettelytavat ja muu asiaankuuluva dokumentaatio, jota käytetään kyberturvallisuusprosessien hallinnassa, mukaan lukien:
   - Toimintaperiaatteet, jotka tarkistetaan ja päivitetään vähintään vuosittain. Kehittyvät kyberriskit saattavat edellyttää, että tarkistuksia ja päivityksiä tehdään useammin.
   - Prosessi, jolla määritetään, ovatko toimintaperiaatteet ja menettelytavat riittäviä kyberturvallisuustoimien tukemiseksi.
   - Laajasti omaksutut viitekehykset (NIST, COBIT ja muut) kyberturvallisuusprosessien ja sisäisten kontrollien vahvistamiseksi.

C. Roolit ja vastuualueet, jotka tukevat kyberturvallisuustavoitteiden saavuttamista, mukaan lukien rakenne, jolla varmistetaan, että kyberturvallisuustoiminto raportoi organisaatiossa sellaiselle tasolle, jolla on riittävä näkyvyys organisaation tuen saavuttamiseksi.
   - Prosessi, jolla arvioidaan säännöllisesti kyberturvallisuustehtävissä toimivan henkilöstön tietoja, taitoja ja kykyjä.

D. Todisteet yhteydenpidosta asiaankuuluviin sidosryhmiin (esimerkiksi ylempi johto, liike- ja operatiivinen toiminta, riskienhallinta, henkilöstöhallinto, lakiasiat,

compliance, strategiset toimittajat ja muut), mukaan lukien viestintä nykyisistä ja kehittyvistä kyberriskeistä ja tunnetuista mahdollisista haavoittuvuuksista. Todisteet viestinnästä voivat sisältää kokouspöytäkirjoja, raportteja tai sähköpostiviestejä.

Riskienhallintaan liittyviä näkökohtia

Arvioidakseen, miten riskienhallintaprosesseja sovelletaan kyberturvallisuustavoitteisiin, sisäiset tarkastajat voivat käydä läpi:

A. Miten organisaatio arvioi ja hallitsee kyberturvallisuusriskiä, mukaan lukien miten uhkia ja haavoittuvuuksia:
   - Ensin tunnistetaan ja raportoidaan.
   - Analysoidaan organisaation tavoitteiden saavuttamiseen liittyvien riskien arvioimiseksi.
   - Pienennetään, mukaan lukien toimintasuunnitelmat riskin vähentämiseksi hyväksyttävälle tasolle.
   - Seurataan (monitoroidaan), mukaan lukien suunnitelma jatkuvaa raportointia varten, kunnes uhat on täysin ratkaistu.

B. Miten organisaatio saa säännöllisesti kyberturvallisuusriskien hallintaan liittyvää palautetta eri osa-alueilta ja yksiköistä, kuten tietotekniikasta, riskienhallinnasta, henkilöstöhallinnosta, lakiasioista, compliancesta, liike- ja operatiivisesta toiminnasta, laskentatoimesta ja rahoituksesta. Tietojen hankkimiseen voidaan käyttää monialaista kyberturvallisuustyöryhmää tai IT-ohjausryhmää.

C. Miten organisaatio on määrittänyt kyberturvallisuusriskien hallinnan vastuun yksittäiselle henkilölle tai ryhmälle.
   - Vastuuhenkilön (vastuuhenkilöiden) tulisi tiedottaa koko organisaatiolle säännöllisesti (neljännesvuosittain, kuukausittain tai tarpeen mukaan) käynnissä olevista kyberturvallisuusriskien päivityksistä. Tähän voivat sisältyä myös riskien pienentämisstrategioiden resurssitarpeet.

D. Kyberturvallisuusriskien eskalointiprosessit, mukaan lukien se, miten uhan tai riskin taso arvioidaan, osoitetaan ja priorisoidaan. Tarkasteluun voi sisältyä seuraavien seikkojen tunnistaminen:
   - Organisaation määrittelemät riskitasot - kuten korkea, kohtalainen ja matala - sekä yksityiskohtaiset kuvaukset kustakin riskitasosta ja kunkin riskiluokan eskalointimenettelyistä.
   - Luettelo tällä hetkellä tunnistetuista kyberturvallisuusriskeistä ja kunkin riskitapahtuman pienentämisen tilanne.
   - Sovellettavat oikeudelliset, sääntelyyn liittyvät ja vaatimustenmukaisuusvaatimukset.

- Sekä taloudelliset että muut kuin taloudelliset (esimerkiksi maine) riskivaikutukset.

E. Prosessi, jolla kyberturvallisuusriskeistä tiedotetaan johdolle ja työntekijöille, mukaan lukien:

- Säännöllinen (vähintään vuosittainen) työntekijöiden kyberturvallisuuskoulutus, kuten ennalta ilmoittamattomat, simuloidut tietojenkalastelukampanjat, joilla testataan ja seurataan organisaation tietoisuutta.
- Päivitykset olemassaolevien kyberturvallisuushavaintojen korjaamisesta ja niiden odotetut valmistumisajankohdat.
- Sääntöjen noudattamatta jättämisen seuranta, johon sisältyy päivityksiä hallitukselle ja ylimmälle johdolle.
- Uhkien uudelleenarviointi, kun organisaation riskinottohalukkuus ja riskinsietokyky muuttuvat.

F. Prosessit, jotka organisaatio on ottanut käyttöön häiriöihin (insidentteihin) reagoimiseksi ja niistä toipumiseksi ja joihin kuuluvat:

- Dokumentoitu suunnitelma, jota tarkistetaan ja päivitetään organisaation toiminnan muuttuessa ajan myötä. Suunnitelman tulisi sisältää:
  - Miten häiriöt (insidentit) havaitaan ja raportoidaan.
  - Miten häiriöt hallitaan lisävahinkojen estämiseksi.
  - Miten organisaatio toipuu ja reagoi toiminnan jatkamiseksi.
  - Miten häiriö analysoidaan, jotta voidaan selvittää, mitä siitä on opittu ja miten vastaavat tapahtumat voidaan estää tulevaisuudessa.
- Säännöllinen (vähintään vuosittainen) testaus (tabletop-harjoitus) ja tulosten raportointi ylimmälle johdolle ja relevanteille sidosryhmille. Testauksen perusteella voidaan laatia toimintasuunnitelmia.

Valvonta(kontrolli)prosessia koskevia näkökohtia

Arvioidakseen, miten valvontaprosesseja sovelletaan kyberturvallisuustavoitteisiin, sisäiset tarkastajat voivat käydä läpi:

A. Johdon lähestymistapaa tehokkaan kyberturvallisuuden sisäisen valvontaympäristön rakentamiseen, mukaan lukien:

- Miten arvioidaan ja toteutetaan sisäinen valvonta (kontrollit), joita tarvitaan sekä kohonneiden riskien lieventämiseksi että organisaation riskiarvioprosessissa havaittujen arkaluonteisten, kriittisten, henkilö- tai luottamuksellisten tietojen suojaamiseksi.
- Resurssitarpeiden määrittäminen keskeisten kyberturvallisuuden kontrollien ylläpitämiseksi.

- Toimittajien kontrollien huomioon ottaminen osana valvontaympäristöä, johon kuuluu toimittajien SOC (service organization controls) raporttien läpi käynti ennen liikesuhteen aloittamista ja koko liikesuhteen keston ajan.
- Säännöllinen testaus, jolla varmistetaan, että kyberturvallisuuden valvonta toimii tavalla, joka vähentää riskejä ja tukee kyberturvallisuustavoitteiden saavuttamista.
- Prosessi, jolla korjataan sisäisen valvonnan puutteita tai käsitellään sisäisen tarkastuksen tai muiden varmennuksenantajien (esimerkiksi penetraatiotestien) havaintoja.

B. Organisaation osaamisen johtamisen prosessi kyberturvallisuuden ammattilaisten rekrytoimiseksi ja kouluttamiseksi, mukaan lukien se, miten organisaatio tunnistaa mahdollisuuksia lisätä kyberturvallisuuden ammattilaisten valmiuksia teknisen tietämyksen tukemiseksi ja organisaation tietoisuuden parantamiseksi kehittyvistä kyberturvallisuusasioista.
   - Esimerkkeinä voidaan mainita osallistuminen koulutukseen ja tiedonjakoryhmiin sekä ammatillinen täydennyskoulutus, johon kuuluu myös kyberalaan liittyvien sertifikaattien hankkiminen.

C. Johdon prosessi, jolla jatkuvasti tunnistetaan, priorisoidaan, seurataan ja raportoidaan kehittyviä kyberturvallisuuden uhkia ja haavoittuvuuksia, ja joka keskittyy päivittäiseen toimintaan. Läpikäyntiin voi sisältyä se, onko luotu prosessit, joilla arvioidaan uusiin tai kehittyviin teknologioihin, kuten tekoälyn käyttöön, liittyviä uhkia ja haavoittuvuuksia.

D. Johdon prosessit ja kontrollit, jotka on luotu IT varantojen hallinnoimiseksi ja suojaamiseksi koko elinkaaren ajan, mukaan lukien laitteistojen, ohjelmistojen ja toimittajien(palveluiden) valinta, käyttö, ylläpito ja käytöstä poistaminen. Laitteistoon kuuluvat palvelimet, verkkolaitteet (kuten reitittimet tai palomuurit), pöytäkoneet, kannettavat tietokoneet, matkapuhelimet, tabletit ja oheislaitteet. Ohjelmistoihin kuuluvat käyttöjärjestelmät (kuten Windows), toiminnanohjausjärjestelmät (ERP-järjestelmät), sovellukset, virustorjuntaohjelmat ja muut. Laitteistoon ja ohjelmistoon liittyviä näkökohtia voivat olla mm:
   - Organisaatio käyttää salausta, virustorjuntaohjelmistoja, mobiililaitteiden hallintaa, monimutkaisia salasanavaatimuksia, virtuaalista yksityisverkkoa (VPN) / nollaluottamusverkkoa (ZTN) käyttäjän identiteetin todennukseen ja laiteohjelmiston säännöllinen päivittäminen.
   - Laitteisto-omaisuuden hallintaprosessi, jolla varmistetaan, että yrityksen käyttöön ottamat laitteistot suojataan käyttöönotettaessa asianmukaisesti ja että laitteet hävitetään asianmukaisesti, kun ne poistetaan käytöstä.
   - Tietokantoihin liittyvät kontrollit, joihin kuuluvat käyttäjien ja järjestelmänylläpitäjien käyttöoikeuksien rajoittaminen, salauksen käytön varmistaminen, tietokantojen varmuuskopiointi ja testaus sekä vahvat verkkoturvallisuuden kontrollit.

- Miten kyberturvallisuusuhat tai -haavoittuvuudet otetaan huomioon järjestelmäkehityksen elinkaaressa (SDLC).
- Lähestymistapa, jota kehitys, tietoturva sekä liiketoiminta (operatiivinen toiminta) (DevSecOps) käyttävät varmistaakseen, että ohjelmistokehitysprosessi sisältää kyberturvallisuuden, jotta haavoittuvuudet voidaan tunnistaa ennakoivasti.

E. Kyberturvallisuuden vahvistamiseen käytettävät prosessit, mukaan lukien:
   - Tietoturva-asetusten konfigurointi kyberturvallisuusriskin minimoimiseksi.
   - Mobiililaitteiden hallinta (mukaan lukien sähköpostin ja sovellusten käyttö) on konfiguroitu siten, että kyberturvallisuusriskit vähenevät ja laitteita voidaan hallita etänä, jos käyttäjän laite vaarantuu.
   - Salauksen käyttö "lepotilassa olevaan (at rest)" dataan, kuten kiintolevylle tallennettuihin tietoihin, tai "siirrossa olevaan (in transit)" dataan, kuten sähköpostien salaukseen.
   - Palvelimien tai ohjelmistojen (kuten käyttöjärjestelmän) päivittäminen uusimmilla tietoturvaversioilla.
   - Käyttäjien pääsynhallinta, kuten monivaiheinen tunnistautuminen (MFA) ja henkilökohtaisten käyttäjätunnusten (UID) sekä monimutkaisten salasanojen käyttö, jotka vanhenevat määräajoin.
   - Seurataan käytössä olevia kontrolleja, joilla määritetään, toimivatko saatavuus ja resurssien käyttö asianmukaisesti siten, että voidaan käydä läpi ja analysoida mahdollisia kyberturvallisuusongelmia, jotka uhkaavat suorituskykyä.
   - Kyberturvallisuuden sisällyttäminen SDLC:hen, jotta kyberturvallisuuden haavoittuvuudet voidaan tunnistaa ja korjata ennen kuin ohjelmisto siirretään tuotantoon.

F. Verkkoon liittyvät kontrollit, jotka turvaavat organisaation ulkoisen kehän, mukaan lukien:
   - Verkon segmentointi.
   - Palomuurit.
   - Käyttöoikeuksien valvonta.
   - Sekä ulkoisia että sisäisiä yhteyksiä koskevat rajoitukset.
   - Esineiden internetiin (IoT) liittyvät kontrollit yhteenliitettyjä verkkoja varten.
   - Tunkeutumisen havaitsemis- ja torjuntajärjestelmät, joilla voidaan estää, havaita ja toipua kyberturvallisuushyökkäyksistä.

G. Päätepisteviestinnän suojaustoimenpiteet, joita sovelletaan sellaisiin palveluihin kuin sähköposti, Internet-selaimet, videoneuvottelut, viestinvälitys (Zoom, MS Teams ja muut), sosiaalinen media, pilvipalvelut ja tiedostojen siirtomenetelmät. Kontrolleihin voi kuulua tiettyjen tiedostolaajennusten (kuten .exe-tiedostojen) käytön rajoittaminen ja monivaiheinen tunnistautuminen tiedostojen siirrossa.

Liite A. Käytännön soveltamisesimerkkejä

Seuraavissa esimerkeissä kuvataan skenaarioita, joissa kyberturvallisuuden Aihekohtaista vaatimusta tulisi soveltaa:

Esimerkki 1: Kyberturvallisuus kuuluu sisäisen tarkastuksen suunnitelmaan sisältyvään toimeksiantoon.

Kun sisäinen tarkastus saa valmiiksi riskiperusteisen suunnittelun ja sisällyttää yhden tai useamman kyberturvallisuutta koskevan toimeksiannon sisäisen tarkastuksen suunnitelmaan, Aihekohtainen vaatimus on pakollinen tällaisia toimeksiantoja tehtäessä. Vaatimustenmukaisuus voidaan saavuttaa sisällyttämällä aihekohtaiset vaatimukset yhteen tai useampaan sisäisen tarkastuksen suunnitelmaan sisältyvään toimeksiantoon.

Kyberturvallisuus on laaja aihealue, eikä kaikkia Aihekohtaisen vaatimuksen sisältämiä vaatimuksia aina voida soveltaa kaikkiin toimeksiantoihin. Kun sisäiset tarkastajat käyttävät ammatillista harkintaa ja päättävät, että kyberturvallisuuden Aihekohtaisen vaatimuksen yhtä tai useampaa vaatimusta ei voida soveltaa ja että se tai ne olisi sen vuoksi jätettävä pois toimeksiannosta, sisäisten tarkastajien täytyy dokumentoida ja säilyttää perustelut kyseisten vaatimusten poisjättämiselle. Joidenkin vaatimusten poisjättämistä voidaan perustella esimerkiksi sillä, että sisäinen tarkastus tekee useita kyberturvallisuuteen liittyviä toimeksiantoja kiertävällä periaatteella tai on todennut, että riskin merkitys toimeksiannon kannalta on vähäinen.

Esimerkki 2: Kyberturvallisuusriskit havaitaan sellaisen tarkastustoimeksiannon aikana, jossa ei keskitytä kyberturvallisuuteen.

Sisäiset tarkastajat saattavat tunnistaa kyberturvallisuusriskejä arvioidessaan prosessia, joka ei liity suoraan kyberturvallisuuteen. Sisäiset tarkastajat saattavat esimerkiksi arvioida ostovelkaprosessia toimeksiannossa, joka ei keskity kyberturvallisuuteen, eivätkä he toimeksiantoa suunnitellessaan tunnista kyberturvallisuusriskejä toimeksiannon laajuuteen kuuluviksi. Alustavan läpikäynnin jälkeen sisäiset tarkastajat kuitenkin toteavat, että tällaisten riskien pitäisi kuulua tarkastuksen laajuuteen; he esimerkiksi tunnistavat kyberturvallisuusriskit, jotka liittyvät alkuperäisen ostotilauspyynnön verkkopohjaiseen (web-based) toimittamiseen (Standardi 13.2 Toimeksiannon riskiarvio).

Kun relevantit riskit on tunnistettu, sisäisten tarkastajien täytyy käydä läpi kyberturvallisuuden Aihekohtainen vaatimus ja määritettävä, mitä vaatimuksia sovelletaan. Tässä esimerkissä he saattavat sulkea pois kyberturvallisuuden hallinnointiprosessin tai kyberturvallisuusriskien hallintaprosessin. Sisäisen tarkastajan täytyy dokumentoida toimeksiannon työpapereihin

perustelut kyberturvallisuuden Aihekohtaisen vaatimuksen poisjätettävistä vaatimuksista ja säilytettävä dokumentaatio.

Esimerkki 3: Pyydetään kyberturvallisuutta koskevaa toimeksiantoa, joka ei alun perin sisältynyt sisäisen tarkastuksen suunnitelmaan.

Sidosryhmät, kuten hallitus, johto tai valvontaviranomainen, voivat pyytää sisäistä tarkastusta tekemään kyberturvallisuuden arviointeja, jotka eivät sisälly alkuperäiseen tarkastussuunnitelmaan. Esimerkiksi kun organisaatiot joutuvat kyberhyökkäyksen kohteeksi, hallitus voi pyytää sisäistä tarkastusta arvioimaan kyberturvallisuuden kontrolleja. Tällöin Aihekohtaista vaatimusta sovelletaan, vaatimukset täytyy arvioida ja mahdolliset poisjättämiset täytyy dokumentoida.

Liite B. Kartoitus viitekehyksiin

Organisaatiolla voi olla omia kyberturvallisuuteen liittyviä toimia, joissa käytetään COBITin tai NISTin kaltaisia organisaatioiden riskienhallinta- ja hallintoviitekehyksiä. Sisäiset tarkastajat ovat mahdollisesti jo kehittäneet näihin viitekehyksiin perustuvia tarkastusohjelmia ja testausmenettelyjä. Sisäisten tarkastajien tulisi verrata suunniteltuja kyberturvallisuuskontrollien testauksia Aihekohtaisen vaatimuksen kanssa riittävän kattavuuden varmistamiseksi. Alla olevassa kaaviossa on kuvattu kyberturvallisuuden Aihekohtainen vaatimus suhteessa kolmeen yleisesti käytettyyn viitekehykseen: NIST Cybersecurity Framework 2.0, COBIT 2019 ja NIST 800-53. Näitä viitekehyksiä on käytetty, koska ne ovat helposti ja maksutta saatavilla.

Hallintoa koskevat vaatimukset	Viitekehysviittaukset		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Virallinen kyberturvallisuusstrategia ja -tavoitteet on laadittu ja niitä päivitetään säännöllisesti. Kyberturvallisuustavoitteiden saavuttamisesta tiedotetaan säännöllisesti, ja hallitus käy niitä läpi säännöllisesti, mukaan lukien resurssit ja talousarvioon liittyvät näkökohdat kyberturvallisuusstrategian tukemiseksi.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28.	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Kyberturvallisuuteen liittyvät toimintaperiaatteet ja menettelytavat on laadittu, niitä päivitetään säännöllisesti ja ne vahvistavat valvontaympäristöä.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
C. Kyberturvallisuustavoitteita tukevat roolit ja vastuualueet on määritetty, ja käytössä on prosessi, jonka avulla määräajoin arvioidaan näitä tehtäviä hoitavien tietoja, taitoja ja kykyjä.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Relevantit sidosryhmät ovat mukana keskustelemassa ja tunnistavat sekä varautuvat kyberturvallisuusympäristön olemassa oleviin haavoittuvuuksiin ja kehittyviin uhkiin. Sidosryhmiin kuuluvat ylin johto, operatiivinen- ja liiketoiminta, riskienhallinta, henkilöstöhallinto, lakiasiat, compliance, toimittajat ja muut.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Riskienhallintavaatimukset	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Organisaation riskiarvio- ja riskienhallintaprosesseihin kuuluu tunnistaa, arvioida, pienentää ja seurata kyberturvallisuusuhkia ja niiden vaikutusta strategisten tavoitteiden saavuttamiseen.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Kyberturvallisuusriskien hallintaa toteutetaan koko organisaatiossa, johon voivat kuulua seuraavat alueet: tietotekniikka, kokonaisvaltainen riskienhallinta (ERM), henkilöstöhallinto, lakiasiat, compliance, operatiivinen- ja liiketoiminta, toimitusketjut, laskentatoimi, rahoitus ja muut.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28.	EDM03; APO01; APO10; APO12
C. Kyberturvallisuusriskien hallinta on vastuutettu, ja on nimetty henkilö tai ryhmä, joka seuraa ja raportoi säännöllisesti, miten kyberturvallisuusriskejä hallitaan, mukaan lukien resurssit, joita tarvitaan riskien pienentämiseen ja kehittyvien kyberturvallisuusuhkien tunnistamiseen.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12

D. Käytössä on prosessi, jonka avulla voidaan nopeasti eskaloida kaikki (kehittyvät tai aiemmin tunnistetut) kyberturvallisuusriskit, jotka nousevat organisaation riskienhallintaohjeiden perusteella liian korkeiksi, tai noudattaa sovellettavia oikeudellisia ja sääntelyvaatimuksia. Kyberturvallisuusriskin taloudelliset ja muut kuin taloudelliset vaikutukset tulisi ottaa huomioon.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Käytössä on prosessi, jonka avulla kyberturvallisuusriskitietoisuudesta viestitään johdolle ja työntekijöille ja jonka avulla johto käy läpi säännöllisesti havaintoja, puutteita, eroavuuksia tai kontrollivirheitä ja raportoi niistä ja korjaa ne.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
G. Organisaatio on ottanut käyttöön kyberturvallisuushäiriöihin (insidentteihin) reagointi- ja palautumisprosessin, joka sisältää havaitsemisen, rajoittamisen, palautumisen ja häiriön jälkianalyysin. Kyberturvallisuushäiriöiden reagointi- ja palautumisprosessi testataan säännöllisesti.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07

Valvonta(kontrolli)prosessin vaatimukset	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. On luotu prosessi, jolla varmistetaan, että organisaation järjestelmien ja datan luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi on käytössä sekä sisäiset kontrollit että toimittajapohjainen valvonta. Kontrolleja arvioidaan säännöllisesti sen määrittämiseksi, toimivatko ne tavalla, joka edistää organisaation kyberturvallisuustavoitteiden saavuttamista ja ongelmien oikea-aikaista ratkaisemista.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2.	MEA02; MEA04; EDM03; APO09; APO10; DSS01
B. Kyberturvallisuusoperaatioita varten luodaan ja säännöllisesti tarkistetaan osaamisen johtamisen prosessi, johon sisältyy koulutusta teknisen osaamisen kehittämiseksi ja ylläpitämiseksi.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Käytössä on prosessi, jonka avulla seurataan jatkuvasti kehittyviä kyberturvallisuusuhkia ja -haavoittuvuuksia ja raportoidaan niistä sekä tunnistetaan, priorisoidaan ja toteutetaan mahdollisuuksia parantaa kyberturvallisuustoimia.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Kyberturvallisuus sisällytetään kaiken IT varannon, mukaan lukien laitteistot, ohjelmistot ja toimittajat(palveluiden), elinkaaren hallintaan (valinta, käyttö, ylläpito ja käytöstä poistaminen).	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7.	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06

E. Käytössä on prosesseja kyberturvallisuuden edistämiseksi, mukaan lukien konfigurointi, loppukäyttäjän laitteiden hallinta, salaus, päivittäminen, käyttäjien pääsynhallinta sekä saatavuuden ja suorituskyvyn seuranta. Kyberturvallisuusnäkökohdat otetaan huomioon ohjelmistokehityksessä (DevSecOps).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18.	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
F. Verkkoon liittyvät valvontatoimet, kuten verkkoon pääsyn valvonta ja segmentointi, palomuurien käyttö ja sijoittaminen, rajoitetut yhteydet ulkoisista verkoista ja ulkoisiin verkkoihin, virtuaalinen yksityisverkko (VPN) / nollaluottamusverkkoyhteys (ZTNA), esineiden internetin (IoT) verkkovalvonta sekä tunkeutumisen havaitsemis- ja estämisjärjestelmät (IDS ja IPS), on otettu käyttöön.	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
G. Päätepisteviestinnän turvallisuusvalvonta on otettu käyttöön sähköpostin, internetselaimien, videoneuvottelujen, viestinvälityksen, sosiaalisen median, pilvipalveluiden ja tiedostojen siirtomenettelyjen kaltaisten palvelujen osalta.	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

Liite C. Valinnainen dokumentointityökalu

Sisäisten tarkastajien odotetaan käyttävän ammatillista harkintaa määritellessään riskiarvioon perustuvien vaatimusten soveltuvuutta ja dokumentoivan asianmukaisesti tiettyjen vaatimusten poisjättämisen. 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. Allaoleva tulostettava lomake on yksi vaihtoehto dokumentoida kyberturvallisuutta koskevan Aihekohtaisen vaatimuksen noudattaminen, mutta sen käyttö ei ole pakollista.

Kyberturvallisuus – Hallinto

Vaatimus	Toteutettu kattaminen tai poisjättämisen perusteet	Dokumentaation viite
A. Virallinen kyberturvallisuusstrategia ja -tavoitteet on laadittu ja niitä päivitetään säännöllisesti. Kyberturvallisuustavoitteiden saavuttamisesta tiedotetaan säännöllisesti, ja hallitus tarkastelee niitä säännöllisesti, mukaan lukien resurssit ja talousarvioon liittyvät näkökohdat kyberturvallisuusstrategian tukemiseksi.		
B. Kyberturvallisuuteen liittyvät toimintaperiaatteet ja menettelytavat on laadittu, niitä päivitetään säännöllisesti ja ne vahvistavat valvontaympäristöä.		
C. Kyberturvallisuustavoitteita tukevat tehtävät ja vastuualueet on vahvistettu, ja käytössä on prosessi, jonka avulla arvioidaan säännöllisesti tehtävissä toimivien tietoja, taitoja ja kykyjä.		

Vaatimus	Toteutettu kattaminen tai poisjättämisen perusteet	Dokumentaation viite
D. Relevantit sidosryhmät otetaan mukaan keskustelemaan kyberturvallisuusympäristön haavoittuvuuksista ja kehittyvistä uhkista ja toimimaan niiden osalta. Sidosryhmiin kuuluvat ylin johto, operatiivinen ja liiketoiminta, riskienhallinta, henkilöstöhallinto, lakiasiat, compliance, toimittajat ja muut.		

Kyberturvallisuus – Riskienhallinta

Vaatimus	Toteutettu kattaminen tai poisjättämisen perusteet	Dokumentaation viite
A. Organisaation riskiarvio- ja riskienhallintaprosesseihin kuuluu tunnistaa, analysoida, pienentää ja seurata (monitoroida) kyberturvallisuusuhkia ja niiden vaikutusta strategisten tavoitteiden saavuttamiseen.		
B. Kyberturvallisuusriskien hallintaa toteutetaan koko organisaatiossa, ja siihen voivat kuulua seuraavat osa-alueet: tietotekniikka, kokonaisvaltainen riskienhallinta (ERM), henkilöstöhallinto, lakiasiat, compliance, operatiivinen ja liiketoiminta, toimitusketjut, laskentatoimi, rahoitus ja muut.		
C. Kyberturvallisuusriskien hallintaan liittyvät vastuut on määritetty. On määritetty henkilö tai ryhmä, joka seuraa ja raportoi säännöllisesti, miten kyberturvallisuusriskejä hallitaan, mukaan lukien resurssit, joita tarvitaan riskien pienentämiseen ja kehittyvien kyberturvallisuusuhkien tunnistamiseen.		

Vaatimus	Toteutettu kattaminen tai poisjättämisen perusteet	Dokumentaation viite
D. Käytössä on prosessi, jonka avulla voidaan nopeasti eskaloida mikä tahansa (kehittyvä tai aiemmin tunnistettu) kyberturvallisuusriski, joka nousee liian korkeaksi organisaation riskienhallintaohjeiden tai sovellettavien oikeudellisten ja säänteyvaatimusten mukaisesti. Kyberturvallisuusriskin taloudelliset ja muut kuin taloudelliset vaikutukset tulisi ottaa huomioon.		
E. Käytössä on prosessi, jonka avulla kyberturvallisuusriskeistä tiedotetaan johdolle ja työntekijöille ja jonka avulla johto tarkastelee määräajoin havaintoja, eroavaisuuksia, puutteita tai kontrollivirheitä ja raportoi niistä oikea-aikaisesti ja korjaa ne.		
F. Organisaatio on ottanut käyttöön kyberturvallisuushäiriöihin reagointi- ja palautumisprosessin, joka sisältää havaitsemisen, rajoittamisen, palautumisen ja häiriön jälkianalyysin. Kyberturvallisuushäiriöihin reagointi- ja palautumisprosessi testataan säännöllisesti.		

Kyberturvallisuus – Valvonta(kontrolli)prosessit

Vaatimus	Toteutettu kattaminen tai poisjättämisen perusteet	Dokumentaation viite
A. On luotu prosessi, jolla varmistetaan, että organisaation järjestelmien ja tietojen luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi on käytössä sekä sisäiset kontrollit että toimittajapohjainen valvonta. Arviointeja tehdään säännöllisesti sen määrittämiseksi, toimivatko kontrollit tavalla, joka edistää organisaation kyberturvallisuustavoitteiden saavuttamista ja ongelmien nopeaa ratkaisemista.		
B. Otetaan käyttöön osaamisen johtamisen prosessi, johon sisältyy koulutusta kyberturvallisuustoimintoihin liittyvän teknisen osaamisen kehittämiseksi ja ylläpitämiseksi. Prosessi käydään läpi säännöllisesti.		
C. Käytössä on prosessi, jonka avulla seurataan jatkuvasti kehittyviä kyberturvallisuusuhkia ja -haavoittuvuuksia ja raportoidaan niistä sekä tunnistetaan, priorisoidaan ja toteutetaan mahdollisuuksia parantaa kyberturvallisuustoimia.		
D. Kyberturvallisuus sisällytetään koko IT varannon, mukaan lukien laitteistot, ohjelmistot ja toimittajat(palvelut), elinkaaren hallintaan (valinta, käyttö, ylläpito ja käytöstä poistaminen).		

Vaatimus	Toteutettu kattaminen tai poisjättämisen perusteet	Dokumentaation viite
E. On luotu prosessit kyberturvallisuuden edistämiseksi, mukaan lukien konfigurointi, loppukäyttäjän laitteiden hallinta, salaus, päivittäminen, käyttäjien pääsynhallinta sekä saatavuuden ja suorituskyvyn seuranta. Kyberturvallisuusnäkökohdat otetaan huomioon ohjelmistokehityksessä (DevSecOps).		
F. Verkkoon liittyvät valvontatoimet, kuten verkon pääsyn valvonta ja segmentointi, palomuurien käyttö ja sijoittaminen, rajoitetut yhteydet ulkoisista verkoista ja ulkoisiin verkkoihin, virtuaalinen yksityisverkko (VPN) / nollaluottamusverkko (ZTNA), esineiden internetin (IoT) verkkovalvonta sekä tunkeutumisen havaitsemis- ja estämisjärjestelmät (IDS ja IPS), on otettu käyttöön.		
G. Päätepisteviestinnän turvallisuusvalvonta on otettu käyttöön sähköpostin, internetselaimien, videokonferenssien, viestinvälityksen, sosiaalisen median, pilvipalvelun ja tiedostojen siirtomenettelyjen kaltaisille palveluille.		

Sisäisten tarkastajien instituutti

Sisäisten tarkastajien instituutti (Institute of Internal Auditors, IIA) on kansainvälinen ammattijärjestö, joka palvelee yli 255 000 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 www.theiia.org.

Vastuuvapauslauseke

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

Tekijänoikeus

Helmikuu 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