SISÄINEN VALVONTA JA RISKIENHALLINTA HELSINGIN KAUPUNKIKONSERNISSA

SISÄLLYSLUETTELO

JOHDANTO

Sisäisen valvonnan ja riskienhallinnan yleiset järjestämisvastuut ja periaatteet on määritelty kaupunginvaltuuston 11.12.2013 (441 §) hyväksymissä Helsingin kaupunkikonsernin sisäisen valvonnan ja riskienhallinnan perusteissa ja johtosäännöissä. Lisäksi kaupunginvaltuuston 16.1.2008 hyväksymässä konserniohjeessa ja kaupunginhallituksen konsernijaoston 21.9.2009 hyväksymissä johtamisen ja hallinnon keskeisissä periaatteissa on annettu määräykset konsernivalvonnan ja -raportoinnin sekä tytäryhteisöjen sisäisen valvonnan ja riskienhallinnan järjestämisestä.

Tässä ohjeessa annetaan ohjeita siitä, mitä virastojen, liikelaitoksien ja tytäryhteisöjen sisäisen valvonnan ja riskienhallinnan järjestämisessä ja toteuttamisessa tulee ottaa huomioon.

Sisäisen valvonnan ja riskienhallinnan toteuttamisen tueksi on myös koottu, virastoille ja liikelaitoksille Helmeen ja tytäryhteisöille Tyyneen, yhteisiä työvälineitä ja menetelmiä.

Ohjeen valmistelussa on huomioitu kuntalain[1] sisäistä valvontaa ja riskienhallintaa koskevat määräykset. Valmistelussa on hyödynnetty soveltuvin osin sisäisen valvonnan ja riskienhallinnan standardeja[2] ja parhaita käytäntöjä.

Virastot, liikelaitokset ja tytäryhteisöt voivat laatia tarkempia ohjeita sisäisen valvonnan ja riskienhallinnan tulokselliseksi toteuttamiseksi. Edellä mainittujen ohjeiden tulee olla tässä ohjeessa esitettyjen periaatteiden mukaisia.

[1] Kuntalaki 410/2015

[2] COSO (Committee of Sponsoring Organizations of the Treadway Commission) Internal Control – Integrated Framework 2013 ja Enterprise Risk Management – Integrated Framework 2004 sekä ISO (International Organization for Standardization) 31000 Risk management – Principles and guidelines 2009

1 SISÄISEN VALVONNAN JA RISKIENHALLINNAN TAVOITTEET JA TOIMINTAPERIAATTEET

1.1. Sisäisen valvonnan ja riskienhallinnan tavoitteet

Sisäisen valvonnan ja riskienhallinnan tavoitteena on varmistaa toiminnan laillisuus ja tuloksellisuus. Laillisuus tarkoittaa lainsäädännön ja hyvän hallintotavan noudattamista kaupunkikonsernin toiminnassa ja päätöksenteossa. Tuloksellisuudella tarkoitetaan asetettujen strategisten ja toiminnallisten tavoitteiden saavuttamista kaupunginvaltuuston hyväksymän talousarvion puitteissa. Tuloksellisuus merkitsee myös toiminnan vaikuttavuutta ja laadukkaita palveluja.

1.2. Sisäisen valvonnan ja riskienhallinnan osatekijät ja toimintaperiaatteet

Johtamisessa ja hallinnon järjestämisessä kaupunginhallitus, lautakunta/johtokunta ja virasto/liikelaitos/tytäryhteisö sitoutuu kaupungin arvoihin ja eettisiin periaatteisiin, asetettuihin tavoitteisiin, valvontavastuiden määrittämiseen, sisäisen valvonnan ja riskienhallinnan järjestämiseen ja kehittämiseen sekä ammattitaitoiseen henkilökuntaan.

Riskienarvioinnilla virasto/liikelaitos/tytäryhteisö tunnistaa, arvioi ja analysoi strategisia, toiminnallisia ja taloudellisia tavoitteitaan uhkaavat riskit koko organisaation laajuisesti, huomioiden toimintaympäristön muutokset, riskien hallintaan käytettävissä olevat menettelyt, väärinkäytösten mahdollisuudet sekä sisäiseen valvontajärjestelmään merkittävästi vaikuttavat muutokset.

Valvontatoimenpiteillä virasto/liikelaitos/tytäryhteisö edistää tavoitteidensa saavuttamista, varmentaa riskienhallinnan toimenpiteiden toimeenpanoa sekä hallinnon ja taloudenhoidon menettelyiden asianmukaisuutta. Riskejä pienentäviä valvontamenettelyjä ovat esim. toimivaltuudet, suunnitelmat, ohjeet, prosessikuvaukset, raportointimenettelyt sekä erilaiset taloudenhoidon ja hallinnon kontrollit, työnjaot ja järjestelmäkontrollit.

Sisäisen valvonnan tukemiseksi virasto/liikelaitos/tytäryhteisö tuottaa ja hankkii johdon käyttöön laadukasta ja merkityksellistä **tietoa sisäisen valvonnan ja riskienhallinnan toimivuudesta.** Johto viestii henkilöstölle sisäisen valvonnan ja riskienhallinnan tavoitteista ja vastuista sekä toimii yhteistyössä ulkopuolisten tahojen kanssa asioissa, jotka vaikuttavat sisäisen valvonnan ja riskienhallinnan toimivuuteen.

Virasto/liikelaitos/tytäryhteisö kehittää ja toteuttaa **sisäisen valvonnan ja riskienhallinnan jatkuvaa seurantaa ja arviointia sekä erillisiä arviointeja** varmistaakseen, että kaikki sisäisen valvonnan ja riskienhallinnan osatekijät ovat olemassa ja toimivat. Virasto/liikelaitos/tytäryhteisö viestii sisäisen valvonnan ja riskienhallinnan puutteista ajantasaisesti niille tahoille, jotka ovat vastuussa korjaavista toimenpiteistä, ja tarvittaessa myös lautakunnalle/johtokunnalle/tytäryhteisön hallitukselle, kaupungin johdolle ja kaupunginhallitukselle.

Seuraavissa luvuissa on kuvattu tarkemmin kutakin osatekijää ja niihin liittyviä toimintaperiaatteita ja menettelyitä.

2 SISÄINEN VALVONTA JA RISKIENHALLINTA OSANA HYVÄÄ JOHTAMIS- JA HALLINTOTAPAA

2.1. Helsingin kaupunkikonsernin hallinnon järjestäminen

Helsingin kaupunkikonsernin muodostavat Helsingin kaupunki emoyhteisönä sekä tytäryhteisöt. Kaupunkikonsernia johdetaan ja kehitetään kaupungin ja sen tytäryhteisöjen muodostamana kokonaisuutena. Kaupunkikonsernin toiminnot järjestetään ja tehtävät hoidetaan siten, että niissä noudatetaan hyvää johtamis- ja hallintotapaa.

Hyvällä johtamis- ja hallintotavalla tarkoitetaan toiminnan ja talouden ohjauksen tilivelvollisuus- ja vastuujärjestelmää, joka edistää hallinnon ja palvelutuotannon laillisuutta ja tuloksellisuutta. Järjestelmän perustana ovat lainsäädäntö, johtosäännöt, kaupungin arvot, eettiset periaatteet sekä kuntalaisten ja muiden asiakkaiden tarpeet. Hyvää johtamis- ja hallintotapaa määrittelevät arvot ja eettiset periaatteet on määritelty kaupungin strategiaohjelmassa.

Keskeistä hyvän johtamis- ja hallintotavan toteuttamisessa ovat sellaiset linjaukset ja menettelyt, joilla ohjataan kaupunkikonsernin toimintoja siten, että saadaan kohtuullinen varmuus asetettujen tavoitteiden saavuttamisesta, toiminnan laillisuudesta, eettisyydestä ja vastuullisuudesta.

Hallinnon järjestämisen ja johtamistavan keskeisiä osatekijöitä ovat:

- lainsäädännön noudattaminen
- johtosäännöt ja organisaatiorakenne
- arvot ja eettiset periaatteet
- johdon toimintatapa ja toimivallan delegointi
- henkilöstöjohtamisen periaatteet
- ammatillinen osaaminen ja kannustimet
- luottamus- ja virkamiesjohdon keskinäinen suhde
- tiedon kulku.

Helsingin kaupunkikonsernin johtamistapa perustuu tulosjohtamiseen. Kaupunkikonsernin hallinnossa tulosjohtamisella tarkoitetaan toiminnan kokonaisvaltaiseen tarkasteluun, tuloksellisuuteen ja yhteistyöhön perustuvaa johtamistapaa. Kaupunkikonsernin ohjausjärjestelmä koostuu strategiatyöstä sekä suunnittelu- ja seurantajärjestelmästä.

Kaupunginvaltuuston hyväksymä strategiaohjelma osoittaa toiminnan tavoitteet. Valtuusto päättää talousarvion yhteydessä sitovista ja muista toiminnallisista tavoitteista. Virastot ja liikelaitokset määrittelevät vuosittain talousarvio- ja taloussuunni-

telmaehdotuksessa, miten ne toteuttavat strategiaohjelmaa ja omaa perustehtäväänsä tavoitteellisesti. Virastot, liikelaitokset ja tytäryhteisöt tukevat vuositavoitteillaan strategioiden toteuttamista.

2.2. Mitä sisäinen valvonta ja riskienhallinta ovat?

Sisäisellä valvonnalla tarkoitetaan sisäisiä menettelyitä ja toimintatapoja, joilla johto pyrkii varmistamaan toiminnan laillisuuden ja tuloksellisuuden. Riskienhallinta tarkoittaa järjestelmällistä ja ennakoivaa tapaa tunnistaa, analysoida ja hallita toimintaan liittyviä uhkia ja mahdollisuuksia. Sisäinen valvonta ja riskienhallinta ovat osa kaupungin johtamisjärjestelmää sekä kaupunginjohdon ja hallinnon työvälineitä, joiden avulla tuetaan ja arvioidaan tavoitteiden asettamista, niiden toteutumista ja toimintaprosesseja.

Sisäinen valvonta ja riskienhallinta eivät ole erillisiä prosesseja tai toimenpidekokonaisuuksia, vaan osa kaikkia kaupunkikonsernin toimintoja, prosesseja ja projekteja. Riskien kartoituksen ja arvioinnin avulla ylläpidetään sisäisen valvontajärjestelmän ajantasaisuutta. Niillä arvioidaan toiminnassa ja toimintaympäristössä tapahtuvien muutosten vaikutusta organisaation toimintaan ja sen riskeihin sekä autetaan sopeuttamaan riskien hallintatoimenpiteet muuttuneisiin olosuhteisin.

Sisäinen valvonta ja riskienhallinta voidaan ajallisesti jakaa seuraaviin vaiheisiin:

Sisäisen valvonnan ja riskienhallinnan sekä niiden ohjauksen järjestäminen perustuen

- organisaation tavoitteiden, strategian, arvojen ja eettisten periaatteiden määrittelyyn,
- hallinnon järjestämiseen (vastuiden ja toimivallan määrittely, henkilöstö, prosessien määrittely ja ohjeistuksen laatiminen)

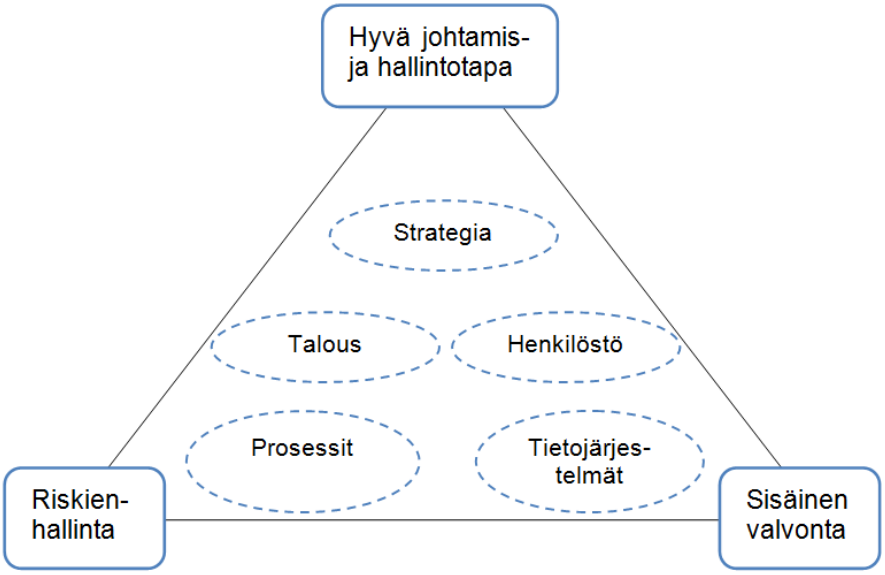
Sisäinen valvonta ja riskienhallinta päivittäisessä toiminnassa, joka toteutuu

- esimiesten ja muun henkilöstön suorittamana riskien tunnistamisena ja arviointina, hallintatoimenpiteiden toteuttamisena sekä valvontana
- valtuuksien, päätösten ja ohjeiden noudattamisena
- prosessien ja tietojärjestelmien kontrolleina.

Jälkikäteen tapahtuva toiminnan seuranta, raportointi ja arviointi, joka johtaa

- virheellisen toiminnan korjaamiseen
- sisäisen valvonnan ja riskienhallinnan kehittämiseen.

Kaupunkikonsernin tehtävät on järjestettävä siten, että kaupunkikonsernin kaikilla tasoilla ja kaikissa toiminnoissa on riittävä sisäinen valvonta ja riskienhallinta. Sisäisen valvonnan ja riskienhallinnan on katettava kaupunkikonsernin oman toiminnan lisäksi myös muu toiminta, josta kaupunkikonserni vastaa lainsäädännön, omistuksen, ohjaus- ja valvontavastuun sekä muiden velvoitteiden tai sopimusten nojalla.



KUVA 1. Hyvä johtamis- ja hallintotapa, sisäinen valvonta ja riskienhallinta asettavat vaatimuksia kaupunkikonsernin toiminnalle.

2.3. Sisäisen valvonnan ja riskienhallinnan kuvaus

Kaupunginvaltuuston hyväksymien sisäisen valvonnan ja riskienhallinnan perusteiden mukaisesti lauta- ja johtokunnat sekä tytäryhteisöjen hallitukset hyväksyvät kuvaukset sisäisestä valvonnasta ja riskienhallinnasta.

Virastot, liikelaitokset ja tytäryhteisöt kuvaavat sisäisen valvonnan ja riskienhallinnan keskeisimmät tavoitteet, toimintaperiaatteet ja menettelyt. Kuvauksessa määritellään miten virastoissa, liikelaitoksissa ja tytäryhteisöissä toteutetaan sisäistä valvontaa ja riskienhallintaa huomioiden toiminnan ominaisluonne ja laajuus, sekä se miten sisäinen valvonta ja riskienhallinta sisältyvät tai kytketään toimintoihin, prosesseihin, projekteihin ja tietojärjestelmiin. Sisäisen valvonnan ja riskienhallinnan kuvausten tulee kattaa kaikki sisäisen valvonnan ja riskienhallinnan osatekijät (katso luku 1.2).

Lauta- ja johtokunnat sekä tytäryhteisöjen hallitukset hyväksyvät kuvaukset. Kuvaus toimii näyttönä sisäisen valvonnan ja riskienhallinnan järjestämisestä sekä luo perustan sisäisen valvonnan ja riskienhallinnan toimivuuden seurannalle, arvioinnille ja kehittämiselle. Lisäksi kuvaus tukee raportointia sisäisen valvonnan ja riskienhallinnan toteutumisesta sisäisen valvonnan ja riskienhallinnan selonteoissa. Kuvaus auttaa tilintarkastajia lainmukaisessa tehtävässä heidän arvioidessaan Helsingin kaupungin sisäisen valvonnan ja riskienhallinnan sekä konsernivalvonnan järjestämisen asianmukaisuutta.

Kuvausten valmistelussa voi hyödyntää kaupunginkanslian laatimaa kuvauspohjaa ja ohjetta, jotka löytyvät Helmi- ja Tyyne-intranetistä.

2.4. Tilivelvollisten valvontavastuu

Kuntalain tarkoittamia tilivelvollisia ovat muun muassa:

- kaupunginhallituksen jäsenet,
- kaupunginhallituksen konsernijaoston ja tietotekniikkajaoston jäsenet,
- lauta-, johto- ja toimikuntien sekä muiden kunnan toimielinten jäsenet,
- kaupunginjohtaja ja apulaiskaupunginjohtajat sekä
- virastojen ja liikelaitosten päälliköt.

Tilivelvollisella on henkilökohtainen vastuu johtamansa toiminnan sisäisen valvonnan ja riskienhallinnan järjestämisestä ja toteutumisesta. Kuntalain tarkoittaman tilivelvollisuusaseman puuttuminen ei vapauta tytäryhteisön johtoa, virastojen ja liikelaitosten osastotasoisten yksiköiden päälliköitä tai muitakaan esimiehiä toiminnan valvontavastuusta. Tytäryhteisöjen on toiminnassaan otettava huomioon myös yhteisökohtaisen lainsäädännön säännökset huolellisuusvelvollisuudesta.

Kaupunginvaltuuston ja tilivelvollisten sisäisen valvonnan ja riskienhallinnan vastuut on määritelty sisäisen valvonnan ja riskienhallinnan perusteissa ja johtosäännöissä. Tytäryhteisöjen osalta sisäisen valvonnan ja riskienhallinnan vastuut on määritelty konserniohjeessa sekä johtamisen ja hallinnon keskeisissä periaatteissa.

2.5. Johdon valvontavastuu

Johdon toimivaltaa ja vastuuta määritellään sisäisen valvonnan ja riskienhallinnan perusteiden ja johtosääntöjen lisäksi virastopäällikköjen hyväksymissä toimintasäännöissä ja delegointipäätöksissä. Johto vastaa toiminnan järjestämisestä siten, että prosesseille, hankkeille, projekteille ja yksittäisille toiminnoille on määritelty vastuutahot. Johdon tehtävänä on luoda toimiva ja kattava ohjaus- ja seurantajärjestelmä.

Johdon on viestitettävä henkilöstölle sisäisen valvonnan ja riskienhallinnan merkityksestä. Aktiivisella tiedottamisella ja viestinnällä varmistetaan, että henkilöstö tuntee tehtävissään sovellettavat valvonnan toimintaperiaatteet ja menettelytavat.

2.6. Esimiehen valvontavastuu

Esimies vastaa johtamiensa yksiköiden sisäisestä valvonnasta ja riskienhallinnasta. Esimies vastaa siitä, että hänen yksikkönsä tavoitteet tukevat ylemmän tason tavoitteita, ja siitä, että hänen alaisuudessaan olevien yksiköiden tavoitteet ovat linjassa koko yksikön tavoitteiden kanssa. Esimies vastaa myös tiedonkulusta ja raportoinnista.

Esimiehellä on vastuu myös yksikkönsä toiminnan ja prosessien järjestämisestä sekä työvälineistä. Hänen tehtäviinsä kuuluu päivittäisen toiminnan valvonta. Esimies vastaa johtamiensa yksiköiden osalta siitä, että henkilöstön toimivaltuudet, tehtävät ja vastuut on määritelty ajantasaisesti. Esimiehen tehtävänä on luoda edellytykset tehtävistä suoriutumiseen ja tavoitteiden saavuttamiseen. Esimies käy säännöllisesti tulos- ja kehityskeskustelut, joissa tavoitteiden ja niiden toteutumisen

lisäksi käydään läpi alaisen toimivaltuudet ja vastuut sekä tehtävien toteuttamisen edellyttämä osaaminen. Esimiehellä on aktiivinen selonottovelvollisuus.

Esimies ohjaa ja valvoo alaistensa toimintaa. Esimiehen on ryhdyttävä toimenpiteisiin välittömästi, kun ilmenee toimintaa, joka on lain, sääntöjen, ohjeiden tai päätösten vastaista, tehotonta tai epätarkoituksenmukaista.

Yksikkönsä prosessien ja tietojärjestelmien omistajana esimies vastaa sekä tietojärjestelmien käytöstä toiminnan valvonnassa että itse tietojärjestelmien käytönvalvonnasta.

2.7. Muun henkilöstön valvontavastuu

Jokainen työntekijä vastaa osaltaan riskien tunnistamisesta ja arvioinnista omassa tehtävässään ja työympäristössään. Työntekijä on velvollinen toimimaan riskien ennaltaehkäisemiseksi sekä raportoimaan havaitsemistaan riskeistä, mahdollisista väärinkäytöksistä ja läheltä piti -tilanteista esimiehelleen.

3 RISKIENHALLINTA

3.1. Riskienhallinnan näkökulmat ja ulottuvuudet

Riskienhallintaa toteutetaan kaikilla organisaatiotasoilla, eri toiminnoissa ja prosesseissa. Lisäksi edellytetään, että palvelutuottajille ulkoistetuissa palveluissa on riittävä riskienhallinta. Riskienhallinnassa näkökulmina ovat strategian ja talouden riskit, toiminnalliset riskit sekä ulkoiset riskit.

Seuraavassa esitetyt näkökulmat on huomioitava sisäisen valvonnan ja riskienhallinnan järjestämisessä ja toteuttamisessa, päätöksenteossa sekä raportoinnissa.

Kuva 2. Riskienhallinnan näkökulmat ja ulottuvuudet

3.2. Strategian ja talouden riskit

Organisaation tavoitteiden saavuttamiseen, valintoihin ja päätöksentekoon liittyy strategisiksi ja taloudellisiksi kutsuttuja riskejä. Strategisten ja taloudellisten riskien arvioinnin yhteydessä organisaation on päätettävä, millaisia riskejä se on valmis ottamaan. Näiden riskien arviointiin sisältyy usein mahdollisuuksien tunnistaminen ja hyödyntäminen.

Kaupungin strategiset tavoitteet ja toimenpiteet on määritelty strategiaohjelmassa. Talousarvioehdotuksen laatimisen tai sitä vastaavien prosessien yhteydessä virastot, liikelaitokset ja tytäryhteisöt määrittelevät kaupungin strategiaohjelmasta johdetut toiminnalliset ja taloudelliset tavoitteensa. Osana talousarvioprosessia virastot, liikelaitokset ja tytäryhteisöt tunnistavat tavoitteiden toteutumista uhkaavia riskejä ja niiden vaikutuksia sekä laativat ja päivittävät tarvittavat suunnitelmat ja toimenpiteet riskien hallitsemiseksi. Valtuusto päättää talousarvioon sisältyvistä sitovista ja muista toiminnallista tavoitteista.

Talouden riskeillä tarkoitetaan tässä yhteydessä lähinnä kaupungin, viraston, liikelaitoksen tai tytäryhteisön taloudenpitoon, maksuvalmiuteen, rahoitukseen ja sijoituksiin liittyviä valintoja ja riskitekijöitä. Strategian ja talouden riskeissä keskeisintä ovat valinnat ja päätöksenteko sekä näiden yhteydessä tehtävät analyysit näihin liittyvistä riskeistä ja mahdollisuuksista.

3.3. Toiminnalliset riskit

Toiminnalliset riskit ovat organisaation henkilöstöön, toimintaan ja laillisuuteen, prosesseihin sekä tietoihin ja tietojärjestelmiin kohdistuvia riskejä, joilla on pääosin haitallisia vaikutuksia. Tämä riskinäkökulma kattaa myös henkilöstön tai ympäristön turvallisuutta ja omaisuutta uhkaavat vahinkoriskit. Toiminnallisiin riskeihin kuuluu myös vaatimustenmukaisuuteen ja väärinkäytöksiin liittyviä riskejä, joiden toteutumista usein seuraa taloudellisten ja toiminnallisten vaikutusten lisäksi muun muassa maineriskejä.

Toiminnallisten riskien tunnistamista ja arviointia tehdään osana päivittäistä johtamista. Keskeistä toiminnallisten riskien hallinnassa on, että mahdolliset riskitekijät on tunnistettu ja valitut tarkoituksenmukaiset hallintakeinot on toteutettu ja että hallintakeinot toimivat tehokkaasti. Toiminnallisten riskien hallinnalla pyritään varmistamaan, ettei riskeistä aiheudu ennalta arvaamattomia taloudellisia seurauksia tai muita haitallisia vaikutuksia. Toiminnallisten riskien hallinnassa hyödynnetään erilaisia hallintakeinoja, kuten esimiesvalvontaa, ohjeistusta ja kontrolleja. Tunnistetut toiminnalliset riskit huomioidaan organisaation varautumisen ja jatkuvuudenhallinnan suunnittelusta annettujen ohjeiden mukaisesti. Myös vakuuttamisella voidaan pienentää vahinkoriskien taloudellisia vaikutuksia.

3.4. Ulkoiset riskit

Ulkoiset riskit ovat organisaation ulkopuolelta nousevia tekijöitä, joiden syntymistä ei voida itse estää. Näitä ovat muun muassa talouteen tai sääntelyyn liittyvät muutokset sekä paikalliset tai globaalit kriisit ja katastrofit, jotka voivat muuttaa toimintaympäristöä hetkellisesti tai pysyvästi.

Ulkoisten riskien tunnistamista ja arviointia tehdään osana päivittäistä johtamista. Virastojen ja liikelaitosten on tunnistettava ja huomioitava ulkoiset riskit erityisesti vuosittaisissa talousarvioprosesseissaan osana toimintaympäristön analysointia. Tytäryhteisöt noudattavat samoja periaatteita omissa suunnitteluprosesseissaan.

Keskeistä ulkoisten riskien hallinnassa on tunnistaa toimintaympäristössä tapahtuvia muutoksia ja arvioida niiden vaikutuksia. Tulevien muutosten arvioinnissa voi hyödyntää erilaisia ennusteita, skenaarioita ja laskentamalleja. Merkittävimpien riskien seurannan on oltava aktiivista ja jatkuvaa.

Ulkoisten riskien hallinnassa tavoitteena on pyrkiä pienentämään riskien vaikutuksia, mikäli riskit toteutuvat. Kaupungin toiminnassa tämä tarkoittaa muun muassa toiminnallista ja/tai taloudellista varautumista tulevaan sekä sopeutumista ja nopeaa reagointia muuttuneeseen tilanteeseen. Tunnistetut ulkoiset riskit huomioidaan organisaation varautumisen ja jatkuvuudenhallinnan suunnittelussa kaupunkikonsernin valmiusohjeen mukaisesti.

3.5. Kaupunkikonsernin merkittävät riskit

Kaupunkikonsernin merkittävillä riskeillä tarkoitetaan sellaisia strategian ja talouden riskejä sekä toiminnallisia ja ulkoisia riskejä, jotka uhkaavat kaupunkikonsernin tavoitteita tai ovat toteutuessaan muuten hyvin laajoja vaikutuksiltaan. Monet kaupunkikonsernitason riskeistä ovat sellaisia, joita ei pystytä hallitsemaan pelkästään yksittäisen viraston, liikelaitoksen tai tytäryhteisön hallintakeinoilla.

Kaupunginkanslia ja sen johdolla toimiva sisäisen valvonnan ja riskienhallinnan koordinaatioryhmä kokoaa ja laatii arvioita kaupunkikonsernin merkittävistä riskeistä. Riskien tunnistamisessa ja arvioinnissa hyödynnetään muun muassa tietoja virastojen, liikelaitosten ja tytäryhteisöjen tunnistamista ja arvioimista riskeistä. Merkittävistä riskeistä raportoidaan vuosittain tilinpäätöksen toimintakertomuksessa.

3.6. Riskien arviointi

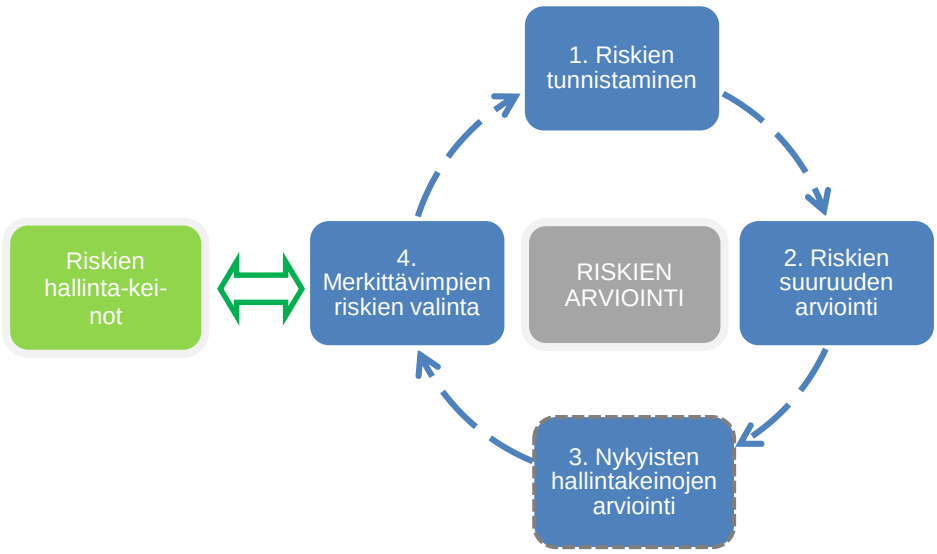
Riskejä arvioidaan osana jokapäiväistä johtamista ja päätöksentekoa. Tällöin riskinäkökulma on yksi päätöksentekoon vaikuttava tekijä. Virastojen, liikelaitosten ja tytäryhteisöjen strategiatyössä ja taloussuunnittelussa on useita elementtejä, jotka ovat riskien arviointia.

Riskien arvioinnin tarkoituksena on tunnistaa arvioinnin kohteen merkittävimmät riskit ja analysoida niiden hallintakeinoja. Ennen riskien arviointiprosessin aloittamista on päätettävä, millä organisaatiotasolla riskejä on tarkoitus tarkastella. Riskien arvioinnissa huomioidaan riskienhallinnan näkökulmat ja ulottuvuudet (katso kuva 2,

sivulla 9). Yksittäisessä arvioinnissa voidaan keskittyä myös tietyn riskinäkökulman tai -lajin arviointiin.

Riskien tunnistamista ja arviointia voidaan toteuttaa myös yksittäisten riskienarviointien avulla. Yksittäinen arviointi tai riskityöpaja ei korvaa jatkuvaa ja laajempaa riskienhallintatyötä, mutta sen avulla saadaan kohtuullisen luotettava kuva arvioidun osa-alueen nykytilasta ja kehittämistarpeesta. Kukin virasto, liikelaitos ja tytäryhteisö määrittelee tarkemmat toteuttamistavat sisäisen valvonnan ja riskienhallinnan kuvauksissaan.

Kuvassa 3 on esitetty riskien arviointimalli, joka soveltuu hyvin muun muassa toiminnallisten riskien arviointiin. Mallia voidaan hyödyntää myös merkittävimpien riskien arvioinnissa, jossa on mukana riskejä useammasta riskienhallinnan näkökulmasta. Arviointia voidaan toteuttaa myös muilla arviointitavoilla.



Kuva 3. Riskien arvioinnin vaiheet

1. Riskien tunnistaminen

Riskien tunnistamisvaiheen tarkoituksena on tunnistaa, mitä sellaista voi tapahtua tai ilmetä, jolla arvioidaan olevan vaikutuksia organisaation tavoitteiden saavuttamiseen. Tunnistamisvaiheen perusteella kootaan merkitykselliset riskit sekä tuotetaan tietoa riskien syistä ja seurauksista. Näiden tietojen perusteella laaditaan riskikuvaukset.

2. Riskien suuruuden arviointi

Tunnistettujen riskien todennäköisyyksiä ja vaikutuksia on arvioitava ennalta päätettyjen arviointikriteereiden mukaisesti. Arviointikriteereissä on otettava kantaa siihen,

että huomioidaanko jo olemassa olevat riskien hallintakeinot osana arviointia. Riskien suuruutta arvioitaessa on huomioitava kuinka riski toteutuessaan uhkaa muun muassa:

- strategisten, taloudellisten ja toiminnallisten tavoitteiden toteutumista
- toiminnan laillisuutta
- toiminnan jatkuvuutta
- terveyttä, turvallisuutta ja ympäristöä.

Arvioinnissa on huomioitava myös mahdollisuus useamman riskin samanaikainen toteutumiseen ja eri riskien keskinäiset vaikutukset.

3. Nykyisten hallintakeinojen arviointi

Mikäli arviointihetkellä käytössä olevia riskien hallintakeinoja ei ole huomioitu osana riskin suuruuden arviointia, on riskin hallinnan tasoa arvioitava erikseen. Tällöin on selvitettävä, mitä hallintakeinoja kyseistä riskiä vastaan on käytössä ja ovatko nykyiset keinot tarkoituksenmukaisia ja tehokkaita. Hallintakeinoja voivat olla esimerkiksi tekniset ratkaisut, menettelytavat sekä ohjeet ja niiden noudattaminen.

4. Merkittävimpien riskien valinta

Riskien tunnistamisen, suuruuden ja nykyisten hallintakeinojen arvioinnin perusteella muodostetaan kuva merkittävimmistä riskeistä ja niiden hallinnasta. Tämän jälkeen on selvitettävä, mitkä riskeistä ovat sellaisia, jotka vaativat vielä tarkempaa arviointia.

Virastojen, liikelaitosten ja tytäryhteisöjen tulee omissa arvioissaan huomioida myös riskien vaikutukset poikkihallinnollisissa prosesseissa. Periaatteena on, ettei riskejä siirretä toiselle yksikölle kaupunkikonsernin sisällä. Mikäli viraston, liikelaitoksen tai tytäryhteisön merkittävistä riskeistä aiheutuu uhkaa toiselle kaupunkikonsernin yksikölle, on asiasta raportoitava ja menettelyistä sovittava osapuolten kesken.

3.7. Riskien hallintakeinoista päättäminen

Riskien hallintakeinojen tarkoituksena on saattaa riskit hyväksyttävälle tasolle. Mikäli todetaan, että merkittävimpien riskien hallintakeinot eivät ole riittäviä, tulee niiden hallintaa kehittää.

Keskeisimpiä vaihtoehtoja riskien hallinnassa ovat riskin poistaminen, välttäminen, pienentäminen, hyväksyminen tai siirtäminen. Riski voidaan siis hyväksyä tietoisella päätöksellä tai ottaa hallittu riski mahdollisuuksien hyödyntämiseksi. Eri vaihtoehdot eivät ole välttämättä toisiaan pois sulkevia. Hallintakeinoja valittaessa otetaan huomioon hallintavaihtoehtojen hyöty, tehokkuus ja kustannukset.

Toteutettavat hallintakeinot on kytkettävä prosesseihin ja käytävä läpi osapuolten ja tarvittavien sidosryhmien kanssa. Riskien hallintakeinot voivat tuoda mukanaan

myös uusia riskejä, joita on edelleen arvioitava ja seurattava. Riskien hallintakeinoja suunniteltaessa ja toteutettaessa on määriteltävä:

- vastuuhenkilö/t, menettelyt, resurssit ja aikataulut
- hallintakeinojen tehokkuuden mittaaminen
- dokumentointi, seuranta ja raportointi.

Riskien hallintakeinojen tulee olla jäljitettävissä. Hallintakeinojen tulee olla dokumentoituina esimerkiksi toimintasuunnitelmassa, prosessikuvauksissa, prosessien työohjeissa tai muissa vastaavissa asiakirjoissa.

Sisäisen valvonnan ja riskienhallinnan kehittämisen edellyttämät toimenpiteet ja hankkeet tulee sisällyttää toimintasuunnitelmaan ja kustannukset tulee huomioida talousarvioehdotuksessa.

4 VALVONTATOIMENPITEET

4.1. Valvontatoimenpiteiden suunnittelu, valinta ja toteuttaminen

Valvontatoimenpiteiden tarkoitus on edistää ja varmistaa tavoitteiden saavuttamista pienentämällä riskejä hyväksyttävälle tasolle. Valvontatoimenpiteet varmistavat päätettyjen menettelytapojen ja ohjeiden noudattamista sekä riskien hallintatoimenpiteiden toteuttamista.

Johto vastaa siitä, että valvontavastuut on määritelty ja että esimiehet ovat ammattitaitoisia ja toimivat päätettyjen menettelytapojen ja ohjeiden edellyttämällä tavalla. Esimiehet vastaavat siitä, että henkilöstö on tietoinen päätetyistä menettelytavoista ja ohjeista sekä omasta roolistaan ja tehtävistään valvontatoimenpiteiden toteuttamisessa. Osa valvontatoimenpiteistä voi olla luonteeltaan sellaisia, että johto antaa niistä tietoa rajoitetusti henkilöstölle tai ulkopuolisille. Esimiehet suorittavat valvontatoimenpiteitä huolellisesti, todentavat tekemänsä valvontatoimenpiteet ja ryhtyvät tarvittaessa korjaaviin toimenpiteisiin.

Valvontatoimenpiteiden valintaan ja kehittämiseen vaikuttavat toiminnan luonne, toimintojen laajuus ja monimutkaisuus, toimintaympäristö ja sen muutokset, teknologioiden käytön määrä sekä riippuvuus tietojärjestelmistä. Valvontatoimenpiteet suunnitellaan riskinäkökulmasta. Suunnittelussa otetaan huomioon valvontatoimenpiteillä saavutettava hyöty suhteessa aiheutuviin kustannuksiin.

Suuri osa valvontatoimenpiteistä toteutuu prosesseihin sisällytettävinä henkilöstön toteuttamina päivittäisinä toimenpiteinä ja varmistuksina. Johdon ja esimiesten on arvioitava säännöllisesti valvontatoimenpiteiden ajantasaisuutta ja tarvittaessa uudistettava niitä. Tarvittaessa valvontatoimenpiteitä täydennetään riskienarvioinnin perusteella tai muutetaan siten, että valvonta keskittyy merkittävimmiksi arvioitujen riskien hallintaan.

4.2. Valvontatoimenpiteiden luonne

Toimintaan ja tietojärjestelmiin sisäänrakennetut ennaltaehkäisevät valvontatoimenpiteet havaitsevat ja estävät tai korjaavat prosessissa, tapahtumien käsittelyssä tai tiedoissa ilmeneviä virheitä.

Toimintaprosesseihin ja tietojärjestelmiin sisäänrakennettuun valvontaan kuuluu kontrolleja, jotka:

- tukevat lakien, päätösten sekä päätettyjen menettelytapojen ja ohjeiden noudattamista
- tukevat prosessin oikeaa kulkua ja tietojärjestelmän käytön oikeellisuutta
- valvovat valtuuksien noudattamista
- varmistavat tapahtumien ja tietojen oikeellisuutta
- suojaavat tietoja
- estävät virheitä ja väärinkäytöksiä
- varmistavat tehtävien riittävää eriyttämistä
- turvaavat toiminnan jatkuvuutta.

Virheitä ja poikkeamia paljastamaan suunniteltuja valvontatoimenpiteitä ovat esimerkiksi:

- taloudellisten tavoitteiden toteutumisen seuranta
- raportoinnin analysointi ja seuranta
- toiminnan ja toimintapoikkeamien seuranta
- erilaiset säännölliset varmistus- ja täsmäytystoimenpiteet
- sovittujen riskirajojen seuranta ja raportointi
- tehtävänvaihto
- fyysiset ja tekniset valvontatoimenpiteet.

Korjaavien valvontatoimenpiteiden tavoitteena on auttaa virheiden tutkimisessa ja korjaamisessa. Korjaava valvontatoimenpide on esimerkiksi tietojen varmistus ja palauttaminen tai virhetilastojen hyödyntäminen.

4.3. Tietojärjestelmien rooli valvonnassa ja ICT-toimintojen valvonta

Valvontatoimenpiteet ja tietotekniikka liittyvät toisiinsa kahdella tavalla. Organisaation prosessien toteutuessa pääosin yhden tai useamman tietojärjestelmän avulla, tarvitaan valvontatoimia, jotka kohdistuvat tietojärjestelmiin sekä niiden käytöstä syntyviin riskeihin. Toisaalta tietojärjestelmillä voidaan joko kokonaan tai osittain toteuttaa prosessissa ja tapahtumien käsittelyssä tarvittavat valvontatoimet. Useimmissa prosesseissa valvonta toteutuu sekä automatisoitujen että henkilöiden tekemien valvontatoimien yhdistelmänä (esim. talousarvion seuranta).

Tietojärjestelmiä hyödyntävissä prosesseissa valvontatoimenpiteet on yleensä tehokkainta toteuttaa tietojärjestelmien avulla. Tietojärjestelmissä valvontaan käytettävissä olevia keinoja ovat muun muassa:

- käyttöoikeuksien ja valtuustasojen määrittely
- tapahtumien ja tietojenkäsittelyn lokit ja muutosten jäljitettävyys
- syöttötietojen tarkistukset
- muut ohjelmalliset tarkistukset ja täsmäytykset
- tietojen turvaluokittelu ja suojaaminen
- virheiden ja poikkeamien seuranta ja raportointi
- järjestelmien käytönvalvonta mm. lokitietojen avulla.

Tietojärjestelmien omistajat ja esimiehet ovat vastuussa näiden valvontatoimien järjestämisestä, niiden toimivuuden valvonnasta sekä valvonnan puutteiden seurannasta, raportoinnista ja korjaamisesta. Tehtävien tehokas eriyttäminen varmistetaan tietojärjestelmien käyttöoikeuksia rajaamalla. Tietojärjestelmiin ei aina voida rakentaa riittäviä automatisoituja kontrolleja, jolloin esimiehen on huolehdittava korvaavien valvontatoimien järjestämisestä ja toimivuuden valvonnasta.

Tietotekniikan toimintaa pitää seurata aktiivisesti ongelmien havaitsemiseksi ja korjaavien toimenpiteiden käynnistämiseksi. ICT-toimintojen kehittämiselle, käytölle ja ylläpidolle pitää olla prosessit, joihin on järjestetty valvontatoimet ICT-prosesseille ominaisten riskien hallintaan.

Organisaation ICT-toiminnoissa toteutettavat yleiset kontrollit auttavat varmistamaan tietojenkäsittelyn eheyttä, virheettömyyttä ja saatavuutta. ICT-prosessien yleisten kontrollien tavoitteena on valvoa tietotekniikkaympäristön toimintaa, tietoliikenneverkkojen ja tietojärjestelmien pääsynhallintaa sekä ohjelmistojen ja laitteistojen hankintaa ja ylläpitoa. Järjestelmätietojen oikeellisuuden näkökulmasta tärkeimmät yleiset ICT-kontrollit ovat muutoshallinta ja käyttövaltuuksien hallinta.

Tietotekniikkatoimintojen ylläpitämiseksi tarvitaan varmistus- ja palauttamismenettelyitä sekä jatkuvuus- ja toipumissuunnittelua, jotka riippuvat mahdollisen käyttökatkoksen riskeistä ja seurauksista. Ulkoisten ICT-palvelujen toimittajien toteuttaessa edellä mainittuja tehtäviä tai osaa niistä, on kaupungin huolehdittava menettelyjen toimivuudesta ja riskienhallinnasta sopimuksilla ja sopimusten valvonnalla. Sopimuksissa pitää olla huomioituna ICT-palvelujen toimittajien tuottamien palvelujen ohjaus, valvonta ja mahdollinen tarkastusoikeus.

4.4. Vaarallisten työyhdistelmien tunnistaminen ja ehkäiseminen

Vaarallisten työyhdistelmien tunnistaminen perustuu prosessien kuvaamiseen ja prosessien riskien arvioimiseen. Vaarallinen työyhdistelmä on kyseessä, jos henkilö käsittelee yksin väärinkäytös- ja virhealttiissa prosessissa koko tapahtumaketjun tai useampia sen osia. Vaarallinen työyhdistelmä mahdollistaa väärinkäytöksen tai vakavan virheen, joka voi jäädä huomaamatta.

Virheiden ja väärinkäytösten välttämiseksi vastuut ja tehtävät on jaettava eli eriytettävä siten, että esimerkiksi tapahtumien hyväksyminen, kirjaaminen ja varojen hoitaminen on jaettu eri henkilöille. Vaarallisia työyhdistelmiä voi esiintyä taloushallinnon lisäksi myös muissa kaupungin toiminnoissa, kuten tietojenkäsittelytoiminnoissa.

Toiminnoissa, joissa ei ole useita työntekijöitä, on suurempi riski vaarallisten työyhdistelmien muodostumiselle. Jos tehtävien jakaminen useammalle henkilölle ei ole mahdollista, käytetään jälkikäteisvalvontaa toiminnan oikeellisuuden varmistamiseksi. Esimerkiksi esimies hyväksyy jälkikäteen tehdyt toimet ja tapahtumat siten, että hyväksyminen on myöhemmin todettavissa.

Tärkeää on myös varmistaa, että työtehtävien hoitajien käyttöoikeudet vastaavat heidän työtehtäviään. Liian laajat käyttöoikeudet murentavat työtehtävien eriyttämisen.

4.5. Väärinkäytösten tunnistaminen ja torjunta

Väärinkäytöksenä pidetään erilaisia epärehellisiä, epäeettisiä tai kaupunkikonsernin ohjeita tai lainsäädäntöä rikkovia tahallisia tekoja.

Helsingin kaupunkikonsernissa ei sallita väärinkäytöksiä. Sisäisen valvonnan tavoitteena on poistaa mahdollisuudet väärinkäytösten tekemiseen. Mikäli väärinkäytös kuitenkin tapahtuu, tarkoituksenmukaisesti toimiva sisäinen valvonta paljastaa väärinkäytöksen. Johto vastaa sisäisen valvonnan toimivuudesta ja on velvollinen puuttumaan havaittuihin väärinkäytöksiin.

Väärinkäytösepäily voi syntyä valvontatoimenpiteiden yhteydessä, tarkastuksen tuloksena, ulkopuolisen ilmiantona tai muista lähteistä.

Tunnusmerkkejä väärinkäytöksestä ovat esimerkiksi:

- päätösvaltaa on käytetty ohjeistuksen tai delegoidun toimivallan vastaisesti
- asiakirjat ovat virheellisiä tai niitä epäillään väärennetyiksi
- asiakirjoja tai omaisuutta on hävitetty tai niiden epäillään hävinneen
- epäillään, että on erehdytetty henkilöä
- käskyvaltaa alaisiin on käytetty väärin.

Henkilöstön on raportoitava havaitsemansa merkit mahdollisista väärinkäytöksistä tai rikkomuksista esimiehelleen tai muulle organisaation osoittamalle taholle. Ilmoituksen voi tarvittaessa tehdä myös kaupunginkanslian sisäiseen tarkastukseen. Väärinkäytösten selvittäminen on ensisijaisesti esimiesten tehtävä. Sisäinen tarkastus voi kaupungin johdon harkinnan mukaan avustaa väärinkäytösten selvittämisessä.

5 TIETO JA VIESTINTÄ

5.1. Tiedon ja viestinnän merkitys ja oikeellisuus

Sisäistä valvontaa ja riskienhallintaa koskevaa ja tukevaa tietoa ja viestintää tarvitaan kaupunkiorganisaation kaikilla tasoilla, jotta toimintaa voidaan johtaa kaupunkikonsernin tavoitteiden mukaisesti. Johto tarvitsee toiminnan ohjaamiseen ja valvontaan tietoja tavoitteista, taloudesta, toiminnasta, hankkeista ja hankinnoista sekä

säännöistä ja päätöksistä sekä niiden noudattamisesta. Tietoa tarvitaan myös toimintaympäristöstä. Sitä kerätään muun muassa omistukseen, sopimukseen, avustukseen tai muuhun yhteistyöhön perustuvilta kumppaneilta.

Toimiva sisäistä valvontaa ja riskienhallintaa tukeva viestintä edellyttää viestinnän tavoitteiden asettamista ja seurantaa sekä selkeitä tiedon tuottamisen ja jakamisen rooleja, vastuita ja tehtäviä. Lisäksi tarvitaan menettelytapoja välittää organisaatiossa kaikkiin suuntiin sisäistä valvontaa ja riskienhallintaa koskevaa ja palvelevaa tietoa.

Tehokasta viestintää tarvitaan myös kaupungin ulkoisten sidosryhmien kuten asiakkaiden, kuntalaisten, palvelujen toimittajien, tilintarkastajien ja valtionhallinnon kanssa. Ulkopuolisilta tahoilta saadaan tietoja myös sisäisen valvonnan puutteista ja toimimattomuudesta sekä toteutuneista riskeistä.

Toiminnan ja sen tuloksellisuuden edellytyksenä on, että päätöksenteon pohjaksi ja sisäisen valvonnan ja riskienhallinnan toteuttamiseksi on käytettävissä oikeat ja riittävät tiedot. Organisaation tietojen oikeellisuutta, saatavuutta ja luottamuksellisuutta suojataan tietoriskien hallinnan avulla. Tietoriskien hallinnan pitää kattaa tietoja käsittelevien tahojen toimintatavat ja menettelyt, tietojärjestelmien tekniset suojaukset sekä tietojen käsittelytilojen suojausjärjestelyt.

Tietoriskien hallinnan ja hallintamenettelyjen valvonnan järjestämisestä ovat vastuussa tietojen omistaja sekä tietoja käsittelevän tietojärjestelmän omistaja. Käsiteltävät tiedot pitää tunnistaa ja luokitella, jotta voidaan estää tärkeiden tietojen muuttuminen, asiaton käsittely, katoaminen ja paljastuminen. Eri olomuodoissa olevien (esimerkiksi sähköiset tiedot tai paperiset asiakirjat) tietojen suojaaminen edellyttää erilaisia suojaustapoja.

Tietoriskien hallinnan työvälineitä ovat muun muassa:

- ohjeistus, koulutus, tiedotus, arviointi ja tarkastukset
- selkeät tietojen omistajuus ja valvontavastuut
- tietojen luokittelu ja suojaus
- tekniset tietoturvan suojauskeinot
- tietojärjestelmien pääsynhallinta
- tärkeiden toimintojen ja tietojärjestelmien dokumentointi
- henkilöstön taustaselvitykset ja salassapitosopimukset
- virheiden ja yllättävien tapahtumien seuranta ja selvittäminen
- toimitilojen suojaus ja kulunvalvonta
- varautuminen häiriöihin ja onnettomuuksiin.

Tietoja ei ole syytä salata, mikäli siihen ei ole perustetta. Tietojen avoimuudella voidaan lisätä tietojen hyödynnettävyyttä sekä muun muassa toimintaan ja varojen käyttöön kohdistuvaa avoimuutta ja luottamusta. Myös julkisten tietojen oikeellisuus ja muuttumattomuus pitää turvata.

5.2. Raportointi

Sisäisen valvonnan ja riskienhallinnan raportoinnista määrätään kaupunkikonsernin sisäisen valvonnan ja riskienhallinnan perusteissa. Tämän lisäksi talousarvion laatimis- ja noudattamisohjeissa voidaan antaa raportointia koskevia ohjeita.

Raportointi tavoitteiden toteutumisesta ja säännösten ja päätösten noudattamisesta sekä niissä ilmenneistä poikkeamista on kaupungin johdon tärkein työväline. Raportoitavan tiedon tulee olla luotettavaa, olennaista, ajantasaista ja oikeassa muodossa. Tiedon laatuun vaikuttavat tiedon soveltuvuus tarkoitukseensa, tiedon ajankohtaisuus, tiedon oikeellisuus ja saatavuus.

Raportoitavan tiedon oikeellisuus ja määrittelyjen mukaisuus on siksi yksi tärkeistä valvonnan kohteista.

Tietojen oikeellisuus varmistetaan tietojen ja raporttien tuotantoprosessien kontrolleilla. Vastuu tiedon oikeellisuuden varmistamisesta, myös ulkoa saadun tiedon, on toiminnon tai prosessin omistajalla. Lisäksi raportoinnin ja tietojen oikeellisuuden valvonnassa pitää ottaa huomioon väärinkäytösten mahdollisuus.

Sisäistä valvontaa ja riskienhallintaa tukevien tietojen ja raporttien tuottaminen edellyttää:

- tarvittavien tietojen määrittelyä
- tietojen lähteiden ja tietoja tuottavien järjestelmien tunnistamista
- tietojen jalostustavoista sopimista
- tietojen keruu- ja jakeluprosesseja sekä tietojen välityskanavia
- seurantajärjestelmää tavoitteineen, mittareineen ja prosesseineen
- poikkeamien selvittämistä ja korjaavien toimenpiteiden valvontaa sekä
- tietojen ja niiden lähteiden ajoittaista uudelleenarviointia.

Tietoja ei kannata tuottaa, jos tietojen tuottamiskustannukset tai aiheutuva työmäärä ylittävät saatavat hyödyt. Tiedot saadaan yleensä tuotettua tietojärjestelmissä tehokkaimmin ja helpoimmin silloin, kun tietotarpeet on otettu huomioon uusien tietojärjestelmähankkeiden vaatimuksissa. Siksi sisäisen valvonnan ja riskienhallinnan tietotarpeet pitää olla mukana jo uusien tietojärjestelmähankkeiden vaatimusmäärittelyissä.

Virastojen, liikelaitosten ja tytäryhteisöjen operatiivisessa toiminnassa tuotettu raportointi tukee niiden omaa sisäistä valvontaa ja riskienhallintaa. Yksiköt eri tasoilla voivat hyödyntää sisäisen valvonnan ja riskienhallinnan toteuttamisessa raportteja muun muassa:

- talouden ja toiminnan seurannasta
- valtuuksista ja niiden käytön seurannasta
- poikkeamista ja virheistä
- vahingoista ja läheltä piti -tilanteista.

6 SISÄISEN VALVONNAN JA RISKIENHALLINNAN SEURANTA, ARVIOINTI JA KEHITTÄMINEN

6.1. Seuranta, arviointi ja kehittäminen kaupunkikonsernin eri tasoilla

Sisäisen valvonnan ja riskienhallinnan toimivuutta seurataan, arvioidaan ja kehitetään kaupunkikonsernin kaikilla tasoilla. Vastuu seurannasta kuuluu johtaville viranhaltijoille, tytäryhteisöjen toimitusjohtajille ja toimielimille. Kaupunkikonsernin tasolla tehtävässä sisäisen valvonnan ja riskienhallinnan arvioinnissa ja kehittämisessä hyödynnetään virastojen, liikelaitosten ja tytäryhteisöjen tekemiä sisäisen valvonnan ja riskienhallinnan kuvauksia, arviointeja ja tietoja raportoiduista kehittämistoimista.

Seuranta ja arviointi ovat tärkeä osa sisäistä valvontaa ja riskienhallintaa. Seurannalla ja arvioinnilla varmistetaan sisäisen valvonnan ja riskienhallinnan toimivuutta sekä tunnistetaan toiminnassa ja sen tuloksissa havaitut poikkeamat. Poikkeamat voivat olla merkki valvonnan puutteesta, jolloin on mahdollista etsiä puutteen juurisyy ja ryhtyä korjaaviin toimenpiteisiin.

Toimintaympäristö, tavoitteet, organisaatiorakenne ja toimintaprosessit muuttuvat ajan kuluessa. Myös valvonnan pitää muuttua muutosten myötä. Seurannan ja arvioinnin avulla voidaan muun muassa:

- varmistaa valvonnan tehokkuutta ja toimivuutta
- havaita toimintaympäristössä, organisaatiossa ja toiminnassa muutoksia, jotka voivat vaikuttaa riskien syntymiseen tai muuttumiseen
- oppia läheltä piti -tilanteista ja epäonnistumisista
- tunnistaa ja arvioida poikkeamia ja uusia riskejä
- kehittää sisäistä valvontaa ja riskienhallintaa.

Johto ja esimiehet seuraavat, arvioivat ja kehittävät sisäistä valvontaa ja riskienhallintaa omilla vastuualueillaan. Heidän tehtävinään on seurata riskejä ja arvioida sisäisen valvonnan ja riskienhallinnan toimivuutta ja tarkoituksenmukaisuutta osana päivittäistä toimintaa. Tietotekniikan tuottama seurantatieto yhdistettynä osaavan henkilöstön suorittamaan tulosten läpikäyntiin mahdollistaa tehokkaan jatkuvan arvioinnin. Päivittäiseen toimintaan ja prosesseihin sisään rakennetun jatkuvan seurannan lisäksi on tehtävä tarpeen mukaan erillisiä, määräajoin toteutettavia arviointeja.

Johdon on harkittava erillisten arviointien tarve ottaen huomioon:

- aikaisempien seurantojen ja arviointien tulokset
- valvontatarpeeseen vaikuttavien muutosten määrä
- muutosten luonne ja laajuus sekä niihin sisältyvät riskit
- valvontaa suorittavien ihmisten pätevyys ja kokemus.

Käytettäessä ulkoista palveluntuottajaa on arvioitava palveluntuottajan valvontajärjestelmää ja sen vaikutuksia palveluja tilaavan organisaation riskeihin ja valvontatarpeisiin. Varmistuakseen ulkoisen palveluntuottajan valvonnan toimivuudesta tilaaja voi tehdä omia erillisiä arviointeja palveluntuottajan sisäisen valvonnan ja riskienhallinnan toimivuudesta. Tämä edellyttää palvelusopimuksessa olevaa mainintaa tarkastusoikeudesta. Riittävä varmuus ulkoisen palvelujentuottajan sisäisen valvonnan toimivuudesta voidaan saada myös tutkimalla riippumattoman tarkastajan raportointia, mikäli saatavilla on tarkoitukseen soveltuvaa raportointia (esim. ISAE 3402 ja ISAE 3000). Myös palveluntuottajan antama raportointi voi joissain tapauksissa tuottaa riittävän tiedon valvonnan toimivuuden varmistamiseksi.

Seurannan ja arvioinnin tuloksena saadut havainnot sisäisen valvonnan ja riskienhallinnan puutteista on raportoitava korjaustoimenpiteistä vastuussa oleville henkilöille. Lisäksi havainnot puutteista on raportoiva organisaatiotasolle, joka on ainakin yhtä tasoa ylempänä kuin korjaustoimenpiteistä vastuussa olevat henkilöt.

6.2. Sisäisen valvonnan ja riskienhallinnan selonteko

Jokainen kaupunkikonsernin tilivelvollinen toimielin antaa osana toimintakertomustaan selonteon sisäisen valvonnan ja riskienhallinnan järjestämisestä, valvonnassa havaituista puutteista ja toimenpiteistä niiden korjaamiseksi.

Sisäisen valvonnan ja riskienhallinnan selonteon laatiminen edellyttää johtamis- ja hallintotavan, sisäisen valvonnan ja riskienhallinnan nykytilan ja kehittämistarpeiden arviointia. Arvioinnin on oltava järjestelmällistä ja organisaation kokoon ja rakenteeseen nähden riittävän kattavaa. Selonteon laadintaprosessissa arvioidaan kaikkia sisäisen valvonnan ja riskienhallinnan osatekijöitä (katso luku 1.2) järjestelmällisesti.

Virastojen, liikelaitosten ja tytäryhtiöiden sisäisen valvonnan ja riskienhallinnan arvioinnissa lähtökohtana käytetään viraston, liikelaitoksen tai tytäryhtiön sisäisen valvonnan kuvausta (katso luku 2.3). Arvioinnissa apuna käytetään muun muassa sisäisen valvonnan muistilistaa ja riskienhallinnan kypsyysmallia (katso Helmi- ja Tyyne-intranet). Selonteon tulee perustua dokumentoituihin arviointiaineistoihin, jotka todentavat arviointien tulokset ja laajuuden.

Sisäisen valvonnan ja riskienhallinnan selonteoista annetaan tarkempia ohjeita vuosittain tilinpäätösohjeissa.

6.3. Sisäisen tarkastuksen arviointitehtävä

Sisäisen tarkastuksen tarkastukset ovat osa sisäisen valvonnan ja riskienhallinnan toimeenpanon arviointia. Sisäinen tarkastus avustaa kaupungin johtoa sisäisen valvonnan toteuttamisessa arvioimalla johtamisen ja hallinnon, sisäisen valvonnan ja riskienhallinnan tuloksellisuutta ja riittävyyttä.

Sisäinen tarkastus tarkastaa kaupungin virastojen, liikelaitosten ja tytäryhteisöjen toimintaa ja taloutta sekä tarvittaessa palveluntuottajille ulkoistettuja toimintoja tai

palveluja. Sisäinen tarkastus arvioi tarkastuksissa, vastaako nykyinen sisäinen valvonta ja riskienhallinta johdon suunnittelemaa toimintatapaa, onko sisäinen valvonta riittävää toiminnon ja siihen sisältyvien riskien hallitsemiseksi sekä antaa suosituksia sisäisen valvonnan ja riskienhallinnan parantamiseksi. Sisäinen tarkastus seuraa annettujen suositusten toteutumista.

Sisäinen tarkastus raportoi valmistuneiden tarkastusten tulokset kaupungin johdolle sekä tarkastuskohteelle toimenpiteitä varten. Sisäisen tarkastuksen vuosikatsauksissa raportoidaan tiivistetysti kunkin vuoden arviointien tulokset. Tarkastusten vuosittaisen seurannan raportissa kuvataan, mikä on tarkastuksissa annettujen sisäistä valvontaa ja riskienhallintaa koskevien toimenpidesuunnitelmien toteuttamisen tilanne.

Sisäinen tarkastus voi antaa sisäisen valvonnan ja riskienhallinnan neuvontaa konsultointina. Konsultointitehtävän sisällöstä ja laajuudesta sovitaan toimeksiantajan kanssa.

Sisäinen tarkastus ei osallistu päätöksentekoon eikä täytäntöönpanoon. Sisäisen tarkastuksen arviointitoiminta ei vähennä johdon ja esimiesten velvollisuutta luoda riittävä ja toimiva sisäinen valvontajärjestelmä vastuullaan olevaan toimintayksikköön ja toimintaprosesseihin.

6.4. Ulkoisen tarkastuksen arviointitehtävä

Ulkoinen valvonta on riippumaton toimivasta johdosta ja muusta organisaatiosta. Ulkoisen valvonnan toimijat ovat tilintarkastaja, tarkastuslautakunta ja tarkastusvirasto.

Tilintarkastaja

Valtuusto valitsee hallinnon ja talouden tarkastamista varten tilintarkastusyhteisön. Tilintarkastajan on julkishallinnon hyvän tilintarkastustavan mukaisesti tarkastettava kunkin tilikauden hallinto, kirjanpito ja tilinpäätös. Tilintarkastajan tulee myös tarkastaa, ovatko valtionosuuksien perusteista annetut tiedot oikeita ja onko kunnan sisäinen valvonta ja riskienhallinta sekä konsernivalvonta järjestetty asianmukaisesti. Tilintarkastaja antaa valtuustolle tilintarkastuskertomuksen ja raportoi tarkastuksen tuloksista lisäksi kaupungin johdolle, tarkastuslautakunnalle ja tarkastuskohteelle.

Tarkastuslautakunta

Tarkastuslautakunta valmistelee valtuuston päätettävät hallinnon ja talouden tarkastusta koskevat asiat sekä arvioi, ovatko valtuuston asettamat toiminnan ja talouden tavoitteet kunnassa ja kuntakonsernissa toteutuneet. Tämän lisäksi lautakunta arvioi, onko kunnan toiminta järjestetty tuloksellisella ja tarkoituksenmukaisella tavalla. Toiminta käsittää kunnan ja kuntakonsernin toiminnan lisäksi osallistumisen kuntien yhteistoimintaan sekä muun omistukseen, sopimukseen ja rahoittamiseen perustuvan toiminnan. Lautakunta valvoo sidonnaisuuksien ilmoittamisvelvollisuuden noudattamista ja saattaa ilmoitukset valtuustolle tiedoksi.

Tarkastuslautakunta antaa valtuustolle kultakin vuodelta arviointikertomuksen ja voi harkintansa mukaan laatia valtuustolle myös erillisiä raportteja kaupungin toiminnan ja taloudenhoidon kannalta merkittävissä asioissa.

Tarkastusvirasto

Tarkastusvirasto arvioi lautakunnan apuna valtuuston asettamien tavoitteiden toteutumista ja toiminnan järjestämisen tarkoituksenmukaisuutta ja tuloksellisuutta. Sen lisäksi tarkastusvirasto tekee lakisääteistä tilintarkastusta tilintarkastajan kanssa sovitulla tavalla ja valmistelee valtuuston päätettäväksi esitettävät, tarkastusta koskevat asiat lautakunnalle.