

Organisaatiokäyttäytyminen

Aihekohtainen vaatimus

Käyttöopas

Topical Requirement



The Institute of
Internal Auditors

Kääntänyt



The Institute of
Internal Auditors
Finland

Sisältö

Yleiskatsaus aihekohtaisiin vaatimuksiin.....	2
Sovellettavuus, riski ja ammatillinen harkinta.....	2
Osat.....	6
Näkökohtia.....	7
Liite A. Käytännön esimerkkejä	21
Liite B. Esimerkkejä tehdyistä tarkastuksista	24
Liite C. Valinnainen dokumentointityökalu.....	29
Liite D. COSO-viitekehyksen mapping (vastaavuuskartoitus)	33
Liite E. Käyttäytymistä koskevat tarkastus- ja varmennustoimenpiteet	37

Yleiskatsaus aihekohtaisiin vaatimuksiin

Aihekohtaiset vaatimukset ovat olennainen osa Sisäisen tarkastuksen ammatillista viitekehystä® (International Professional Practices Framework® - IPPF) 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. Sisäisen tarkastuksen toimivallassa määritellään selkeästi sisäisen tarkastuksen toiminnan laajuus ja palvelutyytit, joihin sisältyy Aihekohtaisten vaatimusten tarkastelu (Standardi 6.1 Sisäisen tarkastuksen toimivalta). Aihekohtaiset vaatimukset määrittävät minimitason ja antavat relevantit kriteerit aiheeseen liittyvien varmennuspalvelujen suorittamiselle (Standardi 13.4 Arviointikriteerit). Aihekohtaisten vaatimusten noudattaminen on pakollista varmennuspalveluiden osalta ja suositeltavaa neuvonantopalveluiden osalta. Aihekohtaisten vaatimusten ei ole tarkoitus kattaa kaikkia mahdollisia näkökohtia, jotka tulisi ottaa huomioon varmennustoimeksiantoja tehtäessä, 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 kontrollit(valvontaprosessit) ensimmäiseen linjaan. Johto on edustettuna sekä ensimmäisessä että toisessa linjassa, kun taas 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 on noudatettava silloin, kun sisäinen tarkastus tekee varmennustoimeksiantoja aiheista, joista on olemassa Aihekohtainen vaatimus, tai kun muissa varmennustoimeksiannoissa tunnistetaan Aihekohtaisen vaatimuksen 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 sisäisten tarkastajien 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 esitettyjä vaatimuksia on käytettävä aiheen arvioinnissa aiheeseen soveltuvien toimeksiantojen yhteydessä. Lisäksi kun sisäiset tarkastajat toteuttavat toimeksiannon (joko suunnitelman sisältämänä tai siihen kuulumattomana) ja Aihekohtaisen vaatimuksen osatekijät nousevat esiin, Aihekohtaisen vaatimuksen soveltuvuus on arvioitava osana toimeksiantoa. Jos pyydetään toimeksiantoa, joka ei alun perin sisältynyt suunnitelmaan ja joka sisältää kyseisen aiheen, 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 määritellessään, mitä näkökohtia kussakin toimeksiannossa käsitellään (Standardit 13.3 Toimeksiannon tavoitteet ja laajuus, 13.4 Arviointikriteerit ja 13.6 Työohjelma), sekä määritellessään toimeksiannon tavoitteiden saavuttamiseen tarvittavat resurssit (Standardi 13.5 Toimeksiannon resurssit).

Todisteet siitä, että kunkin Aihekohtaisen vaatimuksen soveltuvuus on arvioitu, täytyy säilyttää, mukaan lukien perustelut sille, miksi jotakin vaatimusta ei ole sovellettu. Aihekohtaisen vaatimuksen noudattaminen täytyy dokumentoida käyttämällä sisäisten tarkastajien ammatillista harkintaa, kuten Standardissa 14.6 Toimeksiannon asiakirjat on kuvattu.

Aihekohtainen vaatimus määrittää minimitason valvonta(kontrolli) prosesseille. Samanaikaisesti organisaatiot, jotka arvioivat riskin erittäin korkeaksi, saattavat joutua arvioimaan myös muita näkökohtia.

Jos sisäisen tarkastuksen johtaja toteaa, että sisäisellä tarkastuksella ei ole tarvittavaa tietämystä toteuttaa toimeksiantoja, jotka liittyvät Aihekohtaiseen vaatimukseen, toimeksianto voidaan antaa ulkopuolisen palveluntarjoajan tehtäväksi (Standardit 3.1 Ammattitaito, 7.2 Sisäisen tarkastuksen johtajan pätevyysvaatimukset, 10.2 Henkilöresurssien hallinta). Standardeja sovelletaan kaikkiin henkilöihin tai toimintoihin, jotka tarjoavat sisäisen tarkastuksen palveluja, riippumatta siitä, onko organisaatio palkannut sisäisiä tarkastajia työsuhteeseen, vai teettääkö se sisäisen tarkastuksen toimeksiannot ulkopuolisella palveluntarjoajalla vai näiden yhdistelmällä. Sisäisen tarkastuksen johtaja on viime kädessä vastuussa vaatimustenmukaisuuden varmistamisesta. Jos sisäisen tarkastuksen johtaja toteaa, että sisäisen tarkastuksen resurssit ovat riittämättömät, hänen täytyy lisäksi ilmoittaa hallitukselle resurssien riittämättömyyden vaikutuksista ja siitä, miten resurssien puute aiotaan korjata (Standardi 8.2 Resurssit).

Toteuttaminen, dokumentointi ja raportointi

Sisäisten tarkastajien on Aihekohtaisia vaatimuksia soveltaessaan noudatettava myös Standardeja ja suoritettava työnsä Asiakokonaisuus V:n mukaisesti: Sisäisen tarkastuksen palvelujen toteuttaminen. 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).

Aihekohtaiset vaatimukset on suunniteltu tukemaan johdonmukaisia ja laadukkaita sisäisen tarkastuksen käytäntöjä. Niitä sovelletaan yhdessä paikallisten lakien, säännösten, valvojien odotusten ja muiden ammatillisten viitekehysten kanssa, jotka voivat asettaa lisä- tai erityisvaatimuksia. Sisäiset tarkastajat ovat saattaneet jo aikaisemmin kehittää näihin säännöksiin ja viitekehyksiin perustuvia toimeksiantojen työohjelmia ja testausmenettelyjä. Sisäisten tarkastajien tulisi sovittaa yhteen suunnitellut organisaatiokäyttäytymisen kontrollitestaukset ja muiden sisäisten ja ulkoisten varmennuksen antajien (Standardi 9.5 Koordinointi ja tukeutuminen) toteuttamat luotettavat testaukset Aihekohtaisen vaatimuksen kanssa riittävän kattavuuden varmistamiseksi.

Aihekohtaisen vaatimuksen noudattaminen voidaan dokumentoida joko sisäisen tarkastuksen suunnitelmaan tai toimeksiannon työohjelmaan sisäisten tarkastajien ammatillisen harkinnan perusteella. Yksi tai useampi sisäisen tarkastuksen toimeksianto voi kattaa vaatimukset. Lisäksi kaikki vaatimukset eivät välttämättä sovellu tiettyyn toimeksiantoon. Todisteet siitä, että Aihekohtaisen vaatimuksen soveltuvuus on arvioitu, täytyy säilyttää, mukaan lukien perustelut mahdollisten poisjättämisten osalta.

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 noudattaminen tulisi ottaa huomioon toimeksiantojen valvonnassa (Standardi 12.3 Toimeksiannon valvonta ja kehittäminen), ja sitä arvioidaan laadunarvioinneissa.

Organisaatiokäyttäytyminen

Kulttuurin tarkastuksen uudelleenmuotoilu

Sisäisen tarkastuksen ammattikunnassa on ollut tarpeellista siirtyä abstraktina ja epämääräisenä aiheena pidetystä kulttuurin tarkastamisesta kohti organisaatiokäyttäytymisen jäsenneltyä ja täsmällistä arviointia. Vaikka laajalti tunnustetaan, että kulttuuriset puutteet ovat usein merkittävien valvonta(kontrolli)puutteiden taustalla, nämä eivät ole saanut merkittävää jalansijaa sisäisen tarkastuksen käytännöissä. "Kulttuurin" tarkastamisen muuttaminen "organisaation tavoitteiden kanssa ristiriidassa olevan organisaatiokäyttäytymisen" tarkastamiseksi tarjoaa selkeämmän, jäsennellymmän ja täsmällisemmän lähtökohdan tarkastamiselle. Organisaatiot voivat hallita tätä riskiä kuten kaikkia muitakin riskejä suunnittelemalla asianmukaiset kontrollit ja panemalla ne tehokkaasti täytäntöön.

Huomautus:

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



Organisaatiokäyttäytymistä koskevassa Aihekohtaisessa vaatimuksessa omaksutaan tämä filosofia ja vahvistetaan pakolliset minimivaatimukset käyttäytymisen arvioimiseksi silloin, kun riskiarviossa todetaan, että se kuuluu tarkastelun piiriin. Nämä vaatimukset ovat täysin yhteensopivia perinteisen riskiperusteisen tarkastuslähestymistavan kanssa, ja niitä voidaan soveltaa vähäisin muutoksin kaikissa tarkastustoiminnoissa. Tässä käyttöoppaassa annetaan käytännön esimerkkejä siitä, miten tämä lähestymistapa voidaan sisällyttää tavanomaisiin tarkastustoimeksiantoihin, sekä ohjeita myös laaja-alaiseen organisaatiokäyttäytymisen tai yksittäisten osien tarkasteluun. Tämän aiheen merkittävä vaikutus organisaation tavoitteisiin edellyttää ennakoivaa harkintaa ja käyttöönottoa.

Seuraavien keskeisten termien määritelmät ovat välttämättömiä Aihekohtaisen vaatimuksen ymmärtämiseksi ja soveltamiseksi. Koska tämä aihe on vielä kypsyvätön, organisaatiot käyttävät näitä termejä epäjohdonmukaisesti. Määritelmien tulisi auttaa käyttäjiä sovittamaan organisaationsa terminologia yhteen Aihekohtaisessa vaatimuksessa ja tässä käyttöoppaassa esitetyn terminologian kanssa.

- **käyttäytymisinsentiivit(kannustimet)** - Kaikki, mitä voidaan antaa käyttäytymisen motivoimiseksi, mukaan lukien rahalliset kannustimet, kuten palkankorotukset, bonukset tai osakeoptiot, tai muut kuin rahalliset kannustimet, kuten kehuminen, toivotut työtehtävät tai vapaapäivät.
- **käyttäytymismallit** - Mallit, joissa käyttäytyminen toistuu tai tapahtuu säännöllisesti. Mallit tunnistetaan laajemmin "miten asiat tehdään"-tyylisinä, toisin kuin yksittäiset tilanteet.
- **käyttäytymisriski** - Riski siitä, että käyttäytyminen on ristiriidassa organisaation tavoitteiden kanssa.
- **käyttäytymisen riski-indikaattorit** - Käytännönläheistä ja johtamista tukevaa tietoa käyttäytymisestä.
- **hallitus** - Organisaation korkein hallintoelin.
- **toimintatapa** - Käyttäytyminen suhteessa sääntelyvaatimuksiin ja odotuksiin.
- **kulttuuri** - Työntekijöiden tekemät valinnat työssään ja yhteistyössään muiden kanssa, sekä näiden organisaatiokäyttäytymisen muotojen taustatekijät. Ohjaaviin tekijöihin kuuluvat viralliset mekanismit, kuten kannustimet ja tavoitteet, sekä epäviralliset mekanismit, kuten kollektiiviset arvot ja uskomukset.
- **organisaatiokäyttäytyminen** - Työntekijöiden työssään ja yhteistyössään tekemät havaittavat valinnat. Tämä käyttäytyminen vaikuttaa suoriin ja organisaation tavoitteiden saavuttamiseen. Yksinkertaisesti sanottuna organisaatiokäyttäytyminen on "tapa, jolla teemme asioita", ja se on osa organisaatiokulttuuria.
- **suoritus arvioinnit** - Yksilöiden tai ryhmien arviot oman työn riittävydestä.
- **sidosryhmä** - Osapuoli, jolla on suora tai epäsuora intressi organisaation toimintaan ja tuloksiin. Sidosryhmiin voivat kuulua hallitus, johto, työntekijät, asiakkaat, myyjät, osakkeenomistajat, sääntelyviranomaiset, rahoituslaitokset, tilintarkastajat, yleisö ja muut.
- **arvot** - Periaatteet, jotka ohjaavat sitä, miten ihmisten odotetaan käyttäytyvän.



Osat

Organisaatiokäyttäytymistä koskevan Aihekohtaisen vaatimuksen pakolliset vaatimukset ja tämän käyttöoppaan ei-pakolliset näkökohdat on jaettu kolmeen osaan:

- **Hallinnointi** - Selkeästi määritellyt organisaatiokäyttäytymisen perustavoitteet ja -strategiat, jotka tukevat organisaation tavoitteita, toimintaperiaatteita ja menettelytapoja.
- **Riskienhallinta** - Prosessit, joilla tunnistetaan, analysoidaan, hallitaan ja seurataan organisaatiokäyttäytymiseen liittyviä riskejä, mukaan lukien prosessi, jolla vaaratilanteet eskaloidaan nopeasti.
- **Valvontatoimenpiteet (kontrollit)** - Johdon asettamat, säännöllisesti arvioitavat valvontatoimenpiteet, joilla vähennetään organisaatiokäyttäytymiseen liittyviä riskejä.

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



Näkökohtia

Sisäiset tarkastajat voivat käyttää seuraavia näkökohtia organisaatiokäyttäytymistä koskevan Aihekohtaisen vaatimuksen arvioinnin apuna. Kukin jäljempänä esitettävä näkökohta on ristiviitattu aihekohtaisen vaatimuksen vastaavaan vaatimukseen. Nämä näkökohdat ovat esimerkinomaisia, mutta eivät pakollisia. Sisäisten tarkastajien tulisi käyttää ammatillista harkintaa päättäessään, mitä he sisällyttävät arviointeihinsa.

Julkisen sektorin sisäisen tarkastuksen toimeksiantojen rajoitukset, kuten lainsäädäntö, hallintorakenne tai poliittinen ympäristö, ovat mahdollisia esteitä tiettyjen näkökohtien käsittelylle. Julkisen sektorin sisäisten tarkastajien tulisi dokumentoida tarkastuksen laajuuden rajoitukset osana riskiarvioprosessiaan ja heidän tulisi käyttää ammatillista harkintaa määritellessään ja viestiessään selkeästi tarkastuksen mukautettu laajuus.

Hallintoa koskevia näkökohtia

Arvioidakseen, miten hallintoprosesseja voidaan soveltaa organisaatiokäyttäytymiseen, sisäiset tarkastajat voivat tarkastella:

- A. Rooleja ja vastuualueita, joilla varmistetaan, että hallitus säilyttää näkyvyyden ja vaikutusvallan organisaation käyttäytymiseen. Näyttöä voi olla muun muassa se, että:
 - Hallintokomitea:
 - Perustaa ja ylläpitää organisaatiokäyttäytymiseen keskittyvän hallintoelimen tai alakomitean (alakomiteoita), jolla on selkeät toimintaohjeet organisaatiokäyttäytymisen valvonnan kytkemiseksi strategian toteuttamiseen.
 - Tekee säännöllisiä arviointeja käyttäytymisriskien indikaattoreista, jotka ovat linjassa pitkän aikavälin liiketoimintatavoitteiden kanssa. Käyttäytymisriskien indikaattorit ovat mittareita, joiden avulla määritetään, tarvitaanko toimenpiteitä sen varmistamiseksi, että käyttäytyminen pysyy linjassa organisaation tavoitteiden, niihin liittyvien arvojen ja organisaation tarkoituksen kanssa.
 - Sisällyttää käyttäytymiseen liittyvät tavoitteet johdon suorituksen arviointiin ja palkitsemiseen.
 - Hallitusraportoinnin viitekehykset:
 - Tarjoavat tietoa käyttäytymisriskien indikaattoreista hyödyntäen dashboardeja (esimerkiksi henkilöstön sitoutuminen, poikkeamien trendit, asiakastytyväisyys, arvoihin perustuva tunnustus).
 - Integroivat kulttuuriin liittyvät mittarit hallitustason strategiseen tuloksetraportointiin.
 - Sidosryhmien palautemekanismit, kuten kyselyt, mahdollistavat:
 - Hallitus saa suoraa palautetta työntekijöiltä, asiakkailta ja muilta sidosryhmiltä siitä, miten käyttäytyminen vastaa arvoja ja strategiaa.



- Palaute auttaa muotoilemaan strategista suuntaa ja käyttäytymiseen vaikuttavia toimenpiteitä.
- B.** Organisaatiokäyttäytymisen tehokas johtaminen toteutuu koko organisaation kattavien, selkeästi määriteltyjen vastuiden kautta. Hallitus on viime kädessä vastuussa sen varmistamisesta, että organisaatio edistää ja ylläpitää organisaation tavoitteiden mukaista käyttäytymistä; tähän kuuluu selkeiden käytösodotusten asettaminen, käyttäytymisriskien raportoinnin valvonta sekä johdon haastaminen, mikäli havaitaan poikkeamia. Näyttöä voi olla se, että:
- Hallitus:
 - Hyväksyy organisaatiokäyttäytymiseen liittyvän riskinottohalukkuuden ja keskeiset kulttuuriset tavoitteet.
 - Edellyttää säännöllistä raportointia käyttäytymisriskien indikaattoreista (esimerkiksi trendit, poikkeamien toistuvuudet, whistleblowing teemat).
 - Pitää toimivaa johtoa vastuullisena kulttuurisesta suoriutumisesta hyödyntäen mekanismeja, kuten kannustinjärjestelmiä ja johdon esimerkkiä (*tone at the top*).
 - Tapaa toisen ja kolmannen linjan toimintoja asioissa, jotka koskevat käyttäytymisriskien eskalointia, valvonnan puutteita sekä korjaavien toimenpiteiden riittävyyttä.
 - Liiketoimintayksiköt ja operatiivinen johto sisällyttävät käyttäytymisodotukset osaksi päivittäistä toimintaa ja varmistavat, että päätökset, viestintä ja ryhmädynamiikka heijastavat organisaation määriteltyjä arvoja. Tähän voi sisältyä vastuun ottaminen seuraavista:
 - Toivotun käyttäytymisen mallintaminen ja psykologisesti turvallisen ympäristön ylläpitäminen.
 - Käyttäytymiseen vaikuttavien valvontatoimenpiteiden, kuten rekrytoinnin, palkitsemisen, viestinnän ja johtamisrutiinien toteuttaminen.
 - Käyttäytymisriskien ennakoiva tunnistaminen ja eskalointi, kun niitä ilmenee operatiivisissa tilanteissa.
 - Sellaisten käyttäytymisriskien pienentäminen, jotka johtuvat ryhmien sisäisestä tavoitteiden vastaisesta toiminnasta, sekä tarve (muodollisille ja epämuodollisille) valvontatoimenpiteille.
 - Riskienhallinta, compliance, henkilöstöhallinto ja muut vastaavat valvontatoiminnot suunnittelevat ja ylläpitävät organisaation käyttäytymisriskien viitekehystä, johon kuuluu:
 - Määriteltyt roolit ja vastuut käyttäytymisen valvonnassa.
 - Eskaloinnin menettelytavat ja datan analysointiprosessit.
 - Dashboardit (raportointinäkömät), teema-analyysit ja säännölliset arvioinnit, jotka tarjoavat ennakoivaa näkemystä organisaation käyttäytymisen tilasta.



- Oikeus kyseenalaistaa käytäntöjä, joissa kannustimet, viestintä tai johtamiskäyttäytyminen poikkeavat asetetuista tavoitteista.
 - Konsultointi kaikista olennaisista muutoksista, jotka koskevat henkilöstöön liittyviä valvontatoimenpiteitä, hallintomalleja tai strategisia muutosaloitteita, jotka voivat vaikuttaa organisaatiokulttuuriin.
 - Poikkeamaraporteista, tarkastushavainnoista ja muista varmennusmekanismeista ilmenevien sellaisten trendien tarkastelu, jotka viittaavat käyttäytymiseen liittyviin ongelmiin.
- c.** Hallintoprosessi, jolla varmistetaan käyttäytymisen valvonta, säännöllinen seuranta, arviointi sekä käyttäytymismallien ja organisaation tavoitteiden yhdenmukaisuus. Prosessi voi sisältää:
- Dashboardin hyödyntäminen keskeisten tunnuslukujen tarjoamiseksi sellaisista lähteistä, kuten henkilöstötyytyväisyys- ja integriteettikyselyiden tulokset, henkilöstön vaihtuvuus ja poissaolot, eettisen ilmoituskanavan (speak-up) sisältö, poikkeamatiedot sekä suoriutumisen ja innovaatioiden mittarit. Vaikuttavan organisaatiokäyttäytymisen dashboardin (raportointinäköymän) ominaispiirteitä ovat muun muassa:
 - Määritellyt kynnyksarvot, joiden avulla tunnistetaan mahdollisuudet käyttäytymisen kehittämiseksi.
 - Käyttäytymistä koskevan datan (kuten ilmoituskanavan tiedot) erottaminen ohjaustiedosta (kuten roolien ja vastuiden selkeys) ja tulosdatasta (kuten asiakasvalitukset).
 - Määrällisen tiedon (kuten kyselytutkimuksista saadun datan) yhdistäminen laadulliseen tietoon (kuten kohderyhmäkeskustelujen ja ilmoituskanavan tietoihin).
 - Hallituksen ymmärrys siitä, miten organisaatiokäyttäytymisen nykyisiä näkökohtia voitaisiin käsitellä organisaation tehokkuuden ja tuloksellisuuden parantamiseksi. Nämä osa-alueet sisältävät sen, miten:
 - Tehdään päätöksiä, mukaan lukien erilaisten näkökulmien etsiminen ja kriittinen tarkastelu.
 - Työntekijät viestivät keskenään, mukaan lukien huolien ja odotusten esiintuominen.
 - Työntekijät tekevät yhteistyötä, mukaan lukien tiimien välinen yhteistyö ja ristiriitojen käsittely.
 - Työntekijät suhtautuvat epäonnistumisiin esimerkiksi oppimalla virheistä tai vastaamalla niihin syyllistämällä tai kieltämisellä.
 - Keskijohdon ja ylimmän johdon johtamiskäyttäytyminen vaikuttaa muihin käyttäytymiskategorioihin (esimerkiksi siihen, miten johtajat reagoivat virheisiin ja miten he kannustavat tarkastelemaan päätöksentekoa kriittisesti.)



- Strategia ja liiketoimintamalli ohjaavat päätöksentekoa, toimintaohjeita (codes of conduct) sekä kannustimia/rajoitteita ja suorituksen johtamista.
- Hallitus edellyttää jatkuvan oppimisen järjestelmää, jossa tunnistetaan kehityskohteita ja käsitellään niitä aktiivisesti ja mitattavasti seuraavin tavoin:
 - Käyttämällä näyttöön perustuvaa tietoa, joka pohjautuu työntekijöiden todelliseen käyttäytymiseen
 - Keskittymällä siihen, mitä organisaatiossa tiedetään tapahtuvan, eikä siihen, mikä on tavoiteltua tai toivottua.
 - Arvioimalla laadullisen ja määrällisen tiedon yhdistelmää, jota kerätään usein kyselyillä, ilmoituskanavilla, luottamuksellisilla keskusteluilla ja kohderyhmäkeskusteluilla.
 - Hyödyntämällä saatuja tietoja sellaisten toimenpiteiden määrittelemiseksi, joilla vahvistetaan ja kehitetään tiettyjä organisaatiokäyttäytymisen osa-alueita.
 - Laatimalla toimintasuunnitelma, jossa yhdistetään kohdennettuja toimenpiteitä kriittisillä alueilla (esimerkiksi viestintästrategia, koulutus, johtamisen kehittäminen ja ryhmä(tiimi)tason keskustelut).
- D. Laatimalla käyttäytymisriskiä koskevat toimintaperiaatteet ja menettelytavat, arvioimalla ne säännöllisesti, viestimällä niistä tuloksellisesti ja integroimalla ne osaksi liiketoimintaa ja päätöksentekoa. Toimintaperiaatteet ja menettelytavat kattavat etiikan, henkilöstöhallinnon, vaatimustenmukaisuuden (*compliance*), riskienhallinnan, operatiivisen toiminnan sekä päätöksentekovaltuudet sen varmistamiseksi, että:
 - Käyttäytymisodotukset on määritelty muodollisesti asiaankuuluvissa ohjeistuksissa (kuten toimintaohjeissa (code of conduct) ja/tai etiikkaa, henkilöstöhallintoa, kannustimia sekä päätösvallan delegointia koskevista toimintaperiaatteista). Näissä ohjeistuksissa tulisi määritellä hyväksyttävä ja ei-hyväksyttävä käyttäytyminen käytännön esimerkkien avulla ja organisaation riskinottohalukkuuden mukaisesti.
 - Riskienhallintatoiminnot yhdistävät käyttäytymisodotukset keskeisiin toimintaprosesseihin, kuten rekrytointiin, suorituksen arviointiin, perehdytykseen ja asiakkuuksien hallintaan, ja varmistavat, että ne näkyvät päivittäisessä päätöksenteossa. Varmennusarvioinneissa (assurance reviews) tulisi testata, miten nämä odotukset vaikuttavat todelliseen käyttäytymiseen, ja raportoida tuloksista hallitukselle.
 - Hallitus hakee ja saa varmistuksen siitä, että organisaation ohjeistukset ovat helposti saatavilla ja että niistä on viestitty selkeästi useiden eri kanavien kautta (esimerkiksi intranet, koulutukset ja henkilöstöinfot). Tapaustutkimusten (case-tutkimusten) ja päätöspuiden sisällyttäminen auttaa konkretisoimaan käyttäytymisodotuksia. Mittaristojen (dashboards) avulla voidaan seurata ymmärrettävyyttä ja käyttöastetta.



- Kaikkia käyttäytymistä koskevia toimintaperiaatteita ja menettelytapoja tarkistetaan säännöllisesti, ja niitä päivitetään vaaratilanteiden, kyselytulosten tai sääntelymuutosten perusteella. Toisen linjan toimintojen tulisi ylläpitää oppien (lessons-learned) rekisteriä, jotta voidaan tunnistaa todellisen käyttäytymisen ja organisaation tavoitteiden välille syntyvät erot.
- Hallitukselle raportoidaan säännöllisesti ohjeistusten kattavuudesta, selkeydestä ja vaikuttavuudesta. Toisen linjan tulisi analysoida rikkomuksia, ohjeistusten vaikutuksia ja yhdenmukaisuutta tavoitellun käyttäytymisen kanssa. Toimintaohjeiden vaikuttavuutta tulisi arvioida laadullisen palautteen ja käyttäytymiseen liittyvien riskimittareiden (tai indikaattoreiden) avulla.

Riskienhallintaan liittyviä näkökohtia

Arvioidakseen, miten riskienhallintaprosesseja sovelletaan organisaation käyttäytymiseen, sisäiset tarkastajat voivat tarkastella, onko:

- A. Käyttäytymiseen liittyvä riskienhallintaprosessi määritelty selkeästi, ja sisältääkö se ne käyttäytymispiirteet, jotka ovat kriittisiä organisaation tavoitteiden saavuttamiseksi. Riskienhallinnan ominaispiirteitä voivat olla:
 - Roolit ja vastuut ovat linjassa organisaation riskienhallinta- ja hallinnointikehysten (governance) kanssa ja raportointilinjat mahdollistavat riippumattomuuden ja vaikutusmahdollisuudet.
 - Oikeus kyseenalaistaa päätöksiä ja eskaloida käyttäytymiseen liittyviä riskikysymyksiä ilman pelkoa vastatoimista tai asian vesittymisestä.
 - Riippumattomuus operatiivisesta johdosta ja suora yhteys ylimpään johtoon ja hallitukseen.
 - Pääsy useista lähteistä kerätyyn käyttäytymisriskiä koskevaan tietoon, joka on relevanttia, oikea-aikaista ja ristiinverrattua (trianguloitua) eri lähteiden välillä. Tämä tieto sisältää sekä strukturoitua dataa (kuten kyselytutkimusten tulokset ja toimintaohjeiden rikkomukset) että strukturoimatonta dataa (esimerkiksi ilmoituskanavan raportit ja kohderyhmäkeskusteluista saadut näkemykset). Tietolähteitä ovat henkilöstöhallinto (kuten työntekijöiden vaihtuvuus, pysyvyys ja kyselyaineistot), väärinkäytösten ilmoituskanavat, asiakasvalitukset ja tarkastushavainnot.
 - Data-analytiikan käyttö trendien, poikkeamien ja uusien, kehittymässä olevien riskien tunnistamiseksi.
 - Mittaristojen ja riski-indikaattoreiden käyttö johdon ja hallituksen raportoinnin tukena.
 - Organisaation tavoitteisiin sidottujen käyttäytymisriski-indikaattoreiden käyttö.
 - Toimintatapavirheiden ja kulttuurisen ristiriidan juurisyiden selvittäminen tai selvityksen ulkoistaminen.



- Käyttäytymiseen vaikuttavien muodollisten ja epämuodollisten tekijöiden tuntemus (esimerkiksi kannustimet, psykologinen turvallisuus ja johdon esimerkki).
 - Ylempien johtajien uskottavuus ja luottamus operatiivisten tiimien keskuudessa yhdistettynä kykyyn vaikuttaa päätöksentekoon reaaliajassa.
 - Aktiivinen osallistuminen henkilöstöhallintoon liittyvien kontrollien (kuten kannustimien, rekrytoinnin ja koulutuksen) suunnitteluun ja arviointiin.
 - Neuvonantajan rooli strategisissa muutosohjelmissa ja uudistushankkeissa.
 - Yhteistyö liiketoimintajohdon kanssa kulttuurin muovaamiseksi vaikuttamalla, ei vain pakottamalla.
 - Jatkuva datan kerääminen ja analysointi, johon voi sisältyä:
 - Henkilöstön sitoutuneisuus- ja työhyvinvointikyselyt.
 - Arvojen mukaisen toiminnan huomiointi- ja palkitsemisdata.
 - Whistleblowing- raportit ja valitukset.
 - Asiakaspalaute, jossa korostuu sekä tyytyväisyys että tyytymättömyys.
 - Suorituksenarvioinnit, jotka heijastavat yhteistyötä, integriteettiä ja innovointia.
 - Data-analytiikan käyttö haavoittuvuuksien tunnistamiseksi ja trendien havaitsemiseksi.
 - Selkeästi määritelty prosessi riskien ja organisaation tavoitteiden vastaisen toiminnan nopeaan eskalointiin.
 - Johdon toimintasuunnitelmien laadinnan ja toimeenpanon seuranta riskien käsittelemiseksi ja vaadittujen toimintatapojen vahvistamiseksi.
- B. Organisaatiokäyttäytymisen oikea-aikaisiin seurantaprosesseihin kuuluu tulosten raportointi sidosryhmille. Käyttäytymistä, juurisyitä ja seurauksia kuvaavia riski-indikaattoreita sekä raportoitavia poikkeamia ovat esimerkiksi:**
- Päätöksenteko: Toimivan kyseenalaistamisen puute tai eri näkökulmien riittämätön huomioon ottaminen.
 - Viestintä: Henkilöiden tekemien ilmoitusten puutteellinen huomiointi.
 - Yhteistyö: Siiloutuneet työympäristöt, joissa kukin keskittyy vain omaan työhönsä.
 - Puutteiden käsittely: Syllistäminen ja rankaiseminen tahattomista virheistä.
 - Viralliset ohjauskeinot: Epäselvät roolit ja vastuut tai ristiriitaiset tavoitteet.
 - Epäviralliset ohjauskeinot: Vähäinen psykologinen turvallisuus tai toimimaton dynamiikka kolmen linjan välillä.
 - Suoritusdata: Asiakasvalitusten suuri määrä tai innovoinnin tai digitalisaation pysähtyminen.
 - Henkilöstödata: Suuri henkilöstön vaihtuvuus ja poissaolot sekä alhainen tyytyväisyys kyselytutkimustuloksissa.



- Riski- ja oikeudellinen data: Suuri määrä investigaatioita, toimintaohjeiden vastaista toimintaa tai hälytyksiä sekä läheltä piti - tilanteita.
- c. Prosessit, joilla varmistetaan, että odotetun ja havaitun toiminnan väliset poikkeamat tunnistetaan ja ilmoitetaan tahoille, joilla on valtuudet ja kyky toimia. Sisäiset tarkastajat voivat tarkistaa, että:
 - Toimiva viestintä on oikea-aikaista ja tietoon perustuvaa ja perustuu juurisyiden ja taustatekijöiden analysointiin.
 - Viestinnän suunnittelulla ja käytännön toimivuudella vältetään näennäiset korjaukset, mainehaitat tai toistuvat virheet.
 - Tietoja kerätään ja yhdistetään useista eri lähteistä, kuten henkilöstökyselyistä, whistleblowing-raporteista, tarkastushavainnoista ja vaaratilanteiden selvityksistä.
 - Strukturoidut analyysitekniikat - kuten teematarkastukset, käyttäytymistieteelliset mallit ja juurisyiden analyysimallit - menevät pintapuolisia oireita pidemmälle ja paljastavat ristiriitojen taustatekijät (kuten epämääräiset palkitsemisjärjestelmät, matalan psykologisen turvallisuuden tai johdon puutteellisen sitoutumisen).
 - Havaittuja eroja ei raportoida vain sääntöjen noudattamatta jättämisinä tai yksittäisinä tapauksina, vaan tapahtumina, joiden toiminnalliset taustatekijät johtuvat organisaatiokulttuurin, rakenteiden ja johtamisen puutteista.
 - Viestinnässä tuodaan esiin, mitä tapahtui ja miksi, ja johtopäätösten tukena käytetään sekä määrällistä että laadullista dataa
 - Organisaatiossa pidetään erillään käyttäytymismallit, niiden vaikuttamista johtuvat haavoittuvuudet sekä organisaation tulokset (kuten tulosvaikutukset ja sidosryhmien luottamus), mikä mahdollistaa käyttäytymiseen ja sen juurisyihin puuttumisen. Tuloksista tiedotetaan oikeille vastaanottajille ja asianmukaisella tarkkuudella:
 - Operatiiviselle johdolle prosessin välittömiä korjaavia toimenpiteitä varten.
 - Ylimmälle johdolle resurssien kohdentamista, viestintää ja linjauksia varten.
 - Hallitukselle tai valiokunnille valvontaa ja strategista arviointia varten.
 - Visuaaliset ja kerronnalliset työkalut, kuten mittaristot, lämpökartat (heat map) tai tapaustiivistelmät, selittävät havainnot ja tukevat suosituksia ja/tai toimenpidesuunnitelmia.
 - Prosessien läpikäynneissä otetaan huomioon niiden vaikutus kokonaisriskitasoon sekä sisäisen valvonnan toimivuuteen.
 - Havaittujen erojen raportointi liitetään korjaaviin toimenpiteisiin, ja niiden valmistumista seurataan.
 - Toimenpiteiden tulokset arvioidaan ja jaetaan, mikä tukee yhteistä oppimista.
 - Viestintään ei kohdistu epäasiallista vaikuttamista, ja se noudattaa vahvistettuja eskalointikäytäntöjä, jolloin arviointien riippumattomuus ja uskottavuus säilyvät.



- D. Tavoitellun ja havaitun toiminnan väliset erot ratkaistaan jäsennellysti ja osallistavasti, millä varmistetaan, että korjaavat toimenpiteet perustuvat sidosryhmien näkemyksiin, niiden toteutumista seurataan ja niiden vaikuttavuus arvioidaan. Sisäiset tarkastajat voivat arvioida, että:
- Ongelmanratkaisuun osallistuvat ne tahot, joita asia koskee, kuten esimerkiksi linjajohto, HR, liikekumppanit, luottamushenkilöt, compliance-asiantuntijat sekä asianomaiset työntekijät tai tiimit. Heidän osallistumisensa avulla varmistetaan, että toimet ovat:
 - Asiayhteyteen sopivia: Huomioivat operatiiviset realiteetit ja epäviralliset normit, jotka ovat saattaneet vaikuttaa poikkeaman syntymiseen.
 - Uskottavia ja hyväksyttyjä: Saavat suuremmalla todennäköisyydellä kannatusta ja vakiintuvat osaksi arkea, jos toimet ovat niiden henkilöiden muovaamia, joita asia koskee.
 - Rakentavan kyseenalaistavia: Edistävät avointa keskustelua eri johtamistapojen vaikutuksista, sisäisen valvonnan rakenteiden heikkouksista tai ryhmädynamiikasta.
 - Sidosryhmien palautetta kerätään ja analysoidaan, ja se otetaan osaksi toimintasuunnitelmia. Palautteen keräämiseen voidaan käyttää haastatteluja, focus group -ryhmiä, kyselytyökaluja sekä muita menetelmiä.
 - Ratkaisut on dokumentoitu, ja niille on määritelty vastuutaho, aikataulu ja tavoitteet:
 - Toimenpiteet ovat oikeassa suhteessa ongelman vakavuuteen nähden.
 - Tarvittaessa toimenpiteet kohdistetaan sekä virallisiin ohjauskeinoihin (kuten toimintaperiaatteisiin ja palkitsemiseen) että epävirallisiin tekijöihin (kuten psykologiseen turvallisuuteen ja ryhmädynamiikkaan).
 - Jos ratkaisu vaatii useamman toiminnon yhteistyötä (esim. HR koulutusten osalta ja riskienhallinta valvontarakenteiden osalta), toimintojen välinen toteutus ja vastuunjako koordinoidaan ja sovitaan selkeästi.
 - Edistymistä seurataan loppuun asti, jolloin varmistetaan sovittujen asioiden toteutuminen ja ylläpito. Tämä sisältää:
 - Toimintatapaan liittyvien ongelmien ja toimenpidesuunnitelmien rekisterin ylläpidon.
 - Säännölliset seurantalaverit toimenpiteiden vastuutahojen kanssa tilanteen todentamiseksi.
 - Viivästysten, osittaisten toteutusten tai vastustuksen eskaloinnin asianmukaisille hallinto- tai valvontafoorumeille.
 - Ratkaisujen toimivuus arvioidaan sen perusteella, onnistuivatko ne korjaamaan ongelman ja pienentämään toimintatapoihin liittyvää riskiä. Tämä voi sisältää:
 - Toimintatapoihin liittyvien riskimittareiden uudelleenarvioinnin toimenpiteiden toteuttamisen jälkeen.



- Palautteen keräämisen kohderyhmiltä havaituista muutoksista.
- Toimintatapojen muutoksen todentamisen havainnoimalla, kyselytutkimuksilla tai tarkastusmenetelmillä.
- Toimenpiteiden muuttamisen tai tukitoimien lisääminen silloin, kun tulokset jäävät heikoiksi tai epäselviksi.

Valvontaprosessia koskevia näkökohtia

Arvioidakseen, miten valvontaprosesseja sovelletaan vähentämään riskiä siitä, että organisaation toiminta ei ole linjassa organisaation tavoitteiden kanssa, sisäiset tarkastajat voivat tarkastaa:

- A. Toimintatapariskien arvioinnit, joilla selvitetään nykyisen organisaatiokäyttäytymisen aiheuttamat riskit (eli mahdolliset tahattomat seuraukset siitä, miten asioita tehdään). Esimerkkejä tällaisista arvioinneista ovat projektien arvioinnit niiden valmistumisen jälkeen, juurisyyanalyysit ja yksityiskohtaiset käytännön toiminnan tarkastelut.
- B. Strukturoidut palauteprosessit, joiden avulla ymmärretään, mitä mekanismeja johto käyttää käyttäytymisodotusten viestintään (esimerkiksi henkilöstön infotilaisuudet, sähköpostit sekä työntekijöiden ja heidän esihenkilöidensä väliset tapaamiset) ja miten johdon esimerkki vaikuttaa käyttäytymiseen organisaatiossa. Tämä voidaan tehdä arvioimalla prosesseja, joilla kerätään ja analysoidaan työntekijöiden käsityksiä ja ymmärrystä hallituksen ja ylimmän johdon viesteistä. Sisäiset tarkastajat voivat auttaa organisaatioita jatkuvasti kehittämään viestintästrategioitaan ja varmistaa, että johdon näyttämä esimerkki välittyy tehokkaasti kaikille tasoille, arvioimalla seuraavia keskeisiä kontroleja:
 - Säännölliset työntekijäkyselyt, haastattelut ja kohderyhmäkeskustelut, joissa selvitetään johdon viestinnän selkeyttä, johdonmukaisuutta ja vaikutusta ja joista saadaan määrällistä ja laadullista tietoa siitä, miten hyvin viestit otetaan vastaan ja ymmärretään organisaation eri tasoilla.
 - Avoimet kanavat anonyymille palautteelle, jotta työntekijät voivat kertoa rehellisesti mielipiteensä ilman pelkoa vastatoimista. Näitä kanavia tulisi toteuttaa digitaalisilla alustoilla, jotka mahdollistavat reaaliaikaisen palautteen ja ehdotusten antamisen. Näistä kanavista saatua tietoa tulisi analysoida sen tarkistamiseksi, ymmärtävätkö työntekijät hyvin ”tone at the top:n” organisaation kaikilla tasoilla.
 - Ylimmän johdon kokouksista kerätään palautetta kyselyjen, haastattelujen, kohderyhmien, pöytäkirjojen ja anonyymien kanavien avulla, jotta varmistetaan, että ylin johto on tietoinen tehottomasta viestinnästä, väärinkäsityksistä tai kehityskohteista. Ylin johto osoittaa arvostavansa työntekijöiden näkemyksiä vastaamalla aktiivisesti palautteeseen ja toimimalla sen mukaisesti. Jos näin ei tapahdu, työntekijät ei välttämättä anna palautetta, koska he uskovat, että asiat eivät muutu.
 - Ylimmän johdon toiminnasta saatu palaute integroidaan osaksi heidän tulos- ja kehityskeskustelujaan, jotta johdon ohjeistusten vastaanottamista voidaan seurata



jatkuvasti. Tämä vahvistaa johdon viestien tärkeyttä ja varmistaa, että ne näkyvät päivittäisessä toiminnassa.

- c. Organisaatiossa kannustetaan asioiden eteenpäin vientiä (eskalointia) riskien varhaiseksi tunnistamiseksi ja vähentämiseksi sekä psykologisesti turvallisen ympäristön luomiseksi, jossa työntekijät uskaltavat ilmoittaa ongelmista ilman vastatoimien pelkoa. Sisäiset tarkastajat voivat arvioida keskeisiä kontrolleja ja auttaa tehostamaan riskienhallintaa, kuten:
- Helppokäyttöiset palautemekanismit, mukaan lukien suora raportointi ja anonyymit vaihtoehdot, sisäiset ja ulkoiset väärinkäytösten ilmoituskanavat (whistleblower-hotlinet), kyselyt, aloitelaatikot ja digitaaliset alustat, jotka mahdollistavat luottamuksellisen raportoinnin ja sellaisten ongelmien tunnistamisen, joita työntekijät saattavat epäröidä ottaa esille avoimesti.
 - Selkeästi määriteltyt ja helposti ymmärrettävät prosessit ongelmien raportoimiseksi, sisältäen useita suoria ja anonyymejä sisäisiä ja ulkoisia kanavia, sekä toimet työntekijöiden tietoisuuden edistämiseksi. Raportointikanavien ominaisuuksiin tulisi kuulua:
 - Luottamuksellisuuden takaaminen, jolla suojataan ongelmista ilmoittavien henkilöiden henkilöllisyyttä.
 - Tiukat vastatoimien kieltävät käytännöt, joista viestitään selkeästi ja joita noudatetaan johdonmukaisesti ongelmista ilmoittavien henkilöiden suojelemiseksi.
 - Yhteydenpito henkilöihin, jotka eivät ilmoita ongelmista anonyymisti, syystä tai lopputuloksesta riippumatta.
 - Säännölliset koko organisaation kattavat yhteenvedot aiemmin ilmoitetuista ongelmista ja niiden lopputuloksista sen osoittamiseksi, että ongelmiin puututaan ja niistä raportoidaan, sekä varmistetaan avoimuus palautteen perusteella tehdyistä toimenpiteistä.
 - Johdon säännöllinen viestintä, jossa korostetaan avoimen viestinnän ja ongelmista ilmoittamisen tärkeyttä ja osoitetaan, miten johto itse toimii esimerkillisesti.
 - Säännölliset koulutustilaisuudet, joissa korostetaan psykologisen turvallisuuden merkitystä, rohkaistaan henkilöitä ilmoittamaan ongelmista ja annetaan ohjeita siitä, miten asiat voidaan eskaloida asianmukaisesti. Koulutus tulee toistaa säännöllisesti, jotta haluttu toimintatapa vahvistuu ajan myötä.
 - Vapaamuotoinen huomiointi, kuten suullinen tai kirjallinen kiitos ja julkinen tunnustus, ongelmista ilmoittaville henkilöille.
 - Eskalointiprosessin säännölliset arvioinnit sen vaikuttavuuden ja tehokkuuden varmistamiseksi, mukaan lukien työntekijöiden palautteen pyytäminen raportoinnin esteiden tunnistamiseksi ja niiden pikaiseksi käsittelymiseksi.
 - Viestintä palautteen käsittelyn lopputuloksesta.



- D. Kannustin- ja sanktio-ohjelmat ovat yhdenmukaisia organisaation halutun toimintatavan ja organisaation tavoitteiden kanssa, ja niistä tiedotetaan. Sisäiset tarkastajat voivat arvioida esimerkiksi seuraavia kontrolleja:
- Kannustimet - sekä rahalliset (esimerkiksi bonukset, ylennykset) että muut kuin rahalliset (esimerkiksi tunnustukset, kehittymismahdollisuudet) - ovat yhdenmukaisia organisaation tavoitteiden kanssa, ja ne on liitetty haluttujen toimintatapojen noudattamiseen.
 - Tasapainoiset suorituksen arviointikriteerit sisältävät, miten tavoitteet saavutetaan (esimerkiksi yhteistyö, integriteetti ja asiakaskeksisyys), sekä perinteisempiä tulostittareita (kuten taloudelliset tavoitteet).
 - Kannustinkriteerit ja sanktorajat on määritelty selkeästi, niitä sovelletaan johdonmukaisesti ja johto tai henkilöstöhallinto arvioi ne puolueellisuuden ja tahattomien seurausten välttämiseksi.
 - Monialaiset työryhmät varmistavat, että kannustinpäätökset ovat johdonmukaisia ja oikeudenmukaisia kaikissa liiketoimintayksiköissä.
 - Sopimattoman ja arvomaailman vastaisen toiminnan seuraukset sisältävät selkeitä ja oikeasuhteisia sanktioita (esimerkiksi bonusten leikkauksia ja ylennyskieltoja), ja toimenpiteet perustellaan sekä dokumentoidaan avoimuuden varmistamiseksi.
 - Aineeton huomiointi tuo esiin työntekijöitä, jotka toimivat esimerkillisesti yrityskulttuurin arvojen mukaisesti eettisessä päätöksenteossa ja psykologisen turvallisuuden edistämiseksi.
 - Kannustinohjelmien vaikutuksia arvioidaan säännöllisesti työntekijäpalautteen ja käyttäytymistä kuvaavien mittareiden avulla palkitsemismekanismien tarkentamiseksi tai tasapainottamiseksi. Kannustinohjelmia tulisi arvioida ja muuttaa seuraavien asioiden varmistamiseksi:
 - Tavoitteet eivät ole liian suppeat eivätkä liian laajat.
 - Tavoitteet ovat saavutettavissa.
 - Lyhyen aikavälin tavoitteet eivät heikennä pitkän aikavälin tuloksia.
 - Hyväksyttävät riskinottotasot on määritelty selkeästi.
 - Kontrolleja on otettu käyttöön, jotta varmistetaan eettinen käyttäytyminen samalla kun saavutetaan tavoitteet (esimerkiksi johtajat eettisen käyttäytymisen roolimalleina, vilpin kustannukset ovat paljon suuremmat kuin siitä saatava hyöty sekä vahva valvonta).
 - Tavoitteet on räätälöity yksilöllisten kykyjen ja olosuhteiden mukaan oikeudenmukaisuus säilyttäen.
 - Ryhmän tavoitteet eivät ole ristiriidassa yksilön tavoitteiden kanssa.
 - Sisäistä motivaatiota arvioidaan, ja johto tunnistaa, että jotkin tavoitteet voivat heikentää sisäistä motivaatiota.



- Organisaation päämäärät otetaan huomioon, ja tavoitteen (esimerkiksi suoritus- tai oppimistavoite) soveltuvuus arvioidaan.
- Organisaatio yhdistää positiivisen vahvistamisen ja korjaavat toimenpiteet edistääkseen organisaatiokäyttäytymistä, joka on yhdenmukainen organisaation tavoitteiden ja sääntelyvaatimusten kanssa. Keskeisten kontrollien (avainkontrollien) tulisi sisältää:
 - Arvioidaan säännöllisesti viestinnän ja koulutusohjelmien toimivuutta, jotta varmistetaan, että työntekijät ymmärtävät ongelmien ilmoittamisen tärkeyden ja sääntöjen laiminlyönnin seuraukset sekä kokevat saavansa kannustusta ongelmien ilmoittamiseen.
 - Seuranta- ja raportointijärjestelmät seuraavat sääntöjen noudattamista ja tunnistavat mahdollisia epäkohtia aliraportoinnissa.
 - Ohjaustoimenpiteitä sovelletaan johdonmukaisesti ja oikeudenmukaisesti, eivätkä ne ole niin ankaria, että ne vähentäisivät ilmoitusten tekemistä, eivätkä niin lieviä, että ne eivät estäisi epäeettistä käyttäytymistä.
 - Palautekanavia, joiden avulla työntekijät voivat ilmoittaa ongelmista anonyymisti, arvioidaan säännöllisesti sen varmistamiseksi, että ne toimivat ja kannustavat rehelliseen raportointiin.
- E. Organisaation ongelmanhallintaprosessi tunnistaa organisaation tavoitteiden kanssa ristiriidassa olevat käyttäytymismallit ja eskaloi ne tarvittaessa, jotta voidaan laatia toimenpidesuunnitelma heikkojen tulosten riskin pienentämiseksi. Sisäiset tarkastajat voivat arvioida keskeisiä kontrolleja, jotka tavoittelevat tehokasta käyttäytymisen muutosta, kuten:
 - Näyttöön perustuvat toimintatavat: Toimenpidesuunnitelma sisältää näyttöön perustuvia toimintatapoja käyttäytymisen muuttamiseksi, ja se perustuu käyttäytymistieteeseen, käyttäytymismalleihin sekä muutoksenhallintaan. Jos lähestymistapa ei nimenomaisesti perustu tiettyyn käyttäytymisen muutosmalliin, lähestymistavassa tulisi yhdistää toimenpiteitä, jotka koskevat seuraavia asioita:
 - Viestintä: Lisätään jatkuvasti työntekijöiden ja johdon tietoisuutta käyttäytymismuutoksen välttämättömyydestä sekä muutoksen omaksumisesta ja tukemisesta.
 - Työntekijöiden koulutus ja kehittäminen: Investoidaan eri rooleille räätälöityihin koulutusohjelmiin ja varmistetaan työntekijöiden tarvitsema osaaminen ja toimintatavat työpajojen, verkko-oppimisen ja kehittymismahdollisuuksien avulla. Tämä sisältää uuden osaamisen ja sellaisten käyttäytymismallien oppimisen ja kyvyn ottaa ne tehokkaasti käyttöön, joita organisaation tavoittelemien muutosten saavuttaminen edellyttää.
 - Johtamisen kehittäminen: Johtajat pohtivat kaikilla organisaation tasoilla, miten he voivat edistää ja osoittaa käyttäytymisen muutoksia jokapäiväisissä tilanteissa. Tähän voi kuulua, että johto muuttaa omaa käyttäytymistään niin, että henkilöstön on helpompi ottaa käyttöön uusia toimintatapoja, pyytää



työntekijöitä suoraan toteuttamaan uusia käyttäytymismalleja sekä kannustaa oppimiseen ja pyytämään koulutusta vielä tarvittavista taidoista ja käyttäytymismalleista. Johtamiskoulutus ja valmennus voivat kehittää taitoja ja itseluottamusta.

- Johdonmukainen vahvistaminen arjessa: Henkilöt tarvitsevat tukea, kannustusta ja säännöllisiä muistutuksia kehittääkseen uusia toimintatapoja ja integroidakseen ne päivittäisiin työtapoihinsa.
 - Yhdenmukainen vahvistaminen: Toimenpideohjelman tulisi olla yhdenmukainen johdon viestinnän, prosessien, järjestelmien, valmennuksen ja epävirallisten palautekanavien kanssa, jotta se tukee tavoiteltua muutosta. Yhdenmukaisuus poistaa epävarmuutta ja hämmennystä ja varmistaa, että työntekijät ymmärtävät toivotut käyttäytymismuutokset, miten ne otetaan käyttöön ja miksi ne ovat tärkeitä.
 - Käyttäytymisen juurisyihin vaikuttaminen: Pysyvä käyttäytymisen muutos edellyttää, että käsitellään käyttäytymisen taustalla olevia vaikuttimia (ks. Riskienhallinta, C) eikä keskitytä vain itse käyttäytymiseen.
 - Mittaaminen: Toimenpiteiden edistymisen ja tehokkuuden mittaaminen auttaa määrittämään, saavutetaanko niillä toivottu vaikutus ja tarvitaanko muutoksia. Säännölliset tilannekatsaukset toimivat myönteisenä vahvistuksena ja antavat sidosryhmille tietoa edistymisestä. Tehokas mittausmenetelmä yhdistää laadulliset ja määrälliset menetelmät, kuten kyselyt ja haastattelut, minkä avulla saadaan kokonaisvaltainen kuva edistymisestä.
- F. Koulutusohjelmat, joiden tarkoituksena on vaikuttaa käyttäytymiseen, liittyvät nimenomaisesti määriteltyihin käyttäytymisodotuksiin tai riskinottohalukkuutta koskeviin lausumiin. Esimerkkejä koulutusaiheista ovat eettisyys, sääntöjen noudattaminen (compliance), johtajuus, osallisuus (inclusion), riskitietoisuus ja päätöksenteko. Sisäiset tarkastajat voivat tarkastaa, että koulutusohjelmat:
- Vastaavat toivottua toimintatapaa ja asenteita sekä sisältävät selkeät, dokumentoidut oppimistavoitteet.
 - Perustuvat käyttäytymisestä saatavaan tietoon tai vaaratilanteista oppimiseen (esimerkiksi tarkastushavainnot, juurisyyanalyysit ja palautekanavat).
 - Toimitetaan kaikille relevanteille tehtäväryhmille, ja moduulit on räätälöity erikseen ylimmälle johdolle, esihenkilöille sekä henkilöstölle.
 - Ovat pakollisia soveltuvilta osin (esimerkiksi korkean riskin prosessit, säännellyt vastualueet ja valvontaroolit).
 - Päivitetään säännöllisesti, ja sisältö arvioidaan vähintään vuosittain, jotta voidaan varmistaa sen ajantasaisuus ja tehokkuus.
 - Tarkoituksena on:
 - Sisältää käytännön tilanteita tai esimerkkejä, jotka havainnollistavat odotettua käyttäytymistä.



- Aktivoida osallistujia erilaisten keinojen, kuten tarinoiden ja ajatuksia herättävien haastavien kysymysten avulla.
- Sitouttaa ylin johto näyttämään suuntaa ("tone at the top") ja innostaa työntekijöitä muuttamaan käyttäytymistään.
- Kattaa vaikutusten ja varmennuksen kontrolleja, jotka:
 - Seuraavat pakollisen koulutuksen suorittamista ja raportoivat poikkeuksista.
 - Arvioivat käyttäytymismuutoksia ja oppien sisäistämistä vapaamuotoisilla kyselyillä, yksinkertaisilla testeillä tai käytännön havainnoinnin avulla.
 - Kartoittavat osallistujien kokemuksia ja koulutuksen tehoa selkeiden palautekäytäntöjen avulla.
 - Varmistavat, että koulutuksen sisältö on yhdenmukainen riskiitekehysten ja kontrollivaatimusten kanssa, ja että niihin sisältyy virallinen katselmointi- ja hyväksyntä (sign-off) prosessi.
- G. Rekrytointiprosessit vastaavat organisaation käyttäytymisodotuksia ja sisältävät käyttäytymiseen liittyvää osaamista. Sisäiset tarkastajat voivat arvioida esimerkiksi seuraavia kontrolleja:
 - Työkaluja, joilla arvioidaan hakijoiden sopivuutta organisaation arvoihin, mukaan lukien jäsennellyt haastattelurungot ja tilannekohtaiset kysymykset.
 - Käyttäytymistä arvioivia haastatteluja ja vertaispalautetta, joita käytetään empatian, eettisen harkintakyvyn ja vastuuntunnon tarkasteluun.
 - Rekrytointi-ilmoitukset ja työnantajamielikuva ilmentävät organisaation tavoitekulttuuria, jotta voidaan houkutella oikeanlaisia osaajia.
 - Palautekanavien avulla seurataan uusien työntekijöiden sopeutumista yrityskulttuuriin, mikä auttaa puuttumaan haasteisiin ajoissa.
 - Kattava dokumentointi, kuten pisteytysmallit ja haastattelumuistiinpanot, osoittavat, että henkilövalinnat perustuvat yhtenäisiin ja johdonmukaisiin rekrytointikriteereihin.
 - Henkilöstöhallinto ja ylin johto seuraavat rekrytointikäytäntöjä tunnistaakseen riskejä, kuten suosimista, puolueellisuutta tai organisaation toimintatapojen vastaista toimintaa.
 - Rekrytointi- ja ylennyskäytäntöjä arvioidaan säännöllisesti, jotta ne vastaavat organisaation arvoja ja toimivat tehokkaasti käytännössä.



Liite A. Käytännön esimerkkejä

Seuraavissa esimerkeissä kuvataan tilanteita, joihin organisaatiokäyttäjymisen aihealueen vaatimusta olisi sovellettava.

Esimerkki 1: Organisaation toimintatapakehysten itsenäinen arviointi

Sisäinen tarkastus teki erillisarvioinnin organisaation toimintatapakehyksestä. Tavoitteena oli tarkastella sen rakennetta ja toimivuutta käyttäytymisriskien hallinnassa. Toimeksianto kattoi hallintorakenteet, riskienhallintatoimenpiteet ja toimintatapakontrollit, jotka luovat pohjan koko organisaation yhtenäisyydelle.

Sisäiset tarkastajat arvioivat, oliko toimintatapojen valvontavastuut määritelty selkeästi ja olivatko ne vapaita eturistiriidoista. Tiimi arvioi hallituksen työjärjestyksen ja varmisti, että hallitus oli saanut säännöllistä raportointia käyttäytymisriski-indikaattoreista, kuten kyselyjen tuloksista ja speak-up-(eettinen ilmoituskanava) trendeistä. Arviointi sisälsi sen, päivitettiinkö ja toimeenpantiinko kulttuuriin liittyviä toimintaperiaatteita, kuten ilmoituskanavia (whistleblowing) ja eettistä toimintatapaa koskevia ohjeistuksia, säännöllisesti.

Sisäiset tarkastajat arvioivat myös riskienhallinnan osa-alueita lähtien liikkeelle toisen linjan ylläpitämisestä käyttäytymisriskien hallintakehyksestä, ja keskittyivät siihen, tunnistettiinkö siinä keskeiset käyttäytymisriskin aiheuttajat (kuten alhainen psykologinen turvallisuus tai ristiriitaiset tulostavoitteet). Arvioinnissa painotettiin sitä, miten organisaatio seurasi ja käsitteli odotetun ja havaitun käyttäytymisen välistä eroa, mukaan lukien se, eskaloitiinko ja käsiteltiinkö käyttäytymisen poikkeavuudet järjestelmällisesti.

Kontrolliympäristö tarkastettiin sen selvittämiseksi, tukivatko muodolliset prosessit toimintatapaodotuksia. Tarkastajat kartoittivat arvopohjaiseen arviointiin liittyviä rekrytointikäytäntöjä, perehdytysprosessin vastaavuutta organisaatiokulttuurin normien kanssa sekä sitä, missä määrin kannustimien (sekä rahallisten että ei-rahallisten) tahattomia seurauksia oli arvioitu. Lisäksi testattiin koulutusohjelmat, speak-up-ilmoituskanavat, johdon viestintä sekä data-analytiikkaa, jota käytettiin käyttäytymiseen liittyvien huolenaiheiden havaitsemiseen.

Toimeksianto antoi kattavan kuvan siitä, miten käyttäytymisriskejä hallitaan organisaatiotasolla, ja sen perusteella suositeltiin parannuksia organisaation toimintataparakenteeseen.

Esimerkki 2: Kannustinkäytäntöjen teemallinen arviointi

Tarkastustoimeksiannossa keskityttiin arvioimaan, miten organisaation kannustinjärjestelmät vaikuttavat käyttäytymiseen ja ovatko ne yhdenmukaiset organisaation tarkoituksen, arvojen ja sääntelyyn liittyvien odotusten kanssa. Sisäinen tarkastus valitsi tämän teeman, koska huoli väärinkäytösriskeistä on kasvanut ja liiketoimintayksiköissä on havaittu merkkejä paineen alla toimimisesta.



Tarkastus aloitettiin arvioimalla hallintomallit ja -menettelyt, joiden mukaisesti palkitsemisjärjestelmät suunnitellaan ja hyväksytään. Sisäinen tarkastus selvitti, kuuluuko kannustimien suunnittelun muodollinen valvonta hallintomallin päätöksiä toimeenpaneville tahoille, kuten henkilöstöhallinnolle tai palkitsemisvaliokunnalle. Samalla arvioitiin, olivatko nämä prosessit riskinhallinnan, complianceen tai sisäisen tarkastuksen riippumattoman arvioinnin kohteena.

Riskienhallinnan näkökulmasta selvitettiin, huomioitiinko kannustinjärjestelmien kehittämisessä niiden vaikutukset ihmisten käyttäytymiseen. Sisäiset tarkastajat selvittivät, oliko organisaatio testannut eri skenaarioita tai analysoinut palkitsemisjärjestelmiinsä liittyviä käyttäytymisriskejä. Lisäksi he arvioivat, seurattiinko toimintatapoja kuvaavia KPI (tulos) -mittareita – kuten yhteistyön tuloksia – ja hyödynnettiinkö niitä kokonaisarvioinnissa.

Valvontatoimenpiteiden testaus sisälsi erilaisia menetelmiä, joilla pyritään muokkaamaan palkitsemiseen liittyviä toimintatapoja. Näihin kuuluivat tasapainotetut mittaristot (Balanced Scorecard), jotka sisälsivät sekä saavutuksia että toimintatapoja mittaavia suorituskriteereitä, malus-(palkkion menettäminen tai pienentäminen) ja takaisinperintäehtojen (clawback) soveltaminen sekä 360-asteen palautteet. Sisäiset tarkastajat selvittivät myös, miten esihenkilöitä on koulutettu antamaan palautetta toimintatavoista, ja arvioitiin aineettomia palkitsemismalleja, joilla huomioidaan arvojen mukainen käytös.

Tarkastuksen aikana sisäiset tarkastajat pyrkivät tunnistamaan, voivatko kannustinkäytännöt tahattomasti johtaa epäsuotavaan toimintaan, kuten liialliseen riskinottoon, säännöistä joustamiseen tai haluttomuuteen tuoda ongelmia esiin (eskaloida). Suosituksilla pyritään lisäämään läpinäkyvyyttä, sitomaan arvopohjaiset tavoitteet tiiviimmin osaksi kokonaisuutta sekä vahvistamaan toisen linjan riippumatonta valvontaa palkitsemismallien suunnittelussa.

Esimerkki 3: Yhdistäminen osaksi perinteistä tarkastusta - kyberriskien hallinta

Tässä esimerkissä käyttäytymisriskien tarkastelu yhdistettiin osaksi perinteistä kyberriskien hallinnan arviointia. Koska monet kyberhäiriöt johtuvat teknisten ongelmien lisäksi myös ihmisten käyttäytymisestä, sisäiset tarkastajat sisällyttivät käyttäytymisen arvioinnin osaksi koko toimeksiantoa.

Tarkastus aloitettiin selvittämällä, kuinka laajasti käyttäytymisriskit oli otettu huomioon kyberresilienssin hallintomallissa (governance). Sisäiset tarkastajat arvioivat hallituksen ja ylimmän johdon kyberstrategian valvontaa ja etsivät näyttöä siitä, seurasivatko ja keskustelivatko nämä toimielimet siitä, vastaako työntekijöiden käyttäytyminen – kuten turvallisten toimintatapojen noudattaminen tai johdon oma esimerkki turvallisesta käyttäytymisestä – organisaation tavoitteita.

Tiimi arvioi riskienhallinnan osalta huomioitiinko organisaation kyberriskiarvioissa inhimilliset tekijät (human factors). Samalla selvitettiin, hyödynnetäänkö käyttäytymistä kuvaavaa dataa – esimerkiksi tietojenkalastelutestien epäonnistumisia, järjestelmien luvattomia käyttöyrityksiä tai alhaisia koulutusmääriä – riskien seurannassa ja eskaloinnissa. Lisäksi tutkittiin, oliko tietoturvaloukkausten juurisyöt analysoitu sellaisten käyttäytymismallien tunnistamiseksi, kuten epäselvät vastuut tai johdon näyttämä esimerkki, jotka ovat voineet myötävaikuttaa tapahtumiin.



Kontrollitestaus keskittyi käyttäytymismallien muotoiluun ja turvallisiin toimintatapoihin. Sisäiset tarkastajat arvioivat, sisältyikö käyttäytymisen arviointi (behavioral screening) sellaisten tehtävien rekrytointiprosesseihin, joissa on laajennetut oikeudet (privileged access). Palkitsemisjärjestelmiä arvioitiin sen selvittämiseksi, ohjaavatko ne turvallisiin toimintatapoihin verkossa vai suosivatko ne epähuomiossa riskinottoa turvallisuuden kustannuksella. Lisäksi arvioitiin, oliko kyberturvakoulutus osallistavaa ja säännöllisesti päivitettyä sekä sisälsikö se simulaatioita, joilla testataan henkilöstön toimintaa käytännön tietojenkalastelu- ja huijaustilanteissa.

Lopuksi selvitettiin, miten johto edistää tietoturvallista käyttäytymistä viestinnällään ja uskaltaako henkilöstö ilmoittaa havaitsemistaan kyberturvallisuusriskeistä tai vaaratilanteista. Avointa puheeksiottamista (speak up) tukevan organisaatiokulttuurin katsottiin olevan ratkaiseva tekijä resilienssin edistämisessä.

Inhimillisten tekijöiden huomioiminen kyberturvallisuuden tarkastuksessa tuotti syvällistä tietoa ja käytännön suosituksia. Tämä paransi organisaation kykyä hallita riskejä yhdellä sen kaikkein kriittisimmistä osa-alueista.



Liite B. Esimerkkejä tehdyistä tarkastuksista

Esimerkki 1: Asuntoministeriö (julkinen sektori)

Esimerkit osoittavat, miten valtion viraston sisäinen tarkastus soveltaisi organisaatiokäyttäytymistä koskevaa aihekohtaista vaatimusta (Organizational Behavior Topical Requirement) arvioidakseen, kuinka virasto täyttää tavoitteensa tarjota kansalaisille yhdenvertaisia asumispalveluja. Sisäisten tarkastajien tulisi huomioda, että virkamiesten painotukset, poliittiset tekijät, määrärahojen jako sekä osa poliittisista valinnoista eivät kuulu sisäisen tarkastuksen toimivaltaan. Sen sijaan tarkastuksen toimivaltaan kuuluu selkeästi se, miten ylemmät virkamiehet ja johtajat tulkitsevat ja soveltavat näitä toimintaperiaatteita, sekä viraston sisäinen kulttuuri.

Hallinto

- A.** Roolit ja vastuut – Organisaatorakenne on selkeä, ja siinä on erotettu toimintaperiaatteiden suunnittelu (ylin johto) ja käytännön asuntopalveluiden järjestäminen. Sisäisen tarkastuksen toimeksiannon yhtenä tavoitteena on selvittää, onko rakenteelliset eturistiriidat vältetty: onko esimerkiksi vastuu sääntöjen noudattamisesta erotettu urakoitsijoiden valvonnasta?
- B.** Vastuut – Organisaation johdon tulostavoitteet on sidottu toimintakulttuuria kuvaaviin mittareihin, kuten asuntojen jakamisen oikeudenmukaisuuteen ja henkilöstön hyvinvointiin. Sisäinen tarkastus arvioi, toteutuvatko vastuut käytännössä ja onko ne sisäistetty organisaatiossa.
- C.** Valvonta ja seuranta – Johtoryhmätasoisesti vedettävä toimintakulttuurityöryhmä käsittelee neljännesvuosittain henkilöstötutkimusten tuloksia, väärinkäytösepäilyjä sekä sidosryhmiltä saatua palautetta. Sisäiset tarkastajat arvioivat, toimivatko nämä menettelyt varhaisen varoituksen signaaleina, jos toimintatavat alkavat poiketa organisaation arvoista.
- D.** Toimintaperiaatteet ja menettelytavat – Organisaatiossa on käytössä asianmukaisesti vahvistetut eettiset säännöt, asuntojen jakamista koskevat ohjeet ja eturistiriitoja koskevat rekisterit, ja niitä päivitetään säännöllisesti (esimerkiksi vähintään puolivuositain). Sisäinen tarkastus arvioi, onko päivityksissä huomioitu asumispalvelujen aiemmat kriisit ja julkisista tarkastusraporteista saadut opit.

Riskienhallinta

- A.** Käyttäytymisriskien viitekehys - Yksikkö tunnistaa toimintakulttuuriin liittyviä riskejä, jotka voivat vaikuttaa julkisten palvelujen ohjelmien toteuttamiseen. Tällaisia ovat esimerkiksi suosinta asuntotarjonnassa, liiallinen byrokratia tai työntekijöiden



haluttomuus kyseenalaistaa viranomaisten ohjeita. Sisäinen tarkastus varmistaa, että nämä riskit kirjataan virallisesti riskirekisteriin, että johto käsittelee ne ja että tarvittaessa ryhdytään toimenpiteisiin.

- B.** Indikaattorit ja analytiikka – Mittaristoilla (dashboard) seurataan käyttäytymiseen liittyvää dataa, kuten henkilöstön vaihtuvuutta, työtyytymättömyyttä, vuokralaisten ja yleisön tekemien epävirallisten valitusten määrää sekä reagoitua tietopyyntöihin tai julkisuuslakia koskeviin pyyntöihin. Tarkastajat arvioivat, ovatko indikaattorit ja analyysit luotettavia ja keskustellaanko niistä virastossa.
- C.** Poikkeamien hallinta – Kun eroja ilmenee (esimerkiksi whistleblowing-tapaukset, joissa on havaittu poikkeamia oikeudenmukaisuusperiaatteista), ne eskaloitetaan ylimmälle johdolle. Sisäiset tarkastajat varmistavat, johtaako poikkeama-analyysi korjaaviin toimenpiteisiin.
- D.** Sidosryhmien näkemysten hyödyntäminen ratkaisussa – Toimivaltaisia viranomaisia, asuntoyhdistyksiä, ammattiliittoja ja kansalaisryhmiä kuullaan, kun havaitaan toimintakulttuuriin liittyviä ongelmia (kuten asiakaspalveluhenkilöstön epäkohteliasta käytöstä tai puolueellisuutta asuntojen jaossa). Sisäiset tarkastajat varmistavat, että sidosryhmien palaute vaikuttaa ratkaisusuunnitelmiin.

Kontrollit

- A.** Käyttäytymisriskien tarkastelu – Jälkikäteisarviointeja tehdään asuntoprojektien epäonnistumisten jälkeen (esimerkiksi sosiaalisen asuntotuotannon rakentamisen viivästykset). Tarkastajat varmistavat, arvioidaanko käyttäytymisen juurisyitä (kuten huonoa yhteistyötä tai syyttelykulttuuria).
- B.** Organisaatiokulttuurin johtaminen – Ylin johto viestii oikeudenmukaisuutta, puolueettomuutta ja palvelun laatua koskevista odotuksista henkilöstöinfon ja intranet-videoiden välityksellä. Sisäiset tarkastajat varmistavat, että nämä odotukset tunnetaan ja toteutetaan.
- C.** Eskalaatiomenettelyt – Osasto tarjoaa whistleblower-kanavaa ja valitusprosessia vuokralaisille, henkilöstölle ja yleisölle. Sisäiset tarkastajat tarkastavat raportoinnin oikea-aikaisuutta, luottamuksellisuutta sekä näyttöä siitä, ettei ilmoituksista seuraa vastatoimia.
- D.** Palkitseminen – Suorituksen arvioinnissa korostetaan henkilöstön yhteistyötä, sidosryhmien osallistamista ja oikeudenmukaista vuokralaisten kohtelua. Sisäiset tarkastajat arvioivat, tukevatko ylennykset ja palkitseminen tätä toimintaa.
- E.** Käyttäytymisen seuranta – Esimiehet arvioivat henkilöstön toimintatapoja (integriteetti, empatia haavoittuvassa asemassa olevia vuokralaisia kohtaan) vuotuisessa kehityskeskustelussa. Sisäiset tarkastajat selvittävät, ovatko tulokset yhdenmukaisia ja puututaanko huonoon käytökseen.
- F.** Koulutus – Pakolliset kurssit kattavat tiedostamattomat ennakkoluulot, konfliktien ratkaisun ja eettisen päätöksenteon asunnonhaussa. Sisäiset tarkastajat varmistavat, että koulutusten läpimenoprosentit ovat korkeita ja arvioivat koulutusten jälkeisten kyselyjen tuloksia.



- G. Korjaustoimenpiteet - Kun havaitaan toimintakulttuurin rikkomuksia (kuten asuntojen jonotuslistojen manipulointi), tehdään juurisyyanalyyskejä ja seurataan toimintasuunnitelmia. Sisäiset tarkastajat arvioivat, ovatko korjaavat toimenpiteet tehokkaita ja pysyviä.

Keskeinen huomio

Vaikka viranomaisohjaus ja ylätason toimintaperiaatteiden suunnittelu eivät kuulu sisäisen tarkastuksen soveltamisalaan ja valvontaan, viraston toimintatapaan liittyvät hallinto-, riski- ja valvontarakenteet ovat tarkastettavissa. Soveltamalla kaikkia organisaatiokäyttäytymistä koskevan aihekohtaisen vaatimuksen (*Organizational Behavior Topical Requirement*) 15 kriteeriä sisäiset tarkastajat voivat arvioida, vaikuttaako organisaatiokäyttäytyminen asumispalvelujen tuottamiseen – kuten siihen, tapahtuuko se oikeudenmukaisesti, läpinäkyvästi ja arvojen mukaisesti poliittisesta toimintaympäristöstä huolimatta.

Esimerkki 2: Pieni rakennusalan yritys (pieni sisäinen tarkastus)

Esimerkin 50 hengen rakennusalan yrityksen sisäinen tarkastus on kuullut huolia siitä, että organisaatiokäyttäytymistä koskeva aihekohtainen vaatimus on suunniteltu suurille ja laajalaisille organisaatioille. Samat periaatteet pätevät kuitenkin myös tähän – skaalattuina sopiviksi. Vaikka yrityksellä ei olisi hallituksen valiokuntaa tai kehittyneitä seurantajärjestelmiä (dashboardeja), se voi silti osoittaa noudattavansa kaikkia 15:sta aihekohtaisen vaatimuksen velvoitetta.

Hallinto

- A. Roolit ja vastuut – Yrityksen ylin johto delegoi henkilöstöhallinnon vastuun virallisesti toimistopäällikölle ja projektien valvonnan työmaapäälliköille. Sisäiset tarkastajat arvioivat, ovatko roolit selkeitä ja vältetäänkö eturistiriidat (esimerkiksi se, että samassa roolissa oleva (henkilö) sekä hyväksyy että valvoo urakoitsijoiden kuluja).
- B. Vastuut – Jokainen päällikkö allekirjoittaa neljännesvuosittain lausumat, joissa he ottavat vastuun tiiminsä käyttäytymisestä, mukaan lukien turvallisuussääntöjen noudattaminen ja alihankkijoiden kohtelu. Sisäiset tarkastajat arvioivat, ovatko nämä lausumat kohtuullisia ja seurataanko niitä.
- C. Valvonta ja seuranta - Johto kokoontuu kuukausittain käymään läpi henkilöstön vaihtuvuutta, asiakasvalituksia ja projektien turvallisuusraportteja. Sisäiset tarkastajat varmistavat, että toimintakulttuuriin liittyvät asiat otetaan esille ja niitä seurataan.
- D. Toimintaperiaatteet ja menettelytavat – Sisäiset tarkastajat varmistavat, että kirjalliset code of conduct-ohjeet sekä turvallisuus- ja kiusaamisen vastaiset ohjeistukset arvioidaan vuosittain ja viestitään henkilöstölle.

Riskienhallinta

- A. Käyttäytymisriskien viitekehys - Yritys tunnistaa riskit, kuten kiirehtiminen tai vaadittujen turvallisuusmenettelyjen laiminlyönnin määräaikojen saavuttamiseksi,



suosimisen ylitöiden jakamisessa ja häirinnän rakennustyömailla. Sisäiset tarkastajat varmistavat, että nämä riskit sisältyvät riskirekisteriin.

- B.** Indikaattorit ja analytiikka – Dashboardin sijaan yritys käyttää yksinkertaisia taulukkolaskentaohjelmia (kuten Exceliä) poissaolojen, valitusten ja turvallisuusinsidenttien seurantaan. Sisäiset tarkastajat arvioivat, tuovatko ne esiin alueita, joita tulisi tarkastella.
- C.** Poikkeamien hallinta - Jos henkilöstökyselyt paljastavat eron "edellytetyn kunnioituksen" ja "todellisen kokemuksen" välillä, päälliköiden on esitettävä korjaavat toimenpiteet seuraavassa kokouksessa. Sisäiset tarkastajat arvioivat, onko toimenpiteet toteutettu ja loppuunsaatettu.
- D.** Sidosryhmien osallistuminen ratkaisuun - Toimivaltaisia viranomaisia, henkilöstön edustajia ja toisinaan avainasiakkaita pyydetään kommentoimaan, kun kulttuurisia ongelmia ilmenee. Sisäiset tarkastajat toteavat, onko vastaus saatujen palautteiden mukainen.

Kontrollit

- A.** Käyttätymisriskien arvioinnit – Jokaisen projektin epäonnistumisen jälkeen (kuten huonosta yhteistyöstä johtuvat kustannusten ylitykset) ylin johto järjestää "opitut asiat" (lessons learned) -tilaisuuden. Sisäiset tarkastajat varmistavat, että toimintakulttuuriin liittyvät syyt (kuten syyllistäminen ja heikko viestintä) on dokumentoitu ja että hallintakeinot on otettu käyttöön vastaavien tilanteiden korjaamiseksi jatkossa.
- B.** Esimerkillä johtaminen – Ylin johto pitää neljännesvuosittain henkilöstöinfot, joissa korostetaan oikeudenmukaisuuden, laadun ja kunnioituksen arvoja. Sisäiset tarkastajat keräävät henkilöstöltä palautetta arvioidakseen, välittyvätkö johdon viestit ja arvot käytäntöön.
- C.** Eskalaatiokäytännöt – Jos virallista ilmoituskanavaa ei ole, raportointikanavana käytetään lukittua palautelaatikkoa sekä mahdollisuutta ottaa suoraan yhteyttä ylimpään johtoon. Sisäiset tarkastajat selvittävät, hyödyntääkö henkilöstö näitä kanavia ja toimivatko ilmoittajansuojakäytännöt.
- D.** Palkitseminen – Bonukset ovat kohtuullisia, ja ne kytkeytyvät tiimityöskentelyyn sekä asiakaspalautteeseen, ei pelkästään projektin määräaikojen saavuttamiseen. Sisäiset tarkastajat arvioivat, onko palkitseminen johdonmukaista ja perusteltua.
- E.** Toiminnan seuranta – Esimiehet antavat vapaamuotoista palautetta henkilöstön toiminnasta ja käytöksestä kehityskeskusteluissa. Tarkastajat selvittävät, hyödynnetäänkö palautetta johdonmukaisesti eri ryhmissä.
- F.** Koulutus – Vuosittain järjestetään lyhyitä työpajoja, joiden aiheina ovat asiallinen käytös työpaikalla sekä työturvallisuus. Sisäiset tarkastajat todentavat osallistujamäärät ja koulutuksen tehokkuuden pistokoemaisilla haastatteluilla.
- G.** Epäkohtien korjausprosessit - Jos kiusaamista tai epäasiallista käytöstä tapahtuu, ylin johto (tai tarvittaessa tätä ylempi viranomainen) selvittää tilanteen, kirjaa tapauksen tiedot ja varmistaa kurinpidollisten tai muiden seuraamusten toteutumisen. Sisäiset tarkastajat arvioivat, ovatko seuraamukset tai korjaavat toimenpiteet oikea-aikaisia ja kohtuullisia.



Keskeinen huomio

Vaikka pienellä yrityksellä ei olisi toisen linjan toimintoja tai hallituksen valiokuntaa, se pystyy täyttämään organisaatiokäyttämistä koskevan aihekohtaisen vaatimuksen kaikki 15 velvoitetta kevennetyillä käytännöillä. Näitä ovat yksinkertaiset rekisterit, ylimmän johdon suora valvonta, vapaamuotoiset katsaukset sekä oikein mitoitettu koulutus. Tämä osoittaa, että aihekohtainen vaatimus on käytännöllinen ja olennainen kaikille organisaatioille koosta riippumatta.



Liite C. Valinnainen dokumentointityökalu

Sisäisten tarkastajien odotetaan käyttävän ammatillista harkintaa määrittäessään 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. Alla oleva tulostettava lomake on yksi vaihtoehto organisaatiokäyttäytymistä koskevan aihekohtaisen vaatimuksen noudattamisen dokumentointiin, mutta sen käyttö ei ole pakollista.

Organisaatiokäyttäytyminen Hallinto

Vaatus	Toteutunut kattavuus tai poissulkemisen perustelu	Dokumentaatioviite
A. Hallitus valvoo ja ylin johto organisoii roolit ja vastuut siten, että vältetään vääränlaisesta organisaatiokäyttäytymisestä johtuvat tahattomat seuraukset. Tahattomia seurauksia ovat esimerkiksi eturistiriidat tai epäselvät päätöksentekoprosessit.		
B. Hallitus valvoo ja ylin johto määrittää sekä ylläpitää yksilö- ja ryhmätason vastuuta käyttäytymisodotuksista varmistaen, että rooleilla ja vastuilla on omistajuus, ne ymmärretään ja ne ovat johdonmukaisesti linjassa organisaation tavoitteiden kanssa.		
C. Hallinnointiprosessit ovat käytössä sen varmistamiseksi, että käyttäytymistä koskevien havaintojen ja organisaation tavoitteiden välistä yhdenmukaisuutta seurataan, arvioidaan ja kyseenalaistetaan säännöllisesti, ja että mahdollisiin poikkeamiin reagoidaan.		



Vaatus	Toteutunut kattavuus tai poissulkemisen perustelu	Dokumentaatioviite
D. Käyttäytymisriskejä koskevat toimintaperiaatteet ja menettelytavat on laadittu, ja niiden relevanttius sekä tarkkuus arvioidaan säännöllisesti. Nämä toimintaperiaatteet ja menettelytavat viestitään tehokkaasti ja integroidaan osaksi organisaation toimintaa ja päätöksentekoprosesseja.		

Organisaatiokäyttäytyminen Riskienhallinta

Vaatus	Toteutunut kattavuus tai poissulkemisen perustelu	Dokumentaatioviite
A. Organisaatio on määrittänyt asianmukaisen lähestymistavan käyttäytymisriskien hallintaan, mukaan lukien ne käyttäytymispiirteet, jotka ovat kriittisiä organisaation tavoitteiden saavuttamiseksi.		
B. Organisaatiokäyttäytymisen seuranta on riittävää ja oikea-aikaista, ja sen tulokset viestitään sidosryhmille.		
C. Odotetun ja toteutuneen käyttäytymisen väliset erot sekä niihin liittyvät juurisyyanalyysit viestitään sidosryhmille tehokkaasti ja johdonmukaisesti.		
D. Käyttäytymisodotusten ja nykyisten käytäntöjen väliset erot ratkaistaan sidosryhmien myötävaikutuksella. Päätösten ja ratkaisujen toteutumista seurataan loppuun saakka, ja niiden vaikuttavuutta mitataan tehokkaasti riittävien toimenpiteiden varmistamiseksi.		



Organisaatiokäyttäytyminen Kontrollit

Vaatus	Toteutunut kattavuus tai poissulkemisen perustelu	Dokumentaatioviite
A. Organisaatiolla on lähestymistapa tunnistaa ja lieventää sellaisia käyttäytymismalleja, jotka voivat vaarantaa organisaation tavoitteiden saavuttamisen. Tästä voidaan esimerkkeinä mainita käyttäytymiseen keskittyvät suoritusarvioinnit ja operatiivisten riskien arvioinnit.		
B. Organisaatio asettaa selkeän ja johdonmukaisen linjan odotetulle käyttäytymiselle ja viestii näistä odotuksista luotettavien sekä helposti saavutettavien kanavien kautta. Organisaatiossa ylläpidetään jäsenneiltyä palautemekanismia, jonka avulla arvioidaan työntekijöiden ymmärrystä ja tukea sekä mahdollistetaan tarvittaessa muutokset.		
C. Organisaatiossa on käytössä menettelyt, joilla kannustetaan ilmoittamaan sellaisesta organisaatiokäyttäytymisestä, joka on ristiriidassa organisaation tavoitteiden saavuttamisen kanssa. Prosessit sisältävät suojelua ja ratkaisutoimintaa koskevat menettelytavat.		
D. Kannustinjärjestelmät, mukaan lukien palkitseminen ja aineettomat palkkiot, ovat käytössä, niistä on viestitty ja ne on sovitettu yhteen organisaation tavoitteiden sekä sääntelyvaatimusten kanssa. Myös epäasiallisen organisaatiokäyttäytymisen sanktiot ja seuraukset ovat mukana.		
E. Käytössä on prosessi ongelmien hallitsemiseksi, mukaan lukien sellaisten käyttäytymismallien tunnistaminen ja korjaaminen, jotka eivät ole linjassa organisaation tavoitteiden kanssa, sekä ongelmien eskalointi tarvittaessa.		



Vaatus	Toteutunut kattavuus tai poissulkemisen perustelu	Dokumentaatioviite
F. Koulutus- ja perehdytysohjelmia, joiden tavoitteena on varmistaa organisaatiokäyttäjien ja organisaation tavoitteiden yhteensopivuus, toteutetaan säännöllisesti ja tehokkaasti.		
G. Rekrytointi- ja perehdytysprosessit ovat yhdenmukaiset organisaatiokäyttäjien koskevien odotusten kanssa ja sisältävät käyttäjien osaamista. Osaajien rekrytointi- ja perehdytysprosessit ovat linjassa organisaation käyttäjien odotusten kanssa ja sisältävät käyttäjien osaamisen.		



Liite D. COSO-viitekehyksen mapping (vastaavuuskartoitus)

Alla olevassa kaaviossa organisaatiokäyttämisen aihekohtaisen hallinto-, riskienhallinta- ja valvontaprosessivaatimukset on kartoitettu suhteessa COSO IC sisäisen valvonnan viitekehykseen (2013) ja COSO ERM riskienhallinnan viitekehykseen (2017). Tämän ristiviittauksen avulla sisäiset tarkastajat voivat sovittaa yhteen COSO:on perustuvan testauksensa Organisaatiokäyttämistä koskevan Aihekohtaisen vaatimuksen kanssa.

Hallintoa koskevat vaatimukset

Vaatus	COSO IC Sisäinen valvonta (2013) Viite	COSO ERM Riskienhallinta (2017) Viite
A. Hallitus valvoo ja ylin johto organisoii roolit ja vastuut siten, että vältetään vääränlaisesta organisaatiokäyttämisen johtuvat tahattomat seuraukset. Tahattomia seurauksia ovat esimerkiksi eturistiriidat tai epäselvät päätöksentekoprosessit.	Valvontaympäristö - periaatteet 2 (hallituksen riippumattomuus ja eskalaatiokanavien valvonta), 3 (rakenne, toimivalta ja vastuu).	Hallinnointi & Kulttuuri – Periaatteet 1 (toteuttaa hallituksen riskienvalvontaa), 2 (luo toimintarakenteet).
B. Hallitus valvoo ja ylin johto määrittää sekä ylläpitää yksilö- ja ryhmätason vastuuta käyttämisenodotuksista varmistaen, että rooleilla ja vastuilla on omistajuus, ne ymmärretään ja ne ovat johdonmukaisesti linjassa organisaation tavoitteiden kanssa.	Valvontaympäristö - Periaatteet 1 (integriteetti ja eettiset arvot), 5 (vastuullisuus ja suoritustarvit).	Hallinnointi & Kulttuuri - Periaatteet 4-5 (osoittaa sitoutumista perusarvoihin; rekrytoi, kehittää ja sitouttaa päteviä henkilöitä).
C. Hallinnointiprosessit ovat käytössä sen varmistamiseksi, että käyttämistä koskevien havaintojen ja organisaation tavoitteiden välistä yhdenmukaisuutta seurataan, arvioidaan ja kyseenalaistetaan säännöllisesti, ja että mahdollisiin poikkeamiin reagoidaan.	Seuranta – Periaatteet 16 (jatkuvat/erilliset arvioinnit), 17 (arvioi ja viestii puutteista); Informaatio & Viestintä – Periaatteet 13 (käyttää relevanttia tietoa), 14 (viestii sisäisesti), 15 (viestii tarvittaessa ulkoisesti).	Hallinnointi & Kulttuuri – Periaate 1 (toteuttaa hallituksen riskienvalvontaa); Suorituskyky – Periaatteet 10-14 (tunnistaa riskit, arvioi niiden vakavuuden, asettaa riskit tärkeysjärjestykseen, toteuttaa riskienhallintatoimet); Informaatio, Viestintä & Raportointi – Periaatteet 18-20 (koulutusta ja tietoisuutta koskeva raportointi)



Vaatus	COSO IC Sisäinen valvonta (2013) Viite	COSO ERM Riskienhallinta (2017) Viite
D. Käyttäytymisriskejä koskevat toimintaperiaatteet ja menettelytavat on määritetty, ja niiden asiaankuuluvuus sekä tarkkuus arvioidaan säännöllisesti. Näistä toimintaperiaatteista ja menettelytavoista viestitään tehokkaasti ja integroidaan osaksi liiketoimintaa ja päätöksentekoprosesseja.	Valvontatoimenpiteet – Periaatteet 10 (valitsee ja kehittää valvontatoimenpiteitä), 12 (ottaa käyttöön toimintaperiaatteiden ja menettelytapojen avulla).	Arviointi & Tarkistaminen – Periaatteet 15-17 (arvioi muutoksia, tarkastelee suorituskyykyä, pyrkii kehittämään toimintaa).

Riskienhallintavaatimukset

Vaatus	COSO IC Sisäinen valvonta (2013) Viite	COSO ERM Riskienhallinta (2017) Viite
A. Organisaatio on määrittänyt asianmukaisen lähestymistavan käyttäytymisriskien hallintaan, mukaan lukien ne käyttäytymispiirteet, jotka ovat kriittisiä organisaation tavoitteiden saavuttamiseksi.	Riskien arviointi – Periaatteet 6 (määrittelee soveltuvat tavoitteet), 7 (tunnistaa ja analysoi riskit), 8 (arvioi väärinkäytösriskit), 9 (tunnistaa ja analysoi merkittävät muutokset).	Hallinnointi & Kulttuuri – Periaatteet 3-5 (osoittaa sitoutumista perusarvoihin; rekrytoi, kehittää ja sitouttaa kyvykkäitä henkilöitä); Strategian & Tavoitteiden asettaminen – Periaatteet 6-9 (määrittelee riskinottohalun, arvioi vaihtoehtoisia strategioita, ottaa riskit huomioon tavoitteissa).
B. Organisaatiokäyttäytymisen seuranta on riittävää ja oikea-aikaista, ja tulokset viestitään sidosryhmille.	Informaatio & Viestintä – Periaatteet 13 (käyttää asiaankuuluvaa tietoa), 14 (viestii sisäisesti); Seuranta (monitorointi) – Periaatteet 16 (jatkuvat/erilliset arvioinnit), 17 (arvioi ja viestii puutteet).	Suorituskyyky – Periaatteet 10-14 (tunnistaa riskit, arvioi niiden vakavuuden, asettaa riskit tärkeysjärjestykseen, toteuttaa riskienhallintatoimenpiteet); Informaatio, Viestintä & Raportointi – Periaatteet 18-20 (koulutus-/tietoisuusraportointi).
C. Odotetun ja toteutuneen käyttäytymisen väliset erot sekä niihin liittyvät juurisyyanalyysit viestitään sidosryhmille tehokkaasti ja johdonmukaisesti.	Informaatio & Viestintä – Periaatteet 14 (viestii sisäisesti), 15 (viestii tarvittaessa ulkoisesti).	Informaatio, Viestintä & Raportointi – Periaatteet 19-20 (viestii riskitiedosta; raportoi riskeistä, kulttuurista ja suorituskyyvystä).



Vaatus	COSO IC Sisäinen valvonta (2013) Viite	COSO ERM Riskienhallinta (2017) Viite
D. Odotetun käyttäytymisen ja nykyisten käytäntöjen väliset erot ratkaistaan sidosryhmien myötävaikutuksella. Ratkaisujen toteutumista seurataan loppuun asti ja niiden vaikuttavuutta mitataan riittävien toimenpiteiden varmistamiseksi.	Valvontatoimenpiteet – Periaatteet 10 (valitsee ja kehittää valvontatoimenpiteitä), 12 (ottaa käyttöön toimintaperiaatteiden ja menettelytapojen avulla); Seuranta (monitorointi) – Periaatteet 16 (jatkuvat/erilliset arvioinnit), 17 (arvioi ja viestii puutteet).	Arviointi & Tarkastaminen – Periaatteet 15-17 (arvioi muutoksia, käy läpi suorituskkyä, pyrkii kehittämään toimintaa).

Valvontavaatimukset

Vaatus	COSO IC Sisäinen valvonta (2013) Viite	COSO ERM Riskienhallinta (2017) Viite
A. Organisaatiolla on lähestymistapa tunnistaa ja lieventää sellaisia käyttäytymismalleja, jotka voivat vaarantaa organisaation tavoitteiden saavuttamisen. Tästä voidaan esimerkkeinä mainita käyttäytymiseen keskittyvät suoritusarvioinnit ja operatiivisten riskien arvioinnit.	Riskien arviointi – Periaatteet 7 (tunnistaa ja analysoi riskit), 8 (arvioi väärinkäytösriskit), 9 (tunnistaa ja analysoi merkittävät muutokset); Seuranta – Periaatteet 16 (jatkuvat/erilliset arvioinnit), 17 (arvioi ja viestii puutteet).	Suorituskky – Periaatteet 10-14 (tunnistaa riskit, arvioi niiden vakavuuden, asettaa riskit tärkeysjärjestykseen, toteuttaa riskienhallintatoimenpiteet); Arviointi & Tarkastaminen – Periaatteet 15-17 (arvioi muutoksia; käy läpi suorituskkyä; pyrkii kehittämään toimintaa).
B. Organisaatio asettaa selkeän ja johdonmukaisen linjan odotetulle käyttäytymiselle ja viestii näistä odotuksista luotettavien sekä helposti saavutettavien kanavien kautta. Käytössä on jäsennelty palautemekanismit, jolla arvioidaan työntekijöiden ymmärrystä ja tukea ja mahdollistetaan tarvittaessa muutokset.	Valvontaympäristö – Periaatteet 1 (merkitsee sitoutumista integriteettiin/rehellisyyteen ja eettisiin arvoihin), 5 (velvoittaa vastuuseen ja suorituskvyn mittaamiseen); Informaatio & Viestintä – Periaatteet 13 (käyttää asiaankuuluvaa tietoa), 14 (viestii sisäisesti), 15 (viestii tarvittaessa ulkoisesti).	Hallinnointi & Kulttuuri – Periaatteet 1 (hallitus valvoo riskejä), 4 (osoittaa sitoutumista perusarvoihin), 5 (rekrytoi, kehittää ja sitouttaa kyvykkäitä henkilöitä); Informaatio, Viestintä & Raportointi – Periaatteet 18-20 (koulutus-/tietoisuusraportointi).



Vaatus	COSO IC Sisäinen valvonta (2013) Viite	COSO ERM Riskienhallinta (2017) Viite
C. Organisaatiossa on käytössä menettelyt, joilla kannustetaan ilmoittamaan sellaisesta organisaatiokäyttäytymisestä, joka on ristiriidassa organisaation tavoitteiden saavuttamisen kanssa. Prosessit sisältävät suojelua ja ratkaisutoimintaa koskevat menettelytavat.	Informaatio & Viestintä – Periaate 14 (sisäiset viestintäkanavat); Valvontaympäristö – Periaate 2 (hallituksen riippumattomuus ja eskalointikanavien valvonta).	Hallinnointi & Kulttuuri – Periaatteet 1 (hallitus valvoo riskejä), 4 (osoittaa sitoutumista perusarvoihin), 5 (rekrytoi, kehittää ja sitouttaa kyvykkäitä henkilöitä); Informaatio, Viestintä & Raportointi – Periaatteet 19–20 (viestii riskitiedosta; raportoi riskeistä, kulttuurista ja suorituskyvystä).
D. Kannustinjärjestelmät, mukaan lukien palkitseminen ja aineettomat palkkiot, ovat käytössä, niistä on viestitty ja ne on sovitettu yhteen organisaation tavoitteiden sekä sääntelyvaatimusten kanssa. Myös epäasiallisen organisaatiokäyttäytymisen sanktiot ja seuraukset ovat mukana.	Valvontaympäristö – Periaatteet 1 (merkitsee sitoutumista rehellisyyteen/integriteettiin ja eettisiin arvoihin), 5 (velvoittaa vastuuseen ja suorituskyvyn mittaamiseen).	Hallinnointi & Kulttuuri – Periaatteet 4 (osoittaa sitoutumista perusarvoihin), 5 (rekrytoi, kehittää ja sitouttaa kyvykkäitä henkilöitä); Suorituskky – Periaatteet 10–14 (tunnistaa riskit, arvioi niiden vakavuuden, asettaa riskit tärkeysjärjestykseen, toteuttaa riskienhallintatoimenpiteet).
E. Käytössä on prosessi ongelmien hallitsemiseksi, mukaan lukien sellaisten käyttäytymismallien tunnistaminen ja korjaaminen, jotka eivät ole linjassa organisaation tavoitteiden kanssa, sekä ongelmien eskalointi tarvittaessa.	Seuranta – Periaatteet 16 (jatkuvat/erilliset arvioinnit), 17 (arvioi ja viestii puutteet); Informaatio & Viestintä – Periaate 13 (käyttää asiaankuuluvaa tietoa).	Arviointi & Tarkastaminen – Periaatteet 15–17 (arvioi muutoksia; käy läpi suorituskkyä; pyrkii kehittämään toimintaa); Suorituskky – Periaatteet 10–14 (tunnistaa riskit, arvioi niiden vakavuuden, asettaa riskit tärkeysjärjestykseen, toteuttaa riskienhallintatoimenpiteet).
F. Koulutus- ja perehdytysohjelmia, joiden tavoitteena on varmistaa organisaatiokäyttäytymisen ja organisaation tavoitteiden yhteensopivuus, toteutetaan säännöllisesti ja tehokkaasti.	Valvontaympäristö – Periaate 4 (sitoutuminen ammattitaitoon); Informaatio & Viestintä – Periaate 13 (käyttää asiaankuuluvaa tietoa).	Hallinnointi & Kulttuuri – Periaate 5 (rekrytoi, kehittää ja sitouttaa kyvykkäitä työntekijöitä); Informaatio, Viestintä & Raportointi – Periaatteet 18–20 (koulutus-/tietoisuusraportointi).
G. Osaajien rekrytointi- ja perehdytysprosessit vastaavat organisaation käyttäytymisodotuksia ja sisältävät käyttäytymisosaamista.	Valvontaympäristö – Periaatteet 1 (rehellisyys/integriteetti ja eettiset arvot), 4 (sitoutuminen ammattitaitoon).	Hallinnointi & Kulttuuri – Periaate 5 (rekrytoi, kehittää ja sitouttaa osaavat henkilöt).



Liite E. Käyttäytymistä koskevat tarkastus- ja varmennustoimenpiteet

Sisäiset tarkastajat saattavat huomata, että heidän jo tekemänsä työ osoittaa heidän soveltavan Organisaatiokäyttäytymistä koskevaa Aihekohtaista vaatimusta. Tässä taulukossa mainitaan muutamia kohdennettuja tarkastuksia ja yleisiä tarkastuselementtejä, jotka voivat vastata vaatimuksia ja joita voidaan käyttää osoittamaan vaatimustenmukaisuutta soveltuvin osin. Näitä esimerkkejä ei tule pitää vaadittuina tarkastuksina; niiden tarkoituksena on pikemminkin osoittaa, miten yleisesti suoritettavat tarkastustoimenpiteet voivat kattaa Aihekohtaiset vaatimukset.

Esimerkkejä tarkastuksista ja varmennustoimenpiteistä, jotka voivat suoraan tai epäsuorasti kohdistua käyttäytymiseen, ovat muun muassa:

Alue	Kohdennetut tarkastukset	Sisäisissä tarkastuksissa käytettävät yleiset testauselementit
Hallinto:	• Riskikulttuuri • Yrityksen hallinto- ja ohjausjärjestelmä • Hallituksen/johdon tehokkuuden arviointi • Sääntelyyn vastaaminen • Tulospalkkaus • Suorituksen arviointi • Liiketoimintastrategia ja -suunnittelu • Muutosjohtamisen suunnittelu • Yrityskaupat ja -järjestelyt	• Yrityksen toimintaperiaatteet ja menettelytavat • Organisaatiotason kontrollit/johdon arviointikontrollit • Koko organisaation laajuisten viranomaisasioiden korjaustoimenpiteet (esimerkiksi liiketoiminnan kehittämissuunnitelma) • Valtuuksien siirtäminen
Riskienhallinta:	• Lakiasiat ja compliance -toiminto • Riskienhallinnan viitekehys • Eettinen ja compliance -ohjelma • Ympäristöön, yhteiskuntaan ja hyvään hallintotapaan liittyvät asiat (ESG) • Väärinkäytösten tutkinta/ilmoituskanava/whistleblower-hotline	• Riski- ja kontrollimatriisien ylläpito • Johdon itsearviointit • Reagointi valvontapuutteisiin ja tarkastus/muihin havaintoihin



Alue	Kohdennetut tarkastukset	Sisäisissä tarkastuksissa käytettävät yleiset testauselementit
Valvontatoimenpiteet (kontrollit):	• Henkilöstöhallinto (mukaan lukien rekrytointi ja sitouttaminen) • Myyntiprosessit (esimerkiksi myyntitapa ja säännöstenmukaisuus) • Hankinnat (esimerkiksi toimittajariippumattomuus, edustaminen) • Toimipiste/yksikkö (esimerkiksi johtaminen ja arviointi) • Väärinkäytös-/ilmoituskanava (whistleblower-hotline)	• Tehtävien eriyttäminen • Johdon katselmointi ja seurantakontrollit • Yksittäiset väärinkäytösriskit • Osaaminen ja riskitietoisuus • Prosessien ja kontrollien kehittäminen



Sisäisten tarkastajien instituutti

IIA on kansainvälinen ammattijärjestö, joka palvelee yli 275 000 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.

Joulukuu 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