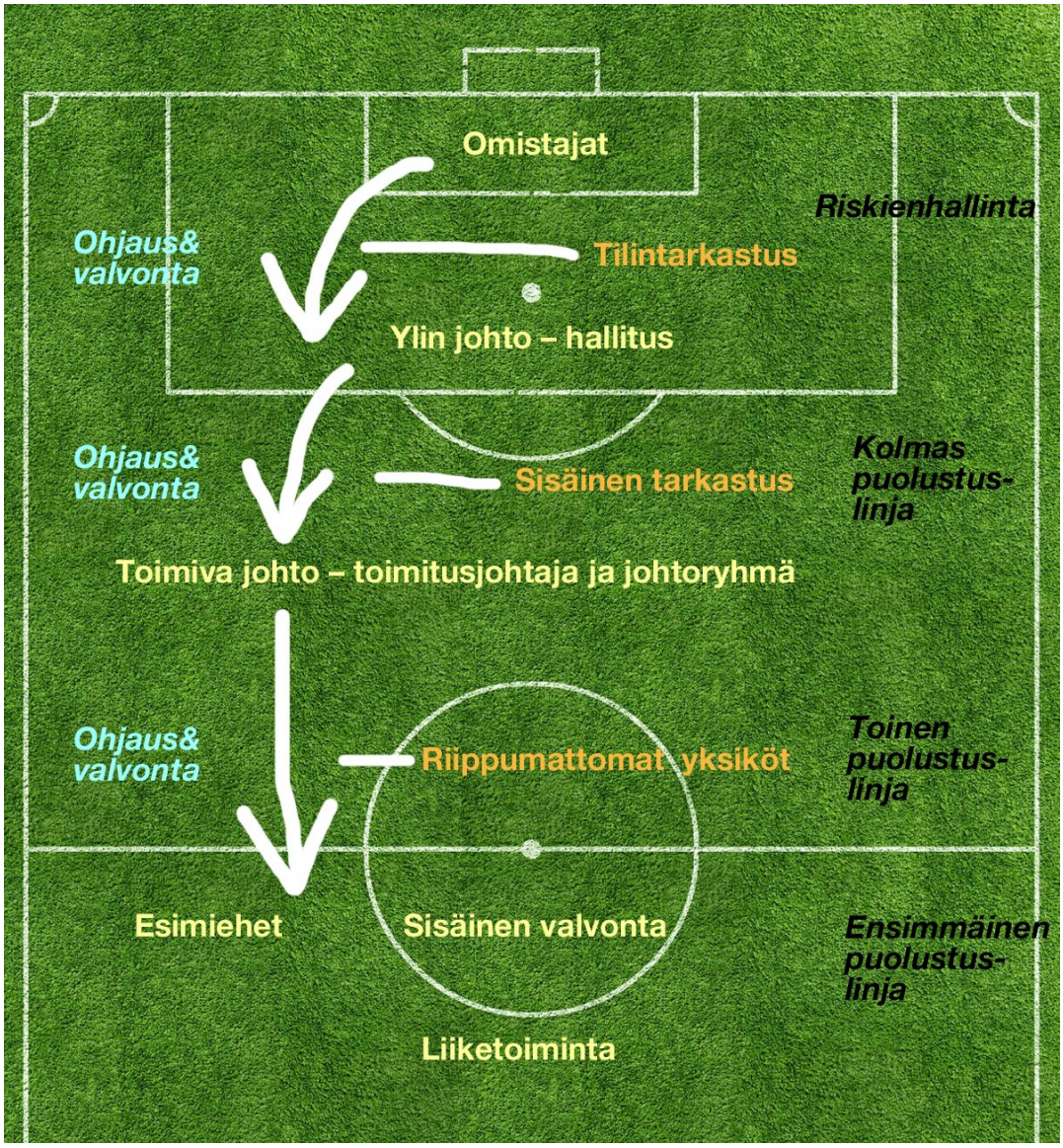
SISÄISET TARKASTAJAT ry

The Institute of Internal Auditors Finland

# Syynissä

Nro 1/2014




*Liiketoiminnan kolme puolustuslinjaa*

## Compliance OP-Pohjola-ryhmässä

Sivu 9

## Riskienhallinta ja sisäinen tarkastus

Sivu 6



Syynissä

Yhteystiedot
Sisäiset tarkastajat ry
Energiakuja 3
00180 Helsinki
Puh. 010 4236 350
www.theiia.fi

Toimituskunta
Jari Korpela, pj
Ulla-Maria Ketola
Minna Korhonen
Tarja Tirri
Matti Mikola

Ilmoitukset
Puh. 010 4236 350
sisaiset.tarkastajat@theiia.fi

Ulkoasu
Antturi Design Oy

**Hannu Kananen**
Sisäiset tarkastajat ry:n
hallituksen puheenjohtaja

IIA Global on viime vuosina pyrkinyt selkiyttämään eri toimijoiden kuten riskienhallinnan ja vaatimustenmukaisuuden varmentajien sekä johtamis- ja raportointimenetelmien rooleja ja kattavuutta. Kehitystyö on osaltaan vastaus taloussuhdanteiden, toimintaympäristöjen ja regulaatiomuutosten aiheuttamiin haasteisiin, jotka heijastuvat organisaatioiden toimintoihin.

Sisäinen valvonta ja riskienhallinta ovat monitahoisia toimintaprosesseja. Sisäisen valvonnan ohjaus- ja toimintaprosesseihin sisältyvillä menettelyillä ja organisaatioratkaisuilla varmennetaan toiminnan taloudellisuutta, tuloksellisuutta ja lainmukaisuutta. Kokonaisvaltaisella riskienhallinnalla tunnistetaan tavoitteiden saavuttamista uhkaavia tekijöitä ja varaudutaan toimintaympäristöjen muutoksiin. Sisäisen tarkastuksen tärkeänä tehtävänä on tukea ja arvioida varmennustoimintojen riittävyyttä ja tuloksellisuutta suhteessa asetettuihin tavoitteisiin ja samalla toimia kehittämistyön katalyyttinä.

COSO -viitekehyksen komponentit ja periaatteet antavat hyvät lähtökohdat efektiiviselle sisäiselle valvonnalle ja korkeatasoiselle tarkastustyölle. Valvontaympäristöihin, riskien arviointeihin, kontrollitoimenpiteisiin, informaatioon ja kommunikointiin sekä kontrollien seurantaan liittyvät varmennustavoitteet selkeyttävät sisäisen valvonnan suunnittelua ja implementointia sekä auttavat ymmärtämään sisäisen valvonnan uudenlaisia vaatimuksia.

Maaliskuun lopussa järjestettävässä Key Elements of COSO – Control Environment -kevätseminaarissa syvennytään COSO:n rakenteisiin ja opitaan soveltamaan mallia. Kansainvälisesti arvostettu luennoitsija Deanna Sullivan (US) saapuu Kalastajatorpalle pitämään innostavan ja inspiroivan workshop -päivän, jonka aikana tarkastusammattilaisille tarjoutuu ainutkertainen mahdollisuus oppia ja saada käytännönläheisiä esimerkkejä omaan työhönsä.

Muutosten keskellä varmennus- ja valvontatoimenpiteiden, Compliance-toimintojen ja riskienhallinnan tehtävät korostuvat ja monipuolistuvat. Syynissä-lehden kirjoitukset avaavat mielenkiintoisia ja tuoreita näkökulmia sisäisen tarkastuksen työkenttään. Suomen Riskienhallintayhdistyksen toiminnanjohtaja Lassi Väisänen kirjoittaa sisäisen tarkastuksen ja riskienhallinnan välisestä vuorovaikutuksesta. Anneli Grönfors-Kallio analysoi Governance, Risk and Compliance (GRC)-varmennusmallin muutoshallintaprosessien hyötyjä. Compliance -toimintojen merkityksiä käsitellään myös Leena Kallasvuon ja Eeva Lipastin kirjoituksessa. Kuntalain osittaisuudistuksen vaikutuksia kunnan johtamiseen ja hallintoon pohditaan Markus Kiviahon ajankohtaisessa kirjoituksessa.

Ennakoimalla muutoksiin liittyviä riskejä ja mahdollisuuksia tuotamme lisäarvoa tavoitteisiin, tuloksiin ja toimintaan.

Leppoisia lukuhetkiä ja kevään odotusta. ■

# Kumpi tuli ensin, muna vai kana?

Aina mielenkiintoinen keskustelun herättäjä ja sitä seuraavat joskus humoristisetkin kehäpäätelmät eivät ole antaneet vastausta kuuluisaan syy-seurauskysymykseen. Niin maallikot kuin tiedekin ovat pyrkineet antamaan selityksiä ja ratkaisuja tähän eräänlaiseen jatkumo-ongelmaan.

Kysymys lienee tässäkin tapauksessa omalta osaltaan roolituksessa. Kumpi aloittaa ja kumpi lopettaa? Kumpi on jatkumossa johtavassa roolissa? Kumpi määrittelee kumpaa? Sovellettuna sisäisten tarkastajien kiehtovaan maailmaan: onko riskienhallinta sisäistä valvontaa vai sisäinen valvonta riskienhallintaa?

Kuten niin useasti ammattikirjallisuudessa kuin tämänkin Syynissä-lehden artikkeleissa, vilahtavat nuo tutut termit meille sisäisille tarkastajille tämän tästä. Olemme tottuneet sisällyttämään käsitteet osaksi lukemaamme tekstiä ja kirjallisuutta niistä lähtökohdista, joista olemme käsitteet alun perin poimineet osaksi kokonaisvaltaisen riskienhallinnan (tai valvonnan) ymmärrystämme. Kohtalaisen jouhevasti ja ymmärrettävästi keskustelemmekin keskenämme, mutta entä sitten kun keskustelijoiden joukko kasvaa riskienhallinnan ja compliancen asiantuntijoilla? Me kyllä ymmärrämme, että sisäisen tarkastuksen tehtävänä on arvioida sisäisen valvonnan riittävyyttä ja riskienhallinnan tarkoituksenmukaisuutta, mutta onko meillä kaikilla keskustelijoilla sama käsitys ja ymmärrys valvonnasta? Riskienhallinta nimetään tämänkin numeron artikkeleissa ”toiminnoksi” ja toisaalta COSO:n määritelmissä riskienhallinta on nimetty koko organisaation kattavaksi prosessiksi, jota toteutetaan organisaation kaikilla tasoilla. Mukaan samaan keitokseen lisätään vielä compliance-riskit. Siis onko tämä kaikki toisin sanoen valvontaa, jota toteutetaan organisaation jokaisella tasolla?

Edelleenkin päivittäin voimme törmätä sisäisen valvonnan ja riskienhallinnan rinnastamiseen, mikä ei välttämättä ole lainkaan toisiaan pois sulkevaa. Vaikka pois sulkevaa se ei olekaan, uskallan väittää, että valvonnan varmistajien joukon kasvaessa näiden rooleja tulisi edelleenkin selkeyttää ja käsitteistöä täsmentää. Tässä Syynissä-lehden numerossa näiden roolien keskinäinen suhde tai jatkokysymykset suhteiden ”järjestyksestä” nousee eittämättä esille.

Omassa valvontamaailmassani sisäinen valvonta on yläkäsite, joka pitää sisällään loogisesti niin kolmen puolustuslinjan mallin kuin COSO-viitekehyksen. Kutsuisinko niitä vaikka valvonnan varmistustoiminnoiksi. Itse valvontaa toteutetaan pääsääntöisesti ensimmäisessä puolustuslinjassa eli operatiivisessa toiminnassa riskienhallinnan ja compliance-toiminnon avustuksella, joiden avustuksen asianmukaisuutta sisäinen tarkastus arvioi. Vai oliko se sittenkin niin, että oikein järjestetty riskienhallinta varmistaa valvonnan toimivuuden. Keskustelu jatkukoon.

Muna vai kana? Hyvää pääsiäisen odotusta!

**Jari Korpela**, CIA
Viestintätoimikunnan puheenjohtaja

**Markus Kiviaho, JHTT, CGAP, CRMA**
**FCG Konsultointi Oy**
**Johtava konsultti, tiimipäällikkö**

# Kunnan toiminnan johtaminen ja hallinta jatkuvasti muuttuvassa toimintaympäristössä

**Kunnan toiminnan tuloksellinen johtaminen ja hallinta ovat yhä merkittävämpien haasteiden edessä. Kunnat joutuvat hallitsemaan riskejä, jotka liittyvät jatkuvasti niukkeneviin taloudellisiin resursseihin, moninaisiin lakisääteisiin tehtäviin, niiden erilaisiin palvelutuotantotapoihin sekä palvelutarpeiden syventymiseen. Samanaikaisesti kunnat muodostavat laajoja konserneja, joiden omistajaohjauksen ja konsernijohtamisen sekä tytäryhtiöiden hallitustyöskentelyn tulisi perustua riittävään asiantuntemukseen ja kokemukseen. Sopimusperustaisten tai muutoin tosiasiallisesti kunnan vastuulla olevien toimintojen riskienhallinnan ja valvonnan merkitys on myös jatkuvasti korostunut. Kuntalakiin sisällytettävän sisäisen tarkastuksen sääntelyllä tulisi edistää kuntien johtamisen ja hallinnan kehittymistä.**

Hallituksen valvonnan ja riskienhallinnan vastuut ovat jo täsmentyneet.

Kuntalain osittaisuudistuksessa täydennettiin kuntalain sisäisen valvonnan ja riskienhallinnan sääntelyä. Vuoden 2014 alusta voimaan tulleiden säännösten mukaisesti kunnanvaltuuston tulee päättää kunnan ja kuntakonsernin sisäisen valvonnan ja riskienhallinnan perusteista. Lisäksi kunnan hallintosäännössä on tullut esittää sisäisen valvonnan ja riskienhallinnan tehtävä- ja vastuujaot. Perusteiden ja hallintosäännön määräysten tehtävänä on ohjata kunnanhallitusta, kunnanjohtajaa tai pormestaria sekä muita valvontavastuullisia toimijoita järjestämään kunnan ja kuntakonsernin sisäinen valvonta ja riskienhallinta asianmukaisella tavalla. Myös kunnanhallituksen raportointivelvollisuus sisäisen valvonnan ja riskienhallinnan järjestämisestä ja keskeisistä johtopäätöksistä on kirjattu kuntalakiin.

## Hallitukset eivät seuraa riittävästi sisäisen valvonnan ja riskienhallinnan tuloksellisuutta

Kuntaliiton vuoden 2012 lopulla tekemä riskienhallintakysely osoittaa, että riskienhallinnan järjestäminen perustuu vastaajista 80 %:n (vastaajia 107) mukaan erittäin huonosti (57 %) tai melko huonosti (23 %) järjestelmälliseen lähestymistapaan. Kyselyn mukaan kunnanhallituksella ei useinkaan ole riittävää tietoa kunnan eri toimintoihin ja konserniyhteisöihin, sopimusperusteisiin palvelutuottajiin tai ulkoistettuihin palveluihin liittyvistä riskeistä, toimintatapojen puutteista ja heikkouksista. Vastaajista vain 18 % oli sitä mieltä, että hallitus seuraa riskienhallinnan tuloksellisuutta melko tai erittäin hyvin.

## Kunnanhallituksen ja johdon tueksi tulisi järjestää ammattitaitoinen sisäinen tarkastus

Kuntalain osittaisuudistuksen perustana olevassa hallituksen esityksessä todettiin, että sisäinen tarkastus on osa kuntien hyvää johtamista ja hallintaa. Tästä huolimatta kunnanhallitukset eivät vielä ole useinkaan järjestäneet sisäistä tarkastusta tukemaan hallituksen valvontatehtävän asianmukaista suorittamista. Sisäisen tarkastuksen järjestämistä puoltavat kuitenkin kuntien toimintaympäristön jatkuvat ja merkittävät muutokset, monimutkaistuvat konserni- ja toimintarakenteet, riskien hallinnan heikkoudet ja toisaalta tiukentuneet valvonnan ja riskienhallinnan säännökset.

Kuntalain kokonaisuudistuksen yhteydessä tulisi vahvistaa kuntien vastuullista johtamista ja hallintaa velvoittamalla kunnanhallitukset järjestämään ammattimainen sisäinen tarkastus, mikäli kunnan ja kuntakonsernin sisäinen valvonta ja riskienhallinta eivät ole asianmukaisesti järjestettyjä ja toimi tuloksellisesti. Järjestämisvelvollisuus tulisi arvioida vuosittain toimintakertomukseen laadittavan kunnan ja kuntakonsernin sisäisen valvonnan ja riskienhallinnan selonteon yhteydessä.

Sääntely osoittaisi sitoutumista hyvään johtamiseen ja hallintaan, millä varmennetaan verovarojen käytön asianmukaisuutta, niihin liittyvien riskien ennaltaehkäisyä ja hallintaa sekä siten toiminnan tuloksellisuutta. Sisäinen tarkastus toimisi tällöin kunnanhallituksen, pormestarin ja kunnanjohtajan sekä konsernijohdon tukena tavoitteiden saavuttamisessa tarjoamalla järjestelmällisen lähestymistavan johtamisen sekä riskienhallinta- ja valvontaprosessien tuloksellisuuden arviointiin ja kehittämiseen. ■

**Lassi Väisänen,**
**toiminnanjohtaja Suomen Riskienhallintayhdistys ry, www.srhy.fi**
**toimitusjohtaja GRC Partners Oy, Vergo Oy**

# Riskienhallinta ja sisäinen tarkastus

**Riskienhallintaa tarkastellaan nykyisin monessa organisaatiossa eri näkökulmista. Aina ei ole varmaa, onko kaikilla osapuolilla sama näkemys siitä, mitä riskienhallinnalla tarkoitetaan, mitä osa-alueita riskienhallinta kattaa ja kenen vastuulla riskienhallinta on. Keskeisenä tavoitteena tulee olla yhtenäisen näkemyksen aikaansaaminen ja selkeä käsitys siitä, mitä riskienhallintaan sisällytetään ja miten asioita hoidetaan osana normaalia liiketoiminnan suunnittelua, seurantaa ja valvontaa.**

## Suomen Riskienhallintayhdistys ry

Suomen Riskienhallintayhdistys ry, SRHY, perustettiin jo yli 25 vuotta sitten Keskuskauppakamarin alaisen työryhmän pohjalta. Tuolloin jäsenistö koostui vakuutusten ostajista ja vakuutusten myyjistä. Ostajat edustivat teollisuutta ja myyjät vakuutusyhtiöitä. Tuolloisen käsityksen mukaan riskienhallinta oli voimakkaasti teollisuuden kannalta keskeisten tuotantolaitosten toiminnan turvaamista erilaisin vakuutus- yms. ratkaisuin. Tänään tarkastelunäkökulmat ovat huomattavasti laajemmat ja riskienhallinta liittyy laajemmin myös yrityksen tekemiin valintoihin ja päätöksiin, kuten millaisia riskejä halutaan ottaa ja kuinka paljon epävarmuutta voidaan sietää.

SRHY on ollut voimakkaasti tukemassa mm. ISO 31000 -kehitystyötä Suomessa yhdessä Suomen standardisoimisliiton, SFS:n, kanssa. Tavoitteena on tukea ISO 31000 -standardin jalkauttamista suomalaisiin organisaatioihin niin yksityisellä kuin julkisellakin sektorilla.

Keskeisiä toimintatapoja ovat

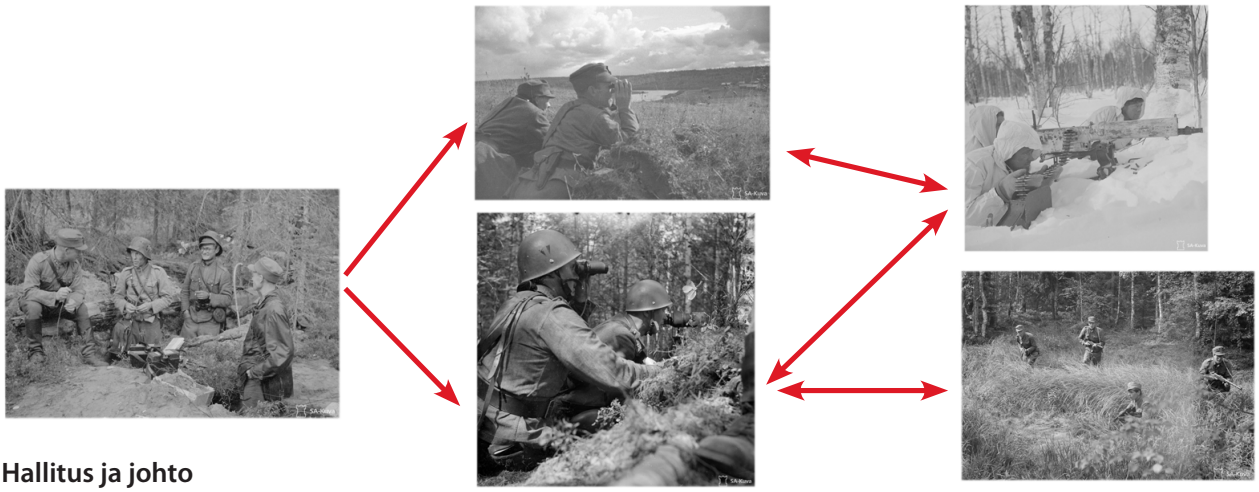
- miniseminaari, jossa välitetään tietoa ja näkemyksiä jäsenistölle ajankohtaisista asioista
- vuosittaiset painopistealueet esim. ISO 31000 -kehitystyö (www.sfs.fi/julkaisus ja palvelut/tuotteet valokeilassa/iso 31000 riskienhallinta)
- pienten ja keskisuurten yritysten riskienhallinnan toteuttamista avustavan PK-RH Forum -aineiston haltuunotto ja jatkokehittäminen (www.pk-rh.fi)
- yhteistyö eri kohderyhmien kanssa


**Kuva 1.**

## Riskienhallinnan näkökulmia

Viimeisen 25 vuoden aikana riskienhallintaa on tarkasteltu vieläkin käytössä olevan nelikentän avulla: strategiset riskit, finanssiriskit, toiminnalliset riskit ja vahinkoriskit (Kuva 1).

## Hallituksen, johdon ja liiketoimintojen roolit



Kuvat: SA-kuva

**Hallitus ja johto**
- **Strategiavalinnat**
- **Vaihtoehtoiset etenemissuunnat**
- **Päätösten teko**

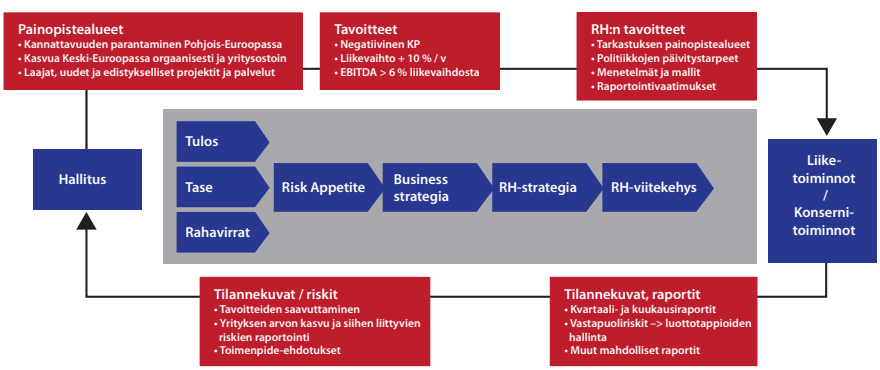
- **Arviointi**
- **Osa-aluekohtainen tilanteen hahmottaminen**

**Liiketoiminnot kentällä**
- **Suunnitelmien jalkauttaminen**
- **Tavoitteiden saavuttaminen**

**Kuva 2.**

Vergo

## Riskienhallinta




**Kuva 3.**

Vergo

### Missä on tapahtunut kehitystä?

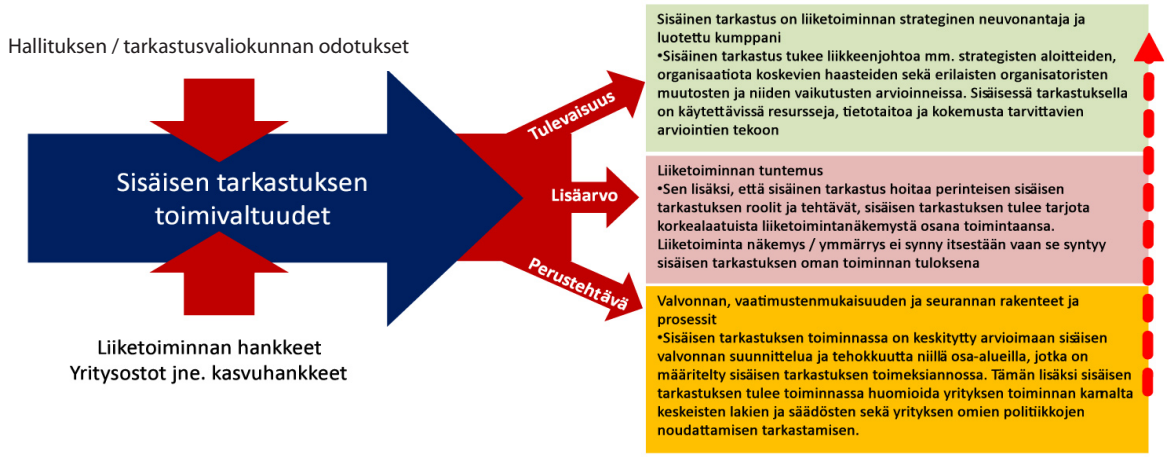
Nykyään riskienhallinnan rinnalle on nostettu myös epävarmuuden hallinta. Epävarmuus otettiin selkeästi esille ISO 31000 -standardissa, minkä johdosta riski käsitteenä on alkanut muuttua perinteisestä negatiivisesta tapahtumasta myös mahdollisuuksien hallintaan. Vuosien varrella on laajennettu tarkastelunäkökulmia ja samaan aikaan riskienhallintaan on alettu kiinnittää huomioita. Tämä on kuitenkin aiheuttanut monessa organisaatiossa ongelman, koska erilaisia riskejä raportoidaan eri aikaan muodostamatta kokonaiskuvaa tai näkemystä asioiden keskinäisistä riippuvuuksista tai vaikutuksista.

### Roolit ja vastuut

Hallitus ja johto ottavat vastuun strategisten vaihtoehtojen arvioinnista, päätöksenteosta sekä riskeistä ja mahdollisuuksista. Liiketoiminnan johto ja liiketoiminta ottavat vastuuta päätösten jalkauttamisesta ja siihen liittyvistä epävarmuuksista ja riskeistä. Onnistumiset ja epäonnistumiset näkyvät välittömästi liiketoiminnan tuloksissa (Kuva 2).

Riskienhallinta on pitkään ollut toiminto toimintojen joukossa. Monessa organisaatiossa se vastaa tietyillä osa-alueilla operatiivisista asioista, kuten vakuuttamisesta ja osaltaan koordinoi riskien prosessointia (tunnistamista, analysointia, raportointia jne.) organisaation eri tasoilla (Kuva 3).

## Sisäisen tarkastuksen roolit ja odotukset




**Kuva 4.**

Vergo

Nykyisin riskienhallintaa kehitettäessä on syytä miettiä riskienhallinnan roolia uusista näkökulmista: 1) onko riskienhallintatoiminto se, joka vastaa riskienhallinnasta kokonaan tai osittain vai 2) vastaako se prosessista, jonka avulla riskejä tunnistetaan, hallitaan, poistetaan tai otetaan tietoisia riskejä tavoitteiden saavuttamiseksi.

### Yhteistyö riskienhallintatoiminnon ja sisäisen tarkastuksen välillä

Sisäinen tarkastus arvioi riskienhallintatoiminnon tarkoituksenmukaisuutta (Kuva 4). Riskienhallinta ja sisäinen tarkastus muodostavat työparin. Työparin on ymmärrettävä ja pystyttävä tarvittaessa osoittamaan riskienarvioinnin ja tarkastuksen tulosten perusteella esim. organisaation kannalta merkittävien riskien, epävarmuuksien tai uhkien olemassaolo, esimerkiksi edellä esitetyn (Kuva 1) nelikentän avulla. ■

Leena Kallasvuo
Tarkastusjohtaja
OP-Pohjola Osk

Eeva Lipasti
Johtaja
OP-Pohjola Osk

# Compliance OP-Pohjola-ryhmässä

**Compliance-toiminnan tarkoituksena on auttaa yrityksen johtoa varmistumaan sääntelyn, eettisten periaatteiden ja asiakassuhteissa asianmukaisten toimintatapojen noudattamisesta. Sisältönsä compliance-toiminta saa lakien, asetusten ja viranomaismääräysten lisäksi yrityksen arvoista, vahvistetusta toimintaperiaatteista ja ohjeista.**

Compliance viestii ja raportoi johdolle sääntelymuutoksista ja niiden edellyttämien toimenpiteiden implementoinnin tilanteesta, toteutetusta valvonnasta sekä valvontahavainnoista. Lisäksi se tukee liiketoimintaa sisäisen valvonnan kehittämisessä sekä compliance-riskien hallinnassa. OP-Pohjola-ryhmässä compliance-toimintaa on vahvistettu ja compliance-verkosto on luotu vuoden 2010 jälkimmäisellä puoliskolla. Compliance on OP-Pohjolan organisaatiossa järjestetty osaksi riippumattoman riskienvalvonnan ja operatiivisten riskien vastuualuetta. Keskitetty compliance- organisaatio tukee ja ohjeistaa osuuspankkien compliance-vastaavia.

### Compliance, sisäisen tarkastuksen kilpailija vai yhteistyökumppani?

Nimenomaiset compliance-toiminnan järjestämistä koskevat vaatimukset ovat finanssitoimialallakin vielä suhteellisen uusia, vaikka luottolaitosten, sijoituspalveluyritysten ja rahastoyhtiöiden toimiluvan edellytyksenä on jo pitkään ollut luotettavan hallinnon järjestäminen. Compliance on viimeisen kymmenen vuoden aikana ”raivannut” tilansa sisäisen tarkastuksen ja lakiasioiden väliin. Sääntelystä tulevat vaateet lisääntyvät ja edellyttävät yhä enemmän varmentavaa toimintaa. Toisaalta tehokkuusvaatimukset ja odotukset toiminnan vaikuttavuudesta kasvavat koko ajan.

Onko sisäinen tarkastus siis saanut perinteiselle toimialueelleen kilpailijan? Sisäinen tarkastus ja compliance tekevät OP-Pohjolassa tiivistä yhteistyötä.

Sisäisen tarkastuksen ja compliancen tehtävistä ja rooleista löytyy yhtäläisyyksiä, mutta myös eroja. Molempien toimintojen objektiivisuutta pyritään varmistamaan edellyttämällä toiminnoilta riippumattomuutta liiketoiminnoista. Molemmilta odotetaan riskiperusteista toiminnan kohdentamista ja aivan uudenlaista tehokkuutta. Yhteistyötä tehdään esimerkiksi sisäisten väärinkäytösten selvittämisessä.

Sisäisen tarkastuksen ja compliancen suhdetta toisiinsa sekä liiketoimintaan kuvaa hyvin riskienhallinnan kolmen puolustuslinjan ajattelu, jossa liiketoiminta edustaa ensimmäistä puolustuslinjaa. Vastuu sääntelyn noudattamisesta on liiketoiminnalla, ennen muuta johdolla ja kaikilla esimiehillä. Osana liiketoiminnasta riippumattomia toimintoja compliance edustaa toista puolustuslinjaa: se luo edellytyksiä sääntelyn noudattamiseen pitämällä yllä compliance-toiminnan periaatteita ja ohjeistusta sekä valvomalla ohjeistuksen noudattamista. Sisäinen tarkastus edustaa kolmatta puolustuslinjaa, joka arvioi riippumattomasti kahden muun puolustuslinjan toimintaa. Sisäinen tarkastus siis arvioi compliancen toimintaa sekä erillisenä että sen kautta, miten liiketoiminnoissa compliance-riskit on otettu huomioon ja miten ohjeistusta noudatetaan.

### Compliance myös sisäisen tarkastuksen arvioinnin kohteena

Sisäisellä tarkastuksella on vakiintunut roolinsa ja tehtävänsä arvioida yrityksen sisäistä valvontaa. Sen tehtävänä on tarkastustoiminnallaan tukea organisaation tavoitteiden saavuttamista ja kehittämistä. Sisäisen tarkastuksen työ kohdistuu koko organisaation toiminnan sisäiseen valvontaan, riskienhallin-

Kuva: Sakari Kiuru

taan sekä johtamis- ja hallintoprosesseihin.

Huolimatta sisäisen tarkastuksen ja compliancen erilaisista rooleista sisäisen valvonnan viitekehyksessä, on hyvän vuorovaikutuksen rakentaminen toimintojen työn onnistumisen kannalta tärkeää. Kun sisäinen tarkastus on tietoinen toteutetun compliance-valvonnan kohteista ja valvonnassa käytetyistä menettelytavoista, se voi tarkastustoiminnassaan keskittyä prosessien toimivuuden tarkastamiseen yksittäisten tehtävien toteuttamisen valvonnan sijasta. Sisäinen tarkastus voi puolestaan tukea compliance-toimintaa mm. kiinnittämällä tarkastuksissaan huomiota compliance-riskin havaitsemiseksi tarpeellisten sisäisten kontrollien käyttöönoton tarpeeseen organisaatiossa. Sisäinen tarkastus voi myös arvioida compliance-riskin osa-alueita ja antaa palautetta compliance-toiminnan vahvuuksista ja heikkouksista ja tukea näin compliance-toiminnan kehittämistä.

Tiedonvaihto on tärkeää, samoin kuin vuosisuunnitelmien koordinointi. OP-Pohjolassa tiedon kulkua varmistetaan sisäisen tarkastuksen ja compliancen säännöllisillä tapaamisilla, joissa käsitellään sekä sisäisen tarkastuksen että compliancen viimeaikaiset havainnot. Compliance antaa säännönmukaisesti sisäiselle tarkastukselle tiedot tekemistään merkittävistä compliance-havainnoista ja niiden pohjalta annetusta suosituksista. Vastaavasti compliance saa käyttöönsä sisäisen tarkastuksen tarkastuskertomukset. Compliancen ja sisäisen tarkastuksen suositusten toteuttamista seurataan yhdenmukaisin menettelytavoin.

### Sisäinen tarkastus ja Compliance – molemmat tärkeitä tarkastusvaliokunnan apuna

Vaatimustenmukaisuus on noussut yhä enemmän myös yritysten johdon ja hallitusten pöydälle. Finanssitoimialalla toimijoiden viime aikoina saamat merkittävät sanktiot ovat johtaneet menettelytapariskin hallinnan merkityksen korostumiseen. Vaatimustenmukaisuus on enemmän kuin lakien noudattamista. Laki riittää viranomaiselle, mutta sekä asiakkaat että yrityksen erilaiset sidosryhmät vaativat enemmän.

Yrityksissä ylimmän johdon apuna valvontaa toteuttavan tarkastusvaliokunnan yhtenä tehtävänä on arvioida toiminnan vaatimuksenmukaisuutta hyvin laajasti ymmärrettynä. Tehtävänsä suorittamiseksi sen tulisi kuulla sekä sisäistä tarkastusta että compliancea, jotka molemmat omasta näkökulmastaan antavat tarkastusvaliokunnalle varmennusta toiminnan vaatimustenmukaisuudesta ja sisäisen valvonnan toimivuudesta. ■

Sisäisten tarkastajien syysseminaari lokakuussa 2013

# Ohjaus ja valvonta teoriasta käytäntöön – COSO 2013

Sisäisten tarkastajien 40. syysseminaarissa Turussa tartuttiin mitä ajankohtaisimpaan aiheeseen, COSO-viitekehyksen päivitykseen. COSO:n päivityksen esitteli **Catherine Jourdan** (PwC), joka on myös ollut kirjoittamassa viitekehystä. Saimme kuulla, että sisäisen valvonnan määritelmää ei ollut muutettu. Viitekehyksen soveltamisessa ja sisäisen valvonnan arvioinnissa hyvällä arvostelukyvyllä ja harkinnalla (use of judgment) on edelleen keskeinen sija. COSO-viitekehyksen osatekijät (components) ovat merkittäviä sisäisen valvonnan tehokkuuden kannalta. Mikä on muuttunut? Viitekehys ottaa nyt paremmin huomioon teknologian merkityksen sisäisessä valvonnassa. Raportointitavoitteet kattavat muutakin kuin taloudellisen raportoinnin (muu ulkoinen ja sisäinen raportointi, sidosryhmäviestintä). COSO:a tuodaan lähemmäksi nykypäivää myös nostamalla viitekehyksessä ulkoistetut palvelut organisaation sisäisen valvonnan piiriin. Uusi COSO painottaa paitsi johdon vaikutusvaltaa (tone at the top) myös keskijohdon merkitystä (tone in the middle) sisäisen valvonnan toteutumisessa. Tässä mainiten vain muutamia muutoksia.

COSO:n 17 periaatetta käytiin läpi tarkemmin IIA:n kansainvälisesti tunnetun luennoitsijan **Deanna Sullivanin** kanssa. Deanna oli luennoitsijana mukaansatempaava, herättelevä, hauskakin ja ennen kaikkea rautainen ammattilainen. Auditorio ei keskustelun kannalta ollut parhain mahdollinen, mutta sitä yritettiin ja onnistuttiinkin. COSO:n periaatteet eivät jääneet teorian tasolle.

Seminaarissa oli kattava osuus kotimaisten esiintyjien luentoja. Koko seminaarin avasi hallitusammattilainen **Tuija Soanjärvi**, joka oli perehtynyt seminaarin aiheeseen ja pohti mielenkiintoisesti hallituksen vastuuta sisäisen valvonnan järjestämisessä ja vastuun kantoa käytännössä. Strategiaa perattiin toimeenpanon ja analytiikan näkökulmista, luennoitsijoina **Ari Aura** (Via Consulting YVG Oy), **Heikki Aho** (Itella Oyj) ja **Antti Syväniemi** (Houston Analytics Oy). Perinteisen talouskatsauksen esitteli meille **Tuulia Asplund** (Handelsbanken).

Seminaarin illalliselta saatiin keskustelunaihetta myös seuraavalle päivälle. Nimittäin siellä ensi-iltansa sai meidän seminaariosallistujien avustavan ideoinnin tuloksena syntynyt ikioma biisi ”Mä haluun laatuu tai hommat kaatuu, täällä kaiken pitää toimia. Mä haluun laatuu tai hommat kaatuu. Mä olen... sisäinen tarkastaja!”. ■

**Maliina Hakala**, CIA
Seminaaritoimikunnan jäsen

## Sisäisten tarkastajien 29. kevätseminaari 31.3.–1.4.2014 Hilton Kalastajatorppa, Helsinki

# Key Elements of COSO – Control Environment

Sisäisten tarkastajien perinteisessä kevätseminaarissa jatketaan viime syksyn seminaarin ajankohtaisesta aiheesta COSO 2013.

Seminaarin ensimmäisen päivän pääteemana on COSO:n viidestä osa-alueesta erityisesti sisäinen valvontaympäristö. Tarjolla on näkemyksiä valvonnasta hallituksen, talousjohdon, etiikan, palkitsemiskäytäntöjen, yritysvastuun ja vielä tunteidenkin näkökulmasta. Luennoitsijoina ovat mm. Mitopron Senior Adviser **Mikael Niskala**, Finnveran hallituksen puheenjohtaja **Markku Pohjola** ja Varman talousjohtaja **Pekka Pajamo.** Kuulemme yritysvastuutietojen laadun varmistuksesta, hallituksen tehtävistä, valvonnasta ja tarkastuksesta osakeyhtiöissä sekä näkökulmia johdon raportointiin. Lisäksi ensimmäisen päivän seminaariantiin sisältyy luento palkitsemisesta ja palkitsemisjärjestelmistä sekä tiukka asialuento sisäisen tarkastuksen roolista eettisten arvojen edistämisessä. Ensimmäisen päivän viimeisenä luentona on Tunneakatemian **Jarkko Rantasen** esitys tarkastajien sielunelämästä ja tunneperäisten reaktioiden hyödyntämisestä tarkastustyössä.

Seminaaripäivä päättyy Kalastajatorpan herkulliseen illalliseen, musiikkiin ja mukavaan yhdessäoloon.

Seminaarin toisen päivän COSO-työpajakoulutuksen vetää yleisön pyynnöstä syysseminaarista tuttu **Deanna Sullivan**. Tällä kertaa emme ole auditoriossa, vaan pöydät on järjestetty työpajatyyliin ja saamme varmasti nauttia vilkkaasta keskustelusta, johon voi halutessaan osallistua tai pysytellä vain kuuntelijan roolissa. Työpajan aluksi saadaan katsaus COSO 2013:sta, minkä jälkeen seuraavat käytännönläheiset osuudet kaikista COSO:n osa-alueista: sisäisestä valvontaympäristöstä, riskien arvioinnista, kontrollitoimenpiteistä, informaatiosta ja kommunikaatiosta, monitoroinnista ja COSO:n toimeenpanosta. Työpajan aikana tehdään itsearviointia oman organisaation sisäisestä valvonnasta ja etsitään siihen kehittämiskohteita. Lisäksi keskustellaan uudistuneen COSO:n hyödyntämisestä ja sen sisäiseen tarkastukseen mukanaan tuomista mahdollisuuksista. ■

**Heli Iirola**, CIA
seminaaritoimikunnan jäsen

**Anneli Grönfors-Kallio**
**CIA**
**Director, Head of Internal Audit, Risk and Compliance**
**KPMG Advisory**

# Governance, Risk and Compliance, GRC – kokonaisvaltainen varmennus liiketoiminnan hyödyksi

**GRC lähestymistavan läpivienti organisaatioon on muutoshallintaprosessi, jossa järjestelmät eivät yksin luo tehokkuutta. Muutosta edesauttavia tekijöitä ovat keskusteleva ja yhteistyöhön perustuva kulttuuri ja toimintatavat. Lähtökohtana on kuitenkin toiminnan kannalta tehokkuus, yhteinen näkemys ja parempaan tietoon perustuva päätöksenteko.**

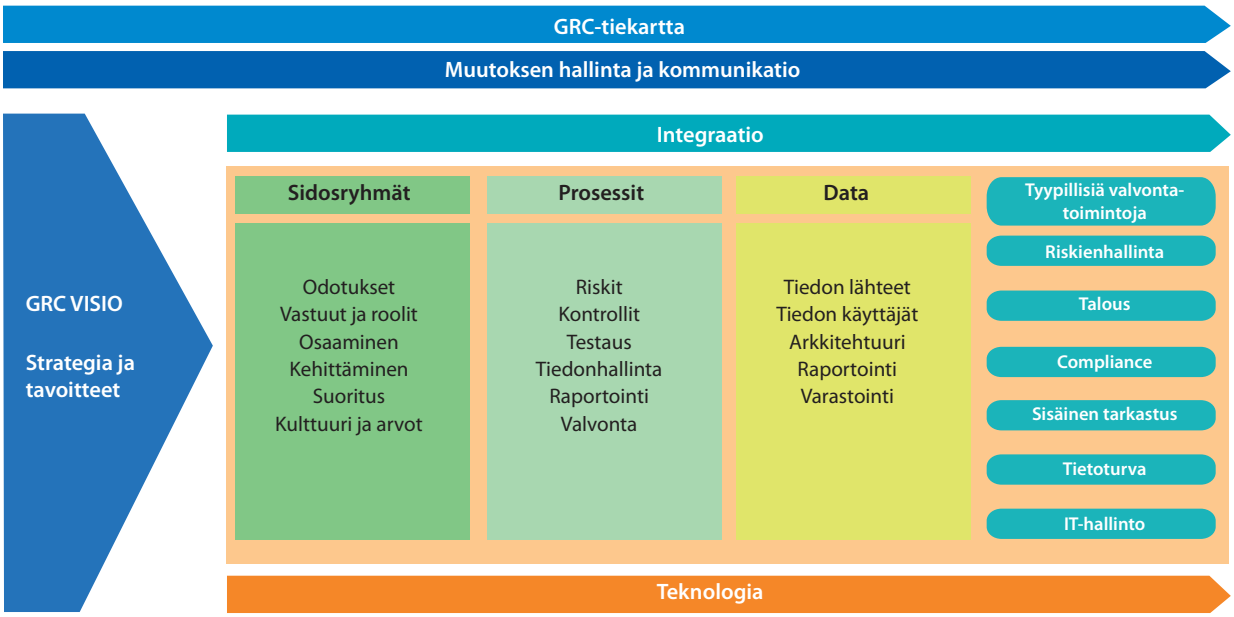
GRC-varmennusmallista hyötyvät organisaation eri toimijat. Tavoitteena on, että ylin johto saa yhtenäistä ja tehokasta raportointia riskeistä ja kontrolleista sekä niihin liittyvistä varmennustoiminnoista. Yhdistämällä prosesseja, järjestelmiä ja vuovuorovaikutusta eri varmennustoimintojen välillä, voidaan selkeästi vähentää kustannuksia läpi organisaation.

Corporate Governance säännökset listayhtiöille ovat edellyttäneet viime vuosikymmenenä sisäisen valvonnan kehittämistä listayhtiöissä sekä toiminnaltaan merkittävissä yhtiöissä. Myös julkishallinnon organisaatioilta edellytetään sisäisen valvonnan ja riskienhallinnan järjestämistä.

Sisäisen valvonnan ja riskienhallinnan haasteet ovat pakottaneet johdon ja asiantuntijat niin kotimaisissa kuin kansainvälissäkin organisaatioissa toteuttamaan merkittäviä hankkeita liittyen riskien tunnistamiseen ja arviointiin, prosessien kuvaamiseen, dokumentointiin ja testaukseen. Eri vaatimusten ja odotusten kautta organisaatioihin on syntynyt varmennustoimintoja kuten riskienhallinta, compliance toiminto, SOX-kehittäminen ja -testaus. Tämän lisäksi tukitoiminnot kuten taloushallinto, IT-hallinto ja henkilöstöhallinto tukevat ja varmentavat vaatimusten ja ohjeiden mukaisen toiminnan. Sisäinen tarkastus puolestaan toimii näistä riippumattomana kokonaisvaltaisena arvioijana, jonka varmennus ja kehitystoiminnan tulisi painottua sekä strategisiin, operatiivisiin että compliance-riskeihin.

Governance, Risk and Compliance GRC-varmennusmalli luo kokonaisvaltaisen viitekehyksen varmennuksen organisointiin ja riskienhallintaan sekä linkittää tekemisen vahvemmin tavoitteisiin ja strategiaan. GRC-varmennusmallin avulla pyritään eliminoimaan siilot ja päällekkäisyydet niin järjestelmien, prosessien kuin toimintojenkin välillä. Tavoitteena on tuottaa ylimmälle johdolle ja hallitukselle tehokkaasti mahdollisimman yksiselitteistä ja yhteismitallista tietoa siitä, miten hyvässä kunnossa sisäinen valvonta ja riskienhallinta ovat ja mitkä ovat keskeiset pullonkaulat ja kehittämisalueet. GRC-varmennusmallilla halutaan yhdistää voimat ja luoda yksi yhteinen tiekartta kehittämiselle (Kuva 1).

Keskeinen sisäisen valvonnan malli on kansainvälisesti hyväksytty COSO -malli. Uusi julkaistu COSO 2013 huomioi vahvemmin operatiiviset prosessit, lainsäädännön, toimintaympäristön vaikutukset sekä laajentaa ajattelua taloudellisesta raportoinnista liiketoiminnan




**Kuva 1: Esimerkki Governance, Risk and Compliance -varmennusmallin läpiviennistä organisaatioon**

prosesseihin. Riskienhallinnan kehittämisen tukena on käytetty COSO ERM -mallia, joka keskittyy selkeämmin ja perusteellisemmin organisaatioiden riskienhallintaan. GRC mallissa liikutaan kokonaisvaltaisesta riskienhallinnasta kokonaisvaltaiseen varmennukseen (Kuva 2). Prosessi edellyttää yhteistyötä ja avointa vuorovaikutusta eri varmennustoimintojen välillä. Kustannussäästöjen lisäksi voidaan saavuttaa tehokkaampia varmennusprosesseja, joissa itse ydintoiminnan tehokkuus saadaan hyötyjen keskiöön. ■


**Kuva 2: Kokonaisvaltaisen riskienhallinnan (ERM) suhde Governance, Risk and Compliance -viitekehykseen.**

# Koulutustoimikunta tutuksi

**Koulutustoimikunnan jäsenet vasemmalta oikealle:**
**Raimo Haapajärvi, tarkastuspäällikkö Hankkija Oy**
**Niina Ratsula, CIA, CCSA, CRMA, tarkastuspäällikkö, Kemira Oyj**
**Jaana Ilomäki, sisäinen tarkastaja, Hyvinkään kaupunki**
**Vesa Putula, sisäinen tarkastaja, Puolustusvoimat**
**Seija Aalto, tarkastuspäällikkö, SOK**
**Arto Pehkonen, CIA, CCSA, Director of Ethics and Compliance, Scala Consulting**
**Kuvasta puuttuu Heli Pietiläinen, MMM, KTK, CIA, CISA, Stockmann Oyj Abp**

Koulutustoimikunnan tehtävänä on suunnitella ja toteuttaa yhdistyksen jäsenille ja muille tarkastuksesta, arvioinnista ja kehittämisestä kiinnostuneille monipuolista ja korkeatasoista koulutusta. Koulutuksen lisäksi tehtävänä on ammatillisen verkottumisen, kokemusten jakamisen ja toinen toisiltaan oppimisen tukeminen.

Yhdistys on asettanut tavoitteekseen jäsenkuntansa ammatillisen osaamisen ylläpitämisen ja jatkuvan kehittämisen. Lisäksi halutaan edistää ammatin tunnettuutta ja arvostusta. Koulutustoimikunnan tehtävä on käytännössä yhteistyössä muiden Sisäiset tarkastajat ry:n toimikuntien ja yhteistyökumppaneidensa kanssa tehdä työtä näiden tavoitteiden saavuttamiseksi. Koulutustoimikunnan työtä ohjaavat yhdistyksen arvot. Vuoden 2014 kehittämiskohteeksi haluamme nostaa jäsenlähtöisyyden. Saamme käyttöömme viestintätoimikunnan toteuttaman jäsenkyselyn tulokset ja suuntaamme koulutusta esiin nousseiden jäsenistön tarpeiden ja vaatimusten mukaisesti.

Vuonna 2013 onnistuimme lanseeraamaan uusia koulutustuotteita kuten CIA-valmennuksen ohjattuna itseopiskeluna ja tarkastuskoulun, jossa osallistujat valmentajansa johdolla kehittivät ja systematisoivat omia tarkastusprosessejaan. Koulutustarjonnan monimuotoisuuteen haluamme panostaa myös 2014. Tavoitteenamme on tarjota erilaisia valmennus- ja oppimisfoorumeita sekä käytännön työkaluja sisäisten tarkastajien työhön. Prosessien hallinta, systematisointi ja arviointi sekä osaamisen johtaminen ovat teemoja, joihin liittyvää koulutusta suunnittelemme ja toteutamme myös jatkossa. Lisäksi kehitämme sisäisen tarkastuksen ammattikurssien sisältöä ottamalla niihin mukaan uusia teemoja ja ajankohtaisia muutostrendejä.

Toimikuntamme tavoitteena on jatkuva, avoin vuoropuhelu yhteistyökumppanien ja jäsenistön kanssa. Vuorovaikutteisuuden lisääminen on kehittämiskohteemme myös koulutustarjonnassa. Koulutusta ja verkottumista kehitetään toteuttamalla koulutusta erilaisilla menetelmillä ja foorumeilla sekä oppimista tukemalla. Koulutustoimikunta haluaa käydä keskustelua yhdistyksen jäsenten kanssa. Koulutustoimikuntaan saat yhteyttä Sisäiset tarkastajat ry:n kotisivujen palautekanavan kautta tai lähettämällä sähköpostia toimikunnan puheenjohtajalle osoitteeseen. ■

**Jaana Ilomäki**
jaana.ilomaki@hyvinkaa.fi.

P.s. Toivomme, että tämän jutun luettuasi tunnet meitä vähän paremmin ja otat rohkeasti yhteyttä aina, kun sinulla on uusia ideoita tai toiveita koulutuksiin ja osaamisen kehittämiseen liittyen.