Organisaation resilienssi

Aihekohtainen vaatimus

Topical Requirement



The Institute of Internal Auditors

Kääntänyt

The Institute of Internal Auditors Finland

Organisaation resilienssi Aihekohtainen vaatimus

IIA:n Sisäisen tarkastuksen ammatillinen viitekehys (International Professional Practices Framework®) 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 antavat määräävän perustan vaadituille käytännöille.

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

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 tulee soveltaa Aihekohtaisia vaatimuksia Kansainvälisten sisäisen tarkastuksen standardien mukaisesti. Aihekohtaisten vaatimusten noudattaminen on pakollista varmennuspalvelujen osalta ja suositeltavaa neuvonantopalvelujen osalta.

Aihekohtaista vaatimusta sovelletaan, kun:

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

Kaikki yksittäiset vaatimukset eivät välttämättä sovellu jokaiseen toimeksiantoon, ja jotkin niistä voidaan täyttää muilla tavoin. Jos jotakin vaatimusta ei sovelleta tai se korvataan muulla sääntely- tai sopimusvaatimuksella, on sen perustelut dokumentoitava ja säilytettävä. Sama koskee tilanteita, joissa vaatimus täytetään muilla Standardien mukaisilla menettelyillä. Vaatimusten noudattamista arvioidaan laadunarvioinneissa.

Lisätietoja on saatavissa Organisaation resilienssi Aihekohtainen vaatimus - käyttöoppaasta.

©2026 The Institute of Internal Auditors. Kaikki oikeudet pidätetään. Vain henkilökohtaiseen käyttöön.

Organisaation resilienssi

Kansainvälinen standardisoimisjärjestö (International Organization for Standardization) määrittelee organisaation resilienssin "organisaation kyvyksi sisäistää ja sopeutua muuttuviin olosuhteisiin" (ISO 22316:2017). Vaikka tämä määritelmä asettaa selkeän tavoitteen, käytännössä organisaatioiden välillä on suuria eroja siinä, miten ne ennakoivat, reagoivat ja sopeutuvat muutoksiin ja häiriöihin, sekä palautuvat niistä. Koska organisaation resilienssi kattaa strategisia, toiminnallisia, teknologisia, henkilöstöön liittyviä, sosiaalisia ja taloudellisia ulottuvuuksia, jotkin organisaatiot pystyvät sopeutumaan muutokseen tuloksellisesti, kun taas toiset kamppailevat sopeutumisen kanssa tai valitsevat erilaisia tapoja epävarmuuden hallitsemiseksi.

Organisaation resilienssi on ylätason käsite, joka keskittyy riskeihin, jotka voivat merkittävästi vaikeuttaa tai heikentää organisaation kykyä toimittaa keskeisiä tuotteitaan ja palveluitaan, ylläpitää sidosryhmien luottamusta tai täyttää strategiset tavoitteensa. Nämä riskit voivat johtua äkillisistä tapahtumista (kuten luonnonkatastrofeista, kyberhyökkäyksistä ja geopoliittisista konflikteista), pitkäkestoisista ympäristöstä aiheutuvista haasteista (kuten resurssien niukkuudesta ja kansanterveydellisistä kriiseistä) tai ulkoisen toimintaympäristön muutoksista (kuten teknologisista häiriöistä, sääntelyn muutoksista ja maineen heikkenemisestä).

Nämä riskit voivat olla myös asteittaisia muutoksia tai hitaasti kasvavia haasteita, jotka ajan mittaan vaarantavat organisaation vakauden ja sopeutumiskyvyn. Tällaiset vähitellen kasvavat riskit voivat usein jäädä huomioimatta. Resilientit organisaatiot ennakoivat ja sopeuttavat toimintaansa sekä äkillisiin että vaikeasti havaittaviin riskeihin menestyäkseen.

Riskitekijöitä, jotka lähtökohtaisesti lisäävät uhkaa resilienssille, ovat esimerkiksi erittäin monimutkaiset toiminnot, globaalit toimitusketjut, keskitetty infrastruktuuri tai tietojärjestelmät, työvoiman rajallinen saatavuus, epävakaat markkinaolosuhteet ja voimakas riippuvuus kriittisistä kolmansista osapuolista tai maantieteellisistä sijainneista. Organisaatioihin, jotka toimivat aloilla, joilta vaaditaan korkeaa toimintavarmuutta tai joita säännellään tiukasti, voi kohdistua myös riskejä, jotka ovat lähtökohtaisesti suurempia julkisten vaikutusten ja vaatimustenmukaisuusvelvoitteiden vuoksi.

Organisaation resilienssi keskittyy riskien hallintaan ennen häiriöitä, niiden aikana ja niiden jälkeen. Sisäiset tarkastajat arvioivat yleisesti tietotekniikan (IT) prosesseja ja kontrolleja, jotka liittyvät liiketoiminnan jatkuvuuteen ja häiriötilanteesta palautumiseen. Liiketoiminnan jatkuvuussuunnitelmassa kuvataan yksityiskohtaisesti toimenpiteet, joita organisaatio toteuttaa kriittisten toimintojen ylläpitämiseksi ja normaaliin toimintaan palaamiseksi häiriötilanteen sattuessa. Palautumissuunnitelmassa kuvataan, miten organisaatiot palauttavat tietojärjestelmänsä, kriittisen datan ja toiminnot häiriötilanteen jälkeen, jotta ne voivat jatkaa normaalia liiketoimintaa.

Organisaation resilienssi, joka sisältää nämä molemmat suunnitelmat, edellyttää strategista suunnittelua, kokonaisvaltaista riskienhallintaa, tehokasta johtamista ja kulttuuria sekä koko organisaation kattavia valvontaprosesseja. Organisaation resilienssiä edistävät vahvat valvontaprosessit antavat organisaatioille mahdollisuuden jatkuvasti ennakoida muutoksia, valmistautua, reagoida ja sopeutua niihin, ja samalla myös selviytyä ja menestyä.

©2026 The Institute of Internal Auditors. Kaikki oikeudet pidätetään. Vain henkilökohtaiseen käyttöön.

Organisaation resilienssin hallinto-, riskienhallinta- ja valvontaprosessien arviointi.

Tämä Aihekohtainen vaatimus antaa johdonmukaisen ja kattavan lähestymistavan organisaation resilienssin hallinto-, riskienhallinta- ja valvontaprosessien suunnittelun ja toteutuksen arviointiin. Vaatimukset määrittävät organisaation resilienssin arvioinnin minimitason.

Hallinto

Vaatimukset

Sisäisten tarkastajien tulee arvioida seuraavia asioita, jotka liittyvät organisaation resilienssin hallinnointiin:

A. Johto laatii virallisen resilienssiä huomioivan strategian, jonka hallitus hyväksyy ja valvoo. Strategia sisältää toiminnan jatkuvuuden ja muutosten hallinnan edellyttämät operatiiviset, teknologiset ja taloudelliset osa-alueet. Resilienssiin liittyvät tavoitteet ovat linjassa organisaation kokonaisvaltaisen riskienhallinnan lähestymistavan kanssa.

B. Hallitukselle kommunikoidaan määräajoin resilienssiin liittyvien tavoitteiden saavuttamisesta. Näin varmistetaan, että resilienssi huomioidaan osana strategista ohjausta ja valvontaa, pitkän aikavälin suunnittelua, seuraajasuunnittelua sekä organisaatiokulttuuria. Lisäksi varmistetaan, että kriittisten liiketoimintojen tukemiseen tarvittavat resurssi- ja budjettitarpeet otetaan asianmukaisesti huomioon.

C. Kriittisiä toiminnallisia, teknisiä ja taloudellisia prosesseja koskevat toimintaperiaatteet ja menettelytavat on määritetty, ja niitä arvioidaan, testataan ja päivitetään säännöllisesti valvontaympäristön vahvistamiseksi.

D. Häiriötilanteiden johtamisrakenne on määritelty ja sen avulla voidaan valvoa ja tukea organisaation resilienssiin liittyviä tavoitteita. Se sisältää päätöksentekohierarkiat, viestintä- ja eskalointimenettelyt sekä johdon ja operatiivisen toiminnan roolit ja vastuut.

E. On määritetty prosessi, jonka avulla validoidaan säännöllisesti resilienssin edellyttämät osaamisvaatimukset ja arvioidaan kriittisissä rooleissa toimivien henkilöiden osaaminen.

F. On määritetty prosessi, jolla varmistetaan, että kaikki relevantit sisäiset ja ulkoiset sidosryhmät tunnistetaan ja priorisoidaan sekä osallistetaan organisaation resilienssiin liittyvien tavoitteiden saavuttamista tukevien tiedonhallinta- ja raportointirakenteiden määrittelyyn ja ylläpitoon. Sidosryhmiin voivat kuulua ylin johto, operatiivinen toiminta, riskienhallinta, IT, hankinta, toimitilahallinto, henkilöstöhallinto, taloushallinto, lakiasiat, varmennuksen antajat (mukaan lukien sisäinen tarkastus), compliance, yhteiskuntasuhteet, kriittiset toimittajat, asiakkaat, viranomaiset ja muut asiaankuuluvat tahot.

©2026 The Institute of Internal Auditors. Kaikki oikeudet pidätetään. Vain henkilökohtaiseen käyttöön.

Riskienhallinta

Vaatimukset

Sisäisten tarkastajien tulee arvioida seuraavia organisaation resilienssin riskienhallintaan liittyviä asioita:

A. Organisaation resilienssiin liittyviä riskejä tunnistetaan, arvioidaan ja hallitaan säännöllisesti koko organisaatiossa. Resilienssiin liittyvät riskit kartoitetaan suhteessa organisaation strategisiin tavoitteisiin. Resilienssin riskienhallintaprosessi sisältää keskeisten prosessien arvioinnin.

B. Vastuu organisaation resilienssin riskienhallinnasta on selkeästi määritelty. Nimetyn henkilön tai ryhmän tehtävänä on seurata ja raportoida säännöllisesti organisaation resilienssiin liittyvien riskien hallinnasta, sisältäen riskien hallitsemiseksi tarvittavat resurssit ja organisaation resilienssiin kohdistuvien uusien uhkien tunnistamisen.

C. On määritetty prosessi, jolla seurataan organisaation uusia tai aiemmin tunnistettuja resilienssiin liittyviä riskejä. Prosessin avulla eskaloidaan nopeasti ne riskit, joita ei voida hyväksyä organisaation vakiintuneiden riskienhallintaohjeiden, riskinsietokyvyn tai sovellettavien oikeudellisten ja sääntelyvaatimusten mukaisesti. Organisaation resilienssiin liittyvien riskien vaikutuksia arvioidaan.

D. Johto on ottanut käyttöön ja testaa säännöllisesti prosessia, jolla reagoidaan kriiseihin, häiriöihin ja hätätilanteisiin sekä palaudutaan niistä. Häiriötilanteiden hallinta- ja palautumisprosessi sisältää häiriöiden tunnistamisen, priorisoinnin, eristämisen tai rajaamisen, palautumistoimenpiteet sekä tapahtuman jälkeisen analyysin. Häiriötilanteiden hallintaan sisältyy skenaarioanalyysejä ja säännöllisiä stressitestejä erilaisten häiriötapahtumien varalta.

Valvontaprosessit

Vaatimukset

Sisäisten tarkastajien tulee arvioida seuraavia organisaation resilienssin valvontaprosesseihin liittyviä asioita:

A. Käytössä on prosessi, jonka avulla tunnistetaan kriittiset kolmannet osapuolet (tavarantoimittajat ja myyjät) ja määritetään keskeisten toimintojen ylläpitämiseksi tarvittavat vähimmäisvarastot. Prosessiin kuuluu myös ajantasaisen luettelon ylläpitäminen vaihtoehtoisista toimittajista.

B. Liiketoiminnan kannalta kriittinen tieto tunnistetaan ja luokitellaan. Tiedon luokitteluun kuuluu tiedon sijainnin, käyttöoikeuksien, käyttötarkoituksen, varmuuskopioinnin ja palauttamisen määrittäminen.

C. Kriittiset IT-kontrollit ja jatkuva seuranta ovat käytössä tietoturvariskien (mukaan lukien kyberriskit) hallitsemiseksi ja arkaluontoisen tiedon suojaamiseksi kriisien, häiriöiden ja hätätilanteiden aikana. Valvontaan ja jatkuvaan seurantaan kuuluvat reaaliaikainen uhkaseuranta ja käyttöoikeuksien rajoittaminen vain käyttöoikeuksien haltijoille.

©2026 The Institute of Internal Auditors. Kaikki oikeudet pidätetään. Vain henkilökohtaiseen käyttöön.

D. Kriittinen IT-omaisuus on inventoitu. Omaisuuteen kuuluvat laitteistot, ohjelmistot ja palvelut, joita tarvitaan liiketoiminnan tukemiseen kriisien, häiriöiden ja hätätilanteiden aikana.

E. On laadittu liiketoiminnan jatkuvuus- ja palautumissuunnitelmat, joissa määritellään nimettyjen henkilöiden ja ryhmien roolit. Suunnitelmia testataan säännöllisesti (esimerkiksi "tabletop -, pöytälaatikko -harjoitus"), ja testauksen tulokset, sisältäen kehittämismahdollisuudet, raportoidaan hallitukselle ja ylimmälle johdolle.

F. On perustettu prosessi työympäristön muuttamiseksi kriisien, häiriötilanteiden ja hätätilanteiden aikana.

G. On määritetty prosessi, jonka avulla jatkuvasti seurataan ja raportoidaan uusista uhkista ja haavoittuvuuksista, jotka voivat vaikuttaa organisaation resilienssiin. Prosessin avulla tunnistetaan, priorisoidaan ja kehitetään organisaation resilienssiin liittyviä toimintatapoja, sisältäen järjestelmät, joilla kerätään whistleblowing -ilmoituksia tai riskitietoja.

H. On laadittu prosessi, jonka avulla henkilöstöä koulutetaan organisaation resilienssistä ja varmistetaan, että henkilöstö on tietoinen noudatettavista toimintaperiaatteista ja menettelytavoista sekä toimista, joihin on ryhdyttävä kriisien, häiriöiden ja hätätilanteiden sattuessa. Prosessiin kuuluu harjoituksia, joissa simuloidaan häiriöskenaarioita.

I. Käytössä on prosessi, jolla varmistetaan, että tarvittavat toiminnalliset, henkilöstö-, tekniset ja taloudelliset resurssit on budjetoitu ja käytettävissä kriisien, häiriöiden ja hätätilanteiden aikana. Organisaation resilienssin tukemiseen tarvittavat taloudelliset resurssit arvioidaan säännöllisesti ja niistä viestitään hallitukselle.

J. On määritetty prosessi, jossa kriisejä, häiriöitä ja hätätilanteita käydään läpi ja arvioidaan niiden tapahtumisen jälkeen. Opit aikaisemmista tapahtumista huomioidaan resilienssisuunnittelussa.

Sisäisten tarkastajien instituutti

Institute of Internal Auditors (IIA) on kansainvälinen ammattijärjestö, jolla on yli 275 000 jäsentä maailmanlaajuisesti ja joka 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 saatavissa osoitteessa theiia.org.

Tekijänoikeus

© 2026 The Institute of Internal Auditors, Inc. Kaikki oikeudet pidätetään. Lupaa jäljentämiseen voi pyytää osoitteesta copyright@theiia.org.

Huhtikuu 2026

The Institute of Internal Auditors

Kansainvälinen päämaja
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, Yhdysvallat
Puhelin: +1-407-937-1111
Faksi: +1-407-1101

 ©2026 The Institute of Internal Auditors. Kaikki oikeudet pidätetään. Vain henkilökohtaiseen käyttöön.