HAMK
Hämeen ammatti-
korkeakoulu

Sisäisen tarkastuksen vuosisuunnittelun riskiarviomallin kehittäminen

[YAMK] opinnäytetyö

Liiketoiminnan kehittäminen

2026

Jani Laaksonen

HAMK
Hämeen ammatti-
korkeakoulu

Tiivistelmä

Koulutus	Liiketoiminnan kehittäminen, YAMK	
Tekijä	Jani Laaksonen	Vuosi 2026
Työn nimi	Sisäisen tarkastuksen vuosisuunnittelun riskiarviomallin kehittäminen	
Ohjaaja	Kyllikki Valkealahti	

Opinnäytetyön tavoitteena oli kehittää suomalaisen finanssialan toimijan sisäisen tarkastuksen riskiperusteista vuosisuunnittelua vahvistamalla erityisesti sen systemaattisuutta ja läpinäkyvyyttä. Työn taustalla oli havainto, että kohdeorganisaation riskienhallintajärjestelmän kypsyystason takia, sisäisen tarkastuksen käytössä ei ollut vuosisuunnittelun tueksi yhtiö- ja yksikkötasoista, dataan perustuvaa riskianalyysiä. Vuosisuunnittelun riskiperusteisuus perustui suppeaan riskien arviointiin ja johdon haastatteluihin. Työn toimeksiantajana toimi suomalainen finanssialan toimijan Sisäisen tarkastuksen toiminto.

Työn teoreettisessa osuudessa kerrotaan sisäisen tarkastuksen kansainvälisistä standardeista, sisäisen valvonnan ja riskienhallinnan malleista sekä tutkimuksista, jotka käsittelevät riskiperusteisen suunnittelun, rotaatioperusteisuuden ja strategialähtöisen arvioinnin vaatimuksia. Teoriaosassa kuvataan sisäisen tarkastuksen tehtävä, ammatillinen viitekehys sekä vuosisuunnittelun keskeiset elementit, kuten riskiperusteisuus, strategialähtöisyys, rotaatio ja tiedonkeruumenetelmät.

Empiirinen osuus toteutettiin toiminnallisena kehittämistyönä, joka perustui opinnäytetyön tekijän ja sisäisen tarkastuksen johtajan havaintoihin sekä organisaatiossa tehtyihin haastatteluihin vuosina 2024–2025.

Kehittämistyön tuloksena luotiin uusi, kevyesti toteutettava ja subjektiivinen, mutta rakenteellisesti johdolle hyvin perusteltava riskiarviomalli. Malli yhdistää määrällisiä sekä laadullisia riskitekijöitä ja huomioi eri yksiköiden volyymin, toiminnan monimutkaisuuden, kriittisyyden, toisen linjan havainnot, muutokset ja sisäisen tarkastuksen oman näkemyksen. Lisäksi otettiin käyttöön jatkuvan seurannan prosessi, jossa riskitietoa kerättiin läpi vuoden eri organisaatiotasoilta. Uudistettu malli mahdollisti aiempaa laajemman riskikuvan muodostamisen ja tarjosi johdonmukaisen perusteen tarkastuskohteiden valinnalle.

Johtopäätöksenä voidaan todeta, että uusi riskiarviomalli vahvisti sisäisen tarkastuksen vuosisuunnittelun läpinäkyvyyttä ja paransi päätöksenteon perusteltavuutta. Jatkuva seuranta mahdollisti lisäksi aiempaa ajantasaisemman ja kokonaisvaltaisemman näkymän yhtiön riskiavaruuteen.

Tulosten perusteella vuosisuunnittelun kehittäminen osoittautui selvästi tarpeelliseksi, ja luotu arviointimalli lisäsi merkittävästi suunnitteluprosessin systemaattisuutta.

Yhteenvetona voi todeta, että kehitetty malli tarjoaa realistisen, skaalautuvan ja riskiperusteisen lähestymistavan vuosisuunnittelun toteuttamiseen. Kehittämistyö toimii myös hyvänä perustana mallin ja tätä kautta koko sisäisen tarkastuksen tulevalle kehitystyölle.

Avainsanat	Sisäinen tarkastus, riskienhallinta, riskinarviointi, toimintasuunnitelmat.
Sivut	56 sivua ja liitteitä 2 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Abstract

DP	Business development, YAMK
Author	Jani Laaksonen
Year	2026
Subject	Development of a risk assessment model for annual internal audit planning
Supervisors	Kyllikki Valkealahti

The aim of the thesis was to develop the risk-based annual planning of the internal audit of a Finnish financial institution strengthening its systematic approach and transparency. The background to the work was the observation that due to the maturity level of the target organization's risk management system, internal audit did not use company- and unit-level and data-based risk analysis to support annual planning. The risk-based annual planning was based on a limited risk assessment and management interviews. The work was commissioned by the Internal Audit function of a Finnish financial institution.

The theoretical part of the thesis describes international internal audit standards, internal control and risk management models, and studies that address the requirements of risk-based planning, rotation-based planning, and strategy-based assessment. The theoretical part describes the role of internal audit, the professional framework, and the key elements of annual planning, such as risk-based planning, strategy-based planning, rotation, and data collection methods.

The empirical part was conducted as functional development work, which was based on the observations of the thesis author and the head of internal audit, as well as interviews conducted in the organization in 2024–2025.

The development work resulted in the creation of a new, easily implemented, and subjective risk assessment model that is structurally well justified to management. The model combines quantitative and qualitative risk factors and considers the volume, complexity, criticality, second-line observations, changes and internal audit's own view of different units. In addition, a continuous monitoring process was introduced, in which risk information was collected throughout the year from different organizational levels. The revised model enabled the formation of a broader risk picture than before and provided a consistent basis for the selection of audit targets.

In conclusion, the new risk assessment model strengthened the transparency of internal audit's annual planning and improved the justification of decision-making. Continuous monitoring also enabled a more up-to-date and comprehensive view of the company's risk landscape.

Based on the results, the development of annual planning proved to be clearly necessary, and the created assessment model significantly increased the systematic nature of the planning process.

In summary, it can be stated that the developed model offers a realistic, scalable and risk-based approach to the implementation of annual planning. The development work also forms a sustainable foundation for the future development of the model and, through it, the entire internal audit.

Keywords	Internal audit, risk management, risk assessment, audit plans.
Pages	56 pages and appendices 2 pages

Sisällys

Kuvat

Taulukot

Liitteet

1 Johdanto

Sisäisen tarkastuksen merkitys organisaation johtamisjärjestelmän, sisäisen valvonnan ja riskienhallinnan varmistajana on kasvanut viime vuosina huomattavasti. Organisaatioiden toimintaympäristöt muuttuvat nopeasti, mikä lisää epävakautta, monimutkaisuutta ja ennakoimattomia riskejä. Samalla sidosryhmien odotukset läpinäkyvästä, riskiperusteisesta ja strategiaa tukevasta tarkastustoiminnasta ovat vahvistuneet. Kansainväliset sisäisen tarkastuksen standardit korostavat erityisesti sitä, että vuosisuunnitelman tulee perustua kattavaan ja dokumentoituun organisaationlaajuiseen riskiarvioon. Riskiperusteinen vuosisuunnittelu on siten keskeinen mekanismi, jonka avulla sisäinen tarkastus voi kohdistaa toimintansa tarkoituksenmukaisesti ja tuottaa organisaatiolle lisäarvoa.

Tämän opinnäytetyön taustalla oli havainto, että kohdeorganisaation riskienhallintajärjestelmän maturiteetti oli vielä kehittymässä, minkä vuoksi sisäisen tarkastuksen käytössä ei ollut numeerisesti arvioitua, kattavaa ja systemaattista riskikuvaa vuosisuunnittelun perustaksi. Aiempi vuosisuunnittelu perustui ylimmän johdon haastatteluihin ja sisäisen tarkastuksen toteuttamaan kevyempään riskiarviointiin, mutta ei antanut täysin kattavaa näkyvyyttä yksikkökohtaiseen riskitasoon, strategisiin riskeihin tai toimintojen välisten erojen arviointiin. Tämä on rajoittanut riskiperusteisuuden toteutumista ja vaikeuttanut tarkastuskohteiden valinnan perusteltavuutta.

Tämän työn tavoitteena on kehittää sisäisen tarkastuksen käyttöön toimiva, selkeä ja kevyesti toteutettava riskiarviomalli, joka vahvistaa vuosisuunnittelun riskiperusteisuutta, strategialähtöisyyttä ja läpinäkyvyyttä. Kehitetty malli tukee myös pienen tarkastusorganisaation tarvetta toteuttaa vaatimusten mukainen, dokumentoitu ja systemaattinen riskien arviointi ilman laajaa GRC-järjestelmää.

Työssä tarkastelu rajataan sisäisen tarkastuksen näkökulmaan ja pienen tarkastusorganisaation toimintaympäristöön. Työ ei pyri kehittämään organisaation riskienhallintajärjestelmää kokonaisuutena, eikä riskiarviomalli ole tarkoitettu korvaamaan GRC-järjestelmää. Tarkastelu keskittyy vuosisuunnitelman perustaksi laadittavan riskiarviomallin rakenteeseen, toteutustapaan ja sovellettavuuteen kohdeorganisaation käytännöissä.

Työn rakenne muodostuu siten, että aluksi esitellään opinnäytetyön lähtökohdat ja tavoitteet sekä kohdeorganisaatio. Tämän jälkeen kuvataan työn toteutustapa ja

tutkimusstrategia. Teoreettinen viitekehys muodostaa perustan riskiperusteisen ja strategiaperusteisen vuosisuunnittelun vaatimuksille, joita vasten kehittämistyötä arvioidaan. Empiirisessä osassa kuvataan kehittämisprosessin vaiheet, riskiarviomallin rakentaminen ja sen soveltaminen kahdessa peräkkäisessä suunnittelusyklissä. Lopuksi esitetään työn keskeiset johtopäätökset, mallin vahvuudet ja kehitysalueet sekä jatkotutkimusaiheet.

1.1 Kohdeorganisaatio

Kohdeorganisaationa on suomalainen finanssialan toimija, jonka sisäisen tarkastuksen toiminto koostuu sisäisen tarkastuksen johtajasta ja yhdestä sisäisestä tarkastajasta. Osa sisäisen tarkastuksen toimeksiannoista ulkoistetaan palveluntuottajalle. Ulkoistetuissa toimeksiannoissa palveluntuottaja toteuttaa tarkastuksen suunnittelun, tarkastuksen kenttätyövaiheen sekä raportoinnin. Sisäisen tarkastuksen johtaja on kuitenkin viime kädessä vastuussa ulkoistetuista toimeksiannoista. Sisäinen tarkastus raportoi hallitukselle ja sen alaiselle tarkastusvaliokunnalle. Organisatorisesti sisäinen tarkastus sijoittuu toimitusjohtajan alaisuuteen.

Kohdeorganisaatiolla käytössä sisäisen valvonnan ja riskienhallinnan ”kolmen linjan malli”, joka määrittelee eri linjojen vastuut ja velvollisuudet. Mallin avulla organisaatio voi varmistaa, että sen sisäisen valvonnan ja riskienhallinnan toimet ovat riittävät ja myös linjojen väliset organisatoriset suhteet on huomioitu ja määritelty riittävästi. (Sinersalo ym., 2021, s. 242) Kolmen linjan mallissa ensimmäisen linjan muodostaa varsinainen liiketoiminta ja siihen kuuluvat operatiiviset johtajat. Ensimmäisellä linjalla on vastuu riskienhallinnan ja sisäisen valvonnan päivittäisestä toteuttamisesta. Toisen linjan muodostavat pääsääntöisesti Riskienhallinta- ja Compliance-toiminto. Toisen linjan tehtävänä on varmentaa ja tukea ensimmäisen linjan toimintaa. Mallin mukaisesti kohdeorganisaation Riskienhallintatoiminto on erillinen ensimmäisestä linjasta, eli liiketoiminnasta (IIA Global, 2023, s. 6). Riskienhallintatoiminnon vastuulla on varmistaa, että liiketoiminta noudattaa riskienhallinnan käytäntöjä ja operatiivinen johto pyrkii edistämään riskienhallinnan käytäntöjä. (Niemi, 2018, ss. 330–331) Compliance-toiminnon eli organisaation sääntelynmukaisuuden varmistamisen toiminnon vastuulla on varmistaa, että organisaatiossa noudatetaan lakeja, sääntöjä ja viranomaismääräyksiä (Ratsula, 2016, luku 1.1). Toinen linja raportoi organisaation johtoryhmälle, hallituksen alaiselle tarkastusvaliokunnalle sekä hallitukselle. Kolmannen linjan muodostaa sisäinen tarkastus. Sisäinen tarkastus tarjoaa koko organisaatiolle riippumatonta ja objektiivista

varmennustoimintaa sekä neuvonantopalveluita. Sisäinen tarkastus on organisatorisesti suoraan toimitusjohtajan alaisuudessa mutta raportoi työstään suoraan hallitukselle ja sen alaiselle tarkastusvaliokunnalle. (Niemi, 2018, ss. 331–332) Sisäinen tarkastus tekee ja hallitus hyväksyy vuosittain vuosisuunnitelman, johon on dokumentoitu strategia- ja riskiperusteisesti valitut tulevan vuoden tarkastukset ja neuvonantopalvelut.

Kohdeorganisaatiolla ei ole itse tehtyä tai ulkopuolelta hankittua kaupallista GRC- (Governance, Risk, Compliance) järjestelmää, jota sisäinen tarkastus voisi hyödyntää oman riski- ja strategiaperusteisen vuosisuunnitelmansa perustana (Holopainen ym., 2013, s. 135). GRC-järjestelmää kutsutaan usein myös riskienhallintajärjestelmäksi, johon kootusti kerätään tietoa yrityksen riskiympäristöstä. Riskienhallinnalla on kuitenkin käytössä riskienhallintajärjestelmä, johon on koottu (riskisalkku) toimintoihin kohdistuvat operatiiviset, strategiset ja Compliance-riskit sekä myös tapahtuneet riskitapahtumat. Compliance-riskit ovat sääntelynmukaisuuteen liittyviä riskejä. Operatiiviset riskit koskevat riskejä, jotka liittyvät yrityksen toimintaan, sen erilaisiin prosesseihin ja järjestelmäympäristöön sekä henkilöstöön. Operatiiviset riskit voivat syntyä tai johtua organisaation vallitsevista toimintatavoista, johtamiskulttuurista, uuden teknologian tuomista riskeistä tai henkilöstön toimintatavoista. (Juvonen ym., 2023, luku 4.3 Operatiiviset riskit, toinen kappale) Strategiset riskit koskevat riskejä, jotka liittyvät organisaation strategiseen suunnitteluun, tavoitteisiin, mittareihin ja päätöksiin. Strategisilla riskeillä on myös vaikutusta organisaation kykyyn saavuttaa strategiset tavoitteensa niin lyhyellä kuin pitkälläkin aikavälillä. (Juvonen ym., 2023, luku 4.1 Strategiset riskit, toinen kappale)

Kohdeorganisaation toimintaympäristöä voidaan pitää melko stabiilina. Tulevat toimintaan liittyvät riskit koskevat hyvin paljon lainsäädännön muutoksia. Kohdeorganisaation kilpailuympäristö koostuu muista Suomessa toimivista saman alan yrityksistä.

1.2 Opinnäytetyön tavoitteet, tutkimuskysymykset ja rajaukset

Sisäisen tarkastuksen riski- ja strategiaperusteista vuosisuunnittelua voidaan toteuttaa systemaattisesti kaupallisen tai itse tehdyn GRC-järjestelmän avulla. GRC-järjestelmä on ratkaisu yrityksen hallintojärjestelmän (Governance), riskienhallinnan (Risk) ja vaatimustenmukaisuuden (Compliance) hallintaan yhdellä koko yrityksen laajuisella työkalulla (Mehta, 2024, s. 2). Sisäinen tarkastus voi kehittää myös oman arviointikehikon tai mallin, jonka avulla se voi osoittaa johdolle vuosisuunnitelmansa perusteet. Tämän opinnäytetyön tarkoituksena on esittää selkeä ja helposti toteutettava oma malli, jonka

avulla sisäinen tarkastus voi läpinäkyvästi suunnitella ja perustella vuosisuunnitelmansa riskiperusteisuuden.

Opinnäytetyön tavoitteena on esittää malli, jolla sisäisen tarkastuksen riskiperusteista vuosisuunnittelua voidaan kehittää siten, että siinä huomioidaan systemaattisesti ja mahdollisimman laaja-alaisesti:

- organisaatioon kohdistuvat riskit
- Compliancen ja Riskienhallintatoiminnon tekemät havainnot
- yhtiön toiminnan laajuuteen liittyvät riskien osa-alueet
- Sisäisen tarkastuksen omat havainnot

Opinnäytetyössä esitetyn riskiarviointimallin tavoitteena on tarjota helposti rakennettava ja joustavasti sovellettava kehikko tarkastustoiminnan riskiperusteisen suunnittelun tueksi.

Tavoitteiden toteuttamiseksi opinnäytetyölle asetettiin yksi päätutkimuskysymys ja kaksi apututkimuskysymystä:

1. Miten pienessä sisäisen tarkastuksen organisaatiossa voidaan laatia riittävän kattava, riski- ja strategiaperusteinen vuosisuunnitelma?

Kysymystä täsmennetään kahdella apututkimuskysymyksellä:

a. Mitkä ovat sisäisen tarkastuksen vuosisuunnittelun keskeiset vaatimukset IIA:n standardien mukaan?

b. Miten riskien ja strategian arviointi sekä priorisointi toteutetaan osana vuosisuunnitteluprosessia?

Opinnäytetyössä esitetyn arviointimallin ei ole tarkoitus korvata varsinaista GRC-järjestelmää vaan toimia kevyempänä vaihtoehtona isoa työtä tai kehittämistä vaativalle kaupalliselle järjestelmälle. Työn tarkoituksena ei ole myöskään luoda valmista, laaja-alaista riskiarviomallia, vaan pikemminkin kehittää alkuvaiheen malli, jota sisäinen tarkastus voi jatkokehittää tarpeidensa mukaan. Työssä ei myöskään syvennytä riskienhallinnan tai strategisen johtamisen järjestelmien kokonaisvaltaiseen kehittämiseen, vaan näkökulma rajautuu siihen, että sisäinen tarkastus voi luoda mallin riskiperusteisen vuosisuunnitelman laadinnan tueksi.

2 Opinnäytetyön toteutus ja tutkimusstrategia

2.1 Tutkimustapa

Opinnäytetyöni tutkimusote on toiminnallinen, mikä tarkoittaa, että työ keskittyy käytännön kehittämiseen ja konkreettisen ratkaisun tuottamiseen. Toiminnallisen opinnäytetyön lähtökohtana on ammatillisen tuotoksen kehittäminen siten, että se tuottaa konkreettista hyötyä sille kohderyhmälle, jota työ palvelee. Kohderyhmänä voivat olla esimerkiksi organisaation työntekijät tai asiakkaat, mutta tuotos voi myös tukea laajemmin jonkin toimintaympäristön, kuten yrityksen, palvelukokonaisuuden tai tiimin, arjen toimintatapojen ja käytäntöjen kehittämistä. Tällaisessa opinnäytetyössä keskeistä on tavoitteellinen toiminta, jota ohjaa pyrkimys yhdistää olemassa oleva teoreettinen tieto käytännönläheiseen toteutukseen. Näin tuotettu kokonaisuus vastaa mahdollisimman tarkoituksenmukaisesti kohderyhmän tunnistettuihin tarpeisiin ja edistää toiminnan kehittämistä käytännön tasolla (Kostamo ym., 2022, luku 1.1, neljäs kappale).

Toiminnallisessa opinnäytetyössä opiskelija tuo esiin ammatillista osaamistaan kehittämis- ja tutkimuslähtöisen kokonaisuuden avulla. Työ koostuu konkreettisesta tuotoksesta sekä sitä täydentävästä raporttiosuudesta. Raportissa tekijä kuvaa ja perustelee yksityiskohtaisesti ne lähtökohdat, suunnitteluun liittyneet ratkaisut sekä toteutusta ohjanneet valinnat, joiden pohjalta lopullinen tuotos on rakennettu (Kostamo ym., 2022, luku 1.1, kuudes kappale).

Opinnäytetyöhön sisältyy aina myös selkeä kehittämisnäkökulma. Sen ydinajatuksena on yhdistää teoriatietoa ja asiantuntijoiden tuottamaa tietoa niihin käytännön kokemuksiin ja toimintamalleihin, jotka ovat jo olemassa organisaatiossa. Kehittämisprosessin menetelmiä hyödyntämällä tavoitteena on tuottaa lisää ymmärrystä sekä luoda organisaatiolle käyttöön soveltuva vuosisuunnittelun malli (Kostamo ym., 2022, luku 1.2, kolmas kappale).

Työ perustuu tekijän omaan työhön sisäisenä tarkastajana ja hänen käytännön kokemukseensa organisaation tarkastusprosessista ja riskienhallinnan toimintamalleista. Ammatillista asiantuntijuutta ja kehittämisnäkökulmaa tuodaan opinnäytetyössä esiin toteuttamalla työ kehittävällä ja tutkimuksellisella otteella, jossa yhdistyvät alan teoreettinen viitekehys ja organisaation käytännön tarpeet. Huolellisesti suunniteltu, kattavaan riskien arviointiin perustuva vuosisuunnitelma tukee sisäisen tarkastuksen työtä monella tavalla. Se auttaa määrittämään, mihin tarkastuksiin ja neuvonantopalveluihin tulisi kulloinkin

keskittyä, ja samalla se ohjaa käytettävissä olevan ajan ja resurssien tarkoituksenmukaista kohdentamista (Fiva, 2024, s. 5).

Kehittämistyön tuloksena syntyy riskiperusteinen arviointimalli, joka auttaa sisäistä tarkastusta kohdistamaan vuosisuunnitelmansa toimeksiannot kattavasti strategia- ja riskiperusteisesti. Arviointimalli myös tukee sisäisen tarkastuksen resurssien tehokasta käyttöä, koska näkyvyys vuosittaisen työn kohdistamiseen saadaan paremmaksi laajalla tausta-analyysillä. Opinnäytetyössä kerrotaan myös käytännön keinot ja perustelut arviointikehikon luontiin. Opinnäytetyö on kohdistettu erityisesti pienille sisäisen tarkastuksen organisaatioille, koska niissä vuosisuunnittelun prosessiin käytettävät resurssit ovat usein niukemmat kuin suurissa tarkastusorganisaatioissa.

Opinnäytetyön toteuttaminen vaatii tutkimusongelman tai -kysymyksen tarkkaa muotoilua sekä menetelmällisesti tarkoituksenmukaisen tutkimusmenetelmän käyttöä. (HAMK, n.d.) Toiminnallisen opinnäytetyön tavoitteena on tuottaa uutta tietoa käytännön toiminnan kautta joko itsenäisesti tai yhteistyössä projektikumppaneiden kanssa (Vilkka & Airaksinen, 2004, s. 11). Tämä opinnäytetyö keskittyy sisäisen tarkastuksen vuosisuunnitelman arviointikäytännön kehittämiseen riski- ja strategiaperusteisista näkökulmista. Toiminnallisessa opinnäytetyössä opiskelijan tulee osoittaa tutkiva ja kehittävä ote ja tämän vuoksi on olennaista, että käytännön toteutus tai kehittämisprojekti nivoutuu systemaattisesti tietoperustaan ja keskeiseen tutkimuskirjallisuuteen. (Vilkka & Airaksinen, 2004, s. 79) Työn tavoitteena onkin kytkeä arviointikäytännön kehittämisen työ olemassa olevaan tietoperustaan, joka koostuu pääsääntöisesti sisäisen tarkastuksen ammattistandardeihin (IIA) ja tutkimuskirjallisuuteen. Näiden avulla on muodostettu viitekehys, jonka pohjalta nykytilaa on analysoitu ja kehittämistarpeet tunnistettu.

2.2 Tutkimusasetelma ja menetelmät

Tämä opinnäytetyö on toiminnallinen kehittämistyö, jonka tavoitteena on suunnitella ja käyttöönottaa kevyt, skaalautuva riskiarviomalli sisäisen tarkastuksen riskiperusteisen vuosisuunnittelun tueksi pienessä tarkastusorganisaatiossa. Opinnäytetyö sitoo kehittämistyön ammatilliseen viitekehykseen (IIA-standardit, ohjeet ja tutkimuskirjallisuus) sekä kohdeorganisaation tarpeisiin.

Opinnäytetyön aineisto koostuu kolmesta toisiaan täydentävästä lähteestä. Ensimmäisenä on organisaatiolähtöinen aineisto, joka koostuu lähinnä sisäisen tarkastuksen omista

havainnoista mutta myös osin vuoden aikana tehtyihin ylimmän johdon ja tarkastusvaliokunnan puheenjohtajan haastatteluihin. Haastatteluja ei kuitenkaan ole erikseen litteroitu ja nostettu esiin opinnäytetyössä. Toisena lähteenä on viranomaistiedotteet, jotka koskevat Finanssivalvonnan teema-arviota ja valvottavatiedotteita. Kolmas lähde koostuu teoreettisesta tietoperustasta, joka pitää sisällään mm. IIA:n standardit ja siihen liittyvät täydentävät ohjeet, kotimaisen ja kansainvälisen tutkimuskirjallisuuden riskiperusteisesta vuosisuunnittelusta, rotaatiosta ja tarkastusavaruus -rakenteesta.

Opinnäytetyön menetelmä noudatti iteratiivista MVP-periaatetta (minimum viable product), jossa kehitystyötä tehtiin kahdessa peräkkäisessä suunnittelusyklissä, jotka käsittivät vuosisuunnittelun vuosille 2025–2026. Ensimmäistä suunnittelusykliä (vuoden 2025 suunnittelu) voidaan pitää peruskehikkona, jossa riskiarviokehikon osa-alueita olivat volyymi, monimutkaisuus, kriittisyys, riskienhallinnan havainnot, Compliancen havainnot, muutokset ja sisäisen tarkastuksen havainnot. Riskiarviokehikossa pisteitä eri yksiköille annettiin näiden osa-alueiden osalta välillä 0–3. Pisteiden annossa ei käytetty painotuksia. Ensimmäisen suunnittelusyklin tavoitteena oli luoda yhtenäinen dokumentoitu perusta riskiperusteiselle arvioinnille ja lisätä vuosisuunnittelun riskien arvioinnin läpinäkyvyyttä.

Toisessa suunnittelusyklissä (vuoden 2026 suunnittelu) lähtökohtana oli luoda täsmennetympi riskiarviomalli. Tavoitteena oli luoda malliin painotukset osa-alueiden keskinäiseen merkittävyyteen ja täsmentää arvostusasteikkoja. Lisäksi oli tarkoitus systematisoida jatkuvan seurannan prosessia.

Kummankin suunnittelusyklin jälkeen riskiarviomallia validoitiin käytännössä vertaamalla pisteytystä jatkuvan seurannan sekä sisäisen tarkastuksen omiin havaintoihin. Riskiarviomallin kynnysarvoja ja määritelmiä muutettiin tarpeen vaatiessa.

Opinnäytetyön tukena on hyödynnetty generatiivista tekoäly (ChatGPT ja Copilot). Tekoälyä hyödynnettiin rakenteen hahmottamiseen sekä kieliasun ja tekstin sujuvuuden tarkistamiseen. Opinnäytetyön tutkimusasetelma, tutkimuskysymykset, empiirinen osuus ja johtopäätökset ovat tekijän itsenäistä työtä.

2.3 Kirjallisuuskatsaus

Sisäisen tarkastuksen oman riskiarviomalliin liittyvää tutkimusta on saatavilla varsin vähän. Malleja, joiden avulla riskiarviointia voidaan sisäisessä tarkastuksessa kehittää, löytyy kansainvälisistä lähteistä. Näiden käytettävyys suomalaisessa pienessä organisaatiossa voi olla haastavaa, koska ne vaativat paljon työtä eivätkä implisiittisesti ota huomioon rotaatiota. Vastaavaa tutkimusta, jossa sisäisen tarkastuksen vuosisuunnittelua olisi lähestytty riski-, strategia- ja rotaatioperusteisesti, ei ole selvityksen mukaan tehty.

Vuosisuunnitteluun liittyvät tutkimukset, ohjeistukset, standardit jne. perustuvat pääsääntöisesti siihen, että mikä on merkityksellistä vuosisuunnittelun osalta ja miten sitä voidaan toteuttaa. Näissä toki nousee esiin riskiperusteisuus, mutta niissä ei nosteta esiin, miten sisäinen tarkastus voisi toteuttaa riski- ja strategiaperusteisen arvioinnin käytännössä. Huomioitavaa on myös se, että kotimaista tutkimusta sisäisen tarkastuksen vuosisuunnittelun/vuosittaisen tarkastussuunnitelman riskiperusteisuudesta löytyy kohtuullisen vähän. Kansainvälistä tutkimuksia, joita tässä opinnäytetyössä kuvataan, on kohtuullisesti mutta niiden käytettävyys tähän opinnäytetyöhön ei ollut kovin hyvä, koska ne koskevat suurempia ja usein kansainvälisiä tarkastusorganisaatioita.

Sisäisen tarkastuksen kansainväliset ammattistandardit on uudistettu tammikuussa 2025. Vanhoja standardeja koskevassa kansainvälisen ammatillisen käytäntöjen viitekehyksen (IPPF) implementointiohjeistuksessa on kerrottu, miten riskiperusteista suunnitelmaa tulisi sisäisessä tarkastuksessa toteuttaa (The Institute of Internal Auditors, 2019, s. 96). Ohjeistus koskee vuosisuunnitelman tekemistä mutta siinä ei ohjeisteta varsinaisen arviointikehikon tekemistä. Vaikka ohjeistus koskee vanhoja standardeja, niin sitä voidaan edelleen hyödyntää sisäisen tarkastuksen kirjallisessa vuosisuunnittelussa.

Implementointiohjeistuksen mukaan sisäisen tarkastuksen suunnitelman keskeisenä tavoitteena on varmistaa, että tarkastustoiminta kohdistuu riittävän laajasti organisaation niihin prosesseihin ja liiketoiminnan osa-alueisiin, jotka altistuvat kaikkein merkittävimmille riskeille ja joilla on suora vaikutus siihen, kuinka hyvin organisaatio pystyy saavuttamaan asetetut tavoitteensa. Suunnitteluvaiheessa sisäisen tarkastuksen johtajan on otettava huomioon myös se, millä tasolla organisaation riskienhallintaprosessien kypsyysaste on. Tämä sisältää muun muassa sen arvioimisen, onko organisaatiolla käytössään kattava ja systemaattinen riskienhallintajärjestelmä, jonka avulla riskit voidaan tunnistaa, arvioida, kirjata ja hallita johdonmukaisesti. Mikäli organisaation riskienhallinnan maturiteetti on vielä kehittymässä tai matalalla tasolla, yritys voi hyödyntää riskien arvioinnissa myös muita

menetelmiä ja tietolähteitä kuin varsinaista riskienhallintajärjestelmää. Tällöin sisäinen tarkastus huomioi riskienhallinnan kehitysvaiheen ja mukauttaa omaa suunnitteluaan sen mukaisesti. Sisäisen tarkastuksen tarkastustoiminnan tulee silti kattaa olennaiset riskialueet ja tukea organisaation tavoitteiden toteutumista. (The Institute of Internal Auditors, 2019, s. 96)

Sisäisen tarkastuksen vuosisuunnittelun lähtökohtana tulee olla systemaattisesti toteutettu ja asianmukaisesti dokumentoitu riskienarviointi. Riskienarvioinnin perusteella muodostetaan niin kutsuttu tarkastusavaruus (audit universe), joka käsittää kaikki ne riskialueet ja -kohteet, joita organisaatiossa voidaan tarkastaa. Käytännössä tarkastusavaruus on kattava luettelo potentiaalisista tarkastuskohteista, ja siihen sisällytetään muun muassa organisaation strategiset hankkeet, ohjelmat sekä keskeiset suunnitelmat. Tarkastusavaruus voidaan jäsentää esimerkiksi liiketoimintayksiköiden, tuotteiden tai palveluiden, prosessien, tietojärjestelmien tai sisäisten kontrollien perusteella sen mukaan, mikä parhaiten tukee organisaation kokonaisrakennetta ja riskienhallinnan tavoitteita. Kun merkittävimmät riskit kytketään selkeästi organisaation tavoitteisiin ja kriittisiin liiketoimintaprosesseihin, sisäisen tarkastuksen johtaja pystyy muodostamaan perustellun näkemyksen, miten riskit tulisi priorisoida ja millaisella tavalla tarkastusresursseja on tarkoituksenmukaista kohdentaa. Riskiperusteinen suunnittelu varmistaa, että tarkastustoiminta keskittyy osa-alueisiin, joilla on suurin vaikutus organisaation tavoitteiden saavuttamiseen. Tilintarkastus- ja tarkastusammattilaiset hyödyntävät arviointityössään niin sanottua riskitekijälähestymistapaa, jonka avulla huomioidaan sekä organisaation sisäiset että sen toimintaympäristöstä nousevat ulkoiset riskit. Riskitekijälähestymistapa mahdollistaa kokonaisvaltaisen riskinäkemyksen muodostamisen ja vahvistaa siten tarkastustoiminnan strategista merkitystä. (The Institute of Internal Auditors, 2019, s. 97)

Kun sisäinen tarkastus on koonnut, analysoinut ja dokumentoinut organisaation riskinarviointiin perustuvan tarkastusavaruuden, laatii sisäisen tarkastuksen johtaja varsinaisen vuosisuunnitelman. Suunnitteluprosessin tavoitteena on tuottaa selkeä ja perusteltu kokonaisuus tarkastus- ja arviointitoimenpiteistä, joihin organisaation tulisi tulevalla kaudella keskittyä. Tyypillisesti sisäisen tarkastuksen suunnitelma sisältää useita keskeisiä elementtejä, jotka ohjaavat tarkastustoiminnan toteuttamista ja varmistavat sen läpinäkyvyyden. (The Institute of Internal Auditors, 2019, s. 98)

Ensinnäkin suunnitelmaan sisällytetään yksityiskohtainen luettelo ehdotetuista tarkastuksista sekä mahdollisista neuvoantopalveluihin liittyvistä toimeksiannoista. Nämä

ehdotukset perustuvat tarkastusavaruudessa tunnistettuihin riskeihin ja niiden merkittävyyteen. Toiseksi jokaiselle suunnitellulle toimeksiannolle esitetään perustelut, jotka voivat pohjautua esimerkiksi riskiperusteiseen valintaan, tarkastuskohteiden rotaatiotarpeisiin tai organisaation toiminnassa tapahtuneisiin muutoksiin. Tämä vaihe tekee suunnitelmasta läpinäkyvän ja auttaa osoittamaan, miksi tietyt kohteet on priorisoitu. Kolmantena kokonaisuutena tarkastussuunnitelma määrittelee kunkin toimeksiannon tavoitteet ja alustavan laajuuden. Näiden tietojen avulla varmistetaan, että tarkastukset ja neuvonantopalvelut kohdistuvat ennalta määriteltyihin osa-alueisiin ja toimeksiantojen rajaukset ovat selkeät. (The Institute of Internal Auditors, 2019, s. 98)

Artikkelissa "A multi-objective optimization approach for integrated risk-based internal audit planning" (Wang, Ferreira & Yan, 2025) esitetään tutkimusta, jossa käsitellään monivaiheista kehystä sisäisen auditoinnin suunnittelun tueksi ja joka yhdistää riskinarvioinnin, auditointitoimien valinnan ja resurssien allokoinnin. Lähestymistapa huomioi sekä kvalitatiiviset, eli laadulliset, että kvantitatiiviset, eli numeeriset tai määrälliset päätöksentekokriteerit. Artikkelissa esitetään myös tapaustutkimus, jossa kehystä sovelletaan sisäisen auditoinnin vuosittaisen suunnitelman laatimiseen, sekä herkkyysanalyysi, joka osoittaa ehdotetun lähestymistavan pätevyyden.

Artikkelissa Wang, Ferreira ja Yan (2025) esitetty tapaustutkimus havainnollistaa, kuinka tämä optimointimalli voidaan soveltaa käytäntöön sisäisen tarkastuksen suunnittelussa, mikä tukee opinnäytetyöni tavoitetta kehittää selkeä ja perusteltu malli tarkastussuunnitelman luomiseksi. Lisäksi artikkelin herkkyysanalyysi tarjoaa syvällistä tietoa siitä, kuinka eri tekijöiden, kuten strategian ja riskin, muuttuminen vaikuttaa suunnitelman toteutukseen. Tämä auttaa ymmärtämään, kuinka suunnitelman joustavuus voidaan varmistaa muutoksissa. Tutkimuksessa ei kuitenkaan oteta huomioon tarkastuksen, auditointien, valvontojen ja rotaation vaikutuksia vuosuunnitelmaan. Tutkimuksen monivaiheisuuden ja monimutkaisuuden takia sen käytettävyys onkin tässä opinnäytetyössä hyvin rajallinen.

Artikkelin “Improving the Efficiency and Effectiveness of Risk-Based Internal Audit Engagements” (Coetzee & Lubbe, 2014) tutkimuksessa kerrotaan sisäisen tarkastuksen riskiperusteisesta suunnittelusta. Tutkimuksessa tarkoituksena oli kehittää malli riskiperusteisen sisäisen tarkastuksen toimeksiantojen tehokkuuden ja vaikuttavuuden parantamiseksi. Tutkimus kuitenkin keskittyi hyvin paljon tunnistettujen riskien todennäköisyyksien, vaikutusten ja näiden riskinsietokyvyn arviointiin. Tutkimuksessa nostettiin kuitenkin esille tarkastuskohteiden tavoitteiden mukaisuuden varmistamisen sekä

tavoitteiden saavuttamista uhkaavien tapahtumien ja tekijöiden huomioimisen tärkeys suunnittelussa. Opinnäytetyön teorian tukena onkin käytetty tutkimuksessa esiin nostettua tavoitteiden mukaisuuden huomioimista osana sisäisen tarkastuksen vuosisuunnittelua.

Developing a Risk-based Internal Audit Plan oppaassa (The Institute of Internal Auditors, 2020) kerrotaan sisäisen tarkastuksen riskiperusteisen tarkastussuunnitelman luomisesta. Oppaassa kerrotaan hyvinkin tarkkaan miten sisäisen tarkastuksen organisaatio voi luoda Excel-pohjaisen riskiperusteisen arviointikehikon. Oppaassa kerrottu arviointikehikko ja malli eivät ota huomioon, että sisäisen tarkastuksen vähäiset resurssit eivät välttämättä anna mahdollisuutta luoda mallin kaltaista hyvin kattavaa ja perusteellista suunnittelua.

Tutkimus ”A multi-objective optimization approach for integrated risk-based internal audit planning” (Wang, Ferreira & Yan, 2025) ja käytännön opas ”Developing a Risk-based Internal Audit Plan” (The Institute of Internal Auditors, 2020) antavat hyviä ja käytännön läheisiä vinkkejä opinnäytetyöhöni sekä sen johtopäätöksiin ja jatkotutkimusaiheille. Jatkotutkimuksista kerron tarkemmin opinnäytetyöni lopussa.

Kirjassa ”Internal Audit Quality: Developing a Quality Assurance and Improvement Program” (Pitt, 2014, s. 178) näytetään malli vuosisuunnitteluun käytettävästä varmennuskartasta. Mallissa kuvattu varmennuskartta on hyvin kattava eikä sovellu kovin hyvin pienen tarkastusorganisaation työstettäväksi. Opinnäytetyön empiirisessä osuudessa ei käsitellä sisäisen tarkastuksen varmennuskartan luomista vaikkakin se on tehty osana sisäisen tarkastuksen vuosisuunnitelman kehittämistä. Varmennuskartan kautta sisäinen tarkastus voi kuitenkin peilata riskiarviomallissa eri yksiköille (auditable entity) annettuja osa-alueiden arvoja.

3 Sisäinen tarkastus

Luvussa avataan yleisesti sisäisen tarkastuksen tehtäviä ja toiminta-ajatusta sekä ammatillista viitekehystä. Tämä auttaa ymmärtämään yleisellä tasolla reunaehtoja, jotka määrittelevät pakolliset ja ei-pakolliset ohjeet ja vaatimukset.

Lisäksi omassa alaluvussa on käsitelty tietoperustana kansainvälisiä sisäisen tarkastuksen standardeja yleisesti sekä tarkemmin niiltä osin, jotka koskevat opinnäytetyön aihetta, eli vuosisuunnittelua. Vuosisuunnitteluun liittyvät standardit on pyritty kuvaamaan kattavasti, jotta niiden velvoittavuudesta saadaan mahdollisimman kattava kuva.

3.1 Sisäisen tarkastuksen organisaatio

Sisäisen tarkastuksen organisaatio voi olla hyvin moninainen ja sisäisen tarkastuksen olemassaolo voi olla lainsäädännöllisesti pakollista tai sitten ei. Arvopaperimarkkinayhdistyksen (Arvopaperimarkkinayhdistys ry, 2025, s. 45) ylläpitämän pörssiyhtiölle tarkoitetussa hallinnointikoodissa todetaan, että sisäisen tarkastuksen organisointi ja työskentelytavat voivat olla riippuvaisia mm. yhtiön harjoittamasta liiketoiminnasta ja laajuudesta sekä henkilökunnan määrästä. Yhtiön ei välttämättä ole tarkoituksenmukaista järjestää sisäisen tarkastuksen tehtäviä omaksi toiminnokseen organisaatiossa vaan ulkoistaa toiminta.

Tämä tutkimus käsittelee finanssialan toimijaa, jossa sisäisen tarkastuksen olemassaolo on määritelty lainsäädännössä. Laki työeläkevakuutusyhtiöistä (354/1997) 4 luku 12 e § ja vakuutusyhtiölaki (521/2008) 6 luku 15 § määräävät, että yhtiöillä on oltava sisäinen tarkastus. Sisäisen tarkastuksen on oltava riippumaton yhtiön operatiivisesta toiminnasta ja sen tehtävänä yrityksessä on arvioida ja varmentaa hallinnon, hallintojärjestelmän ja sisäisen valvonnan riittävyyttä ja tehokkuutta.

Laki edellyttää, että kohdeorganisaation toimialalla tulee olla sisäinen tarkastus mutta käytännössä se tarkoittaa, että yhtiöllä tulee olla sisäisen tarkastuksen johtaja. Yhtiöt voivat itse hallituksen hyväksynnällä päättää, miten muutoin sisäisen tarkastuksen organisaatio muodostetaan. Mahdollisuutena on, että sisäisen tarkastuksen organisaation muodostaa vain sisäisen tarkastuksen johtaja. Tällöin johtaja tekee myös itse tarkastuksia tai hän voi antaa kaikki tai osan tarkastuksista ulkopuolisen palveluntarjoajan tehtäväksi. Sisäisen tarkastuksen voi muodostaa myös sisäisen tarkastuksen johtaja ja sisäinen tarkastaja tai useampi sisäinen tarkastaja. Yhtiö voi myös osittain ulkoistaa sisäisen tarkastuksen, jolloin osa tarkastus- tai varmennustoiminnasta hankintaan ulkopuoliselta kumppanilta. Osittainen ulkoistus voidaan tehdä, vaikka yrityksellä olisikin käytössä omia sisäisiä tarkastajia (Sisäiset tarkastajat ry, 2014, s. 5).

Sisäisen tarkastuksen organisaation muodostumiseen vaikuttaa hyvin paljon, millaisen organisaation yhtiön hallitus näkee tuottavan parhaan lisäarvon yritykselle ja sen sisäiselle valvonnalle. Hallituksen näkemykseen voi vaikuttaa sisäisen tarkastuksen johtajan oma näkemys ja perustelu, että millaisen sisäisen tarkastuksen organisaation hän näkee parhaiten tukevan yrityksen strategiaa, tavoitteita, riskiympäristö sekä sisäistä valvontaa. Sillä, että yhtiö ei täysin ulkoista tarkastuksia, etuna on se, että sisäinen tarkastus toimii suoraan organisaation valvonnassa. Tällöin tarkastajilla on laajempi ymmärrys

organisaation toiminnasta, tulevaisuuden suunnitelmista ja eri toimintojen ja henkilöiden välisistä suhteista, mikä tehostaa itse tarkastus- ja varmennustyötä. (Ratsula, 2016, s. 90)

Sisäisen tarkastuksen resurssienhallinnan suunnittelussa sisäisen tarkastuksen johtajan on arvioitava käytettävissä oleva budjetti sekä erilaisten henkilöstöresurssiratkaisujen kustannustehokkuus ja joustavuus. Suunnittelun tavoitteena on varmistaa, että tarkastustoiminnolla on riittävät ja tarkoituksenmukaiset resurssit suunnitelman toteuttamiseen vuoden aikana. Kustannusten hallintaan ja toiminnalliseen joustavuuteen voidaan vaikuttaa useilla tavoilla, kuten rekrytoimalla organisaatioon oma sisäinen tarkastaja tai hyödyntämällä ulkopuolisia asiantuntijoita sopimusperusteisesti. Molempiin vaihtoehtoihin liittyy erilaisia taloudellisia ja toiminnallisia etuja, ja sopivin ratkaisu riippuu yhtiön toimialasta, organisaation koosta, riskiprofiilista ja tarkastustarpeista. (IIA Finland, 2024, s. 73)

Suomalaisten yritysten sisäisten tarkastuksen yksiköiden henkilömääristä ei ole saatavilla tietoa. Kuvassa 1 esitetään Pohjois-Amerikkalaisten yritysten vertailu sisäisen tarkastuksen (Internal Audit) FTE-lukujen ja Organisaation FTE-lukujen välillä. FTE (Full-Time Equivalent) on mittari, joka kuvaa työntekijöiden määrää kokopäiväisen työntekijän työnä. Vaikka Pohjois-Amerikkaa ei voida vertailla Suomalaisiin yrityksiin saadaan kuvasta indikaatiota yritysten työntekijämäärän ja sisäisen tarkastuksen henkilömäärän suhteesta. Tyypillisesti Suomessa vain isoimmissa yrityksissä on sisäisen tarkastuksen toiminto tai sisäisen tarkastuksen johtaja. Suomessa suurimmat sisäisen tarkastuksen organisaatiot ovat pankki- ja vakuusalan suurissa konserneissa kuten OP Ryhmässä (65 hlö) ja Nordeassa (yli 200 hlö).

Kuva 1. Sisäisen tarkastuksen FTE:t verrattuna organisaation FTE:ihin (Internal Audit Foundation, 2025, s. 34).

Internal Audit FTEs Compared to Organization FTEs						
	Organization FTEs					
Internal audit FTEs	500 or fewer	501 to 1,500	1,501 to 5,000	5,001 to 10,000	10,000+	All
1 to 3	38%	17%	20%	17%	5%	19%
4 to 9	52%	60%	42%	31%	26%	41%
10 to 24	10%	21%	30%	43%	39%	29%
25+	0%	2%	8%	9%	30%	11%
SUM	100%	100%	100%	100%	100%	100%

Vuonna 2025 Suomessa toimivien kohdeorganisaation kilpailijoiden sisäisen tarkastuksen yksiköt olivat rakenteeltaan varsin kevyitä. Eri yhtiöissä sisäisen tarkastuksen organisaatio koostui joko ainoastaan sisäisen tarkastuksen johtajasta tai kahdesta henkilöstä, jossa johtajan lisäksi työskenteli yksi sisäinen tarkastaja.

3.2 Sisäisen tarkastuksen tehtävä ja toiminta-ajatus

Sisäinen tarkastus on riippumaton hallituksen ja ylimmän johdon tukitoiminto. Sen tehtävänä on objektiivisella arviointi- ja varmistus- sekä konsultointitoiminnallaan tukea organisaation kehittämistä ja tavoitteiden saavuttamista, ja tuottaa organisaatiolle siten lisäarvoa.

Sisäisen tarkastuksen tehtäväkenttä ulottuu koko organisaation toiminnan arviointiin, kattaen sisäisen valvonnan rakenteet, riskienhallintajärjestelyt sekä johtamis- ja hallintoprosessit. (IIA Finland, 2025) Sisäinen tarkastus arvioi ja varmentaa objektiivisesti sisäisen valvonnan järjestämisen asianmukaisuutta ja riittävyyttä sekä raportoi tulokset ylimmälle johdolle (Sääskilahti ym., 2024, s. 7) Sisäisen tarkastuksen toimeksiannot tulee toteuttaa ammattistandardien mukaisesti, järjestelmällisesti ja dokumentoidusti, jotta tuloksia voidaan pitää luotettavina, laadukkaina ja vertailukelpoisina. (Niemi, 2018, s. 29)

Niemi (2018, s. 29) on todennut kirjassaan, että sisäisen tarkastuksen yksi keskeisistä tehtävistä on tuottaa lisäarvoa organisaatiolle. Rönkkö (2019, s. 315) on tutkimustyössään täsmentänyt, että tuloksellisesti toimivan sisäisen tarkastuksen toiminnon tulee tuottaa organisaatiolleen aitoa lisäarvoa mm. taloudellisuuden, tuottavuuden, tehokkuuden ja vaikuttavuuden näkökulmista. Ratsula (2016, s. 91) mainitsee, että sisäisellä tarkastuksella tulee olla rooli myös yrityksen riskienhallinnan kehittämisessä sekä sen toiminnan laadun arvioinnissa ja varmentamisessa. Sisäinen tarkastus varmistaa, että riskienhallintaprosessi on asianmukainen, ja arvioi koko riskienhallintaprosessia ja yhtiön riskien raportoinnin laatua. Sisäisen tarkastuksen vuosisuunnittelussa riskienhallinta korostuu valittavien tarkastuskohteiden muodossa.

Rönkkö (2019, s. 312) toteaa, että organisaatioiden toiminta- ja markkinaympäristöt voivat muuttua huomattavan nopeasti, mikä lisää epävarmuutta ja monimutkaisuutta johdon päätöksenteossa. Muutosten myötä yritysten organisaatiorakenteet voivat kehittyä entistä monimuotoisemmiksi, prosessit tehostua ja nopeutua, ja samalla täysin uudenlaiset riskit voivat nousta esille johdon seurattaviksi. Tällaisessa ympäristössä korostuu tarve toimivalle sisäiselle valvonnalle sekä kehittyneelle ja ennakoivalle riskienhallinnalle, jotka tukevat organisaation kykyä reagoida muutoksiin ja varmistaa tavoitteidensa saavuttaminen. Johto tarvitsee rinnalleen asiantuntijoita, jotka ovat erikoistuneet sisäisen valvonnan ja riskienhallinnan kehittämisen tukemiseen. Tässä kehityskulussa sisäisellä tarkastuksella on luonteva mahdollisuus vahvistaa rooliaan organisaation johtamisjärjestelmän keskeisenä tekijänä. Toimintaympäristöjen ja organisaatiorakenteiden monimutkaistuessa sisäisen tarkastuksen tuottama riippumaton arviointi ja varmistus muodostuvat entistä tärkeämmiksi. Sisäisen tarkastuksen merkityksen kasvu liittyy olennaisesti myös siihen, että monet organisaatiot ovat kooltaan ja rakenteeltaan niin laajoja, ettei hallitus tai ylin johto pysty enää kattavasti valvomaan kaikkia vastuualueitaan ilman asiantuntijatukea. Tässä tilanteessa sisäinen tarkastus toimii keskeisenä riippumattomana elimenä, jonka avulla johto ja hallitus voivat saada luotettavaa varmistusta siitä, että organisaation toiminta etenee suunnitellulla tavalla ja sen keskeiset tavoitteet saavutetaan. (Holopainen ym., 2013, s. 98)

Institute of Internal Auditors (2024) kuvaa raportissaan tulevaisuuden toimintaympäristön, jossa teknologinen murros ja globaalit haasteet muokkaavat yritysten kehityssuuntia ja vaatimuksia. Tässä muuttuvassa toimintaympäristössä sisäisen tarkastuksen roolin odotetaan kehittyvän perinteisestä varmistustoiminnasta kohti strategista neuvonantajuutta. Strategisena neuvonantajana toimiva sisäinen tarkastaja työskentelee tehokkaassa

ekosysteemissä, jossa toiminnan ohjaaminen ja varmistustoiminta toteutetaan muun muassa virtuaalitodellisuuden ja lisätyn todellisuuden sovellusten avulla.

Institute of Internal Auditors (2024) myös visioi raportissaan, että tulevaisuudessa sisäinen tarkastus hyödyntää edistynyttä analytiikkaa ja kvanttitietojenkäsittelyn tarjoamia mahdollisuuksia, muodostaakseen aiempaa tarkempaa ja näyttöön perustuvaa tilannekuvaa organisaation tilasta. Näiden teknologioiden avulla voidaan ennakoida organisaatioiden kehityskulkuja ja riskitrendejä huomattavasti tarkemmalla tasolla kuin perinteisillä menetelmillä. Lähestymistapa on kokonaisvaltainen ja se yhdistää kehittyneen teknologian ymmärryksen organisaation ydinriskeihin sekä kontrollien arvioinnin asiantuntemukseen. Hallitus ja organisaation ylin johto saavat näin strategisesti tärkeää ja luotettavaa tietoa sekä organisaation tilanteeseen mukautettua ohjausta toimintaympäristön jatkuvassa muutoksessa.

Samalla, kun tarkastustoimeksiantojen luonne ja laajuus muuttuvat uusien riskien ja teknologisten mahdollisuuksien myötä, myös sisäisen tarkastuksen roolia organisaatiossa on kehitettävä vastaamaan uusiin tarpeisin. Institute of Internal Auditors (2024) arvioi, että vuoteen 2035 mennessä sisäisen tarkastajat eri organisaatioissa hallitsevat tarvittavat taidot ja menetelmät, ja heillä on johdon sekä sidosryhmien tuki, jotta he voivat toimia muuttuvassa riskikentässä ja vastata tulevaisuuden odotuksiin.

Sisäisen tarkastuksen toiminta-ajatuksena on lisätä ja turvata organisaation arvoa tarjoamalla riskiperusteista ja objektiivista varmistusta, neuvonantopalveja ja konsultointia (IIA Finland, 2025). Toiminta-ajatuksen tarkoituksena on kertoa, mitä Sisäisen tarkastuksen toiminto pyrkii saavuttamaan organisaatiossa. Toiminnassa korostuu lisäarvon tuottaminen organisaatiolle ja tähän sen tuleekin pyrkiä, olipa sitten kyse neuvonanto- tai varmennuspalveluista. (Niemi, 2018, s. 29)

3.3 Ammatillinen viitekehys

Sisäisen tarkastuksen uudet kansainväliset ammattistandardit (Global Internal Audit Standars) julkaistiin 9.1. 2024 ja ne otettiin käyttöön 9.1.2025 (IIA Finland, 2025). Samalla myös uudistettiin myös ammatillinen viitekehys IPPF (International Professional Practices Framework). Sisäisen tarkastuksen työtä tekevien tulee hyödyntää ammatillista IPPF-viitekehystä varmistaakseen, että sisäisen tarkastuksen toiminta-ajatus myös käytännössä toteutuu. (IIA Finland, 2025)

Sisäisen tarkastuksen ammatillinen viitekehys kuvaa ne periaatteet ja toimintatavat, jotka ohjaavat sisäisen tarkastuksen toteuttamista eri organisaatioissa. Viitekehyksen tavoitteena on tukea tarkastajia sekä muita sidosryhmiä kaikkialla maailmassa tarjoamalla yhteiset peruslinjaukset, joiden avulla voidaan varmistaa sisäisen tarkastuksen laatu ja johdonmukaisuus erilaisissa toimintaympäristöissä. Sen avulla sisäinen tarkastus pystyy mukautumaan organisaatioiden erilaisiin tarpeisiin riippumatta niiden tehtävästä, koosta tai rakenteellisista erityispiirteistä. (IIA Finland, 2025)

Kuvassa 2 esitetään kokonaisuudessaan uusi sisäisten tarkastajien ammatillinen viitekehys. Viitekehyksen keskiössä ovat velvoittavat kansainväliset sisäisen tarkastuksen ammattistandardit ja tämän jälkeen velvoittavat aihekohtaiset vaatimukset. Viitekehyksen ulkokehällä on suositeltavat kansainväliset ohjeet.

Kuva 2. Sisäisen tarkastuksen ammatillinen viitekehys (IIA Finland, 2025)

3.3.1 Kansainväliset ohjeet

Kansainväliset ohjeet, eli yleiset, ei-pakolliset ohjeet ja neuvot täydentävät pakollisia ohjeistuksia (IIA Finland, 2025). Sisäisen tarkastuksen uusissa standardeissa (IIA Finland, 2024) mainitaan, että kansainväliset ohjeet tukevat standardeja tarjoamalla täydentävää tietoa, neuvoja ja parhaita käytäntöjä sisäisen tarkastuksen toteuttamiseen. IIA vahvistaa ohjeet virallisilla arviointi- ja hyväksymisprosesseilla. Täydentävät ohjeet kertovat tarkastuksen toteutuksesta yksityiskohtaisemmin, kuten esim. tarkastukseen liittyviä työkaluja ja tekniikoita, vaiheittain kuvattuja toimintatapoja, sekä esimerkkejä näiden

tuotoksista. IIA:n täydentävät ohjeet päivittyvät vuoden 2025 aikana uusiutuvan IPPF-viitekehyksen mukaisesti. (IIA Finland, 2025)

3.3.2 Aihekohtaiset vaatimukset

Sisäisten tarkastajien aihekohtaiset vaatimukset vahvistavat sisäisen tarkastuksen tuottamien palveluiden yhdenmukaisuutta, vaikuttavuutta ja laatua. Lisäksi ne parantavat sisäisten tarkastajien ammatillista osaamista ja tarjoavat rakenteen, joka tukee tarkastajia erityisesti silloin, kun toimeksiannot kohdistuvat tiettyihin riskialueisiin. Vaatimusten tarkoituksena on korostaa sisäisen tarkastuksen roolia tilanteissa, joissa riskit muuttuvat ja kehittyvät sekä edellyttävät entistä syvällisempää osaamista. Aihekohtaiset vaatimukset muodostavat vähimmäistason ja määrittelevät keskeiset kriteerit, joiden avulla voidaan arvioida hallinto-, riskienhallinta- ja valvontaprosessien suunnittelua ja toimivuutta tietyillä riskialueilla systemaattisesti ja kattavasti. Sisäisten tarkastajien tulee soveltaa näitä vaatimuksia kansainvälisten sisäisen tarkastuksen standardien edellyttämällä tavalla. (The Institute of Internal Auditors, 2025)

Sisäisen tarkastuksen standardien mukaan (IIA Finland, 2024, s. 5) tarkastajien on noudatettava aihekohtaisia vaatimuksia aina silloin, kun toimeksiannon laajuus kattaa yhden tai useamman niistä. Näiden vaatimusten rooli on keskeinen, sillä ne tukevat sisäisen tarkastuksen valmiuksia käsitellä eri toimialoilla ja sektoreilla esiintyviä muuttuvia riskejä. Niiden noudattaminen ei ole valinnaista, vaan velvoittavaa, ja niiden soveltamista suositellaan myös neuvontapalveluiden yhteydessä, jotta sisäisen tarkastuksen työ perustuu yhdenmukaisiin ja korkealaatuisiin periaatteisiin. (The Institute of Internal Auditors, 2025)

Aihekohtaiset vaatimukset ovat uusien standardien voimaantulon myötä uusiutumassa. Tällä hetkellä on valmistunut kyberturvallisuutta koskevat vaatimukset ja kolmansia osapuolia koskevat vaatimukset ovat lausuntokierroksella. (The Institute of Internal Auditors, 2025)

3.3.3 Sisäisen tarkastuksen standardit

Kansainväliset sisäisen tarkastuksen ammattistandardit ohjaavat sisäisen tarkastuksen toimintaa maailman laajuisesti. Ne ohjaavat ammattikäytäntöjä sekä ovat perustana sisäisen tarkastuksen toiminnan laadun arvioinnissa ja parantamisessa (IIA Finland, 2025,

s. 7). Sisäisessä tarkastuksessa toimivien henkilöiden tulee noudattaa standardeja, mutta kyseessä ei kuitenkaan ole lainsäädännön kaltainen velvoittavuus. (Niemi, 2018, s. 30) Tarkastajien on toiminnassaan pyrittävä huomioimaan myös kaikkien keskeisten sidosryhmien tarpeet, jotta laajamittaiseen tulokselliseen toimintaan on mahdollista päästä. Alan omien ammattistandardien noudattaminen toimii hyvänä lähtökohta, mutta se ei riitä vakuuttamaan hallituksen jäseniä tai organisaation johtoryhmää sisäisen tarkastuksen toiminnan laadusta. (Rönkkö, 2019, s. 314)

Standardien tarkoituksena on ohjata sisäisen tarkastuksen toimintaa ja sen laatua siten, että toiminnalle asetettu missio, visio, pääperiaatteet ja eettiset säännöt toteutuisivat. Standardit antavat hyvän selkänojan sisäisen tarkastuksen käytännön toteuttamiseen ja auttavat nostamaan toiminnan laatua. (Niemi, 2018, s. 30) Sisäisen tarkastuksen standardien (IIA Finland, 2024, s. 8) mukaan standardit koskevat sisäisen tarkastuksen toimintoa, sisäisen tarkastuksen johtajaa sekä yksittäisiä sisäisiä tarkastajia. Sisäisen tarkastuksen johtajan vastuulla on, että sisäisen tarkastuksessa noudatetaan ja sovelletaan kaikkia standardeja.

Sisäisen tarkastuksen standardien perustana ovat viisitoista ohjaavaa periaatetta, jotka muodostavat kokonaisuuden, jonka tarkoituksena on varmistaa sisäisen tarkastuksen tuloksellisuus ja laadukas toteuttaminen. Näitä periaatteita tukevat standardit, jotka sisältävät konkreettisia vaatimuksia, soveltamista koskevia ohjeita sekä esimerkkejä siitä, miten noudattaminen voidaan käytännössä osoittaa. Standardien kokonaisuus muodostaa viitekehyksen, jonka avulla sisäiset tarkastajat pystyvät toteuttamaan sisäisen tarkastuksen tarkoitusta ja keskeisiä periaatteita johdonmukaisesti ja ammatillisesti. (IIA Finland, 2025, s. 7)

Ammattistandardit on jäsennelty viiteen asiakokonaisuuteen (Domain), joista kukin kokoaa yhteen sitä koskevat periaatteet (Principle). Tämä jaottelu luo sisäisen tarkastuksen toiminnan rakenteellisen rungon ja auttaa ymmärtämään, miten tarkastustoiminto tuottaa arvoa eri näkökulmista. (IIA Finland, 2024) Viiden asiakokonaisuuden 15 periaatetta jakautuvat itse standardeihin, joita on yhteensä 52 kappaletta.

Ensimmäinen asiakokonaisuus käsittelee sisäisen tarkastuksen määritelmää. Tämä kokonaisuus selkeyttää sisäisen tarkastuksen roolin organisaatiossa riippumattomana arviointitoimintona, joka tuottaa sekä varmistusta että lisäarvoa toiminnan kehittämiseen. Määritelmä ohjaa tarkastustoiminnon tarkoitusta: arvioida hallinto-, riskienhallinta- ja valvontaprosessien asianmukaisuutta sekä tukea organisaation tavoitteiden saavuttamista.

Toinen asiakokonaisuus käsittelee eettisyyttä ja ammattitaitoa. Tähän kuuluu viisi periaatetta, jotka korostavat integriteetin osoittamista, objektiivisuuden säilyttämistä, ammattitaidon ylläpitämistä ja osoittamista, ammatillisen huolellisuuden noudattamista sekä luottamuksellisuuden säilyttämistä. Näiden periaatteiden noudattaminen varmistaa riippumattoman ja luotettavan työn laadun sekä suojaa sidosryhmien luottamusta tarkastustoimintoon. Eettisyys on olennainen sekä havaintojen muodostamisessa että niiden raportoinnissa.

Kolmas asiakokonaisuus käsittelee sisäisen tarkastuksen hallinnointia. Se määrittää hallituksen roolin tarkastustoiminnon valtuuttajana ja valvojana, varmistaa organisaatiossa sisäisen tarkastuksen riippumattoman aseman ja selkiyttää vastuunjaon suhteessa johtoon ja hallitukseen. Hallinnointiperiaatteiden tavoitteena on luoda puitteet, joissa tarkastustoiminto voi toimia tehokkaasti, riippumattomasti ja riittävin resurssein tuottaakseen luotettavaa varmistusta.

Neljäs asiakokonaisuus käsittelee sisäisen tarkastuksen johtamista. Siihen kuuluvat periaatteet painottavat strategista suunnittelua, resurssien tarkoituksenmukaista hallintaa, vaikuttavaa viestintää sekä jatkuvaa laadun parantamista. Johtamisperiaatteet varmistavat, että tarkastustoiminnolla on selkeä suunta ja osaaminen kohdistaa toiminta arvokkaimpiin riskialueisiin. Laadunvarmistus ja -kehittäminen tukevat menetelmien yhdenmukaista soveltamista sekä toiminnan läpinäkyvyyttä.

Viides asiakokonaisuus käsittelee sisäisen tarkastuksen käytännön toteuttamista. Periaatteet ohjaavat toimeksiantojen tuloksellista suunnittelua, toteutusta sekä tulosten raportointia ja toimenpidesuositusten seurantaa. Järjestelmällinen suunnittelu määrittää mm. tavoitteet, laajuuden ja menetelmä. Toteutus varmistaa mm. aineiston keruun, analyysin ja johtopäätösten perusteltavuuden. Raportointi ja seuranta puolestaan tukevat mm. korjaavien toimenpiteiden toimeenpanoa sekä vaikutusten arviointia. Näin varmistetaan, että tarkastustoimeksiannot ovat luotettavia, vertailukelpoisia ja johdon päätöksentekoa tukevia. (IIA Finland, 2024)

Viiden asiakokonaisuuden ja niihin liittyvien periaatteiden jäsentely tarjoaa systemaattisen tavan toteuttaa tarkastustoimintaa, joka on eettisesti kestävää, hallinnollisesti selkeää, strategisesti johdettua ja menetelmällisesti laadukasta. Rakenne auttaa sisäisiä tarkastajia kohdentamaan työnsä merkittäviin riskeihin ja tuottamaan johdolle läpinäkyvää, perusteltua ja käytännönläheistä varmistusta sekä kehittämisehdotuksia. (IIA Finland, 2025, s. 7, IIA Finland, 2024)

Vaikka sisäisiltä tarkastajilta odotetaan standardien vaatimusten noudattamista, ei kaikkien vaatimusten noudattaminen ole aina mahdollista. Tärkeää on kuitenkin saavuttaa standardien tarkoituksenmukaisuus oleellisin osin. Olosuhteet, jotka voivat vaikeuttaa standardien noudattamista, liittyvät usein resurssien tuomiin rajoituksiin tai toimialan lainsäädännön erityspiirteisiin. Poikkeustilanteissa tulisi tehdä vaihtoehtoisia toimenpiteitä standardin tarkoituksenmukaisuuden täyttämiseksi. Sisäisen tarkastuksen johtajan vastuulla on näiden poikkeamien perusteiden ja hyväksyttyjen vaihtoehtoisten toimenpiteiden dokumentointi ja kommunikointi asianmukaisille tahoille. Sisäisen tarkastuksen mahdollisuuteen noudattaa standardeja kaikilta osin voi vaikuttaa myös Sisäisen tarkastuksen toiminnon tai koko organisaation koko. Vähäisillä resursseilla tiettyjen tehtävien toteuttaminen voi olla haastavaa. (IIA Finland, 2024, ss. 8–9)

4 Sisäisen tarkastuksen vuosisuunnittelu

Toimintasuunnitelmassa sisäinen tarkastus määrittelee toimeksiannot, jotka se toteuttaa tietyn ajanjakson aikana. Käytännössä toimintasuunnitelma on sama kuin sisäisen tarkastuksen vuosisuunnitelma. Vuosisuunnitelman tarkoituksena on varmistautua, että sisäinen tarkastus kohdistaa toimeksiantonsa keskeisiä riskejä sisältäviin alueisiin, toimintoihin tai prosesseihin ja tuottaa organisaatiolle lisäarvoa tukemalla sitä tavoitteiden saavuttamisessa. (Niemi, 2018, s. 170) Jotta vuosisuunnitelman avulla voidaan tuottaa lisäarvoa, tulee sisäisen tarkastuksen ymmärtää täysin organisaation liiketoiminta (Pitt, 2014, s. 170)

Finanssivalvonta (Fiva) suoritti vuonna 2014 teema-arvion vahinko- ja henkivakuutusyhtiöiden sisäisen tarkastuksen toiminnosta. Arvion perusteella toimintojen toimintatavoissa merkittäviä eroavaisuuksia. Teema-arviossa havaittiin, että usean yhtiön vuosisuunnitelmat eivät huomioineet rotaatiota edes merkittävien toimintojen osalta eivätkä suunnitelmat perustuneet järjestelmälliseen ja riskiperusteiseen lähestymistapaan prioriteettien valinnassa. Hyvin laadittu ja laajaan riskien hahmotuskykyyn pohjautuva vuosisuunnitelma auttaa tarkastuskohteiden ja painotusten huomioimisessa sekä ajan ja resurssien allokoimisessa. (Fiva, 2024, s. 5)

Sisäisen tarkastuksen vuosisuunnittelu on tärkeä osa sisäisen tarkastuksen toimintaa. Vuosisuunnittelua voidaan kohdentaa vuodeksi tai useammaksi vuodeksi. Nykyisin vuosisuunnitelma voidaan tehdä jatkuvana, jolloin tehdään esim. koko vuoden kattava vuosisuunnitelma, mutta sitä päivitetään neljännesvuosittain. Jatkuva vuosisuunnittelu

mahdollistaa sisäiselle tarkastukselle paremman valmistautumisen toimintaympäristön mahdollisille muutoksille. (Niemi, 2018, s. 170) Jatkuva vuosisuunnittelu sopii erityisesti organisaatiolle, joihin kohdistuu mm. merkittäviä kehitysprojekteja, lainsäädännön muutoksia tai joiden toimintaympäristössä on odotettavissa muutoksia.

Sisäisen tarkastuksen vuosisuunnitelmassa tulisi ottaa huomioon ensimmäisen (liiketoiminta) ja toisen linjan (Riskienhallinta- ja Compliance-toiminta) valvontojen ja tarkastusten tulokset, toisen linjan seurannassa olevat keskeiset riski-indikaattorit, uusien tuotteiden hyväksyntä-/muutosprosesseissa käsiteltävät olennaiset organisaatiomuutokset, meneillään olevat häiriöt ja makrotaloudelliset tekijät sekä sääntelymuutokset riittävän ajoissa. Eri organisaatioiden kohtaamat riskit riippuvat liiketoiminnasta, sijainnista, organisaatiorakenteesta, tuotteista, asiakkaista ja palveluntarjoajista, joten sisäisen tarkastuksen toiminto tarvitsee joustavuutta reagoidakseen muuttuviin sisäisiin ja ulkoisiin tekijöihin ajoissa. (ECIIA, 2018, s. 5) Joustavuutta reagointiin tuo mahdollisuus muuttaa tarvittaessa vuosisuunnitelmaa tai vuosisuunnitelman tekeminen esim. puolivuosittaiseksi.

Kuten edellä mainittiin, sisäisen tarkastuksen tulee tehdä vuosisuunnittelussa yhteistyötä myös Compliance-toiminnon kanssa. Organisaation toiminta- ja riskiympäristön sekä toiminnan sääntelymukaisuuden varmistamiseksi on ensisijaisen tärkeää, että varmennuspalveluita tarjoavat yksiköt koordinoivat työnsä mahdollisimman tehokkaasti. Koordinoinnin avulla vältetään päällekkäinen varmentaminen ja mahdollistetaan tehokas valvonta. Lisäksi koordinoinnin avulla saadaan tärkeää tietoa sisäisen valvonnan ja Compliancen tilasta yli yksikkörajojen. (Ratsula, 2016, luku 5.8)

4.1 Vuosisuunnitteluun liittyvät standardit

Standardin 9.4 mukaan (IIA Finland, 2024, s. 66) sisäisen tarkastuksen johtajan on laadittava sisäisen tarkastuksen vuosisuunnitelma, joka tukee organisaation tavoitteiden saavuttamista ja ohjaa tarkastustoiminnan suuntaamista merkittävimpiin riskialueisiin. Näin ollen sisäisen tarkastuksen johtaja vastaa koko vuosisuunnitteluprosessista ja sen sisällöllisestä laadusta. Suunnitelman tulee perustua dokumentoituun arviointiin organisaation strategioista, tavoitteista ja riskeistä sekä niihin liittyvästä tarkastusavaruudesta. Arvioinnissa huomioidaan hallituksen ja ylimmän johdon näkemykset sekä sisäisen tarkastuksen johtajan asiantuntemus organisaation hallinto-, riskienhallinta- ja valvontaprosesseista. Arviointi edellytetään tehtäväksi vähintään kerran

vuodessa, jotta suunnitelma pysyy ajantasaisena ja vastaa organisaation toimintaympäristön muutoksiin.

Sisäisen tarkastuksen vuosisuunnitelmassa on esitettävä keskeiset varmennustoimet, joilla tuetaan organisaation hallinto-, riskienhallinta- ja valvontaprosessien arviointia ja kehittämistä. Suunnitelman tulee lisäksi sisällyttää arvio siitä, miten kriittiset riskialueet, kuten tietohallintotavan toimivuus, väärinkäytösriskien hallinta sekä vaatimustenmukaisuus- ja eettisyysohjelmien tehokkuus katetaan tarkastustoiminnan kautta. Näiden riskialueiden huomioiminen varmistaa, että tarkastustoiminto kohdistaa resurssinsa organisaation kannalta keskeisimpiin riskialueisiin. Sisäisen tarkastuksen vuosisuunnitelman on myös oltava dynaaminen ja sitä pitää päivittää tarvittaessa organisaation toiminnan ja riskien muuttuessa. Muutokset voivat liittyä esimerkiksi liiketoiminnan painopisteisiin, uusiin hankkeisiin, järjestelmien uudistuksiin, valvontaympäristön muutoksiin tai organisaatiokulttuurin kehitykseen. Suunnitelman dynaamisuus mahdollistaa, että sisäisen tarkastuksen toiminta pysyy joustavana ja pystyy vastaamaan sekä ennakoituihin että äkillisiin riskeihin. (IIA Finland, 2024, s. 67)

Sisäisen tarkastuksen johtajan täytyy käydä läpi ja muokata sisäisen tarkastuksen suunnitelmaa tarvittaessa sekä kommunikoida muutoksista ajoissa hallitukselle ja ylimmälle johdolle. Sisäisen tarkastuksen johtajan pitää mm. kommunikoida johdolle ja hallitukselle; (i) resurssien rajoitusten vaikutuksesta sisäisen tarkastuksen kattavuuteen, perustelut sille, (ii) miksi suunnitelmassa ei ole määritelty varmennustoimeksiantoa korkean riskin alueelle tai toiminnolle ja (iii) sidosryhmien ristiriitaisista pyynnöistä, esimerkiksi uusiin riskeihin perustuvista kiireellisistä pyynnöistä ja pyynnöistä korvata suunnitellut varmennustoimeksiannot neuvonantotoimeksiannoilla. (IIA Finland, 2024, s. 67)

Standardin 9.4 perusteella sisäisen tarkastuksen johtaja laatii suunnitelman arvioimalla kunkin tarkastettavan yksikön riskitason suhteessa valvontamekanismien vaikuttavuuteen ja suuntaamalla painopisteen alueille, joilla riskit ovat olennaisia ja kontrollit eivät yksin riitä. Suunnitteluun vaikuttavat lisäksi hallituksen ja ylimmän johdon esittämät pyynnöt, organisaatiossa tarkoituksenmukaisena pidetty varmennuksen kattavuus, lainsäädännöstä seuraavat pakolliset toimeksiannot sekä se, missä määrin voidaan luottaa muiden varmennuksen tarjoajien työhön, jotta vältytään päällekkäisiltä toimilta ja kohdennetaan resurssit tehokkaasti. (IIA Finland, 2024, s. 68)

Sisäisen tarkastuksen vuosisuunnitelmaa tehtäessä sisäisen tarkastuksen johtajan tulee ottaa huomioon useita keskeisiä tekijöitä, kuten lakien ja säädösten vaatimat toimeksiannot

sekä organisaation strategian ja perustehtävän kannalta kriittiset tarkastukset. Lisäksi suunnittelussa on arvioitava alueet ja toiminnot, joihin liittyy merkittäviä riskejä, ja varmistettava, että kaikki olennaiset riskit tulevat katetuiksi joko sisäisen tarkastuksen tai muiden varmennuksen tarjoajien toimesta. Suunnitelmaa laadittaessa on otettava huomioon myös neuvonantopalvelut ja tapauskohtaiset johdon pyynnöt sekä arvioitava kunkin mahdollisen toimeksiannon vaatimat resurssit ja ajankäyttö. Tämän lisäksi sisäisen tarkastuksen johtajan on tarkasteltava toimeksiantojen potentiaalista hyötyä organisaatiolle, kuten niiden kykyä tukea hallinnon, riskienhallinnan ja valvontaprosessien kehittämistä. (IIA Finland, 2024, s. 68)

Sisäisen tarkastuksen johtajan, hallituksen ja ylimmän johdon on määriteltävä yhteiset kriteerit niille muutoksille, jotka edellyttävät sisäisen tarkastuksen suunnitelman tarkistamista, ja sovittujen kriteerien sekä menettelytapojen tulee sisältyä sisäisen tarkastuksen dokumentoituihin menetelmiin. Merkittävänä muutoksena voidaan pitää esimerkiksi tilannetta, jossa strategisesti tai riskienhallinnallisesti keskeinen toimeksianto joudutaan peruuttamaan tai siirtämään myöhempään ajankohtaan. Mikäli organisaatiossa ilmenee riskejä tai uusia olosuhteita, jotka edellyttävät suunnitelman välitöntä tarkistamista ennen muodollista keskustelua hallituksen kanssa, muutoksista on ilmoitettava hallitukselle viipymättä. Tällöin hallituksen virallinen hyväksyntä suunnitelman päivittämiselle tulee hankkia mahdollisimman pian, jotta tarkastustoiminta säilyy ajantasaisena ja reagoi muuttuviin riskeihin johdonmukaisesti. (IIA Finland, 2024, s. 69)

4.2 Vuosisuunnittelun riskiperusteisuus

Riskiperusteinen suunnittelu nähdään sisäisen tarkastuksen keskeisenä keinona tuottaa lisäarvoa koko organisaatiolle. Uusien kansainvälisten sisäisen tarkastuksen ammattistandardien mukaan tarkastustoiminnon tulee kohdistaa resurssinsa osa-alueisiin, joissa riskit voivat merkittävimmin heikentää organisaation strategisten tavoitteiden saavuttamista. Tällöin sisäisen tarkastuksen toiminnan painopiste on organisaation kannalta olennaisissa kysymyksissä. Tämä lisää tarkastuksen relevanssia ja hyödyllisyyttä johdon päätöksenteossa. (Deloitte, 2024).

Riskiperusteinen suunnittelu on lähestymistapa, jossa sisäinen tarkastus suunnittelee ja kohdistaa tarkastustoimintansa organisaation merkittävimpiin riskeihin. Sinersalo ym. (2021, s. 246) esittävät, että riskiperusteisen suunnittelun keskeisenä tavoitteena on varmistaa sisäisen tarkastuksen kohdentuminen sellaisille osa-alueille, joihin liittyy

merkittäviä riskejä ja joilla voi olla vaikutusta organisaation strategisten tavoitteiden saavuttamiseen. Samalla suunnittelun avulla pyritään turvaamaan myös muiden toiminnallisten tavoitteiden toteutuminen. Sääntelyyn perustuvat tarkastusaiheet edellyttävät kuitenkin priorisointia, jotta niiden käsittely voidaan varmistaa käytettävissä olevien resurssien puitteissa. Tästä syystä tarkastuskohteiden valinnassa otetaan huomioon sekä tunnistetut riskit että sääntelystä johtuvat vaatimukset.

Lenzin ym. (2014) tutkimus tuo esiin riskiperusteisuuden merkityksen tehokkaan sisäisen tarkastuksen tunnusmerkkinä. Tutkimuksen perusteella kaikki tutkimuksen tehokkaimmiksi arvioidut tarkastustoiminnot hyödynsivät riskiperusteista suunnittelua, kun taas ei-tehokkaiden toimijoiden joukossa riskiperusteisuus oli selvästi harvinaisempaa. Näin ollen voidaan todeta, että riskiperusteisuus toimii eräänlaisena "erottelukriteerinä" tehokkaan ja tehottoman tarkastustoiminnan välillä.

Sisäisen tarkastuksen riskiperusteisuudesta voidaan asettaa vaatimuksia myös sääntelyssä. Komission delegoidun asetuksen (EU) 35/2015 artiklan 271 kohdassa 3. säädetään, että Sisäisen tarkastuksen toiminnon tulee laatia, toteuttaa ja ylläpitää tarkastussuunnitelmaa, jossa määritetään tulevien vuosien kuluessa suoritettava tarkastustyö ottaen huomioon vakuutus- tai jälleenvakuutusyrityksen kaikki toiminta ja koko hallintojärjestelmä, sekä soveltaa riskiperusteista lähestymistapaa prioriteettiensa valinnassa. EIOPA (Euroopan vakuutus- ja eläkevakuutusviranomainen, 2010) ohjeissaan hallintojärjestelmästä (ohje 43) toteaa, että organisaation tulee varmistaa, että sisäisen tarkastuksen vuosisuunnitelma perustuu perusteelliseen riskien analysointiin. Suunnitelmassa tulee lisäksi huomioida yrityksen koko liiketoiminta, hallintojärjestelmä sekä tulevaisuuden mahdolliset kehitystrendit ja innovaatiot.

Toimeksiantojen riskiperusteisen priorisoinnin osalta tulee ensin tunnistaa tarkastusavaruus (engl. audit universe). Tarkastusavaruus muodostuu kaikista mahdollisista riskialueista, joihin sisäisen tarkastuksen toimeksiannot voivat kohdistua. Tarkastusavaruuden priorisoinnin tuloksena syntyy lista mahdollisista sisäisen tarkastuksen varmennus- ja neuvonantopalveluiden toimeksiannoista. Tarkastusavaruuden muodostaminen ja priorisointi auttavat sisäistä tarkastusta riskiperusteisen tarkastussuunnitelman luomisessa. (Niemi, 2018, s. 173)

Yksi tapa valmistella sisäisen tarkastuksen suunnitelmaa on organisoida mahdolliset tarkastettavat kohteet tarkastusavaruudeksi riskien tunnistamisen ja arvioinnin helpottamiseksi (IIA Finland, 2024, s. 67). Tarkastusavaruuteen vaikuttavat monenlaiset

tekijät, jotka voivat tulla sekä organisaation sisäpuolelta että ulkopuolelta. Näihin kuuluvat muun muassa organisaation strategia, toimiala, koko ja henkilöstömäärä, sen toiminnot ja prosessit, tuotteet, suoritteet, projektit ja hankkeet, lakisääteiset velvoitteet, johdon esittämät ehdotukset, ERM-riskit, sekä muutokset tavoitteissa ja keskeisissä fokusalueissa. (Niemi, 2018, s. 173)

Sisäisen tarkastuksen johtajan tulisi keskustella tarkastusavaruudesta ylimmän johdon kanssa tunnistaakseen ja ymmärtääkseen niihin liittyviä riskejä sekä riskien potentiaalisia vaikutuksia. Ylimmältä johdolta tulee tiedustella myös, mitä muutoksia on suunnitteilla tarkastusavaruuteen kohdistuville toiminnoille. (Niemi, 2018, s. 174) Tarkastusavaruus on hyödyllisin, kun se perustuu organisaation tavoitteiden ja strategisten aloitteiden ymmärtämiseen ja on linjassa organisaation rakenteen tai riskiympäristön kanssa. Sisäisen tarkastuksen johtaja voi yhdistää nämä tarkastuskohteet keskeisiin riskeihin, kun hän valmistelee organisaation kattavaa riskinarviointia ja määrittelee koko organisaation varmennuksen kattavuutta. Tämän prosessin avulla sisäisen tarkastuksen johtaja voi priorisoida riskejä, joiden arviointia jatketaan sisäisen tarkastuksen toimeksiantojen aikana. (IIA Finland, 2024, s. 67)

Sisäisen tarkastuksen toiminnot eivät välttämättä ole dokumentoineet organisaationsa tarkastusavaruutta. Tämä voi johtua siitä, että sisäinen tarkastus ei täysin ymmärrä yrityksen toimintaympäristöstä, tarkastus nojaa liikaa aiempiin tarkastuksiin tulevan tarkastussuunnittelun perustana tai sisäisellä tarkastuksella on rajalliset resurssit riskiympäristön kattavaan kartoittamiseen. Tämä voi johtaa siihen, että sisäisen tarkastuksen resursseja käytetään organisaatiossa vähemmän tärkeille alueille. Sisäisen tarkastuksen johtaja voi myös päättää olla kehittämättä täydellistä tarkastusuniversumia, koska se keskittyy tunnistettuihin riskeihin. Vaikka tämä on kohtuullista, se aiheuttaa oman riskinsä, että organisaation merkittäville, olennaisille alueille tai toiminnoille tai strategisille tavoitteille ei anneta riittävää varmuutta. (Pitt, 2014, ss.175–176)

Parhaassa tapauksessa sisäinen tarkastus hyödyntää organisaatiossa laadittuja riskienhallintasuunnitelmia riskien tunnistamiseksi. Näitä voidaan tukea sisäisen tarkastuksen omalla riskinarvioinnilla. (Pitt, 2014, s.171)

4.3 Vuosisuunnittelun strategiaperusteisuus

Sisäisen tarkastuksen kansainvälisten ammattistandardin 9.4 vaatimuksena (IIA Finland, 2024, s. 66) on, että sisäisen tarkastuksen johtajan täytyy laatia sisäisen tarkastuksen suunnitelma, joka tukee organisaation tavoitteiden saavuttamista. Sisäisen tarkastuksen suunnitelman täytyy perustua dokumentoituun arviointiin organisaation strategioista, tavoitteista ja riskeistä. Usein myös yrityksen tavoitteet heijastavat strategiassa määriteltyjä tavoitteita. Strategiaperusteisuuden huomioiminen ei tarkoita ainoastaan strategisten asiakirjojen tarkastelua, vaan yksiköiden systemaattista tarkastelua suhteessa organisaation tavoitteisiin.

Standardin 9.4 soveltamisohjeen (IIA Finland, 2024, s. 67) mukaan organisaationlaajuisen riskiarvion suorittamiseksi sisäisen tarkastuksen johtajan tulee pohtia tavoitteita ja strategioita, ei vain laajalla organisaatiotasolla, vaan myös yksittäisten tarkastettavien yksiköiden tasolla. Sisäisen tarkastuksen suunnitelmaa laatiessaan sisäisen tarkastuksen johtajan tue ottaa huomioon organisaation tehtävän tai strategian kannalta kriittiset toimeksiannot, eli tarkastukset ja neuvonantopalvelut (IIA Finland, 2024, s. 68).

Standardin 4.2 mukaan (IIA Finland. 2024, s. 32) asianmukaisen ammatillisen huolellisuuden huomioimiseksi, sisäisen tarkastuksen johtajan täytyy ottaa huomioon mm. organisaation strategia ja tavoitteet toteuttaessaan sisäisen tarkastuksen suunnitelman perustana olevaa riskinarviointia.

4.4 Tiedonkeruumenetelmät

Tarkastusavaruuden sekä toimeksiantojen priorisointia varten sisäisen tarkastuksen tulee kerätä tietoa mm. organisaation tilasta. Sisäinen tarkastus voi kerätä tietoa monella eri tavalla. Sisäisen tarkastuksen johtajan tulisi aloittaa sisäisen tarkastuksen suunnitelman laatiminen konsultoimalla ylintä johtoa ja hallitusta ymmärtääkseen organisaation strategiat, liiketoimintatavoitteet, riskit ja riskienhallintaprosessit. (The Institute of Internal Auditors, 2019, s. 96)

Sisäisen tarkastuksen on tarkastusavaruuden määrittämiseksi ja toimeksiantojen priorisoinnin tueksi hankittava tietoa muun muassa organisaation kokonaisvaltaisesta tilasta. Tätä varten sisäinen tarkastus voi hyödyntää useita erilaisia tiedonkeruumenetelmiä. Sisäisen tarkastuksen johtajan tulisi aloittaa vuosisuunnitelman

laatiminen keskustelemalla ylimmän johdon ja hallituksen kanssa, jotta hän voi muodostaa kattavan käsityksen organisaation strategiasta, liiketoiminnallisista tavoitteista sekä riskeistä ja käytännöistä, joilla riskienhallintaa organisaatiossa toteutetaan. (The Institute of Internal Auditors, 2019, s. 96) Sisäisen tarkastuksen tulisi esimerkiksi haastatella hallituksen puheenjohtaja ja mahdollisesti tarkastusvaliokunnan jäseniä. Sisäisen tarkastuksen tulisi lisäksi haastatella yhtiön liiketoimintajohtoa sekä mahdollisten tarkastuskohteiden johtoa. Myös yrityksen avainhenkilöitä, kuten yrityksen asiantuntijoita, tietosuoja- ja tietoturvavastaava, Compliance Officer tulisi haastatella. Sisäisellä tarkastuksella on mahdollisuus toteuttaa tiedon keruuta myös erityyppisillä kyselylomakkeilla. (Niemi, 2018, s. 175) Sisäinen tarkastus voi halutessaan tunnistaa riskejä myös riskinarviointeihin perustuvien kyselyiden, fasilitoitujen riskinarviointien ja sidosryhmähaastattelujen avulla (Pitt, 2014, s.171).

Sisäinen tarkastus voi hyödyntää riskiympäristön tiedonkeruussaan Compliancen tekemiä valvontoja tai tarkastuksia. On tärkeää, että eri varmennuspalveluita tarjoavat yksiköt koordinoivat työnsä mahdollisimman hyvin, jotta vältytään päällekkäiseltä varmentamiselta ja tehottomuudelta (Ratsula, 2016, luku 5.8).

Sisäisen tarkastuksen vuosisuunnitelman tulee perustua perusteelliseen riskianalyysiin ja analyysissä tulee ottaa huomioon mahdolliset yrityksen ja toimintaympäristön muutokset sekä innovaatiot (EIOPA, 2017, s. 19). Näin ollen varmistaakseen mahdollisimman kattavan ja riskiperusteisen vuosisuunnitelman, sisäinen tarkastus voi kerätä tietoa toimintaympäristön mahdollisista muutoksista ja kehityssuunnista esim. konsulttiyhtiöiden tutkimuksista, talousennusteista ja erilaisista toimintaympäristön analyyseistä. Lisäksi sisäinen tarkastus voi kerätä tietoa organisaation strategisista suunnitelmista ja liiketoimintasuunnitelmista sekä aiemmista sisäisten ja ulkoisten tarkastusraporttien havainnoista (Pitt, 2014, s.171).

4.5 Vuosisuunnitteluun liittyvä riskiarvio

Standardissa 9.4 edellytetään (IIA Finland, 2024, s. 67), että sisäisen tarkastuksen vuosisuunnitelmaa varten tulee tehdä vähintään vuosittain organisaation kattava riskien arviointi. Riskiarviota sekä sisäisen tarkastuksen vuosisuunnitelmaa tulee päivittää tarpeen vaatiessa. Myös eri viranomaiset voivat ohjata sisäisen tarkastuksen toiminnon suunnittelua. Euroopan pankkiviranomainen (EBA) edellyttää, että luottolaitosten sisäiset tarkastajat noudattavat sisäisen tarkastuksen ammattistandardeja ja soveltavat

tarkastustoiminnan suunnittelussa riskiperusteista lähestymistapaa. Sisäisen tarkastuksen tulee myös laatia vähintään kerran vuodessa tarkastussuunnitelma vuosittaisten sisäisen tarkastuksen valvontatavoitteiden perusteella. (EBA, 2018, s. 45)

Sisäisen tarkastuksen suunnitelmaa voi olla tarve päivittää useammin kuin vuosittain. Sitä voidaan päivittää esimerkiksi puolivuosittain, neljännesvuosittain tai jopa kuukausittain. Organisaatiossa tapahtuvien muutosten koko, monimutkaisuus ja tyyppi suhteessa organisaation hallinto-, riskienhallinta- ja valvontaprosessien kypsyyteen tulisi ottaa huomioon määritettäessä asianmukaista työmäärää riskiarvion päivittämiseksi.

Sisäisen tarkastuksen tehtävänä on systemaattisesti tarkastella organisaation riskejä ja varmistaa, että tunnistetut keskeiset riskit on validoitu. Usein nämä riskit on koottu organisaation riskienhallintajärjestelmään, jota sisäinen tarkastus voi hyödyntää arviointinsa pohjana. Näiden analyysien avulla sisäinen tarkastus pystyy varmistumaan, että sen oma tarkastusavaruus ja siihen liittyvät riskiarviot kattavat organisaation olennaisimmat riskialueet. Johdon toimittamiin riskitietoihin voidaan tukeutua vain silloin, kun sisäinen tarkastus on todennut organisaation riskienhallintaprosessien toimivan tehokkaasti ja tuottavan luotettavaa tietoa. (IIA Finland, 2024, s. 67)

Standardissa 9.4 (IIA Finland, 2024, ss. 67–68) mainitaan, että koko organisaatiota käsittävän riskiarvion suorittamiseksi sisäisen tarkastuksen johtajan tulee miettiä tavoitteita ja strategiaa sekä laajasti koko organisaation kattavalla tasolla että yksittäisten tarkastettavien yksiköiden tasolla. Riskinarvioinnin perusteeksi sisäinen tarkastus voi kerätä tietoja päättyneistä sisäisistä tarkastuksista ja neuvonantopalveluista sekä keskusteluista hallituksen jäsenten ja ylimmän johdon kanssa. Sisäisen tarkastuksen johtajan vastuisiin kuuluu myös prosessin kehittäminen sellaisten merkittävien, uusien ja esiin nousevien riskien havaitsemiseksi ja arvioimiseksi, jotka voivat vaikuttaa organisaation toimintaan. Järjestelmällinen riskienhallintaprosessien kehittäminen mahdollistaa, että relevantit riskit tunnistetaan ajoissa ja ne voidaan tarvittaessa sisällyttää sisäisen tarkastuksen vuosisuunnitelmaan. Vähäisten resurssien vuoksi sisäisen tarkastuksen voi olla mahdotonta arvioida vuosittain kaikkia tarkastusavaruuden riskejä, jolloin sisäisen tarkastuksen johtajalla voi luottaa enemmän riskitietojen lähteisiin, kuten johdon riskinarviointeihin, hallituksen ja ylimmän johdon tapaamisiin sekä aiempien toimeksiantojen ja muun tarkastustyön tuloksiin.

4.6 Vuosisuunnittelun rotaatioperusteisuus

Rotaatiolla sisäisen tarkastuksen kontekstissa tarkoitetaan suunnitelmallista käytäntöä, jossa eri liiketoiminta-alueita, prosesseja tai muita riskialueita tarkastetaan tietyin aikavälein. Rotaation tavoitteena on varmistaa, että organisaation toiminnan kaikki keskeiset osa-alueet, jotka liittyvät olennaisiin riskeihin tai muutoksiin, tulevat tarkastetuiksi jollain aikavälillä tai riittävän usein.

Finanssialan toimijoihin (pankit, vahinko- ja henkivakuutusyhtiöt sekä työeläkeyhtiöt) kohdistuu yksityiskohtaista sääntelyä, esimerkiksi riskien, likviditeetin, sijoitustoiminnan ja omien varojen riittävyyden osalta. Sääntely sisältää myös vaatimuksia tiettyjen aihealueiden tarkastamiseen, joko sisäisen tarkastuksen tai muun riippumattoman tahon toimesta. Näitä aihealueita ovat mm. hallintojärjestelmä, palkitseminen, vakavaraisuuden hallinta. EIOPA (Euroopan vakuutus- ja eläkevakuutusviranomainen, 2010) ohjeissaan hallintojärjestelmästä (ohje 43) mainitsee, että yrityksen tulisi varmistaa, että sisäisen tarkastuksen suunnitelma kattaa kaikki merkittävät toiminnat, jotka on määrä tarkastaa kohtuullisessa ajassa.

Vaatimuksia tiettyjen aihealueiden tarkastamiseen on eniten pankkipuolelle ja sen jälkeen vahinko- ja henkivakuutusyhtiöön. Sääntely ei sisällä vaatimuksia työeläkeyhtiöiden sisäiselle tarkastukselle tiettyjen aihealueiden tarkastamiseen. Osa tarkastettavista aiheista tulee tarkastaa säännöllisesti, esimerkiksi vähintään vuosittain. Vaikka sääntely asettaa sisäisen tarkastuksen vuosisuunnittelulle riskiperusteisuuden yleiseksi periaatteeksi, käytännön toteutuksessa tämä periaate ei kuitenkaan aina toteudu täysin johdonmukaisesti. Sääntelyyn sisältyvät velvoitteet edellyttävät, että tietyt tarkastusaiheet sisällytetään tarkastussuunnitelmaan riippumatta siitä, kuinka merkittäviä ne ovat sisäisen tarkastuksen tai organisaation omien riskiarvioiden näkökulmasta. Toisin sanoen osa tarkastuskohteista on sisällytettävä suunnitelmaan, koska lainsäädännölliset vaatimukset eivät jätä näiden osalta harkinnanvaraa. Tämä johtaa tilanteeseen, jossa kaikki vuosisuunnitelman tarkastuskohteet eivät ole riskiperusteisen priorisoinnin näkökulmasta keskeisimpiä. Tämä muodostaa ristiriidan riskilähtöisen tarkastustyön ja normiperusteisten pakollisten tarkastusten välillä. Normiperusteisuus lisää sisäisen tarkastuksen työmäärää erityisesti finanssialalla, jossa sääntelyyn perustuvat velvoitteet ovat laajoja sekä tarkastusaiheiden määrän että raportointivaatimusten osalta. Näin ollen sääntelyn aiheuttama velvoittavuus vaikuttaa tarkastustoiminnan kokonaisresurssitarpeeseen ja tarkastussuunnittelun käytännön toteutukseen. (Sinersalo ym., 2021, ss. 244–245)

Vuosisuunnittelun rotaatioperusteisuudesta voidaan myös säätä viranomaisten ohjeilla, laeilla ja määräyksillä. Finanssivalvonta (2024) on vahinko- ja henkivakuutusyhtiöihin kohdistuneessa teema-arviossaan todennut, että yhtiöiden tarkastussuunnitelmien laadintaprosesseissa ja suunnitelmien varsinaisessa sisällössä ilmeni kyselyvastauksiin perustuvia, selkeitä eroavaisuuksia. Arvion mukaan useissa yhtiöissä tarkastussuunnitelmat eivät ottaneet huomioon rotaatiovaatimuksia edes kaikkein keskeisimpien toimintojen osalta. Tarkastussuunnitelmien laatiminen ei myöskään perustunut systemaattiseen ja riskiperusteiseen menetelmään, jonka tulisi tukea prioriteettien valintaa. Hyvin rakennettu ja riskien kokonaiskuvan ymmärtämiseen perustuva tarkastussuunnitelma ovat keskeisiä elementtejä sekä tarkastuskohteiden valintaan, että niiden painotusten määrittelyyn. Tällainen suunnitelma auttaa kohdentamaan sisäisen tarkastuksen käytettävissä olevan ajan ja tarkastusresurssit tarkoituksenmukaisesti ja suhteessa toiminnan olennaisiin riskitekijöihin.

Sisäisen tarkastuksen vanhoihin standardeihin perustuvassa kansainvälisten ammatillisten käytäntöjen viitekehyksen (IPPF) täydentävien ohjeiden käytännön oppaan ”Developing a Risk-based Internal Audit Plan (The Institute of Internal Auditors, 2020, s. 18) mukaan Puhtaasti riskiin perustuvassa sisäisen tarkastuksen suunnitelmassa sisäisen tarkastuksen johtajat voivat soveltaa yhtä kahdesta strategiasta saavuttaakseen ihanteellisen suunniteltujen toimeksiantojen rotaation:

1. Tarkastussuunnitelma voi perustua jatkuvaan riskinarviointiin ilman ennalta määriteltyä rotaatiota. Kun huomioidaan nykyinen riskiympäristön kiihtyvä muutosvauhti, monet organisaatiot ovat nykyisessä riskiympäristössä, ottaneet käyttöön jatkuvat auditoinnit. Tämä antaa heille mahdollisuuden vastata ketterästi ja dynaamisesti muutoksiin ympäri vuoden, kun tarkastussuunnitelmaan tehdään muutoksia tarpeen mukaan. Tällaiset tarkastussuunnitelmat tunnistetaan rullaaviksi, tai dynaamisiksi.
2. Tarkastusten rotaatio perustuu riskiarvioinnissa määritettyyn jäännösriskin tasoon. Tarkastettavat yksiköt voidaan tarkastaa riskiperusteisesti esimerkiksi alla oleviin määräaikoihin perustuen:

    - Korkeariskisiksi luokitellut tarkastettavat yksiköt voidaan tarkastaa esim. vähintään kerran vuodessa
    - Yksiköt, joiden riskitaso on kohtuullinen, voidaan tarkistaa vähintään kahden vuoden välein

- Alhaisen riskin yksiköt voidaan tarkastaa vain kerran kolmessa vuodessa (tai ei ollenkaan)

Rotaatioperusteisessa tarkastussuunnitelmassa voidaan huomioida sisäisen tarkastuksen suorittamien tarkastusten ja neuvonantopalveluiden lisäksi Compliancen tarkastukset/valvonnat, erilaiset kolmannen osapuolen tekemät auditoinnit (mm. tietohallinnon eri prosessit tai järjestelmät) ja tilintarkastajien työ. Vaikka opinnäytetyö ei kohdistu julkiselle sektorille, voidaan sen hallintovaatimuksista johtaa rotaatioperusteiselle tarkastamiselle tärkeitä perusteita. Hallintopolitiikka paperin ”Enhancing Co-operation Between Internal and External Auditors in the Public Sector” (OECD, 2024, s.18) mukaan parempi riskienhallinta ja sisäinen valvonta nähdään hyötyinä, jotka ovat yhtä merkittäviä kuin tarkastusresurssien tehokas käyttö. Sisäisten tarkastajien ja tilintarkastajien välinen yhteistyö mahdollistaa laajemman tehtäväkokonaisuuden sisällyttämisen tarkastuksen piiriin sekä tehostaa tarkastussuositusten toimeenpanon seurantaa. Yhteistyön nähtiin tuottavan synergiaa, koska sisäisten tarkastajien ja tilintarkastajien vaikutusalueet sisäiseen valvontaan nähden eroavat toisistaan. Tilintarkastajien kokonaisuuden sisällyttäminen tarkastuksen piiriin laajentaa tehtäväkokonaisuutta mutta toisaalta se myös indikoi sisäiselle tarkastukselle, että se voi jättää pois omasta tarkastuksen sisällöstä tilintarkastajien tarkastaman kokonaisuuden. Sisäisen tarkastuksen pitää kuitenkin olla tällöin tietoinen, että mitä ja miten tilintarkastus on oman tarkastuksensa tehnyt. Tilintarkastajan tekemän työn hyödyntäminen voi näin olleen vapauttaa lisäresursseja sisäisen tarkastuksen käyttöön.

Vuosisuunnittelun rotaatioperusteisuudessa voidaan hyödyntää myös varmennuskarttaa (assurance map), johon on koottu kaikki yritykseen kohdistetut sisäiset ja ulkoisten toimijoiden tekemät varmennukset, tarkastukset ja auditoinnit. Ulkoisia varmennuksia voivat mm. olla tietojärjestelmiin tai tietoturvaan kohdistetut auditoinnit ja Finanssivalvonnan tekemät tarkastukset tai teema-arviot. Sisäisen tarkastuksen toiminnot työskentelevät organisaatioissa tukeakseen hallinnon, riskienhallinnan ja valvontaprosessien parantamista. Onnistuminen edellyttää sisäisen tarkastuksen ja johdon sekä muiden sisäisten ja ulkoisten varmennuspalvelujen tarjoajien välistä yhteistyötä. On epätodennäköistä, että sisäisen tarkastuksen toiminnalla olisi riittävästi resursseja varmennuksen tarjoamiseen koko organisaatiolle. Varmennustyön koordinoinnissa sisäisen tarkastuksen ja muiden varmennuspalveluja tarjoavien kanssa voidaan saavuttaa tehokkuusetuja, joka on erityisen tärkeää pienille tarkastusorganisaatioille. Sisäisen tarkastuksen johtajilla tulisikin olla selkeä käsitys sidosryhmien toteuttamista tarkastuksista,

varmennuksista ja auditoinneista. Tämä saavutetaan parhaiten varmennuskartoituksen avulla. (Pitt, 2014, ss.176–177).

Rotaatioperiaate kytketään myöhemmin esitettävään riskiarviomalliin siten, että yksiköt, joita ei ole tarkastettu viime vuosina riittävän usein, nostetaan vuosisuunnitelmalle riippumatta riskipistemallin tuloksesta.

4.7 Vuosisuunnitelman muuttaminen

Sisäinen tarkastus voi tarpeen vaatiessa muuttaa jo hallituksessa hyväksyttyä vuosisuunnitelmaansa. Sisäisen tarkastuksen johtajan täytyy tällöin käydä läpi koko tarkastussuunnitelma ja muokata sitä tarvittavilta osin. Lisäksi muutoksista tulee kommunikoida ajoissa hallitukselle ja ylimmälle johdolle (IIA Finland, 2024, s. 67). Sisäisen tarkastuksen johtajalla on vastuu tehdä vuosisuunnitelma mahdollisimman joustavaksi niin, että sisäinen tarkastus voi muuttaa sitä tarpeen vaatiessa vuoden aikana. Sisäisen tarkastuksen johtajan pitää sopia hallitus- ja tarkastusvaliokunnan jäsenien kanssa käytännön toimintatavoista, joilla mahdolliset vuoden aikana tehtävät vuosisuunnitelman muutokset viedään organisaation johdon, hallituksen ja tarkastusvaliokunnan käsiteltäväksi sekä hyväksytettäväksi. (Niemi, 2018, ss. 178–179) Mikäli vuoden aikana havaitaan sellaisia riskejä, jotka edellyttävät vuosisuunnitelman uudelleenarviointia ennen muodollisen keskustelun käymistä hallituksen kanssa, tulee hallitukselle antaa välitön tieto näistä muutostarpeista. Lisäksi suunnitelmaan tehtävät tarkennukset ja muutokset tulee hyväksyä virallisesti mahdollisimman pikaisesti, jotta päätöksenteko ja valvontatehtävät voivat edetä asianmukaisesti (IIA Finland, 2024, s. 69).

Sisäisen tarkastuksen vuosisuunnitelman tarkistamiselle tai täydentämiselle voi yrityksessä syntyä tarvetta aina, kun sen toimintaan tai toimintaympäristöön kohdistuu merkittäviä muutoksia. Suunnitelmaa voidaan joutua päivittämään myös silloin, kun sisäisen tarkastuksen omat resurssiolosuhteet, kuten henkilöstön määrä tai käytettävissä oleva työaika, muuttuvat. Yrityksen sisäisiä muutoksia voivat olla esimerkiksi taloudellisen tilanteen heikentyminen tai vahvistuminen, ennakoimattomat organisaatiouudistukset, yritysostot sekä strategian uudelleen suuntaaminen. Toimintaympäristön tasolla muutosta voivat puolestaan aiheuttaa esimerkiksi markkinoiden kilpailutilanteen äkillinen muutos, maailmanlaajuiset tai alueelliset pandemiat sekä erilaiset turvallisuutta heikentävät tekijät tai alueellinen levottomuus. (Niemi, 2018, s. 179)

4.8 Isojen ja pienien tarkastusorganisaatioiden erot vuosisuunnittelussa

Tutkimuksen (Zainal Abidin, 2017, s. 361) löydöksien mukaan tarkastusvaliokunnan aktiivinen osallistuminen sekä organisaation riskienhallintajärjestelmän olemassaolo ovat merkittävästi ja positiivisesti yhteydessä riskiperusteisten tarkastusten käyttöönottoon. Sisäisen tarkastuksen kokemus, sisäisen tarkastuksen toiminnon koko, tarkastusvaliokunnan pätevyys, ja sisäinen valvontajärjestelmä eivät ole merkittäviä riskiperusteisen tarkastuksen olemassaolon ennustamisessa. Vaikka tutkimus ei kohdistunut pelkästään tarkastussuunnitteluun, voidaan perustellusti olettaa, että nämä tekijät luovat edellytyksiä myös systemaattiselle ja riskiperusteiselle suunnittelulle. Riskiperusteinen tarkastaminen edellyttää kattavaa ymmärrystä organisaation riskiympäristöstä, minkä vuoksi muodollinen riskienhallintaprosessi ja tarkastusvaliokunnan kiinnostus tukevat sen tehokasta toteuttamista.

Tutkimuksessa "Factors associated with the size of internal audit functions: evidence from Kuwait" (Alhajri, 2017) tarkastellaan sisäisen tarkastuksen yksikön kokoa ja siihen vaikuttavia tekijöitä. Tutkimuksessa todetaan, että suuremmilla organisaatioilla on yleensä laajemmat ja kattavammat sisäisen tarkastuksen resurssit. Tämä mahdollistaa laajemman tarkastustoiminnan ja potentiaalisesti kattavamman vuosisuunnittelun. Pienissä organisaatioissa resurssit ovat rajallisemmat, mikä voi rajoittaa vuosisuunnitelman laajuutta ja tarkastusten määrää.

Tutkimuksessa "The effect of audit committee effectiveness, internal audit size and outsourcing on greenhouse gas emissions disclosure" (Abdalla ym., 2025) todetaan, että sisäisen tarkastuksen yksikön koko on positiivisesti yhteydessä tarkastustoiminnan laatuun ja kattavuuteen. Suurempi tarkastusorganisaatio pystyy kattamaan laajemmin erilaisia riskejä ja toimintoja, mikä viittaa siihen, että myös vuosisuunnittelun kattavuus paranee yksikön koon kasvaessa.

Pienemmissä sisäisen tarkastuksen yksiköissä resurssien rajallisuus rajoittaa systemaattista riskien arviointia, tarkastustoiminnan kattavuutta ja jatkuvaa auditointisuunnitelman päivittämistä. Tällöin voidaan olettaa, että vuosisuunnittelun riski- ja strategiaperusteisuus ei ole niin kattavaa eikä vuosisuunnittelun kattavuus ole niin laajaa kuin suuremmissa yksiköissä. Tutkimuksissa (Alhajri, 2017, Abdalla, Alodat, Salleh & Al-Ahdal, 2025, Zainal Abidin, 2017) ei kuitenkaan ole löytynyt selvää havaintoa siitä, että pienemmät tarkastusorganisaatiot toteuttaisivat riskiperusteista vuosisuunnitelmaa huonommin kuin suuret tarkastusorganisaatiot.

5 Opinnäytetyön empiirinen osuus

Tässä luvussa kuvataan opinnäytetyön empiirinen osuus, joka keskittyy kohdeorganisaation sisäisen tarkastuksen riskiperusteisen vuosisuunnittelun kehittämiseen. Kehittämistyö aloitettiin kesällä 2024 ja se kohdistui vuoden 2025 tarkastussuunnitelmaan. Kehittämistyössä otetaan huomioon myös vuoden 2026 tarkastussuunnitelma, jonka prosessi käynnistyi vuoden 2025 alussa ja sitä tehtiin vuoden lopulle asti. Empiirisen osuuden tarkoituksena on syventää teoriaosuudessa esitettyjä periaatteita tuomalla niihin käytännönläheinen näkökulma sekä tarkastella niiden sovellettavuutta organisaation toimintaympäristössä. Empiirinen aineisto pohjautuu tekijän omiin havaintoihin sekä sisäisen tarkastuksen johtajan kanssa käytyihin keskusteluihin. Näiden avulla tunnistettiin vuosisuunnitteluun liittyvät keskeiset puutteet ja kehittämistarpeet, joiden perusteella laadittiin uusi malli vuosisuunnittelun toteuttamiseksi.

Luvun alussa esitellään kohdeorganisaation aikaisempi käytäntö sisäisen tarkastuksen vuosisuunnittelussa. Tämän jälkeen kuvataan kehittämisprosessin eteneminen vaihe vaiheelta vuodesta 2024 lähtien aina vuoden 2025 lopulle asti. Kehittämisprosessin kuvauksessa kerrotaan ja havainnollistetaan, millaisia menetelmiä ja työvälineitä hyödynnettiin, millaista aineistoa kerättiin sekä miten tietoa analysoitiin. Lisäksi tarkastellaan, millaisia havaintoja ja tuloksia kehittämistyö tuotti organisaation näkökulmasta.

Luvun lopussa arvioidaan empiirisen osuuden tuloksia suhteessa työn tavoitteisiin ja pohditaan, millaisia vaikutuksia kehittämistyöllä on kohdeorganisaation sisäisen tarkastuksen toimintaan ja sen tulevaisuuden suunnitteluun.

5.1 Sisäisen tarkastuksen vuosisuunnittelun lähtötilanne kohdeorganisaatiossa

Kohdeorganisaation sisäisen tarkastuksen vuosisuunnittelua on perinteisesti toteutettu sisäisen tarkastuksen standardien mukaisesti strategia- sekä riskilähtöisen tarkastelun pohjalta (IIA Finland, 2024, s. 66). Vuosisuunnitelman toteuttamiseen on osallistunut sisäisen tarkastuksen johtaja ja sisäinen tarkastaja. Vaikka lähestymistapa vuosisuunnitteluun noudatti muodollisesti standardeja, suunnitelman kokonaisvaltainen laajuus jäi kuitenkin melko rajalliseksi. Keskeinen puute liittyi siihen, että sisäisen tarkastuksen käyttöön oli laadittu kevyt riskiarvio. IIA:n implementointiohjeistus (The Institute of Internal Auditors, 2019, s. 96) edellyttää, että riskiperusteinen suunnittelu

pohjautuu dokumentoituun, organisaatiotasoiseen riskinarvioon. Kohdeorganisaatiolta puuttui tällainen laaja riskiarvio ja tämä heikensi teorian edellyttämää riskiarvioinnin systemaattisuutta.

Vuosisuunnitteluprosessia ohjasi vahvasti sisäisen tarkastuksen rajalliset resurssit, joka johti siihen, että suunnitteluun panostaminen jäi vähäiseksi. Tämän seurauksena myös vuosisuunnitelman riskiperusteisuuden ja strategisen kohdentamisen syvyys jäi vähäiseksi. Käytännössä seuraavan vuoden suunnittelutyö käynnistettiin lokakuussa johdon haastatteluilla.

Ennen vuotta 2024 vuosisuunnitteluun kuului toimitusjohtajan ja muun ylemmän johdon haastattelut. Sisäinen tarkastus teki myös omaa riskianalyysiä, joka perustui eri riskilähteistä mm. operatiivisten riskien ilmoituskanavasta saatuihin tietoihin sekä sisäisen tarkastuksen itse tekemiin havaintoihin. Johdon haastattelujen ja kevyen riskianalyysin perusteella sisäinen tarkastus kohdisti vuosisuunnitelmansa tarkastukset johdon määrittämiin strategisiin vahvuuksiin.

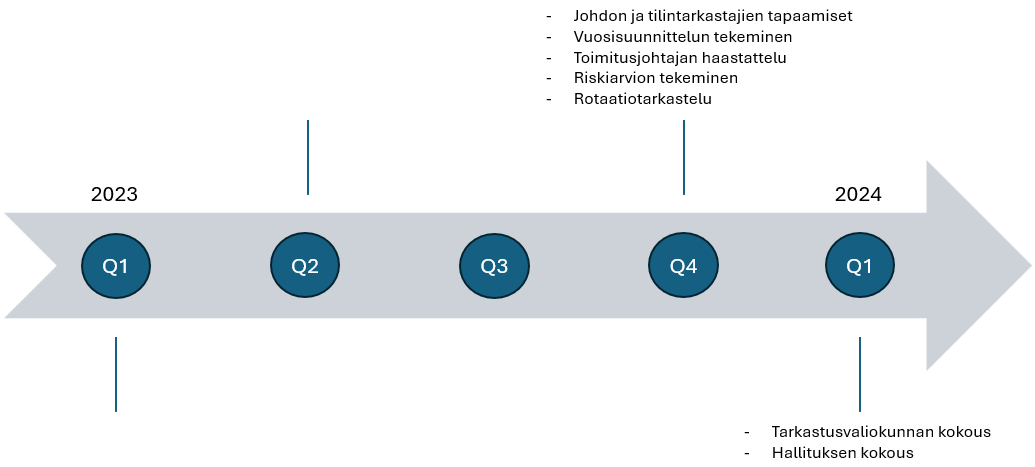
Riskianalyysissä eri yksiköille annettiin väri sen sisältämän riskin perusteella. Taulukossa 1 on kuvattu ennen vuotta 2024 riskianalyysissä käytettyjen värien ja niiden tarkoittamien riskiarvioiden värien selitykset.

Taulukko 1. Ennen vuotta 2024 käytetty riskiarvion väri ja värin selitys

Riskiarvion väri	Riskiarvion värin selitys
Vihreä	Vähän riskiä
Keltainen	Jonkin verran riskiä
Oranssi	Kohtalaisesti riskiä
Punainen	Paljon riskiä

Kuvassa 3 esitetty aikajana osoittaa, että varsinainen vuosisuunnittelutyö painottui vuoden neljännelle kvartaalille. Kvartaalin aikana toteutettiin johdon ja tilintarkastajien tapaamiset, toimitusjohtajan haastattelu sekä riskien ja rotaatioiden arviointi, joiden pohjalta vuosisuunnitelma laadittiin. Seuraavan vuoden ensimmäisellä kvartaalilla suunnitelma vietiin edelleen tarkastusvaliokunnan ja hallituksen käsiteltäväksi, mikä päätti vuosisuunnitteluprosessin.

Kuva 3. Vuosisuunnittelun aikataulu vuoteen 2023 asti.



5.2 Riskiperusteisen vuosisuunnittelun kehittäminen kohdeorganisaatiossa

5.2.1 Vuosisuunnitelma vuodelle 2025

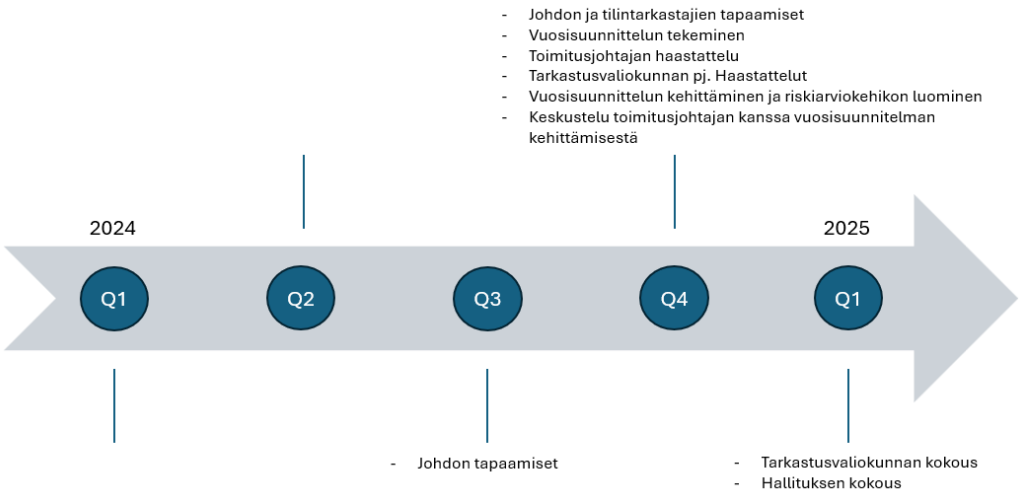
Sisäinen tarkastus aloitti vuoden 2025 vuosisuunnittelun syyskuussa 2024. Sisäinen tarkastus teki alustavan suunnitelman vuosisuunnitelman sisällöstä ja kattavuudesta. Kattavuuden arvioinnissa otettiin huomioon sisäisen tarkastuksen resurssien tuomat rajoitteet. Sisäinen tarkastus katsoi, että vuosisuunnittelun yhteydessä tehtävään riskianalyysiin tulisi sisällyttää sisäisen tarkastuksen oma riskiarvio, sen tulisi olla mahdollisimman kattava ja siinä tulisi arvioida riskejä värien sijasta numeerisesti, jolloin riskillisyyden arvottaminen ja havainnollistaminen olisi selkeämpää. Lisäksi tunnistettiin, että riskianalyysissä tulisi ottaa huomioon rotaatioperusteisuus, varmuuskartta (assurance map) ja strategiaperusteisuuden arviointi. Sisäinen tarkastus tunnisti tarpeen myös yhtiön eri toimintojen ja prosessien paremmalle seurannalle, jotta yhtiön toimintaan sisältyvistä riskeistä saataisiin kattavampi kuva. Tätä seurantaa sisäinen tarkastus alkoi kutsumaan jatkuvaksi seurannaksi. Lopuksi sisäinen tarkastus arvioi, että onko sen mahdollista kokonaisvaltaisesti toteuttaa vuosisuunnittelun kehitystyö olemassa olevilla henkilöresursseilla ja tuli siihen tulokseen, että toteuttaminen voidaan tehdä jatkuvan kehittämisen kautta. Sisäinen tarkastus arvioi vuosisuunnitteluun liittyviä sisäisen tarkastuksen kansainvälisten ammattistandardien vaatimuksia ja päätti lähteä ensimmäisenä kehittämään omaa riskiperusteista arviointimallia. Mallia kehitettiin MVP- (minimum viable product) periaatteella, jolloin tavoitteena ei ollut heti luoda valmista

tuotetta, vaan mahdollisimman kevyesti toteutettu versio, joka oli kuitenkin toimiva ja jonka kautta saadaan nopeasti tietoa käytettävyydestä jatkokehityksen tueksi.

Vuosisuunnittelun kehittäminen aloitettiin vasta syyskuussa 2024, joten jatkuvan seurannan systemaattinen toteuttaminen ei ollut enää mahdollista, koska se olisi vaatinut koko vuoden ajan tehtävää yhtiön toiminnan seurannan. Loppuvuoden osalta oli aikataulusyistä mahdollista toteuttaa ainoastaan tarkastusvaliokunnan puheenjohtajan, toimitusjohtajan, johtoryhmän, toisen puolustuslinjan (Compliance ja riskienhallinta) ja tilintarkastajien haastattelut.

Kuvassa 4 kuvataan vuoden 2024 aikana tehtyä vuoden 2025 suunnitteluprosessia. Vuosisuunnitteluprosessi oli laajempi kuin aikaisemmin ja se piti sisällään; johdon haastattelut, rotaation, yhtiöanalyysin, ympäristön analyysin ja sisäisen tarkastuksen oman riskianalyysin. Vuosisuunnittelun ja riskiarviokehikon systemaattinen kehittäminen aloitettiin vuoden viimeisellä kvartaalilla. Tästä keskusteltiin myös yhtiön toimitusjohtajan kanssa.

Kuva 4. Vuoden 2025 vuosisuunnittelun aikajana.



Vuosisuunnitelmassa tulevia tarkastuksia kohdistettiin yhtiön eri yksiköihin. Finanssivalvonnan (2/2017) työeläkevakuutusyhtiöiden hallintoa koskevissa määräyksissä ja ohjeissa todetaan, että työeläkevakuutusyhtiön hallintojärjestelmällä pyritään varmistamaan se, että yhtiötä johdetaan terveiden ja varovaisten liikeperiaatteiden mukaisesti ja että yhtiön toiminnassa noudatetaan näitä periaatteita. Esityksen mukaan hallintojärjestelmän avulla toteutetaan vastuiden jako yhtiön kaikilla organisaatiotasoilla, ja sen avulla seurataan yhtiön johdon antamien ohjeiden noudattamista yhtiön toiminnassa. (kohta 6(7), s. 12)

Vuoden 2024 suunnittelun yhteydessä sisäinen tarkastus teki oman kevyen riskianalyysin, jossa riskejä kohdistettiin vuosisuunnitelmasta poiketen, eri yksiköihin. Riskikuvaa kerättiin sisäisen tarkastuksen omista havainnoista, riskienhallintajärjestelmästä, yhtiön sijoitussuunnitelmasta sekä omaa riski- ja vakavaraisuusasemaa koskevasta arviosta (EIOPA, 2013). Sisäisen tarkastuksen tekemässä yhtiöanalyysissä oli vähäisesti otettu huomioon havaintoja mm. tietoturvasta, johdon suunnittelupäiviltä, vastuullisuusmittarista sekä strategiaan liittyvistä painopisteistä. Ympäristön analyysissä oli huomioitu Finanssivalvonnan vuonna 2023 tekemät tarkastukset, teema-arviot sekä konsulttitoimistojen tekemät sisäisen tarkastukseen liittyvät tutkimukset.

Edellä kerrotun perusteella sisäisen tarkastuksen vuosisuunnittelu ei pohjautunut yhtiön riskien tai riskiympäristön systemaattiseen ja laaja-alaiseen numeeriseen analyysiin. Vaikka rotaatio, toimintaympäristö- ja yhtiöanalyysi olivat osa vuosisuunnittelua, oli ne dokumentoitu suppeasti. Toimitusjohtajan ja ylemmän johdon haastattelut antoivat vuosisuunnittelun tueksi ylätason kuvan yhtiön tilasta mutta ns. alemman organisaatiotason näkemys jäi puuttumaan. Koska yhtiön ja eri toimintojen riskiympäristöä ei analysoitu kattavasti, oli sisäisen tarkastuksen hankala muodostaa kattavaa kuvaa yhtiön riskienhallinnan, sisäisen valvonnan ja hallintojärjestelmän tilasta.

Vuoden 2025 vuosisuunnitelma piti sisällään; johdon, tarkastusvaliokunnan puheenjohtajan ja tilintarkastajien haastattelut, rotaation, laajan yhtiö- ja ympäristöanalyysin ja assurance mapin. Näiden tietojen pohjalta sisäinen tarkastus teki oman dokumentoidun riskiarvion. Lisäksi riskiarviokehikko jäsennettiin osa-alueisiin ja numeerisiin pisteisiin, mikä lisäsi läpinäkyvyyttä verrattuna aiempaan värikohtaiseen arviointiin.

5.2.2 Vuosisuunnitelma vuodelle 2026

Vuoden 2026 systemaattinen vuosisuunnittelu aloitettiin jo heti vuoden 2025 alussa, jotta sisäinen tarkastus saisi mahdollisimman laajan kuvan yhtiöön kohdistuvista riskeistä. Tämä mahdollisti myös jatkuvan seurannan toteuttamisen. Riskiarviokehikon kehittämistä lähdettiin systemaattisesti tekemään kevään aikana. Kehittämisessä otettiin huomioon havainnot, jotka tehtiin vuoden 2024 lopulla tehdyn riskiarvion yhteydessä.

Läpi vuoden jatkuva riskiympäristön analysointi antaa sisäiselle tarkastukselle enemmän aikaa tunnistaa yritykseen, toimintoihin ja toimintaympäristöön kohdistuvia riskejä. Jatkuva seuranta antaa myös laajemman riskikuvan, kun haastatteluita tehdään läpi vuoden. Eniten kehittävää tunnistettiin jatkuvassa seurannassa, jossa läpi vuoden seurataan

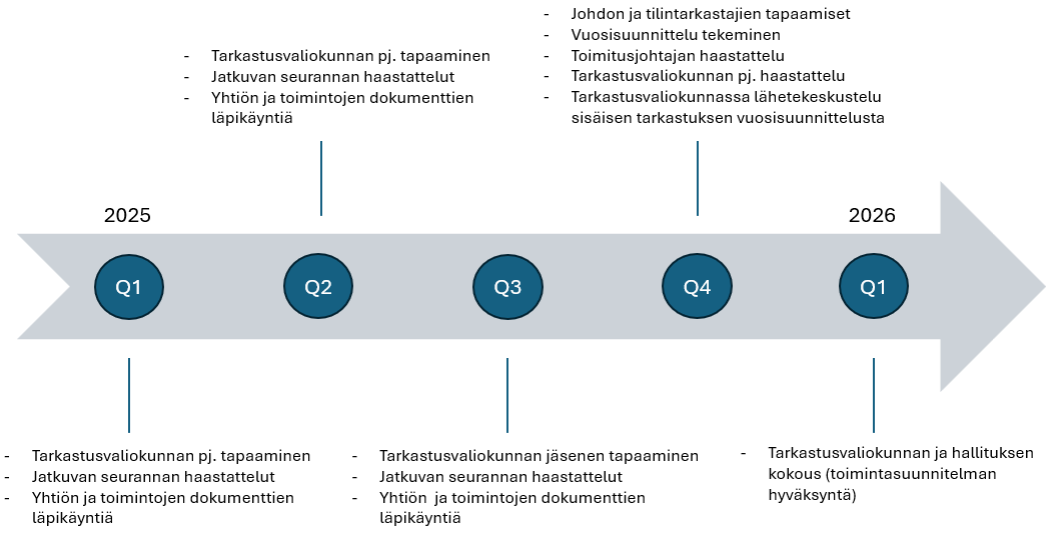
systemaattisesti yhtiön riskiympäristöä mm. seuraamalla toimintojen johtoryhmien pöytäkirjoja, seuraamalla kehittämisen työ- ja ohjausryhmiä, haastatellaan yhtiön avainhenkilöitä. Lisäksi erittäin tärkeäksi osaksi tunnistettiin oman riskianalyysin kehittäminen.

Riskiperusteisen vuosisuunnittelun lähtökohtana oli, että sisäinen tarkastus voi muodostaa mahdollisimman kattavan kokonaiskuvan yksiköiden riskikuvasta. Sisäisen tarkastuksen pitää lisäksi voida käyttää riskiarviota tukena ja perusteluna, kun se esittää vuosisuunnittelun yhteydessä tarkastusten ja neuvonantopalveluiden kohdistamista riski-, strategiaperusteisesti. Riskiarvion tulee näin ollen olla myös hyvin perusteltu, informatiivinen ja selkeä.

Vuoden 2026 vuosisuunnitelmakokonaisuus piti sisällään; johdon ja tarkastusvaliokunnan jäsenten haastatteluita, keskijohdon, asiantuntijoiden sekä muiden avainhenkilöiden haastatteluita, yhtiön toiminnan jatkuvan seurannan, rotaatiotarkastelun, laajan yhtiö- ja ympäristöanalyysin ja varmennuskartan. Näiden tietojen pohjalta sisäinen tarkastus teki oman dokumentoidun riskiarvion.

Kuvassa 5 havainnollistetaan, miten sisäinen tarkastus toteutti vuonna 2025 vuoden suunnittelua. Edellisiin vuosiin verrattuna sisäinen tarkastus aloitti myös jatkuvan seurannan, joka pitää sisällään esihenkilöiden, asiantuntijoiden ja muiden avainhenkilöiden haastattelut. Lisäksi koko vuoden ajan kerättiin tietoa mm. eri toimintojen johtoryhmien merkittävistä asioista ja projektien tilanteista. Näiden toimenpiteiden kautta tavoitteena oli saada laajempi riskikuva eri toiminnoista ja koko yhtiöstä, kuin saataisiin pelkillä johdon haastatteluilla. Jatkuvaa seurantaa toteutettiin vuoden kolmen ensimmäisen kvartaalin aikana ja johdon haastattelut toteutettiin vuoden viimeisellä kvartaalilla.

Kuva 5. Vuoden 2026 vuosisuunnittelun aikajana.



5.2.3 Tiedon kerääminen yhtiöön kohdistuvista riskeistä

Sisäisen tarkastuksen vuoden 2025 vuosisuunnitteluun kuului yhtiöön kohdistuvien riskien kartoittaminen haastatteluilla toimintojen johtajien ja johtoryhmän jäsenien, tietosuojavastaavan, tietoturvapäällikön, Compliance Officerin ja tilintarkastajien kanssa. Ennen vuosisuunnittelun esittelyä tarkastusvaliokunnalle keskusteltiin myös toimitusjohtajan kanssa. Haastatteluista kerättiin tietoa tarkastusten riskiperusteiseen arviointiin ja priorisointiin. Samalla muodostettiin riskialueiden tarkastusavaruutta, joka auttoi sisäistä tarkastusta riskiperusteisen tarkastussuunnitelman luomisessa (Niemi, 2018, s. 173). Menettely oli linjassa myös Coetzee & Lubbe (2014) esiin nostaman vaatimuksen kanssa, jonka mukaan sisäisen tarkastuksen tulee ymmärtää riskien yhteys toiminnan tavoitteisiin.

Sisäisten tarkastajien kansainvälisten ammattistandardien mukaisesti (IIA Finland, 2024, s. 67) vuosisuunnitelmasta keskusteltiin hallituksen alaisen tarkastusvaliokunnan kanssa ja itse vuosisuunnitelma hyväksyttiin hallituksen kokouksessa tammikuussa 2025.

Sisäisen tarkastuksen vuoden 2026 vuosisuunnitteluun tähtäävät haastattelut aloitettiin jo heti vuoden 2025 alkupuolella. Lokakuuhun 2025 mennessä sisäinen tarkastus haastatteli yli 20 henkilöä keskijohdosta, asiantuntijoista ja muista avainhenkilöistä. Avainhenkilöt koostuivat mm. projekteihin osallistuvista henkilöistä, toimintojen riskeistä ja Compliancesta vastaavista henkilöistä. Lisäksi vuoden aikana keskusteltiin säännöllisesti

tietosuojavastaavan, tietoturvapäällikön, riskienhallintapäällikön, Compliance Officerin ja tarkastusvaliokunnan puheenjohtajan kanssa. Lokakuun jälkeen haastateltiin vuoden 2024 mukaisesti johtoryhmän jäsenet, tilintarkastajat ja toimitusjohtaja. Laajoilla, koko organisaatioon sekä eri organisaatiotasoihin ulottuvien haastatteluiden tavoitteena oli muodostaa mahdollisimman kattava tarkastusavaruuden riskikuva, joka auttaisi sisäistä tarkastusta riskiperusteisen tarkastussuunnitelman luomisessa (Niemi, 2018, s. 173). Sisäinen tarkastus nimesi vuoden aikana tehtävät haastattelut jatkuvan seurannan haastatteluiksi, jotta haastateltaville muodostuisi kuva, että sisäisen tarkastuksen normaaliin toimintatapaan kuuluu vuosittaiset haastattelut osana sisäisen valvonnan laadun ja riskikuvan muodostamisen seurantaa.

Rönkkö (2019, s. 312) on todennut, että organisaatioiden toimintaympäristöt ja markkinat muuttuvat nopeasti ja samalla täysin uudenlaisia riskejä ilmaantuu johdon tutkakuvaan. Vuosien 2025 ja 2026 vuosisuunnittelun yhteydessä toiminta- ja riskiympäristön muutoksiin varautumiseksi sisäinen tarkastus keräsi ja analysoi tietoa aiempaa laajemmin erilaisista konsulttiyhtiöiden tulevaisuuteen luotaavista sisäisen tarkastuksen, talouden ja teknologiseen kehittymisen tutkimuksista.

Sisäisten tarkastajien kansainvälisen ammatillisen käytäntöjen viitekehyksen (The Institute of Internal Auditors, 2019, s. 96) mukaan sisäisen tarkastuksen suunnitelman tarkoitus on varmistaa, että sen kattavuus huomioi riittävästi yrityksen prosesseja ja liiketoiminta-alueita, jotka ovat eniten alttiita keskeisille riskeille. Yhtiöön kohdistuvia operatiivisia, strategisia ja compliance-riskejä arvioitiin vuosisuunnittelun yhteydessä haastattelujen lisäksi riskienhallintajärjestelmän riskisalkuun toimintojen kartoittamia mahdollisia riskejä sekä jo toteutuneiden riskien näkökulmasta. Strategisia riskejä arvioitiin myös yhtiön strategisten tavoitteiden perusteella ja nämä kohdistettiin erikseen myös jokaiselle toiminnolle. Strategisia riskejä sekä mahdollisia ja toteutuneita riskejä arvioitiin sekä vuoden 2025 että 2026 vuosisuunnittelun yhteydessä. Mahdollisten ja jo toteutuneiden riskien sekä strategisten riskien arvioinnin avulla sisäinen tarkastus sai selkeän kuvan, mitä strategian toteutumiseen vaikuttavia riskejä kohdistui kullekin toiminnolle. Vuoden 2026 suunnittelun osalta sisäiselle tarkastukselle muodostui yhtiön riskikuvaa jo läpi vuoden 2025, kun ns. jatkuvan seurannan haastatteluita toteutettiin systemaattisesti läpi vuoden.

5.2.4 Riskien arviointikehikon kehittäminen

Sisäisen tarkastuksen tulee ottaa huomioon organisaation riskienhallintaprosessien kypsyys ja virallisen riskienhallintajärjestelmän toimivuus yhtiön kokonaisvaltaiseen

riskienhallintaan (arviointi, dokumentointi ja hallinta). Yrityksen, joiden riskienhallinnan maturiteetti on alhaisempi, voivat käyttää muutakin kuin riskienhallintajärjestelmää riskien arviointiin (The Institute of Internal Auditors, 2019, s. 96). Kohdeorganisaation riskienhallintajärjestelmästä ei voida havainnoida kattavasti yrityksen toimintojen välistä riskiympäristöä niin, että ne olisivat keskenään arvotettu ja niissä olisi huomioitu mm. kulujen ja henkilöstön vaikutukset. Tästä johtuen sisäinen tarkastus päätti kehittää vuoden 2025 vuosisuunnittelun tueksi itse tehdyn riskiarvioinnin kehikon, joka toimisi vuosisuunnittelun riskiperusteisen tarkastussuunnitelman tukena ja perusteena.

Riskiarviointikehikon suurin suunnittelu- ja kehittämistyö tehtiin vuoden 2024 viimeisen kvartaalin sekä alkuvuoden 2025 aikana. Suunnittelun aikana päätettiin, mitä riskiarviokehikolla halutaan saada selville, mitä osa-alueita sen tulisi sisältää, miten laaja-alaisesti sen tulee huomioida yhtiön toiminta sekä miten tarkkoja ja täsmällisiä tietojen tulisi olla.

Sisäinen tarkastus päätti, että riskiarviokehikon kautta halutaan saada riittävä ja selkeä kuva yhtiön eri toimintojen riskillisyydestä, jotta sen perusteella voidaan perustella sisäisen tarkastuksen vuosittaisten tarkastusten kohdistamista. Arviointikehikon osa-alueiksi valittiin yhtiön yksiköt, koska se koetiin kaikille helpoksi ja havainnollisimmaksi tavaksi osoittaa kohteet, joihin tarkastuksia tulisi kohdentaa. Sisäisen tarkastuksen resurssit huomioiden arviointikehikon laajuus päätettiin toteuttaa suppeahkona, joka sisältäsi noin 5–8 osa-aluetta, joita jokaisen yksikön osalta arvioitaisiin. Tietojen tarkkuuden ja täsmällisyyden tavoitteeksi asetettiin, että ne ovat riittävät tarkastusten kohdistamiseen. Tarkkojen ja täsmällisten tietojen saaminen vaatisi lisäresursseja sisäiseen tarkastukseen kuin mahdollisesti myös tietoja toimittaviin dataa tuottaviin palveluihin.

Sisäinen tarkastus arvioi vuoden 2024 lopussa osa-alueet, jotka sen tulisi ottaa huomioon omassa riskiarviomallissa. Samalla kuitenkin tunnistettiin, että mallin kehittäminen tulee olemaan iteratiivista eli sen sisältöä ja rakennetta tullaan muuttamaan seuraavien vuosien aikana. Lisäksi vuoden 2024 lopussa sisäisellä oli suhteellisen vähän aikaa toteuttaa kehikko riskien arviointiin, joten se toteutettiin yksinkertaisena ja kattavuudessakin todettiin olevan kehitettävää

Rotaatioperusteisuuden osalta päätettiin, että sitä ei pisteytetä erillisenä osa-alueena, sitä sovelletaan lopullisessa priorisoinnissa siten, että yksiköt, joita ei ole tarkastettu viime vuosina riittävän usein, nostetaan vuosisuunnitelmalle riippumatta riskipistemallin tuloksesta.

Vuosisuunnittelun Excel-pohjaisessa mallissa riskejä kohdistettiin rotaatioperusteisen arvioinnin sekä varmennuskartan mukaisesti eri yksiköihin. Vuoden 2024 lopussa sisäisellä tarkastuksella oli suhteellisen vähän aikaa toteuttaa mallia riskien arviointiin, joten se toteutettiin mahdollisimman yksinkertaisena mutta kattavana. Riskiarviomallin osa-alueina otettiin huomioon taulukon 2 mukaisesti volyymi, monimutkaisuus, kriittisyys, riskienhallinnan havainnot, Compliance-havainnot, muutokset ja sisäisen tarkastuksen havainnot. Jokaisessa osa-alueessa minimipistearvo oli 0 pistettä ja maksimipistearvo 3 pistettä. Osa-alueiden pisteitä ei painotettu laajuuden tai merkittävyyden mukaan, vaan ne katsottiin keskenään yhtä merkittäviksi. Yksikkökohtaisesti maksimikokonaisarvio oli 21 pistettä.

Taulukko 2. Sisäisen tarkastuksen riskiarviomalli (2024).

	Riskiarvio							Riskipisteet
	Volyymi	Monimutkaisuus	Kriittisyys	RH havainnot	Compl.havainnot	Muutokset	SisTark.havainnot	Kokonaisarvio
Auditable entity 1	3	2	3	3	2	2	2	17
Auditable entity 2	2	2	3	2	2	2	2	15
Auditable entity 3	2	2	3	2	3	2	3	17
Auditable entity 4	2	2	3	2	2	2	3	16
Auditable entity 5	1	3	2	1	1	2	1	11
Auditable entity 6	2	3	2	2	1	2	1	13
Auditable entity 7	1	3	2	1	0	2	2	11
Auditable entity 8	3	3	3	2	1	3	2	17
Auditable entity 9	1	2	3	2	1	2	1	12

Sisäinen tarkastus arvioi riskiarviomallin osa-alueita omien objektiivisten havaintojen ja arvioiden perusteella. Mallissa volyymi tarkoitti toimintoon kohdistuneita euroja sekä henkilöstön määrää, jotka perustuivat sisäisen tarkastuksen omaan arvioon. Monimutkaisuudessa otettiin huomioon toiminnon prosessien monimutkaisuus, manuaalisuus sekä kumppanien määrä. Kriittisyydessä arviointiin toiminnon kriittisyys yhtiön perustehtävän kannalta. Riskienhallinnan ja Compliance-havainnot pitivät sisällään toisen linjan tekemien havaintojen määrän ja merkittävyyden. Muutokset osa-alueessa arvioitiin toimintoihin kohdistuvia muutoksia, kuten lainsäädännön ja tietojärjestelmähankkeiden aiheuttamat muutokset. Sisäisen tarkastuksen havainnot pitivät sisällään sisäisen tarkastuksen tekemät muut kuin tarkastusten varsinaisten tarkastusten ja neuvontapalveluiden havainnot. Näitä olivat mm. johdon haastatteluissa esiin nostamat asiat tai muutoin sisäisen tarkastuksen työssään tekemät havainnot toimintojen osalta.

Sisäinen tarkastus tunnisti vuoden 2025 suunnittelun yhteydessä, että mallin osa-alueiden arvioissa olisi hyvä käyttää tarkempia esim. todellisiin kuluin ja henkilöstömääriin perustuvia lukuja. Samalla myös tunnistettiin, että osa-alueita voisi painottaa keskenään, koska näiden välisessä tärkeydessä, sisäisen tarkastuksen riskiarvioinnin kontekstissa,

tunnistettiin eroja. Coetzee & Lubbe (2014) tutkimuksessa tuotiin esille tarkastuskohteiden tavoitteiden mukaisuuden varmistamisen sekä tavoitteiden saavuttamista uhkaavien tapahtumien ja tekijöiden huomioimisen tärkeys sisäisen tarkastuksen vuosisuunnittelussa. Sisäinen tarkastus arvioi, että sisäisen tarkastuksen, Compliancen sekä riskienhallinnan arviot ovat vuosisuunnittelun riskiarvioinnin perusteella merkittävämpiä osa-alueita yhtiön ja yksiköiden tavoitteiden saavuttamisen näkökulmasta. Näiden lisäksi tärkeäksi riskiarviotyökalun osa-alueeksi arvioitiin yksiköihin sitoutuvien euromääräisten kulujen määrä tai niiden hallinnassa olevat euromääräiset varat (tasearvo). Vaikka riskiarviomallin osa-alueiden osalta tunnistettiin kehitettävää vuonna 2024 tapahtuneen vuoden 2025 suunnittelun yhteydessä, päätettiin jatkokehitys tehdä vasta vuonna 2025, kun suunnittelua tehtiin vuosisuunnittelun 2026 osalta.

Vuoden 2026 suunnittelussa kiinnitettiin näin ollen erityistä huomiota, jo vuoden 2025 aikana tunnistettuun tarpeeseen sisäisen tarkastuksen riskiarvion kehittämiseen. Kehittämisen lähtökohdaksi otettiin riskiarviomallin osa-alueiden tarkempi määrittely sekä niiden keskinäinen painopisteiden luominen. Riskiarviomallissa haluttiin tuoda havainnollisesti esiin Wang, Ferreira & Yan (2025) tutkimuksen mukaisesti sekä laadullinen että määrällinen näkökulma. Näkökulmassa piti kuitenkin huomioida, että sisäisen tarkastuksen resurssit kehittämiseen ovat hyvin rajalliset, joten mallin tuli olla mahdollisimman yksinkertainen, selkeä ja informatiivinen.

Määrällinen ja laadullinen näkökulma päätettiin tuoda esiin riskiarvion osa-alueiden keskinäisten painopisteiden avulla. Tällä pyrittiin havainnollistamaan, että kaikki osa-alueet eivät ole sisäisen tarkastuksen näkökulmasta saman arvoisia tai niiden merkitystä pitää voida erotella toisistaan vuosisuunnittelun yhteydessä. Riskiarvioinnin osa-alueiden keskinäinen painotus on keskeinen tekijä, sillä se määrittää, kuinka paljon kukin osa-alue vaikuttaa kokonaisriskipisteisiin: mitä suurempi maksimipistemäärä osa-alueelle on annettu, sitä suurempi sen suhteellinen vaikutus kokonaisarvioon. Pisteiden painotus perustuu osa-alueen merkitykseen sisäisen tarkastuksen oman arvioinnin perusteella. Tämä lähestymistavan katsottiin varmistavan, että sisäisen tarkastuksen näkemyksen mukaan kriittisimmät ja taloudellisesti merkittävimmät tekijät, kuten taloudelliset volyymit tai tarkastuksen prioriteetit, saavat suuremman painoarvon kuin vähemmän merkittävät tekijät, kuten henkilöstön määrä tai prosessin monimutkaisuus.

Sisäinen tarkastus arvioi, että osa-alueiden tarkka määrittely sekä näiden keskinäinen painotus lisää riskiarvioinnin ymmärrettävyyttä, läpinäkyvyyttä ja johdonmukaisuutta.

Lisäksi se helpottaa ja vahvistaa riskiperusteisen tarkastussuunnitelman toteutumista sekä sen perusteltavuutta hallitukselle, tarkastusvaliokunnalle sekä ylimmälle johdolle.

Taulukossa 3 on kuvattu vuoden 2026 suunnittelussa huomioidut riskiarviomallin osa-alueet ja kokonaisriskipisteet. Taulukon lopussa on ”Max. Riskipisteet”, joka kuvaa osa-alueiden keskinäistä painotusta. Mitä isompi maksimipistemäärä on, sitä suurempi painoarvo sille on kokonaisuudessa annettu. Henkilöstön määrä ja kriittisyys saavat taulukossa maksimissaan 2 pistettä, joten niiden kokonaispainoarvot ovat pienimmät. Eurot ja sisäisen tarkastuksen pistemäärät ovat maksimissaan 3 pistettä, joten niiden painoarvot ovat suurimmat. % -osuus pisteistä -rivi kuvaa painotusten jakaumaa, kokonaisarvon ollessa 100 %.

Taulukko 3. Sisäisen tarkastuksen riskiarviomalli (2025).

	Riskiarvio							Riskipisteet
	Henkilöstön määrä	Eurot	Monimutkaisuus	Kriittisyys	RH ja Compl. näkemys	Muutokset	Sis.tark. näkemys	Kokonaisarvio
Auditable entity 1	2	5	2	3	2	3	4	21
Auditable entity 2	2	4	2	3	2	3	3	19
Auditable entity 3	2	3	2	2	4	1	2	16
Auditable entity 4	1	1	1	2	0	1	1	7
Auditable entity 5	2	5	2	3	3	3	5	23
Auditable entity 6	0	1	1	2	2	1	3	10
Auditable entity 7	1	2	2	2	1	3	3	14
Auditable entity 8	2	3	2	3	2	2	4	18
Auditable entity 9	1	0	1	2	0	2	1	7
Max. Riskipisteet	2	5	2	3	4	3	5	24
% -osuus pisteistä	8,3 %	20,8 %	8,3 %	12,5 %	16,7 %	12,5 %	20,8 %	100 %

Vuoden 2026 vuosisuunnittelussa riskiarvion osa-alueiden arvot määriteltiin ja dokumentoitiin. Riskiarviossa käytettiin seitsemää osa-aluetta ja niille määriteltyjä arvoasteikkoja. Tässä opinnäytetyössä esitetyt osa-alueiden pistemäärät ja kokonaisriskipisteet ovat havainnollistavia ja kuvitteellisia, eikä niitä tule tulkita yhtiön todellisiksi riskitasoiksi, toiminnan laajuutta kuvaaviksi arvoiksi tai sisäisen tarkastuksen tosiasiallisiksi priorisoinneiksi. Ratkaisulla varmistetaan, ettei opinnäytetyössä paljasteta yhtiön kannalta salassa pidettävää tietoa. Luvussa 2.3 esitetyn Wang ym. (2025) -tutkimuksen tapaan riskiarviomallissa yhdistettiin kvalitatiivisia ja kvantitatiivisia tekijöitä. Vaikka mallia ei voitu toteuttaa tutkimuksen laajuudessa, sen periaate, jossa arvioidaan usean tekijää systemaattisesti, tuki mallin rakentamista.

Henkilöstön määrä. Rajaukset perustuvat siihen, että alle 10 henkilön organisaatioissa riskit liittyvät usein henkilöstön vähäisyyteen ja avainhenkilöihin, kun taas yli 50 henkilön organisaatioissa korostuvat hallinnolliset, johtamis- ja koordinointiriskit sekä organisaation monimutkaisuus ja kommunikointitarpeet.

Arvo 0 = Alle 10 henkilöä
Arvo 1 = 10–50 henkilöä
Arvo 2 = Yli 50 henkilöä

Euro (liikekulut tai osuus taseesta). Rajaukset perustuvat organisaation taloudellisen toiminnan laajuuteen. Mitä suuremmat liikekulut, sitä enemmän hallinnollisia ja operatiivisia riskejä syntyy, esimerkiksi sopimusten hallinnassa, hankinnoissa ja talousraportoinnissa. Lisäksi liikekulujen tai yksikössä, kuten Sijoitustoiminnassa hallinnoitavien varojen määrä vaikuttaa suurelta osin toiminnan riskillisyyteen.

Arvo 0 = Liikekulut alle 0,5 milj.€
Arvo 1 = Liikekulut 0,5–1 milj.€
Arvo 2 = Liikekulut 1–2 milj.€
Arvo 3 = Liikekulut 2–3 milj.€
Arvo 4 = Liikekulut 3–6 milj.€
Arvo 5 = Liikekulut yli 6 milj.€

Monimutkaisuus (toiminnan monimutkaisuus). Osa-alue on otettu mukaan, koska monimutkaisempi toiminta lisää virheiden, väärinkäsitysten ja hallinnan puutteiden riskiä. Useat järjestelmät ja kumppanit tuovat riippuvuuksia ja tietovirtoja, joita on vaikeampi hallita. Prosessien läpileikkaavuus voi taas vaikuttaa siihen, kuinka hyvin kontrollit toimivat ja kuinka moni yksikkö vaikuttaa tietyn prosessin läpimenoon.

Arvo 1 = Käytössä vähän järjestelmiä, vähän toimintojen läpi leikkaavia prosesseja, vähän kumppaneita.
Arvo 2= Käytössä paljon järjestelmiä, vähän toimintoja läpileikkaavia prosesseja, useampia kumppaneita.

Kriittisyys (toiminnan kriittisyys yhtiön menestymisen kannalta). Kriittisyyttä on peilattu yhtiön ja yksiköiden toimintaan ja laajuuteen. Osa-alueessa on otettu myös huomioon yhtiön strategiassa ja visiossa nostetut painopistealueet. Tarkempaa määritelmää kriittisyydelle ei ole luotu.

Arvo 0 = Ei kriittinen
Arvo 1= Vähän kriittinen
Arvo 2 = Keskimääräinen kriittisyys
Arvo 3 = Erittäin kriittinen

Riskienhallinnan ja Compliancen näkemys (Compliancen ja Riskienhallinnan näkemys sisäisen valvonnan tilasta). Riskienhallinta ja Compliance antavat vuosiraportoinnin yhteydessä arvion sisäisen valvonnan tilasta ja arvioon perustuu häihin havaintoihin.

Arvo 0= Ei lainkaan havaintoja
Arvo 1= Yksittäinen vähäinen havainto tai riski
Arvo 2 = Vähäisiä havaintoja tai riskejä
Arvo 3 = Vähäistä enemmän havaintoja ja riskejä
Arvo 4 = Paljon havaintoja ja riskejä

Muutokset (toimintaa koskevien muutokset määrä tai laajuus mm. lainsäädäntö, järjestelmät ja organisaatio). Muutosten määrä perustuu sisäisen tarkastuksen omaan arvioon muutosten määrästä tai niiden merkityksestä. Muutosten arvon sisäinen tarkastus on itse arvioinut, eikä niille ole asetettu tarkempaa määritelmää tai lukumäärää.

Arvo 0 = Ei muutoksia
Arvo 1 = Vähäisiä muutoksia
Arvo 2 = Jonkin verran muutoksia
Arvo 3 = Paljon tai merkittäviä muutoksia

Sisäisen tarkastuksen näkemys (Sisäisen tarkastuksen näkemys toiminnan riskillisyydestä ja sisäisen valvonnan tilasta). Osa-alueen arvon sisäinen tarkastus on itse määritellyt havaintojensa sekä jatkuvan seurannan perustella, koska sisäisellä tarkastuksella ei ole erillistä riskikartoitusta tai tilastoa riskien määrästä.

Arvo 1 = Ei riskejä
Arvo 2 = Vähäisiä riskejä
Arvo 3 = Jonkin verran riskejä
Arvo 4 = Paljon riskejä
Arvo 5 = Merkittäviä riskejä

Riskipisteiden kokonaisarvio kertoo yksikköön (auditable entity) kohdistuneiden pisteiden määrän. Mitä suurempi pisteluku on, sitä riskillisemmäksi toiminto on arvotettu. Sisäisen tarkastuksen tulisi kohdistaa vuosisuunnitelmassaan tarkastukset ja neuvonantopalvelut erityisesti korkeamman riskiluvun saaneisiin toimintoihin.

Riskiarviomallin osa-alueissa ei ole kohtaa, jossa arvioitaisiin strategianmukaisuutta yhtenä erillisenä kokonaisuutena, vaikka se on oleellinen osa sisäisen tarkastuksen vuosisuunnittelua (IIA Finland, 2024, s. 67). Strategiaa arvioidaan osana riskiarviomallin kriittisyys osa-aluetta sekä myös täysin omana kokonaisuutena, joka ei ole kytköksissä riskiarviomalliin. Tässä arvioinnissa arvosanaan vaikutti, että kuinka monta strategista tavoitetta osuu kuhunkin yksikköön. Strategianmukaisuuden erillistä arviointia ei ole avattu tarkemmin tässä opinnäytetyöhön, koska se oma kokonaisuutensa vuosisuunnittelussa. Strategianmukaisuuden huomioiminen riskiarviomallissa on kuitenkin nostettu esiin johtopäätöksissä.

5.2.5 Riskiarviomallin käytännön soveltaminen

Riskiarviomallin toimivuuden havainnollistamiseksi taulukossa 4 esitetään kuvitteellinen esimerkki Asiakaspalveluyksiköstä, joka arvioitiin vuoden 2026 suunnittelun yhteydessä. Taulukossa on kuvattu, miten yksikön (auditable entity) pisteet muodostuvat konkreettisesti ja millä perusteilla yksikön riskillisyyttä vuosisuunnitelman näkökulmasta määriteltiin. Taulukossa olevat osa-alueet eivät ole kuvitteellisia vaan kuvitteellisia ovat taulukossa kerrotut yksittäiset arvot ja perustelut.

Taulukko 4. Kuvitteellinen esimerkki Asiakaspalveluyksikön riskipisteiden muodostumisesta

Osa-alue	**Arvo**	**Perustelu**
Henkilöstön määrä	2	Yli 50 hengen yksikkö. Suuri vaihtuvuus lisää operatiivisia riskejä
Eurot (liikekulut)	4	Kulut noin 15 000 000 €. Merkittävä kustannuserä ja ulkoistettujen palvelujen osuus kasvanut.
Monimutkaisuus	2	Useita järjestelmiä ja kumppaneita. Useat prosessit ovat läpileikkaavia.
Kriittisyys	3	Erittäin kriittinen yksikkö yhtiön kannalta. Yksi yhtiön strategiassa määritetyistä ydinprosesseista.
Riskienhallinnan ja Compliancen näkemys	2	Useita vähäisiä havaintoja liittyen dokumentointiin ja prosessikontrolleihin.
Muutokset	3	Asiakaspalvelun käyttöön tulossa uusi CRM-järjestelmä

Sisäisen tarkastuksen näkemys	4	Jatkuvassa seurannassa noussut esiin useita epäselvyyksiä vastuunjaossa ja prosessien yhtenäisyydessä

Asiakaspalveluyksikkö sai 20/24 pistettä. Yksikkö nousi riskillisten toimintojen kärkeen erityisesti suuren henkilöstömäärän, suurien liikekulujen, kriittisyyden, muutoksien ja sisäisen tarkastuksen näkemysten takia. Taulukko auttoi syventämään keskusteluja johdon ja tarkastusvaliokunnan kanssa ja riskitasot voitiin perustella numeerisesti ja läpinäkyvästi.

Mallin tuottama numeerinen pistemäärä tukee luvussa 2.3 esitettyä havaintoa (Lenz ym., 2014), jonka mukaan tehokkaat sisäisen tarkastuksen toiminnot hyödyntävät riskiperusteista arviointia tarkastuskohteiden valinnassa. Pisteytys myös mahdollisti standardin 9.4 mukaisen (IIA Finland, 2024, s. 66) perustelun siitä, miksi yksikkö nousi merkittävänä riskialueena vuosisuunnittelun prioriteettilistan kärkeen.

6 Johtopäätökset

Tämän opinnäytetyön tavoitteena oli kehittää kohdeorganisaation sisäisen tarkastuksen riskiperusteista vuosisuunnittelua siten, että suunnitelma perustuu aiempaa systemaattisemmin organisaation riskeihin, strategisiin tavoitteisiin ja rotaatioperiaatteisiin.

Työn tulokset osoittavat, että vuosisuunnitteluprosessissa oli merkittäviä kehittämistarpeita erityisesti riskien systemaattisessa arvioinnissa, strategian huomioimisessa sekä tarkastustoiminnan kattavuuden perustelemisessa. Kehittämistyö oli siten selvästi tarpeellinen

6.1 Keskeiset johtopäätökset

Työssä laadittu riskiarviokehikko toi kohdeorganisaatiolle rakenteisen ja dokumentoidun tavan arvioida toimintojen riskitasoa. Aiemmin ei ollut muodostettu kattavaa kvantitatiivista organisaatiotasoista riskikuvaa. Riskien arviointi oli hajanaista, perustui pitkälti johdon haastatteluihin ja sisäisen tarkastuksen kevyeen riskiarvioon.

Kehitetty riskiarviomalli osoittautui toimivaksi ja lisäarvoa tuottavaksi, koska se yhdistää määrällisiä ja laadullisia riskitekijöitä, huomioi sisäisen tarkastuksen sekä toisen linjan havainnot ja ottaa huomioon yksiköiden volyymin, monimutkaisuuden, kriittisyyden sekä

muutokset. Malli tuottaa vertailukelpoisen pistemäärän yksiköiden välisestä riskitasosta, mikä tekee tarkastuskohteiden valinnasta johdonmukaista ja perusteltua.

Riskiarviomallin haasteena on kuitenkin se, että se kuvaa yhtiön eri yksiköiden riskiympäristöä melko yleisellä tasolla. Yksiköt koostuvat usein useasta osastoista ja mallin nykyinen rakenne ei erittele näiden toimintojen välisiä riskieroja. Toimintotason analyysi lisäisi mallin tarkkuutta, mutta sen toteuttaminen edellyttäisi huomattavasti nykyistä enemmän resursseja sekä tarkempaa dataa.

Strategian huomiointi sisäisen tarkastuksen suunnittelussa vahvistui selvästi kahden vuoden aikana. Riskiperusteisuuden rinnalle nousi strategiatason arviointi ja strategisten tavoitteiden tukeminen. Riskiarviomallista puuttuu kuitenkin edelleen systemaattinen strategiatason osa-alue, mikä tarkoittaa, että strategisiin riskeihin liittyvä arviointia tehdään omana kokonaisuutena. Strategiaperusteisuus tulisi jatkossa liittää riskiarviomallin osa-alueisiin, jotta strategia- ja riskiperusteisuus muodostaisivat yhtenäisen kokonaisuuden. Strategiaperusteisuuden huomioimisessa olisi hyvä tarkastella yksiköiden systemaattista toimintaa suhteessa organisaation tavoitteisiin. Tätä eri yksiköiden strategista tarkastelua voisi jatkossa käyttää riskiarviomallin strategiamittarin muodostamisessa.

Rotaatioperusteisuuden lisäämistä arviointikehikkoon voisi myös tulevaisuudessa miettiä. Jos yksikköä ei ole tarkastettu määritellyn rotaatiojakson (2–3 vuotta) aikana, sen kokonaisriskipistemäärää voitaisiin esim. korottaa tietyllä painotuksella. Tällä varmistettaisiin, että mallin numeerinen priorisointi huomioisi myös tarkastamattomuuden eli rotaation aiheuttaman riskin.

Vuoden 2026 suunnittelussa käyttöön otettu jatkuva seuranta oli merkittävä parannus aiempaan käytäntöön verrattuna. Jatkuvan seurannan ansiosta sisäinen tarkastus sai ajantasaisen, laaja-alaisen ja eri organisaatiotasoihin ulottuvan näkymän yhtiön riskiympäristöön. Tämä vähensi riippuvuutta pelkistä loppuvuoden johtotason haastatteluista. Jatkuva seuranta oli kuitenkin hyvin resurssi-intensiivistä, ja prosessin keventäminen on siksi perusteltua.

Lisäksi työ osoitti, että kohdeorganisaation riskienhallintajärjestelmä ei nykyisellään mahdollista organisaation riskiavaruuden täsmällistä analysointia esimerkiksi volyymien tai toimintokohtaisten resurssien osalta. Sisäisen tarkastuksen kehittämä riskiarviomalli on tällä hetkellä välttämätön väline riskiperusteisuuden osoittamiseen, mutta samalla se kasvattaa sisäisen tarkastuksen työkuormaa ja sisältää subjektiivisuuden riskin. Mallin

edelleen kehittäminen edellyttää riskienhallintajärjestelmän kypsymistä ja tietoperusteisen analytiikan vahvistumista.

Kokonaisuutena opinnäytetyö osoittaa, että myös pieni, kahden hengen sisäisen tarkastuksen organisaatio kykenee rakentamaan systemaattisen riski- ja strategiaperusteisen vuosisuunnitteluprosessin, kun riskiarviomallin osa-alueet pidetään kevyinä, ymmärrettävinä ja kehittämistä jatketaan vaiheittain. Malli tarjoaa realistisen, skaalautuvan ja standardien mukaisen tavan toteuttaa riskiperusteista vuosisuunnittelua pienessä organisaatiossa.

7 Jatkotutkimusaiheet

Opinnäytetyön tulokset nostavat esiin teemoja, joiden syvällisempi tutkimus tukisi sisäisen tarkastuksen tulevaa vuosisuunnittelun kehitystyötä sekä organisaation riskienhallinnan ja hallinnon kehitystä.

Kehitetty riskiarviomalli toimii tarkoituksenmukaisesti, mutta jatkotutkimuksessa voisi selvittää, mitkä arviointimallin osa-alueet ennustavat parhaiten todellisia riskitapahtumia. Arviointimallin painotus perustuu tällä hetkellä subjektiiviseen arvioon ja jatkotutkimuksena voisi selvittää, tulisiko osa-alueiden painotuksia säätää tieteellisemmäksi tai tieteellisen analyysin pohjalta.

Deloitte (2024b) esittää, että tulevaisuudessa sisäinen tarkastus voi hyödyntää digital twin -malleja simuloidakseen riskien ja kontrollien muutoksia ennen päätöksentekoa. Tämä tukee ajatusta siitä, että sisäisen tarkastuksen riskiarvioinnin tulisi kehittyä kohti ennakoivuutta ja datavetoisuutta. Tämä herättää kysymyksiä, että millä edellytyksillä pienikin tarkastusorganisaatio voisi tehdä aktiivista jatkuvaa seurantaa tekoälyn avulla.

Jatkossa voisi myös tutkia, millaiset rakenteet parhaiten tukevat pienen tarkastustoiminnon riskiperusteista toimintaa: millaiset yhteistyömallit sisäisen tarkastuksen, riskienhallinnan ja Compliancen kanssa koetaan parhaiksi ja miten tarkastusvaliokunta voisi parhaiten tukea riskiperusteista vuosisuunnittelua.

8 Yhteenveto

Tämän opinnäytetyön tavoitteena oli kehittää suomalaisen finanssialan toimijan sisäisen tarkastuksen riskiperusteista vuosisuunnittelua vahvistamalla sen systemaattisuutta, läpinäkyvyyttä ja strategialähtöisyyttä. Kehitystyö oli tarpeellinen, sillä kohdeorganisaation riskienhallintajärjestelmän kypsyystaso ei tarjonnut sisäiselle tarkastukselle organisaationlaajuista, numeerista riskiarviota suunnittelun tueksi. Vuosisuunnittelu perustui aiemmin rajallisiin tietolähteisiin, kuten johdon haastatteluihin ja kevyeen riskiarvioon, mikä heikensi vuosisuunnitelmaan sisältyvien tarkastuskohteiden valinnan perusteltavuutta.

Työn keskeinen tulos oli uuden, kevyen ja skaalautuvan riskiarviomallin rakentaminen sekä kahdessa suunnittelusyklissä testattu käytännön soveltaminen. Malli yhdistää numeerisia ja laadullisia tekijöitä, kuten yksiköiden volyymin, monimutkaisuuden, kriittisyyden, toisen linjan havainnot, muutokset ja sisäisen tarkastuksen näkemyksen, ja muuntaa ne vertailukelpoiseksi pisteytykseksi. Mallin avulla sisäinen tarkastus pystyy perustelemaan riskiperusteisesti valitut tarkastuskohteet läpinäkyvästi ja johdonmukaisesti.

Opinnäytetyön yhteydessä kehitettiin lisäksi jatkuvan seurannan prosessi, joka täydensi mallia tarjoamalla ajantasaisen ja eri organisaatiotasoihin ulottuvan riskikuvan. Tämä paransi riskien tunnistamista merkittävästi verrattuna aiempaan, yksinomaan loppuvuoden johdon haastatteluihin pohjautuvaan malliin. Samalla vuosisuunnittelu muuttui aidosti dynaamiseksi ja paremmin organisaation muutoksiin reagoivaksi.

Kehitystyö osoitti selvästi, että riskiperusteisuuden, strategiapohjaisuuden ja rotaation huomioiminen edellyttävät käytännössä selkeää ja dokumentoitua mallia. Laadittu riskiarviokehikko toi kohdeorganisaatiolle ensimmäistä kertaa rakenteen, jonka avulla vuosisuunnittelussa voidaan huomioida laajasti liiketoimintayksikköihin sisältyvät riskit. Samalla malli tekee päätöksenteosta läpinäkyvää hallitukselle, tarkastusvaliokunnalle ja ylimmälle johdolle.

Opinnäytetyö osoittaa, että pieni sisäisen tarkastuksen organisaatio kykenee toteuttamaan standardien mukaisen, perustellun ja systemaattisen riskiperusteisen vuosisuunnittelun. Riskienhallintajärjestelmän kypsyystaso asettaa kuitenkin edelleen rajoitteita. Mallin tarkkuus perustuu osin sisäisen tarkastuksen subjektiiviseen arvioon, ja yksikkökohtaiseen analytiikkaan perustuva tarkempi mallintaminen edellyttäisi parempaa dataa ja resursseja.

Opinnäytetyö luo vahvan pohjan sisäisen tarkastuksen tulevalle kehittämiselle. Mallin seuraavat kehitysaskeleet liittyvät erityisesti strategisen merkittävyyden integroimiseen osaksi mallia. Mallin käytön merkittävä parantaminen ja tehostaminen vaatii kuitenkin organisaatiotasoisen riskienhallintajärjestelmän kypsyystason kasvua ja sitä kautta tietoperusteisen riskianalyysin vahvistumista. Opinnäytetyön keskeinen viesti on, että pienelläkin tarkastusorganisaatiolla on täysin realistiset edellytykset rakentaa vaikuttava, läpinäkyvä ja standardien mukainen riskiarviomalli. Mallin luonnin tulee kuitenkin perustua keveyteen, selkeyteen ja jatkuvaan kehittämiseen.

Lähteet

Abdalla, A. A. A., Alodat, A. Y., Salleh, Z., & Al-Ahdal, W. M. (2025). *The effect of audit committee effectiveness, internal audit size and outsourcing on greenhouse gas emissions disclosure*. International Journal of Disclosure and Governance, 22, 1072–1087. https://doi.org/10.1057/s41310-025-00297-0

Alhajri, M. O. (2017). *Factors associated with the size of internal audit functions: Evidence from Kuwait.* Managerial Auditing Journal, *32*(1), 75–89. https://doi.org/10.1108/MAJ-12-2015-1289

Arvopaperimarkkinayhdistys ry. (2025). *Corporate Governance – Hallinnointikoodi 2025*. Arvopaperimarkkinayhdistys ry. https://www.cgfinland.fi/wp-content/uploads/2024/11/hallinnointikoodi-2025.

Coetzee, P., & Lubbe, D. (2014). *Improving the efficiency and effectiveness of risk-based internal audit engagements.* International Journal of Auditing, 18(2), 115–125. https://doi.org/10.1111/ijau.12016

EBA. (2018). *Ohjeet hallinnosta ja ohjauksesta* (EBA-GL-2017-11). Kohdat 204–206. https://www.eba.europa.eu/sites/default/files/document_library/Guidelines%20on%20Internal%20Governance%20(EBA-GL-2017-11)_COR_FI.pdf

ECIIA. (2018). *Position paper – Audit planning approach*. https://www.internerevision.at/fileadmin/01_Web/04_Standards/06_ECIIA_Publikationen/ECIIA-Audit-planning_.pdf

EIOPA. (2010). *Guidelines on system of governance*. Euroopan vakuutus- ja eläkevakuutusviranomainen. https://www.eiopa.europa.eu/document/download/26a64164-1ffa-44e7-b9f4-f00859bbdbb6_fi?filename=Guidelines%20on%20System%20of%20Governance

EIOPA. (2013). *Ennakoivaa riskiarviota koskevat ohjeet (ORSA-periaatteisiin perustuva)* (EIOPA-CP-13/09 FI). https://www.eiopa.europa.eu/document/download/3b05df5c-d29b-4185-a2ac-f28d2178cf7d_fi?filename=Guidelines%20on%20Forward%20Looking%20assessment%20of%20own%20risks%20based%20on%20the%20ORSA%20principles

Deloitte. (2024). *Implementing the New Global Internal Audit Standards*. Luettu 25.3.2025 osoitteesta https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Advisory/us-global-internal-audit-standards.pdf

Deloitte. (2024b). *Impact unleashed: The rise of internal audit in a digital world. https://www.deloitte.com/content/dam/assets-zone3/us/en/docs/services/consulting/2025/us-advisory-impact-unleashed-the-rise-of-internal-audit-in-a-digital-world.pdf*

Finanssivalvonta. (2017). *Määräykset ja ohjeet 2/2017: Työeläkevakuutusyhtiöiden hallinto* (Dnro FIVA/2022/799). Finanssivalvonta.

Fiva. (2024). Finanssivalvonta. *Teema-arvio vahinko- ja henkivakuutusyhtiöiden sisäisen tarkastuksen toiminnosta – toimintatavoissa ja resursoinnissa merkittäviä eroavaisuuksia* (Valvottavatiedote FIVA/2024/875). https://www.finanssivalvonta.fi/globalassets/fi/tiedotteet-ja-

julkaisut/valvottavatiedotteet/2024/laaja-valvottavatiedote---sisaisen-tarkastuksen-toiminnon-teema-arvio.pdf

Granite. (n.d.). https://granite.fi/

Holopainen, A., Koivu, E., Kuuluvainen, A., Lappalainen, K., Leppiniemi, J., Mikola, M. & Vehmas, K. (2013). *Sisäinen tarkastus.* Tietosanoma Oy.

HAMK. (n.d.). Toiminnallinen opinnäytetyö. Luettu 4.4.2025 osoitteesta https://www.hamk.fi/opiskelijalle/opintojen-suunnittelu/opinnaytetyo/

IIA Finland. (n.d.). *Mitä on sisäinen tarkastus?* Luettu 4.4.2025 osoitteesta https://theiia.fi/sisainen-tarkastus/

IIA Finland. (n.d.). *Ammattistandardit*. Luettu 7.4.2025 osoitteesta suomi-2024--gias-kansainvaliset-sisaisen-tarkastuksen-standardit-iia.pdf

IIA Finland. (n.d.*). Ammatillinen ohjeistus*. Luettu 7.4.2025 osoitteesta https://theiia.fi/sisainen-tarkastus/ammatillinen-ohjeistus/

IIA Finland. (2024). *Kansainväliset sisäisen tarkastuksen standardit* (suomennos). https://theiia.fi/wp-content/uploads/2025/01/suomi-2024--gias-kansainvaliset-sisaisen-tarkastuksen-standardit-iia.pdf

IIA Global. (2023). *IIA:n kolmen linjan malli, "Kolmen puolustuslinjan mallin" päivitys*. Luettu 4.9.2025 osoitteesta https://theiia.fi/wp-content/uploads/2023/03/iian-kolmen-linjan-malli-kolmen-puolustuslinjan-mallin-paivitys.pdf

Internal Audit Foundation. (2025). *2025 North American Pulse of Internal Audit: Benchmarks for internal audit leaders*. The Institute of Internal Auditors. https://www.theiia.org/globalassets/site/resources/research-and-reports/pulse-of-internal-audit/2025-iia-pulse-report.pdf

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Kämppi, P., & Talala, T. (2023). *Yrityksen riskienhallinta.* Aalto University Executive Education.

Komission delegoitu asetus (EU) 35/2015. (2015). *Vakuutus- ja jälleenvakuutustoiminnan aloittamisesta ja harjoittamisesta annetun Euroopan parlamentin ja neuvoston direktiivin 2009/138/EU täydentämiseksi (Solvenssi II)*. *Euroopan unionin virallinen lehti*, L 12/1. https://publications.europa.eu/resource/cellar/e0c803af-9e0f-11e4-872e-01aa75ed71a1.0008.03/DOC_477

Kostamo, P., Airaksinen, T. & Vilkka, H. (2022). *Kirjoita itsesi asiantuntijaksi, Opas toiminnalliseen opinnäytetyöhön.* Art House Oy.

Laki työeläkevakuutusyhtiöistä 354/1997. https://www.finlex.fi/fi/lainsaadanto/1997/354

Lenz, R., Sarens, G., & D'Silva, K. (2014). *Probing the Discriminatory Power of Characteristics of Internal Audit Functions: Sorting the Wheat from the Chaff*. International Journal of Auditing, 18(2), 126–138. https://doi.org/10.1111/ijau.12017

Mehta, H. (2024). *Managing cyberrisk with the help of GRC*. Isaca Journal, 5. Luettu 9.9.2025 osoitteesta https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2024/volume-5/managing-cyberrisk-with-the-help-of-grc_joa_eng_0924.pdf

Niemi, P. (2018). *Sisäinen tarkastus käytännössä*. Alma Talent Oy.

Niemi, P. (2018). *Sisäinen tarkastus käytännössä*. [e-kirja]. Alma Talent Oy. https://ezproxy.hamk.fi/login?

OECD. (2024). *Enhancing co-operation between internal and external auditors in the public sector: Towards a well-co-ordinated and strengthened public sector audit to ensure public accountability* (OECD Public Governance Policy Papers). OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/enhancing-co-operation-between-internal-and-external-auditors_bb0f2668/0d4976ed-en.pdf

Pitt, S-A. (2014). *Internal Audit Quality: Developing a Quality Assurance and Improvement Program*. John Wiley & Sons, Incorporated.

Ratsula, N. (2016). *Yrityksen sisäinen valvonta*. Edita Publishing Oy.

Ratsula, N. (2016). *Compliance – Eettinen ja vastuullinen liiketoiminta*. Alma Talent Oy.

Rönkkö, J. (4/2019). Sisäinen tarkastus – tuloksellinen lisäarvon tuottaja vai paikkaansa hakeva tukitoiminto? *Hallinnon tutkimus*, 38(4), 312–316.

Sinersalo, K., Ojala, S., Rinne, S., Koivunen, R., Sipiläinen, N., Hakala-Kivinen, M., & Malin, H. (2021). Sisäinen tarkastus osana corporate governancea. Teoksessa L. Kihn, L. Oulasvirta, M. Järvenpää, J. Pellinen, J. Stenvall, & J. Vakkuri (Toim.), *Tarkastus, arviointi ja valvonta murroksessa* (ss. 239–262). https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/50460/KIHN_OULASVIRTA_YM_Tarkastus_arviointi_valvonta_murroksessa_2021.pdf?sequence=1&isAllowed=y

Sisäiset tarkastajat ry. (2014). *Sisäisen tarkastajan arkipäivä – sisäisen tarkastajan moninaiset tehtävät*. https://theiia.fi/wp-content/uploads/2016/12/all_in_a_days_work_fi_20140813.pdf

Sääskilahti, T., Mustonen, E. & IIrola, H. (2024). *Sisäinen valvonta valtionhallinnossa*. Valtionvarainministeriö. Valtiovarainministeriön julkaisuja – 2024:50. https://urn.fi/URN:ISBN:978-952-367-848-4

Syntetos, A., Petropoulos, F., & Boylan, J. (2023). A multi-criteria optimization model for risk-based internal audit annual planning. *Computers & Operations Research*, 157, 105128. https://doi.org/10.1007/s10479-023-05228-2

The Institute of Internal Auditors. (2019*). Implementation guides for the International Professional Practices Framework*. https://www.theiia.org/globalassets/documents/standards/implementation-guides-gated/2019-implementation-guides-all.pdf

The Institute of Internal Auditors. (2025*). Frequently Asked Questions, What is the purpose of topical requirements?* Luettu 7.4.2025 osoitteesta https://www.theiia.org/en/standards/2024-standards/topical-requirements/

The Institute of Internal Auditors. (2025). *Cybersecurity, Topical Requirement.* https://www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_topical_requirement.pdf

The Institute of Internal Auditors. (2024). *Internal audit: Vision 2035: Creating our future together*. https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/vision-2035-report.pdf

The Institute of Internal Auditors. (2020). *Developing a risk-based internal audit plan*. https://www.theiia.org/globalassets/documents/content/articles/guidance/practice-guides/developing-a-risk-based-internal-audit-plan/pg-developing-a-risk-based-internal-audit-plan.pdf

Vakuutusyhtiölaki 521/2008. https://www.finlex.fi/fi/lainsaadanto/2008/521

Vilkka, H. & Airaksinen, T. (2004). *Toiminnallisen opinnäytetyön ohjaajan käsikirja*. Tammi.

Wang, X., Ferreira, D. & Yan, H. (2025). A multi-objective optimization approach for integrated risk-based internal audit planning. Annals of Operations Research (2025), 346:1811–1840. https://doi.org/10.1007/s10479-023-05228-2.

Zainal Abidin, N. H. (2017). *Factors influencing the implementation of risk-based auditing.* Asian Review of Accounting, 25(3), 361–375. https://doi.org/10.1108/ARA-10-2016-0118

Liite 1 Aineistonhallintasuunnitelma

1. Opinnäytetyön aineiston kuvaus

Opinnäytetyön aineistona ovat työnantajani sisäisen tarkastuksen toiminnon vuosisuunnittelussa käytetyt dokumentit tai Excel-muodossa olevat raportit. Opinnäytetyön kannalta kuitenkaan Excel-taulukoissa olevat luvut eivät ole relevantteja, joten ne tullaan poistamaan ennen mahdollista opinnäytetyöaineistoon tuontia.

Opinnäytetyössä ei tehdä kyselyjä tai haastatteluja. Työssä käytetyt dokumentit tai aineistot ovat yleisesti kaikkien saatavilla tai ne ovat luonteeltaan sellaiseksi luoteltavia. Asiantuntijapalveluyritykseltä mahdollisesti saatavien materiaalien osalta täytyy selvittää, että ovatko ne yleisesti jaettavia vai ovatko ne luottamuksellisia.

Alla on kuvattu opinnäytetyön aineistoa: mistä aineisto on peräisin, miten se on kerätty ja missä muodossa kerätty aineisto on.

- Kuvat, joita mahdollisesti käytän toiminnallisessa osuudessa ovat nykyisessä työssäni tehtyjen PowerPoint- tai Excel- tiedostojen kuvia
- Kirjalliset lähteet, joita pääsääntöisesti käytän opinnäytetyössä ovat yleisesti julkisesti jaettavia. Ne ovat joko fyysisesti painettua kirjallisuutta, E-kirjoja tai poimittu Internetistä
- Lähteiden osalta, jotka mahdollisesti saan sähköpostitse Asiantuntijapalveluyrityksiltä ovat pdf-muodossa

2. Aineiston tallennus ja säilytys

Opinnäytetyössä tarvittava tutkimusaineistoa käsitellään työnantajan antamalla tietokoneella, joka on suojattu salasanalla. Tutkimusaineisto tallennetaan tietokoneen henkilökohtaiselle verkkolevylle ja työnantajan henkilökohtaiseen käyttöön tarkoitetulle OneDrive-tiedostoon. Varmuuskopiot tallennetaan erilliseen kansioon, jotka on nimetty ”Varmuuskopiot” -nimisiksi. Pääasiallinen aineisto säilytetään tietokoneen verkkolevyllä mutta opinnäytetyön kirjoittaminen tehdään OneDrive-tiedostossa.

Opinnäytetyöllä ei ole varsinaisesti toimeksiantajaa, vaikka se käsitteleekin nykyisessä työtehtävissä tehtyjä toimenpiteitä.

Aineistoa ei pääse käsittelemään muut henkilöt eikä opinnäytetyössä käsitellä henkilötietoja. Aineisto varmuuskopioidaan henkilökohtaiselta verkkolevyltä OneDrive-tiedostoon ja OneDrive-tiedosto varmuuskopioidaan henkilökohtaiselle verkkolevylle.

3. Henkilötietojen ja arkaluonteisten tietojen käsittely

Opinnäytetyössä ei käsitellä henkilötietoja eikä arkaluonteisia tietoja.

4. Aineiston omistajuus

Opinnäytetyön aineistoon ja tulokset omistaa Jani Laaksonen.

5. Aineiston jatkokäyttö työn valmistumisen jälkeen

Tutkimusaineistoa ei jatko käytetä. Opinnäytetyön tekijä säilyttää aineiston tietoturvallisesti vuoden ajan opinnäytetyön hyväksymispäivästä, jotta opinnäytetyön tulokset voidaan tarvittaessa varmistaa ja hävittää tämän jälkeen aineiston tietoturvallisesti.