SISÄISET TARKASTAJAT ry

The Institute of Internal Auditors Finland

Syynissä

Nro 1/2015

Tietoturvallisuus

Potilastietojärjestelmä ja tietosuojan kompastuskivet
Sivu 4

Sisäisen tarkastustuksen ja tietohallinnon välinen yhteistyö
Sivu 7

3 Pääkirjoitus

4 Potilastietojärjestelmä ja tietosuojan kompastuskivet

7 Sisäisen tarkastuksen ja tietohallinnon välinen yhteistyö

9 Sisäisiä petoksia tehtaillaan yhä enemmän

11 Työskentely omilla päätelaitteilla – Bring Your Own Device

13 Sisäisten tarkastajien kevätseminaari 2015

14 Sisäisen tarkastuksen rooli hyvän IT-hallinnon varmentajana ja kehittäjänä

17 Katsaus Sisäiset tarkastajat ry:n kevään koulutustarjontaan

19 Poimintoja syksyn seminaarista

20 Matkalla loistavaksi tarkastajaksi

21 Eettinen toimikunta tutuksi

Kuvat: Eero Antturi

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
Eija Pirskanen

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

Ulkoasu
Antturi Design Oy

Syynissä – tietoturvallisuus

Hannu Kananen
Sisäiset tarkastajat ry:n
hallituksen puheenjohtaja

Tietoturvallisuuden merkitys organisaatioiden toimintakyvyn varmistamisessa ja strategisessa johtamisessa korostuu, kun toimintaympäristöissä ilmenee riskejä. Riippumaton ja objektiivinen sisäinen tarkastus analysoi, tutkii ja arvioi johtamis- ja hallintoprosesseja sekä organisaatioiden toimintaa tukevia riskienhallinta- ja valvontajärjestelmiä. Sisäisen tarkastuksen velvollisuutena on tuottaa tietoturvallisuutta koskevaa informaatiota ylimmälle johdolle ja osaltaan kehittää organisaatioiden toimintaa.

Huhtikuussa Kalastajatorpalla järjestettävässä *Lisääntyvä data, sen hyödyt ja riskit* -kevätseminaarissa luennoidaan ajankohtaisista tietoturvallisuuteen liittyvistä teemoista. Kyberturvallisuus, big data, mobiliteetti ja liiketoiminnan pilviratkaisut ovat ajankohtaisia aiheita, joiden ymmärtäminen vaatii huolellista perehtymistä ja asiantuntijuutta. Seminaarin pääpuhujaksi saapuvat ISACA Internationalin varapuheenjohtaja **Steven Babb** ja kansainvälisesti tunnustettu Cobit-asiantuntija **Hendrik Ceulemans**. Kansainvälisten vierailijoiden lisäksi seminaarissa esiintyy useita tieto- ja kyberturvallisuuden asiantuntijoita, joiden luennoissa tietoturvaan liittyviä uhkia lähestytään sisäisen tarkastuksen näkökulmasta.

Tämä Syynissä-lehti tarjoaa ajatuksia tietoturvaan, tietosuojaan ja tietohallintoon liittyen. **Lasse Lehtonen** pohtii potilasjärjestelmän ja tietosuojan kompastuskiviä. **Maarit Turunen** ja **Minna Hynninen** analysoivat sisäisen tarkastuksen ja tietohallinnon välistä vuorovaikutusta. Tampereen syysseminaarin tunnelmat ja tulokset muistuvat elävästi mieleen **Maliina Hakalan** artikkelista, jossa korostetaan riskienhallinnan ja sisäisen tarkastuksen kumppanuutta.

Tietoturvallisuuteen liittyviä uhkia ei voida täysin poistaa, mutta näiden vaikutuksia voidaan vähentää pitkäjännitteisellä tieto- ja kyberturvallisuuden kehittämistyöllä. Varmentamalla organisaation toimintojen luotettavuutta, jatkuvuutta ja varautumista vähennetään riskien vaikutuksia ja kohotetaan organisaation toimintavalmiutta.

Miellyttäviä lukuhetkiä. ■

Lasse Lehtonen
LTT, OTT
Hallintoylilääkäri, HUS-kuntayhtymä
Terveysoikeuden professori, Helsingin yliopisto
Tietosuojalautakunnan varajäsen

Potilastietojärjestelmä ja tietosuojan kompastuskivet

Lääkärin ja muun terveydenhuoltohenkilöstön velvollisuus pitää potilaan tiedot salassa on osa klassista lääkintäetiikkaa. Salassapidon velvoite on ollut olemassa jo antiikin aikana ja sisältyy kuuluun Hippokrateen valaan. Potilaan hyvä hoito edellyttää, että potilaalla on luottamuksellinen hoitosuhde häntä hoitaviin ammattihenkilöihin. Vain lääkäriinsä luottava potilas uskaltaa kertoa kaiken tarpeellisen terveydentilastaan ja sairastumiseen tai vammautumiseen johtaneesta tilanteesta.

Terveydenhuollon toiminta perustuu kuitenkin pitkälti siihen, että potilaan siirtyessä toimipisteestä toiseen tai vaihtaessa hoitavaa lääkäriä, myös potilaan sairautta ja hoitoa koskevat tiedot siirtyvät. Potilasasiakirjojen laatiminen on alun perin ollut osa hoidon ammattistandardia, jolla varmistetaan hoidon jatkuvuus. Terveydenhuoltojärjestelmä on nykyaikaisessa hyvinvointivaltiossa hyvin suuri kokonaisuus, jossa tuhannet ammattihenkilöt vaihtavat tietoja keskenään samoista potilaista. Potilastietoja kerätään paitsi yksittäisen potilaan hoidon tarpeisiin, myös hoidon hallinnointia ja tilastointia varten. Potilastietojärjestelmistä on tämän takia tullut yhä suurempia ja monimutkaisempia kokonaisuuksia. Samalla niihin liittyvät tiedonhallintaan ja tietosuojaan liittyvät riskit ovat kasvaneet.

Potilastietojen tietosuojan perusteet

Tietosuojan perusperiaatteet ovat syntyneet automaattisen tietojenkäsittelyn kehittymisen myötä 1970-luvulla. Ne on kirjattu Euroopan Neuvoston vuonna 1981 hyväksymään tietosuojasopimukseen (ETS No. 108), jonka Suomi on ratifioinut.

Euroopan neuvoston tietosuojasopimuksen periaatteet ovat olleet pohjana Euroopan unionin vuonna 1995 voimaan tulleelle henkilötietodirektiiville (95/46/EC). Tämä direktiivi rakentuu paitsi tietosuojasopimukselle, myös henkilötietojen käsittelyn -käsitteen ympärille.

Suomessa henkilötietodirektiivi on implementoitu vuonna 1999 voimaan tulleella henkilötietolailla (523/1999). Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettu laki (asiakastietolaki, 159/2007) ja potilaan asemasta ja oikeuksista annetun lain (potilaslaki, 785/1992) säännökset salassapidosta ja tietojen luovuttamisesta syrjäyttävät erityislakeina henkilötietolain säännökset. Asiakastietolaki velvoittaa suomalaiset terveydenhuoltopalvelujen tuottajat liittymään kansalliseen potilastietojen sähköiseen arkistoon (KanTa).

Käyttötarkoitussidonnaisuus ja kokonaisarkkitehtuuri

Suomessa käynnissä olevan sosiaali- ja terveydenhuollon järjestämislainsäädäntöä koskevan uudistuksen tarkoituksena on integroida julkiset terveydenhuollon ja sosiaalihuollon palvelut paremmin toimivaksi kokonaisuudeksi. Tavoitteen toteuttaminen edellyttää myös mahdollisuutta käsitellä potilas- ja asiakastietoja aiempaa paremmin yli nykyisten organisaatioiden rajojen.

Eurooppalaisessa lainsäädännössä terveydentilaa koskevat tiedot ja sosiaaliturvaa koskevat tiedot ovat kuitenkin eri kategoriassa.

Henkilötietodirektiivien ja henkilötietolain (7 §:n) mukainen henkilötietojen käyttötarkoitussidonnaisuus edellyttää, että henkilötietoja ei käsitellä tavalla, joka ei ole yhteensopiva tietojen käsittelyn alkuperäisen tarkoituksen kanssa. Sääntely merkitsee käytännössä sitä, että esimerkiksi päihde- tai mielenterveyspotilaasta terveydenhuollon tarkoituksiin (so. potilaan hoitoa varten) kerättyjä tietoja ei saa ilman potilaan lupaa käyttää häntä koskevia sosiaalipalveluja koskevassa päätöksenteossa.

Terveydentilatietojen salassapidosta on kuitenkin olemassa lukuisia poikkeuksia. Esimerkiksi laissa sosiaalihuollon asiakkaan asemasta ja oikeuksista (asiakaslaki, 812/2000) ja lastensuojelulaissa (417/2007) paitsi annetaan sosiaalihuollon viranomaiselle oikeus saada ja käsitellä arkaluonteisia terveydentilatietoja, myös velvoitetaan terveydenhuollon ammattihenkilöt ilmoittamaan määrätyistä asioista sosiaalihuollon viranomaisille (esim. lastensuojeluilmoitus). Tietojen luovuttamisen yhteydessä luovutetut tiedot tyypillisesti tallennetaan sosiaalihuollon viranomaisten tietojärjestelmiin, mikä tietojärjestelmäarkkitehtuurin kannalta on ongelmallista. Viranomaisten tietokannat kun voivat näin pitää sisällään useaan paikkaan talletettuja samoja tietoja. Tällöin eri viranomaisten tiedot eivät välttämättä aikaa myöten pysy identtisinä (eli tiedon eheys kärsii), mikä voi johtaa päätöksenteon virheisiin.

Käytännön tasolla integraation tuomiin tietojen käyttötarkoitusta koskeviin ongelmiin tulee vastata kehittämällä

Eero Anturi

kansallista tietojärjestelmäarkkitehtuuria sellaiseksi, että eri viranomaisten tarvitsemat samat tiedot tallennetaan vain yhteen kertaan ja että käyttöoikeuksien hallinnalla huolehditaan siitä, että tietoja toiminnassaan tarvitsevilla viranomaisilla on riittävät käyttöoikeudet tarpeellisiin tietokantoihin. Käyttöoikeuksien hallinnan kehittäminen ja aiempaa mielekkäämpien käyttöoikeusprofiilien määrittely ja ylläpito onkin olennainen osa terveydenhuollon tietohallinnon kehittämistä.

Rekisteröidyn oikeudet

Henkilötietolaki antaa rekisteröidylle oikeuden mm. tarkastaa tietonsa ja vaatia virheellisinä pitämiensä tietojen korjaamista. Rekisteröidyt haluavat lisäksi varmistaa, että heidän arkaluonteisia tietojaan eivät ole käsitelleet sellaiset henkilöt, joilla ei tietojen käsittelyyn ole oikeutta.

Henkilötietolain mukainen tarkastusoikeus ja viranomaisten toiminnan julkisuudesta annetun lain mukainen tiedonsaantioikeus menevät käytännössä usein sekaisin. Henkilötietolain mukaisen tarkastusoikeuden tarkoituksena on varmistaa rekisterissä olevien tietojen oikeellisuus ja lain mukainen käyttö. Julkisuuslain mukaisessa tiedonsaantioikeudessa tarkoituksena on saada viranomaisen hallussa olevat tiedot tietoja pyytävän käyttöön. Henkilötietolain mukainen tarkastusoikeus on henkilökohtainen (henkilöoikeus) kun taas julkisuuslain mukainen tiedonsaantioikeus on julkisuusperiaatteen mukaan lähtökohtaisesti jokaisella. Potilastietojen salassapito rajoittaa julkisuuslain mukaista tiedonsaantia, mutta monissa tapauksissa asianosaisella on tiedonsaantioikeus myös salassa pidettävistä tiedoista.

Tietojärjestelmien laajeneminen on lisännyt riskiä luvattomaan tietojen katseluun. Tietojärjestelmien lokitiedot ovat usein salassa pidettäviä (KHO:2014:69), koska järjestelmien tietoturvallisuus vaarantuisi, mikäli tiedot käyttäjistä päätyisivät julkisuuteen ja tiedonkalastelijoiden käsiin. Asiakastietolaki sisältää kuitenkin lokitietojen tarkistamista koskevan erityissäännöksen. Asiakastietolain 18 §.n mukaan asiakkaalla on oikeus saada asiakastietojensa käsittelyyn liittyvien oikeuksiensa selvittämistä tai toteuttamista varten sosiaalihuollon ja terveydenhuollon palvelujen antajalta kirjallisesta pyynnöstä viivytyksettä lokirekisterin perusteella maksutta tieto siitä, kuka on käyttänyt tai kenelle on luovutettu häntä koskevia tietoja sekä mikä on ollut käytön tai luovutuksen peruste.

Tietosuojaan liittyvät riskit

Lähtökohtaisesti potilastietoja saavat käsitellä vain potilaan hoitoon osallistu-

Eero Antturi

vat. Tämä henkilöjoukko voi kuitenkin olla varsin laaja ja sisältää henkilöitä, joita potilas ei ollenkaan henkilökohtaisesti tapaa (esim. ajanvarausta tekevät jonohoitajat taikka saneluja purkavat osastosihteerit). Lokitietojaan läpikäyvät potilaat kyselevätkin usein syytä, miksi niin moni tuntematon henkilö on heidän tietojaan käsitellyt

Myös luvatonta tietojen katselua esiintyy terveydenhuollon toimintayksiköissä. Tilanteet vaihtelevat esim. oman alaikäisen lapsen tietojen katselusta työkavereiden tietojen katseluun. Rikkomuksiin ja rikoksiin tulee suhtautua tiukasti, koska julkinen luottamus terveydenhuoltoon rapisee nopeasti, jollei tietosuojaloukkauksiin puututa.

Henkilörekisterin pitäjä on henkilötietolain 47 §:n mukaan velvollinen korvaamaan taloudellisen ja muun vahingon, joka on aiheutunut rekisteröidylle tai muulle henkilölle tämän lain vastaisesta henkilötietojen käsittelystä

Henkilötietoasetus

Euroopan unionin parlamentti käsittelee parhaillaan komission ehdotusta henkilötietojen käsittelyn uudeksi eurooppalaiseksi sääntelyksi. Euroopan unionin henkilötietoasetus tulee lähivuosina korvaamaan henkilötietodirektiivin sekä syrjäyttämään henkilötietojen käsittelyä koskevat kansalliset säädökset. Tietosuojan perusperiaatteet pysyvät kuitenkin ennallaan, vaikka tietotekniikan nopea kehittyminen (esim. pilvipalvelut, big data, erilaiset mobiililaitteiden applikaatiot jne.) pakottaa hakemaan periaatteiden soveltamiseen uusia näkökulmia.

Keskeinen muutos uudessa sääntelyssä tulee olemaan rekisterinpitäjien ja käsittelijöiden hallinnollisten velvollisuuksien merkittävä lisääntyminen sekä korvausvastuun kasvu. Parlamentissa käsiteltävänä olevan ehdotuksen mukaan henkilötietoja käsittelevien organisaatioiden tulee nimetä tietosuojavastaavat, tehdä erilliset riskianalyysit ja henkilötietojen käsittelyn vaikutustenarvioinnit. Valvontaviranomaiselle on tulossa sakotusoikeus, samaan tapaan kuin kilpailuviranomaisilla jo on. Sakko olisi enimmillään 100 M€ tai 5 % yrityksen globaalista liikevaihdosta. Rekisteröity voi jatkossa kohdistaa korvausvaatimuksensa sekä rekisterinpitäjään että käsittelijään.

Henkilötietoasetuksen mukanaan tuoma valvonnan lisääntyminen ja korvausvastuun kasvu pakottaa jatkossa kiinnittämään entistä enemmän huomiota potilastietojärjestelmien tietosuojariskeihin. ■

Maarit Turunen, CISA, CISM, CGEIT, johtaja, Sisäisen tarkastuksen yksikkö, Verohallinto

Minna Hynninen, CISA Chief Audit Executive Evli Pankki Oyj

Sisäisen tarkastuksen ja tietohallinnon välinen yhteistyö

Viimeisen 20 vuoden aikana tiedosta on tullut organisaation merkittävin pääoma ja ICT:stä yhä tärkeämpi osa toimintaa. Siksi sisäisen tarkastuksen on syytä kohdistaa tarkastuksia myös tietojenkäsittelyyn.

Organisaatiossa on yleensä tietohallintoyksikkö, joka vastaa tietojärjestelmäratkaisuista ja -palveluista koostuvista sovelluksista, tietovarannoista ja -verkoista, muusta ICT-infrastruktuurista oheisjärjestelmineen ja tietoturvallisuudesta sekä niihin liittyvästä ylläpidosta, järjestelmähallinnasta ja teknisestä tuesta. Tärkein perusedellytys ICT-toiminnalle on sen käyttövarmuus ja turvallisuus. Sekä tietohallinto että sisäinen tarkastus tukevat organisaatiota sen tavoitteiden saavuttamisessa, sisäinen tarkastus arvioimalla riskienhallinta-, valvonta- sekä johtamis- ja hallintoprosessien tehokkuutta, tietohallinto ICT-teknologian avulla. Molempien intressissä on prosessien tehokkuus. Kumpikin haluaa välttää tilannetta, jossa tietotekniikka vaarantaisi organisaation toiminnan. Yhteiset tavoitteet eivät kuitenkaan takaa yhteistyön toimivuutta.

Säännöllistä keskustelua

Sisäinen tarkastus voi tukea tietohallinnon johtoa arvioimalla tietohallinnon toimintaa, sen johtamista ja menettelytapoja, tarkastamalla tuotannossa olevien tietojärjestelmien kontrolleja sekä konsultoimalla kehitteillä olevan järjestelmän kontrollivaatimuksia. Tämän lisäksi sisäinen tarkastus voi myös auttaa tietohallinnon riskien arvioinnissa ja hallintatoimenpiteiden määrittelyssä.

Sisäinen tarkastaja hyötyy yhteydenpidosta tietohallintoon erityisesti aloittaessaan organisaatiossa uutena tarkastajana, mutta ei kokeneen tarkastajankaan kannata väheksyä sitä. Koska lähes kaikki toiminta perustuu tietojärjestelmien käyttöön, tietohallintoa kuuntelemalla tarkastaja saa nopeasti käsityksen organisaation toiminnasta ja siinä tapahtuvista muutoksista.

Asiantuntevasti

Tietohallinnon tarkastaminen vaatii erityisosaamista. Osaamista tarvitaan tietohallinnon johtamisesta, projektienhallinnasta, järjestelmien hankkimisesta ja kehittämisestä sekä niihin liittyvistä menettelyistä, käyttöpalveluista, teknisestä infrastruktuurista, tietoturvallisuudesta sekä ICT-hankinnoista ml. sopimuksista.

Jos sisäisessä tarkastuksessa ei ole tietojärjestelmätarkastajia, tulee riittävä osaaminen hankkia kouluttautumalla, rekrytoimalla tai ostopalveluina. Joskus voi olla helpompaa siirtää tietohallinnon moniosaaja sisäiseen tarkastukseen ja opettaa hänelle tarkastuksen tekemistä kuin kouluttaa muihin tarkastuskohteisiin perehtyneestä tarkastajasta tietojärjestelmätarkastaja. Tällöin tulee kuitenkin huolehtia siitä, että tietohallinnosta siirtynyt ei voi tarkastaa asiaa, josta on vastannut viimeksi kuluneen vuoden aikana. Tietojärjestelmätarkastajan osaamisen ylläpito on haastavaa, koska teknologia kehittyy kiihtyvään tahtiin, joten ammattitaidon kehittämiseen tulee panosta riittävästi.

Sanoilla, jotka ymmärrän

Yhteistyö voi kärsiä siitä, etteivät tietohallinto ja sisäinen tarkastus puhu samaa kieltä. Tietohallinto viljelee mielellään englanninkielisiä termejä ja lyhenteitä. Toisaalta sisäinen tarkastajakin voi puhua sujuvasti sisäisestä valvonnasta ja kontrolleista, muttei kerro, mitä niillä tarkoitetaan. Hän voi suositella tunnistamaan vaaralliset työyhdistelmät ja eliminoimaan niistä aiheutuvat riskit ilman että konkretisoi, mistä oikeastaan on kyse. Vastaanottajan voi olla vaikea hahmottaa, miten todennäköisestä riskistä on kyse, mitä vahinkoja siitä saattaa aiheutua ja minkä verran vahinkojen torjumiseen kannattaa käyttää resursseja.

Viesti välittyy perille tehokkaasti vain, jos termit ja lyhenteet ovat osapuolten tuntemia ja niistä on yhteinen käsitys. Kannattaa myöntää reilusti, jos ei pysy keskustelussa mukana.

Huomio olennaisessa

Tietohallinnon resurssit ovat rajalliset ja ne kohdistetaan ensisijaisesti työhön, joka tukee liiketoiminnan keskeisimpiä tavoitteita. On selvää, että järjestelmiin jää kontrollipuutteita, jotka voivat johtaa virheisiin ja väärinkäytöksiin. Tietohallinto ei välttämättä pysty reagoimaan kaikkiin sisäisen tarkastuksen havaitsemiin kontrollipuutteisiin. Sen vuoksi tarkastajan kannattaa raportoida puutteista siten, että myös tietohallinto pystyy arvioimaan niiden kriittisyyttä. Sen sijaan, että raportoidaan pelkästään, kuinka monella henkilöllä on käyttöoikeuksiensa puitteissa mahdollisuus (can do) siirtää itse tekemänsä ohjelmamuutokset tuotantoon ilman liiketoiminnan hyväksyntää, on hyvä tuoda ilmi, kuinka monta kertaa edeltävän vuoden aikana näin on tapahtunut (did do).

Dataa murskaten

Tarkastushavaintoja kerätään haastatteluin, dokumentteihin tutustumalla ja järjestelmien käyttöä seuraamalla, mutta myös järjestelmiin tallentuneita tietoja analysoimalla.

Data-analyysien etuna on, että niiden avulla paitsi havaitaan poikkeamia ja tunnistetaan kontrollipuutteita, myös tuotetaan tietoa, joka lähes poikkeuksetta kiinnostaa tarkastuskohdetta ja auttaa perustelemaan suosituksia kontrollien kehittämiseksi.

Tarkastuksella ei aina ole riittävästi tietoa järjestelmiin tallentuvista tiedoista. Ei myöskään siitä, miten tiedot ovat saatavissa analyysia varten. Tietohallinto pystyy auttamaan datan poiminnassa, usein myös sen analysoinnissa.

Edes pienin askelin

Osapuolten välille voi aiheutua kitkaa, jos tarkastus pitää tiukasti kiinni tietohallinnon ylimitoitettuna pitämästä suosituksesta. Tällöin kannattaa miettiä, voidaanko suosituksesta tavalla tai toisella tinkiä ilman, että riskit kasvavat hallitsemattomaksi. Muutos ei aina tapahdu kerralla. Joskus eteenpäin ei pääse kuin pienin askelin. Pelisilmä on tarpeen myös sisäisen tarkastuksen tehtävissä.

Ilman yllätyksiä

Yhteistyötä tietohallinnon ja tarkastuksen välillä hankaloittaa se, että sisäisen tarkastuksen raportointi on poikkeamaraportointia. Kontrollit, joissa ei havaita puutteita, jäävät usein vähälle huomiolle, jolloin kokonaisuus voi vaikuttaa puutteellisemmalta, kuin se tarkastuksen perusteella on. Väärinkäsitysten välttämiseksi on hyvä sisällyttää raporttiin arvio kunkin osa-alueen kontrollien toimivuudesta ja merkityksestä liiketoiminnalle.

Tarkastettavaa ei pidä koskaan yllättää. Raportointi tulee käydä läpi siten, että osapuolille muodostuu yhteinen näkemys siitä, mitä havainnot ovat, mihin ne perustuvat ja vallitseeko niistä yksimielisyys. Erot näkemyksissä on hyvä tunnistaa ennen kuin raportti lähtee jakeluun. ■

David Porter
Head of Fraud Strategy, SAS Institute

Sisäisiä petoksia tehtaillaan yhä enemmän

Sisäiset petokset voivat johtaa huomattaviin taloudellisiin menetyksiin ja maineriskeihin. Ongelmia voidaan kuitenkin ehkäistä luomalla läpinäkyvä kulttuuri ja hyödyntämällä uutta teknologiaa. Järjestäytynyt rikollisuus ja heikentynyt taloustilanne ovat lisänneet maailmanlaajuisesti sisäisten petosten määrää.

Yksilöiden tekemät petokset kulkevat käsi kädessä huonon taloustilanteen kanssa. Kovina aikoina organisaatiot tiukentavat sääntöjään. Vastaavasti yhä useampi työntekijä vastustaa järjestelmää ja tulkitsee sääntöjä oman mielensä mukaan. Jos tällaista tapahtuu kerran, kyseessä ei välttämättä ole iso asia. Lähes kaikki työntekijät ovat rehellisiä ja luotettavia huonoimpinakin aikoina. Silloin tällöin jotkut kuitenkin päättävät käyttää järjestelmällisesti vilpillisiä keinoja taloudellisten etujen saavuttamiseksi.

Järjestäytynyt rikollisuus puolestaan on huolellisesti suunniteltua. Ammattirikolliset tehtailevat petoksia, joista on mahdollisimman suuri rahallinen hyöty ja matala kiinnijäämisen riski. Sisäisiin petoksiin liittyy tyypillisesti hyvin matala riski, sillä niitä on vaikea havaita, ja syyllisiä on vaikea saada asetettua syytteeseen. Me SASilla näemme järjestäytyneen rikollisuuden pyrkivän hyödyntämään maailmanlaajuisesti juuri tätä mahdollisuutta. Kaksi sisäisille petoksille altteinta sektoria ovat myös kaksi

kaikkein säännöstellyintä: rahoituspalvelut ja julkishallinto.

Työskentelin kerran tapauksen parissa, jossa rikollisjärjestö oli maksanut eräälle henkilölle yliopistotutkinnon saadakseen tämän lopulta tiettyyn asemaan. He olivat valmiita odottamaan viisi vuotta kestävän koulutuksen ajan, jotta henkilö saatiin solutettua kohteeksi valitulle osastolle. Yksinkertaisempi tapa soluttautua organisaatioon on lahjoa organisaation työntekijä. Rikolliset käyttävät usein aluksi sosiaalista mediaa, jolla ottavat selvää kohteensa suosikkiyökerhoista ja harrastuksista, ennen kuin ottavat yhteyttä henkilöön. Korruption kohteeksi joutuneet eivät yleensä edes huomaa tulleensa rekrytoiduksi rikollisjärjestöön ennen kuin on liian myöhäistä.

Big data auttaa petosten havaitsemisessa

Sisäisiin petoksiin puuttumisessa on kaksi suurta haastetta. Ensimmäinen haaste on kulttuurinen ja pätee erityisesti Pohjoismaissa, jossa työntekijöiden oletetaan yleisesti olevan rehellisiä. Vaikka työyhteisö huomaisi muutoksen kollegansa käytöksessä, kukaan ei välttämättä kohteliaisuudesta huomauta asiasta.

Ensimmäinen askel petosten ehkäisyssä on koulutuksen tarjoaminen organisaation sisäisesti, erityisesti korruptiota ja järjestäytynyttä rikollisuutta vastaan. Olisi erittäin tärkeää luoda sellainen kulttuuri, jossa työntekijät voivat tuoda esille huolenaiheitaan ilman pelkoa nolatuksi tulemisesta.

Toinen haaste on läpinäkyvän kulttuurin yhdistäminen tehokkaaseen teknologiaan. Useimmat petoksentunnistusjärjestelmät pyrkivät estämään vain ulkopuolisten pääsyn organisaatioon, ja niissä harvoin keskitytään organisaation sisäpiiriläisiin. Jopa tunnistusjärjestelmää jo hyödyntävissä organisaatioissa on havaittu viime aikoina, että perinteiset lähestymistavat eivät enää toimi tarkoituksenmukaisesti.

Petostentunnistusjärjestelmien merkittävin puute on usein käytöksen analyysi pitkällä aikavälillä. Järjestelmän avulla tulisi selvittää, millainen käyttäytyminen on normaalia tietyssä ihmisryhmässä tietyllä aikavälillä ja millainen käyttäytyminen ei ole normaalia. Kyky käsitellä näin suurta määrää raakatietoa on SASin ydinvahvuuksia. Olemme pitkän linjan asiantuntijoita monimutkaisen tiedon käsittelyssä – jopa sellaisen tiedon, jota ei ole luotu analysoitavaksi, kuten koneen suorituskyvyn lokitiedot.

Näkymättömästi olemassa

Kun organisaatio ottaa käyttöön tehokkaamman petostentunnistusratkaisun, sen ei tulisi vaikuttaa työntekijöiden arkeen millään tavalla. Järjestelmän tulee toimia syvällä organisaatiossa näkymättömällä tavalla. Petostentunnistamisprojektin ensimmäisessä vaiheessa analysoidaan tietoja kaikessa hiljaisuudessa, eikä käyttöönotosta ilmoiteta organisaatiossa laajassa mittakaavassa.

Suurella osalla petostentunnistusratkaisuja ostaneista yrityksistä on jo ensikäden kokemusta tietorikkeistä. Osa niistä yrittää hoitaa asian jälkijunassa, eivätkä tulokset puhu puolestaan. Yrityksillä on tarve osoittaa asiakkailleen ja sidosryhmilleen, että ne suhtautuvat näihin asioihin vakavasti.

Laadukkaan petostentunnistusjärjestelmän merkitys kasvaa tulevaisuudessa, sillä vuonna 2016 voimaan astuvan uuden EU-lainsäädännön edellyttämät kansalliset lait organisaatioiden välisen tiedon jakamisesta ja suojelemisesta tiukentuvat. ■

David Porter luennoi kevätseminaarissa 21.4.2015 aiheesta ”Insider Fraud – The Threat from Within”

Eija Pirskanen, CIA, CCSA, CISA
tarkastuspäällikkö, Restel Oy
viestintätoimikunnan jäsen

Minna Korhonen
sisäinen tarkastaja, Tilastokeskus
viestintätoimikunnan jäsen

Työskentely omilla päätelaitteilla – Bring Your Own Device

Viime vuosina on kirjoitettu paljon BYOD-ilmiöstä: työntekijät haluavat tehdä töitä omilla, tutuilla laitteillaan, ei työnantajan määräämillä laitteilla ja käyttöjärjestelmillä. Kun tietohallinto antaa tälle trendille periksi, asia nousee myös tarkastuksen agendalle. Mistä siis aloittaa? Vinkkiä voi saada muun muassa Internal Auditor -lehden artikkeleista. Tämä on vapaa lyhennelmämme helmikuussa 2014 ilmestyneestä artikkelista "BYOD Business Issues". Kirjoittaja on rehtori Stephen Coates, CIA, CGAP, CRMA, CISA, Moore Stephens, Brisbane, Australia.

BYOD-ilmiön kasvaessa sisäisten tarkastajien on pohdittava millä tavoin organisaatio voi sallia, että hallituksen jäsenet, johtajat ja työntekijät käyttävät omia päätelaitteita ja toisaalta, miten laitteiden käytön valvonta järjestetään. Vastaus voi olla käyttöönoton tiekartta, jolla pyritään varmistamaan sekä (liike) toiminnan tarpeet että joustavat mahdollisuudet päätelaitteiden käyttöön.

Tiekartta

Käyttöönoton tiekartta sisältää selkeät säännöt, joiden tarkoituksena on varmistaa, että BYOD-riskejä hallitaan organisaation odotusten mukaisesti. Jos BYOD-ohjelman toteuttajat eivät ymmärrä sääntöjä, voi organisaatio altistua uusille, hallitsemattomille riskeille. Tietojärjestelmätarkastajat voivat neuvoa johtoa nostamalla esiin BYOD:n organisaatiolle tuomia riskejä ja auttamalla organisaatiota varmistumaan siitä, että käyttöönotolle luodaan alusta alkaen hyvät perusteet.

Suunnittelu

Onko organisaatiolla hallituksen hyväksymä riskienhallintasuunnitelma omien ja mobiililaitteiden käytölle? Arvioidaanko sitä säännöllisesti? Suunnitelmassa tulee tunnistaa uudet, mobiililaitteiden mukanaan tuomat riskit, varmistaa ylimmän johdon tuki hallituksen hyväksynnällä ja selkeästi kommunikoida johdon valvontavastuu ja odotukset. Sisäisen tarkastajan roolina suunnitteluvaiheessa on varmistua siitä, että hallituksen hyväksymä suunnitelma on olemassa ja että se huomioi jatkuvasti muuttuvat teknologiat ja ratkaisut.

Perehdytys

Onko organisaatiolla mobiili- ja omien laitteiden käyttöä koskeva koulutussuunnitelma, jolla varmistutaan siitä, että käyttäjät ymmärtävät vastuunsa? Koulutusohjelmassa tulisi käsitellä käytölle asetettuja odotuksia, siihen kohdistettavaa valvontaa sekä seuraamuksia rikkomuksista. Sisäiset tarkastajat voivat arvioida näitä menettelyjä.

Osallistaminen

Onko organisaatio osallistanut HR-, laki-, hankinta-, IT- ja taloustoiminnot prosessiin? BYOD tulee nähdä koko organisaation laajuisena, ei vain IT:n asiana.

Hallinnointi

Johdetaanko BYOD-toimintoja tehokkaasti? Henkilökohtaisten laitteiden käytön salliminen vaatii valvontaa, kuten esimerkiksi laitteiden automaattista paikannusta tai palveluita laitevarkauksien varalle. Tietojärjestelmätarkastajan osaamista voidaan hyödyntää näiden valvontaa tukevien menettelyiden ja välineiden valinnassa.

Freeimages.com

Valinnat

Onko organisaatio määritellyt, millä laitteilla, ml. käyttöjärjestelmä, pääsy organisaation järjestelmiin sallitaan ja miten tuki järjestetään?

Mobiililaitteiden käyttöjärjestelmiä voidaan pitää yhtenä vakavimpana organisaation turvallisuushaasteena. Tietoturva-asioihin perehtynyt tietojärjestelmätarkastaja voi valaista johtoa niihin liittyvistä heikkouksista.

Menettelytapaohjeet

Ovatko organisaation mobiili- ja BYOD-ohjeet hyvin laaditut, käyttäjille ymmärrettävät ja toteutuskelpoiset? BYOD-strategian kannalta tärkeää on se, että käyttäjät hyväksyvät käyttöehdot ja rikkomusten seuraamukset. Sisäisen tarkastajan tehtävänä voi olla varmistua siitä, että työntekijät ovat allekirjoittaneet käyttöluvat ja että yksityisyyttä koskevat menettelytavat on selitetty heille.

Arviointi

Onko organisaatio arvioinut valmiuttaan vastata mobiili- ja BYOD-laitteiden tuomiin vaatimuksiin, varmistunut kypsyystasostaan ja tulevaisuuden investointitarpeista? Sisäinen tarkastaja voi tehdä arvion organisaation nykytilasta verrattuna tavoitetilaan, erityisesti työntekijöiden sitoutumisen, teknisen tietoturvan ja liiketoimintayksiköiden osallistamisen osalta.

Kadonneet ja varastetut laitteet

Mobiililaitteiden katoaminen merkitsee organisaatiolle ainakin hetkellistä tuottavuuden menetystä, joten laitteiden katoamisen ja varkauden varalle on oltavat menettelyt. Sisäiset tarkastajat voivat arvioida ja antaa suosituksia näistä menettelyistä.

Tiedonsiirto

Organisaation tietojen käsittely organisaation ulkopuolella muodostaa aina riskin, mutta kun mukaan otetaan työntekijöiden omat laitteet ja tavat käsitellä tietoa, turvallisuus ei välttämättä ole organisaation edellyttämällä tasolla. Sisäiset tarkastajat voivat tarjota riippumatonta varmennusta tiedostojen siirron ja pilvipalvelujen turvallisuudesta.

Seuranta

Onko organisaatio arvioinut BYOD-toimintaa? Sisäisten tarkastajien roolina voi olla tarkastella johdon valvontavastuun toteutumista.

Sisäisen tarkastuksen rooli

Sisäisillä tarkastajilla on keskeinen rooli BYOD:n käyttöönotossa, koska he voivat tarjota johdolle riippumattoman arvion erilaisten laitteiden ja käyttöjärjestelmien tuomista haasteista. Lisäksi he voivat auttaa johtoa varmistumaan siitä, että organisaatio on käsitellyt kaikkia omien päätelaitteiden käyttöön liittyviä erityiskysymyksiä. ■

Jani Heikkala, CIA, CCSA
Yksityispankkiiri, Evli Pankki Oyj
seminaaritoimikunnan puheenjohtaja

Sisäisten tarkastajien kevätseminaari 2015

Lisääntyvä data, sen hyödyt ja riskit

Sisäisten tarkastajien kevätseminaari järjestetään yhteistyössä ISACA Finlandin (Tietojärjestelmien tarkastus ja valvonta ry) kanssa Kalastajatorpalla Helsingissä 21.–22.4.2015. Seminaarin teemana on jatkuvasti lisääntyvän tiedon tarjoamat hyödyt ja mahdollisuudet, mutta erityisesti tähän kehitykseen liittyvät riskit ja kyberturvallisuus niin hallituksen kuin tarkastuksenkin näkökulmista.

Kyberturvallisuus on noussut nopeasti median kautta esille siten, että tietoturvallisuuteen ja jatkuvuuden hallintaan on alettu kiinnittää organisaatioissa erityistä huomiota. Yhtenä esimerkkinä kehityksestä on Kyberturvallisuuskeskuksen perustaminen vahvistamaan Viestintäviraston tietoturvatehtäviä vuoden 2014 alusta.

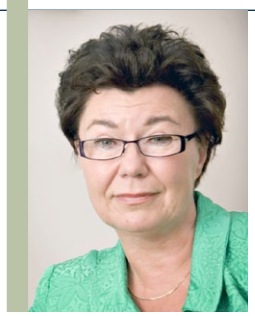
Kyberturvallisuuskeskuksen mukaan sen ensimmäinen toimintavuosi 2014 muistetaan Suomessa etenkin toisia haittaohjelmia lataavien haittaohjelmien, vakavien haavoittuvuuksien ja tehokkaiden huijauskampanjoiden vuotena. Merkittävistä tietoturvauhkista huolimatta Suomi loisti maana, jossa on maailman vähiten haittaohjelmien saastuttamia tietokoneita.

Kyberturvallisuuskeskuksen ensimmäisen toimintavuoden aikana paljastui internetin perusrakenteita horjuttaneita vakavia ohjelmistovirheitä ja tehtiin tuloksekasta kyberturvallisuuden uhkien ennaltaehkäisyä. Kyberturvallisuuskeskuksen vuosikatsauksen (2014) tärkeimmät havainnot Suomen näkökulmasta olivat:

1. Tietojenkalastelu yleistyy
2. Havainnot vakoiluhaittaohjelmista lisääntyvät
3. Palvelunestohyökkäyksien voima kasvaa
4. Kansallinen havainnointikyky paranee
5. Teleoperaattoreiden toimilla on merkitystä
6. Suomalaisia salaustuotteita on edelleen vähän
7. Yhteistoiminta on elinehto.

Hyvä ja avoin yhteistyö eri sidosryhmien kanssa kannustaa entistä parempaan verkostoitumiseen. Yhteisen tilannekuvan luomiseksi jokainen tiedonjyvä on tärkeä. Seminaarissamme tuomme näitä tiedonjyviä yhteen ja tarkennamme tilannekuvaa uusien mahdollisuuksien löytämiseksi ja turvallisuutemme vahvistamiseksi. Kalastajatorpalla tiedonjyviä jakaa monipuolinen joukko alan huippuasiantuntijoita, mm: **Steven Babb** – International Vice President, ISACA, **Kimmo Rasila** – hallituksen pj, Nixu Oyj, hallituksen vpj, Hallitusammattilaiset ry, **Erka Koivunen** – Kyberturvallisuuskeskus, **Reijo Aarnio**, Tietosuojavaltuutettu ja **David Porter** –Fraud & Financial Crime, EMEA & AP, SAS Institute Inc. Porterin artikkeli, joka avaa tiedon ja teknologian hyödyntämistä petosten havaitsemisessa, löytyy myös tästä lehdestä.

Tervetuloa Kalastajatorpalle! Ilmoittautuminen seminaariin Sisäiset tarkastajat ry:n kotisivuilla www.theiia.fi.



Tuulikki Help
Tarkastuskoulu, rehtori
Sisäisen tarkastuksen Personal Trainer

Sisäisen tarkastuksen rooli hyvän IT-hallinnon varmentajana ja kehittäjänä

Liiketoiminta ja sitä tukeva IT-toiminta ovat organisaatiossa yhtenäisiin tavoitteisiin sitoutuneita kumppaneita, joiden toimintaan sisäisen tarkastuksen tulisi entistä enemmän kiinnittää huomiota. Sisäisen tarkastuksen yhtenä merkittävänä tehtävänä on edistää tuon kumppanuuden tehokkuutta ja asianmukaisuutta.

Liiketoiminnan tavoitteiden saavuttaminen asettaa toiminnassa käytettävälle tiedolle, sen tuottamiselle ja käytölle yhä enenevässä määrin merkittäviä vaatimuksia, jotka liittyvät tiedon tehokkuuteen, taloudellisuuteen, luottamuksellisuuteen, eheyteen, saatavuuteen, luotettavuuteen ja laillisuuteen. Myös tietoturvaan liittyvät asiat korostuvat jatkuvasti. Tieto ja IT:n rooli sen tuottajana on minkä tahansa organisaation johtamisen kannalta niin merkityksellistä, ettei sisäinen tarkastus mielestäni missään nimessä pysty ohittamaan omassa tarkastustoiminnassaan sen asianmukaisuuden arviointia. IT-Governance eli hyvä IT-hallinto kertoo kaikille meille sisäisille tarkastajille, ei ainoastaan IT-tarkastajille, mistä pohjimmiltaan on kysymys: tiedolla johtamisesta. Meidän roolimme on varmistua hyvien IT:n johtamiseen liittyvien sisäisten kontrollien olemassaolosta ja asianmukaisuudesta.

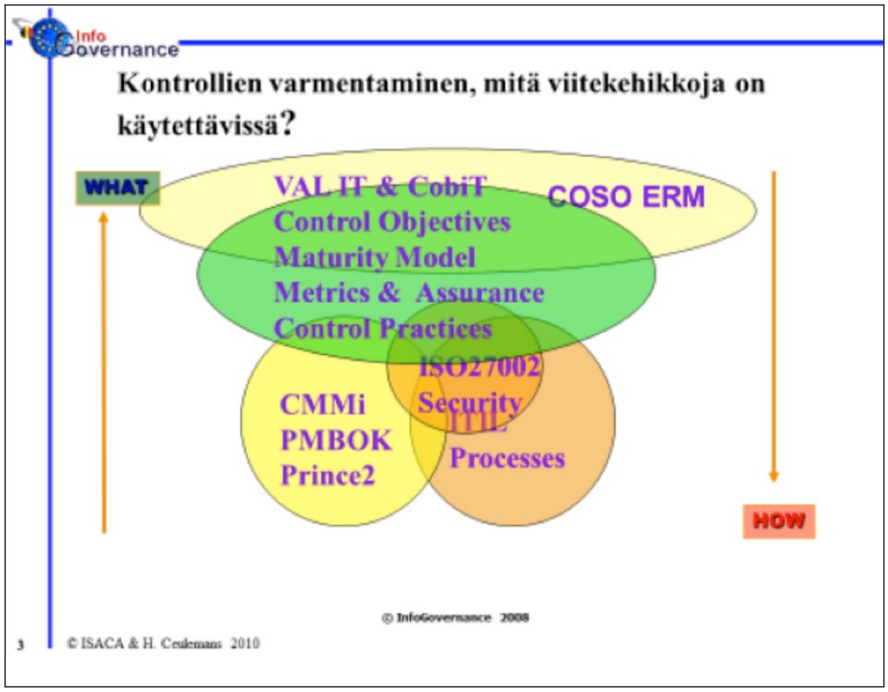
Hyvän IT-toiminnan johtamisen arviointiin liittyen olen ilolla pannut merkille yhdistyksen aktiivisuuden jäsenkuntansa IT-tarkastusvalmiuksien kehittäjänä. Tänä keväänä, 20.–21.5, yhdistys tarjoaa koulutusta otsikolla ”Basics of IT and Information Security for non-IT Auditors”. Kouluttajana toimii kevätseminaarissakin luennoiva **Hendrik Ceulemans** (Executive Manager of InfoGovernance). Suosittelen, että käytte yhdistyksen kotisivuilla tutustumassa tarkemmin koulutuksen ohjelmaan. Tässä artikkelissa jäljempänä esitetyt kuvat eri viitekehikoista ja niiden keskinäisestä vertailusta ovat Hendrik Ceulemansin laatimia.

Hyvän hallinnon kontrolleja kuvaavia viitekehikoita

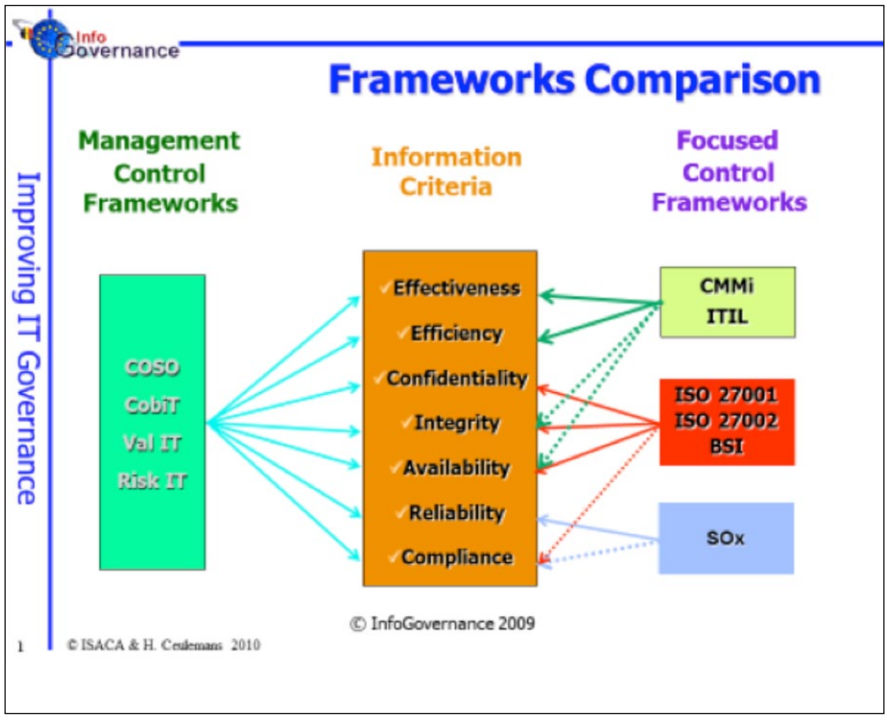
Liiketoiminnan ja IT-toiminnon hyvän hallinnon toimivuuden arvioimiseksi ja edelleen kehittämiseksi on luotu kansainvälisesti hyväksyttyjä kontrolliviitekehikoita, joista merkittävimmät on esitetty kuvassa 1.

Kuvassa 1 ylimpänä olevat viitekehikot CobiT ja COSO ERM edustavat strategisen tason kattavia viitekehikoita, kun taas kuviossa esitetyt muut, suppeammat viitekehikot soveltuvat enemmän taktisella ja operatiivisella tasolla tapahtuvan toiminnan arviointiin ja kehittämiseen.

CobiT (Control objectives for IT related Technologies) -viitekehikon on luonut vuonna 1998 perustettu IT Governance Institute. Järjestö toimii läheisessä yhteistyössä ISACAn (Information Systems Audit and Control Assocation) kanssa. IT-toiminta on CobiT-viitekehikon mukaan jaettu neljään toiminnalliseen pääprosessiin: Planning&Organisation, Acquisition& Implementation, Delivery&Support ja Monitoring. Kukin pääprosessi jakautuu alaprosesseihin, joita on kaiken kaikkiaan 34. CobiT-viitekehikko kattaa laajasti IT:n toiminnalliset suhteet organisaation sisäisiin liiketoimintayksiköihin, ulkoistettuihin palvelun-



Kuva 1. Kansainvälisiä viitekehikoita.



Kuva 2. Tiedolle asetettavia kriteereitä ja eri viitekehikoiden kattavuus.

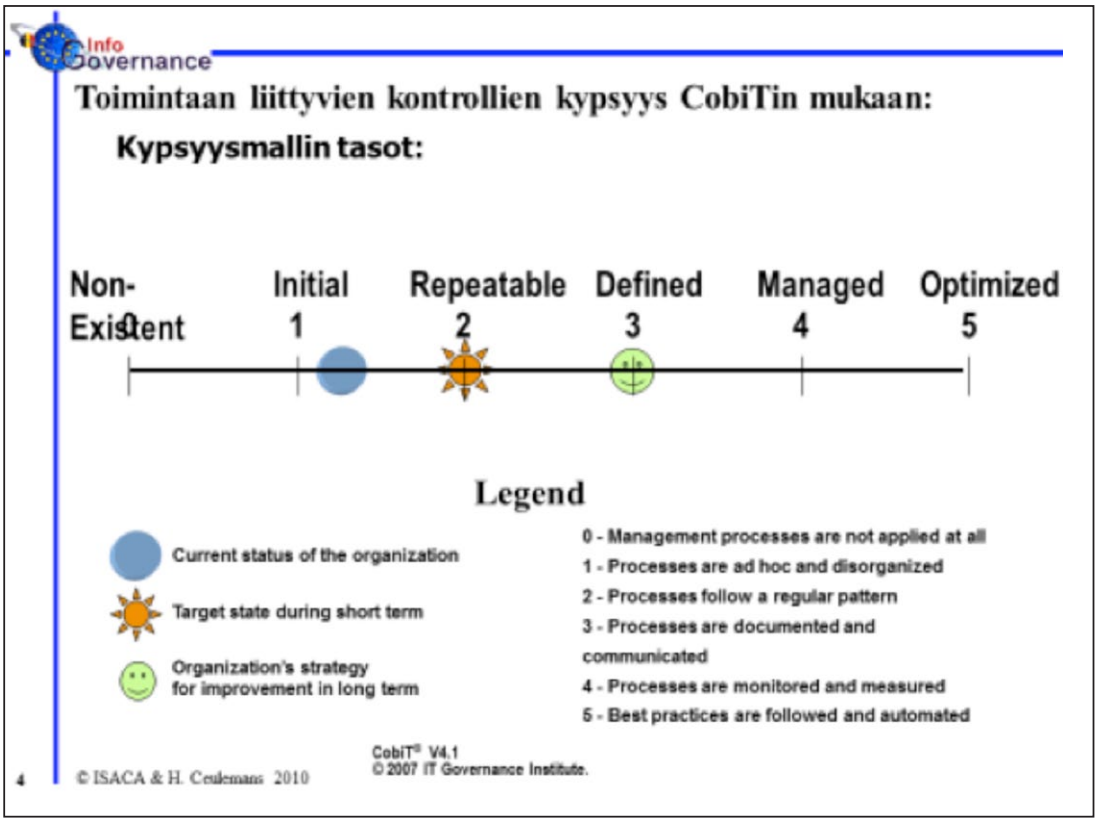
tuottajiin sekä organisaation ylimpään johtoon. CobiT-viitekehikon avulla voidaan kullekin alaprosessille määritellä prosessin kontrollitavoitteet, hyötyä tuottavat argumentit, prosessiin liittyvät riskit, hyvät kontrollikäytännöt sekä tarkastustoimenpiteet. CobiT-viitekehikon tarkempi sisältö ja sen käyttöä IT:n tarkastamisessa käydään läpi em. Hendrik Ceulemansin toukokuussa pitämässä koulutuksessa.

UK Office of Government Commerce:n luoma ITIL on lyhennelmä sanoista IT Infrastructure Library. Tämä viitekehikko on keskittynyt pääasiassa IT-palvelun tuottamiseen, joka vastaa lähinnä CobiTin yhtä pääprosessia, DS eli Delivery and Support.

Kuvassa 1 mainittu ISO-standardi määrittelee ohjeita ja yleisiä periaatteita organisaation tietoturvan käynnistämiseen ja hallintaan. CMMI (Capability Maturity Model Integration) on tuotekehityksen kypsyysmalli, joka sisältää organisaation tuotekehitysprosesseihin ja käytäntöihin sisältyviä prosessialueita.

Tiedolle asetettavat kriteerit ja eri viitekehikoiden kattavuus

COSO ERM ja CobiT ovat kuvan 1 muita viitekehikoita käyttökelpoisempia sisäiselle tarkastajalle, jonka tehtävänä on arvioida kokonaisuudessaan hyvän hallinnon tiedolle ja sen turvallisuudelle asettamia vaatimuksia. Kuvassa 2 verrataan toisiinsa eri viitekehikoita suhteessa tiedolle esitettyihin seitsemään vaatimukseen.



Kuva 3. CobiT-viitekehikon mukainen prosessin kypsyysmalli.

Hyvä IT-hallintotapa ja CobiT sekä toiminnan kypsyyden arviointi

CobiT-viitekehikko sisältää myös ns. IT-prosessien kypsyystasojen itsearviointimallin. Kullekin CobiTin 34 prosessille on määritelty kriteerit, joiden avulla voidaan asteikolla 0-5 identifioida, millä kypsyystasolla IT-toiminta on. Kypsyystasojen yleiset kriteerit on esitetty kuvassa 3. Itsearviointimallia voi tarkastajan ohella hyödyntää myös operatiivinen IT-johto, ja mallin avulla on mahdollista määrittää konkreettisia toimenpiteitä asianmukaisen IT-toiminnan edelleen kehittämiseksi.

Organisaation kokonaisvaltainen hyvä hallintotapa ja sisäisen valvonnan kypsyystaso

Onko mahdollista hyödyntää CobiTiin sisältyvää sisäisen valvonnan kypsyysajattelua myös COSO ERM-mallin eri osa-alueille? Mielestäni kyllä, ja aihetta käsitellään myös Tarkastuskoulussa. Sisäisen valvonnan kypsyyden arviointikriteereitä ovat esimerkiksi toiminnan systemaattisuus, säännöllisyys, ohjeiden ja prosessikuvausten sisällön kattavuus ja ajantasaisuus, informoinnin kattavuus, seurantafrekvenssit, yksikkökohtaisten toimintojen yhdenmukaisuus suhteessa organisaation kokonaistasoon, reagointi poikkeustapauksissa jne. Sisäisen valvonnan kypsyyden kokonaisarviointi voi antaa sisäiselle tarkastukselle mahdollisuuden edistää oman organisaationsa sisäisen valvonnan ja riskienhallinnan kulttuuria ja samanaikaisesti kehittää synergiaa ja ymmärrystä IT-tarkastuksen ja ns. perinteisen tarkastuksen välillä. ■

Niina Ratsula, CIA, CRMA, CCSA, CCEP-I
Director, Ethics & Compliance, Kemira Oyj
koulutustoimikunnan puheenjohtaja

Katsaus Sisäiset tarkastajat ry:n kevään koulutustarjontaan

Kevään 2015 kurssitarjonta koostuu sekä jatkuvassa tarjonnassa olevista vakiokoulutuksistamme, että mielenkiintoisista teemapäivistä.

Kevään koulutustarjonnan avasi helmikuun lopulla *Fraud*-teemapäivä, jossa pohdittiin sisäisen tarkastuksen roolia väärinkäytöstapausten tunnistamisessa, tutkinnassa ja raportoimisessa. Kouluttajina tilaisuudessa toimivat CFE **Paula Niemi** Microsoftilta sekä JHTT, CIA, CCSA, CISA, CFE Helge Vuoti BDO:lta.

Sisäisen tarkastuksen ammattikurssit (STAK I ja II) toteutetaan helmimaaliskuun aikana. STAK I on hyvä perusasioista koostuva kokonaisuus erityisesti sisäisen tarkastuksen uusille toimijoille. Kurssi sopii myös kaikille niille tarkastuksessa työskenteleville, joilla on tarvetta päivittää tietämystään sisäisen tarkastuksen ammatillisesta viitekehyksestä, standardeista ja työkaluista. STAK II -kurssi puolestaan on tarkoitettu ensisijaisesti sisäisen tarkastuksen toiminnosta vastaaville henkilöille. Tavoitteena on syventää osaamista erityisesti sisäisen tarkastuksen johtamisesta, tarkastustyön suunnittelusta ja ohjaamisesta, tarkastuksen ja sen sidosryhmien (tarkastuskohteet ja ylin johto) välisestä viestinnästä sekä ammattistandardien mukaisesta laadun ja toiminnan kehittämisestä. STAK II kurssin sisältöä on uudistettu viime keväänä toteutetun kehitystyön seurauksena. Kummatkin koulutuskokonaisuudet tarjoavat myös oivallisen foorumin tavata kollegoita ja pohtia yhteisiä haasteita ja kysymyksiä saman pöydän äressä.

Syksyllä 2013 startannut *Tarkastuskoulu*, jota luotsaa pitkän tarkastusuran tehnyt **Tuulikki Help**, jatkaa kevään koulutustarjonnassa. Tarkastuskoulu tarjoaa konkreettisen lähestymistavan ja käytännön työkaluja tarkastusprosessin läpiviemiseen: tarkastussuunnitelma, tarkastuksen työpaperit sekä tarkastuksen suorittaminen ja tarkastusraportin laatiminen. Tarkastuskoulussa käydään läpi myös sisäisen tarkastuksen toimintaohje, vuosisuunnitelma ja vuosikertomus. Tarkastuskoulun oppilaat laativat kurssin aikana itsenäisesti tarkastukseen liittyvät dokumentit annetun casen pohjalta ja kouluttaja kommentoi niitä henkilökohtaisesti kurssijaksojen välissä. Koulutuspäivät järjestetään 15.4.–3.6 välisenä aikana. Tarkemmat tiedot aikataulusta ja ohjelmasta löytyvät yhdistyksen kotisivuilta.

Suurta suosiota ja positiivista palautetta saanut *Maineriskit ja niiden hallinnan työkalut* -teemapäivä järjestetään 16.4. uusintana viime vuodelta. Koulutuksessa pohditaan, miten sisäinen tarkastus voi tukea organisaatiota maineriskien hallinnassa. Alustajana ja työpajatyöskentelyn vetäjänä toimii **Salla-Maaria Laaksonen** Helsingin yliopiston Viestinnän tutkimuskeskuksesta. Lisäksi kuulemme mielenkiintoisen case-puheenvuoron Sosiaali- ja Terveysministeriön **Katja Sibenbergin** esittämänä.

IIA järjestää mahdollisuuksien mukaan myös kansainvälistä koulutusta. Tämän kevään kansainvälisestä koulutustarjonnasta pitää huolen *Basics of IT and Information Security for non-IT Auditors* nimikettä kantava koulutus, joka järjestetään 20.–21.5. Luennoitsijana toimii **Hendrik Ceulemans** (CGEIT, CISA, MBA, MCA), jolla on 25 vuoden kokemus tietohallinnan, tietoturvan sekä riskienhallinnan eri osa-alueilta. Ceulemans pitää myös kevätseminaarissa key note -esityksen.

CSA – Control Self-Assessment -kurssi toteutetaan 27.–28.5. CSA on me-

123RF.com

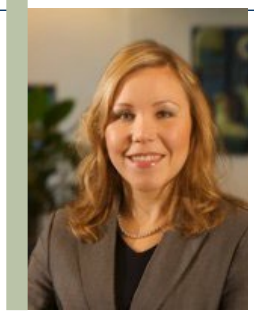
netelmä, jonka avulla liiketoiminnan vastuuhenkilöt itse arvioivat riskienhallinnan ja sisäisen valvonnan riittävyyttä, tavoitteena parempi riskienhallinnan ymmärtäminen ja tehokkaammat sisäisen valvonnan toimenpiteet. Onnistunut itsearviointi myös sitouttaa vastuuhenkilöt sisäisen valvonnan arviointiin, kehittämiseen ja toteuttamiseen. Koulutus tarjoaa valmiudet ohjata ja avustaa itsearviointiprosessin toteuttamisessa. Kurssilla käydään läpi keskeiset itsearvioinnin perusteet ja harjoitellaan ohjatun itsearvioinnin toteuttamista käytännössä. Kouluttajana toimii kurssin jo useampaan otteeseen mainioin arvosanoin vetänyt **Arto Pehkonen**, CIA, CCSA.

CIA-tutkintoon valmentavasta koulutuksesta on tullut paljon kyselyitä alkuvuonna. Seuraavan kerran valmennus järjestetään heti alkusyksystä. Valmennusryhmä kokoontuu neljä kertaa syksyn aikana. Tutustu tarkempaan ohjelmaan ja aikatauluun yhdistyksen nettisivuilla. Huomaathan, että ilmoittautumalla toukokuun loppuun mennessä säästät 10 % kurssimaksusta.

Syksyllä on luvassa myös muita mielenkiintoisia teemapäiviä, seuraattehan ilmoittelua!

Lämpimästi tervetuloa vuoden 2015 koulutuksiin! Lisätietoja sekä ilmoittautumisohjeet löytyvät yhdistyksen verkkosivuilta. Otamme mielellään vastaan kysymyksiä, ideoita ja palautetta kaikkea yhdistyksen tarjoamaa koulutusta koskien. ■

Lisätietoja:
Koulutustoimikunnan puheenjohtaja **Niina Ratsula** (niina.a.ratsula@utu.fi / 0504869821)
Yhdistyksen toiminnanjohtaja **Matti Mikola** (matti.mikola@theiia.fi / 0445451813)



Maliina Hakala, CIA,
Lead Auditor, PHOENIX group
seminaaritoimikunnan jäsen

Poimintoja syksyn seminaarista

Matti Mikola

Syysseminaari (28.–29.10.2014) suuntuuden karheassa Tampereen Sokos Hotel Tornissa keräsi mukavan määrän osallistujia ja syystäkin. Seminaarin teemana oli riskienhallinta ja näkökulmana erityisesti kumppanuus ja yhteistyö organisaatioissa. Tässä artikkelissa mainitut ja muut ansiokkaat luennot muodostivat antoisan kokonaisuuden.

Pääpuhujaksi kutsuttu **Phil Tarling** (Huawei Technologies Ltd.) pohti teemaa sisäisen tarkastuksen riippumattomuuden lähtökohdista. Tarling korosti ERM-mallin kolmen puolustuslinjan vastuiden pysymistä selkeänä ja sisäisen tarkastuksen riippumattomuuden säilymistä. GRC-mallin mukaista riskitoimintojen yhdistämistä hän tarkasteli kriittisesti. Yhteistyö on tarpeellista päällekkäisyyksien välttämiseksi ja tehokkuuden vuoksi, mutta roolien ja raportoinnin linjat on määriteltävä selkeästi. Käytännön esimerkin yhteistyön edistämisestä esittelivät SOK:n **Päivi Karhu** ja **Anna Koskenniemi**. Yhteistyön osa-alueita on tunnistettu riskitiedon hyödyntämisessä, asiantuntemuksen jakamisessa ja sisäisen valvonnan ja riskienhallinnan edistämisessä. Yhteistyöllä voitaisiin entisestään tehostaa toiminnan suunnittelua, yhteisprojektien löytämistä, konsernitasoista riskiraportointia ja riskien hallintaa.

Annukka Jokipiin (Vaasan yliopisto) ja **Timo Raikaslehdon** (PwC) luennoilla pohdittiin sisäisen tarkastuksen merkitystä sidosryhmille ja kehitystä tulevaisuudessa. Jokipiin tutkimusta käsittelevä luento esitteli näkemyksiä sisäisen tarkastuksen tulevaisuudesta vuonna 2030. Tutkimuksessa havaittiin, että sisäisellä tarkastuksella ja sen sidosryhmillä oli eriäviä näkemyksiä tulevaisuuden kehityksestä ja tutkimuksessa tunnistettiin erilaisia mahdollisia tulevaisuuden skenaarioita. Yhteistä näkemyksille oli regulaation lisääntyminen sisäiselle tarkastukselle, yhteistyö organisaation sisällä ja sisäisen tarkastuksen potentiaalin parempi hyödyntäminen tulevaisuudessa. Raikaslehto kävi läpi tuloksia kahdesta PwC:n survey-tutkimuksesta: ”2014 Risk in Review” ja ”2014 State of the Internal Audit Profession Study”. Merkittävimpiä tuloksia oli, että johdon näkemyksen mukaan sisäisen tarkastuksen on vielä paremmin linjattava työnsä ja kykynsä vastaamaan sidosryhmien odotuksia tuottaakseen sidosryhmille lisäarvoa. **Kristiina Lagerstedt** esitteli Sanomassa toteutettua lähestymistapaa organisaation strategian, riskien ja tarkastuksen linjaamiseen.

Ammatillista ajankohtaisasiaa toi mukanaan **Charlotta Löfstrand-Hjelm** (Swedish National Grid) kertoessaan sisäisen tarkastuksen ammattistandardien muutoksista. Työryhmässä (IPPF Relook Task Force) mukana ollut Löfstrand-Hjelm esitteli valmistelevan tahon näkökulmia muutosten tarpeellisuudesta ja suhtautui kriittiseenkin palautteeseen avoimesti.

Julkissektoritoimikunnan valmistelemalla linjalla kuultiin luentoja aiheista ISO 31000 (**Kattelus**, Espoon kaupunki), sisäministeriön ja poliisin riskienhallinnan tarpeiden huomioiminen ja toteutus (**Pennanen**, sisäministeriö & **Tienhaara**, Poliisihallitus) sekä kuntalain uudistus (**Kiviaho**, FCG Konsultointi Oy). ■

Matkalla loistavaksi tarkastajaksi

Johanna Salo, CIA
sisäinen tarkastaja, UPM-Kymmene Oyj
koulutustoimikunnan jäsen

Puolisentoista vuotta sitten sain mahdollisuuden siirtyä sisäisen tarkastajan tehtävään monialaisessa kansainvälisessä pörssiyhtiössä. Tuore tarkastusjohtaja oli vakuuttava. Hän kuvasi visionsa tarkastusosastosta juuri sellaiseksi kuin olin toivonut; strateginen, lisäarvoa ja faktapohjaista läpinäkyvyyttä ylemmälle johdolle tuottava, ketterästi toimiva ja ammattistandardeja kunnioittava erikoisrykmentti, johon halutaan eikä jouduta.

Päätin ottaa riskin ja toivoa, että toimintaympäristön tahtotila ja kypsyysaste osuisivat edes lähelle tulevan esimieheni näkemystä.

Tarkastusjohtaja totesi palkkaustilanteessa, että sinusta tulee vielä loistava tarkastaja. Paino sanoilla ”tulee” ja ”vielä”, joita mielessäni silloin hämmästelin. Nyt tiedän paremmin. Vielä viidentoista vuoden työ- ja puolentoistavuoden tarkastuskokemuksen jälkeen olen nöyrästi, mutta määrätietoisesti, matkalla.

Arvostus on ansaittava

Mielestäni sisäisen tarkastuksen tulisi olla sisäisen valvonnan keihäänkärki, sillä se keskittyy koko yrityksen toiminnan kirjoon objektiivisesti ja riippumattomasti. Sisäinen tarkastus katsoo strategisia tavoitteita riskivinkkelistä nykyhetkestä eteenpäin, toisin kuin tilintarkastus, joka katsoo pääsääntöisesti tilitietojen oikeellisuuden näkökulmasta mennyttä maailmaa. Linjan vaatimustenmukaisuus ja kontrollitoiminnot taas keskittyvät kukin omiin operatiivisiin siiloihinsa.

Suotuisista lähtökohdista huolimatta sisäinen tarkastus joutuu monessa yrityksessä kamppailemaan olemassaolonsa puolesta. Todellinen mandaatti ja arvostus eivät synny hallituksen hyväksymää toimintaohjetta lukemalla. Oikotietä onneen ei ole.

Arvostukseen päästään näkemäni perusteella vain ja ainoastaan piinkovalla ammattitaidolla, jonka ansiosta Korporaation ykköstykkien moninaisiin avauksiin voidaan vastata kumppanuudella eikä tynnyrin sisältä huutelemalla.

Ei riitä että osaa tarkastustonttinsa salat ja sisäisen tarkastuksen ammattistandardit selkäytimestä. Huippuosaajat kykenevät verkostoitumaan hyvin erilaisten persoonallisuuksien kanssa, viestimään vakuuttavasti niin kirjallisesti kuin suullisesti ja ymmärtämään että juuri tarkastustehtävissä ollaan ensisijaisesti palveluammatissa. Näiden perusseikkojen oivaltaminen ja käytäntöön vieminen johtavat väistämättä lisäarvon tuottamiseen.

Kun kovaa evidenssiä lisäarvon tuottamisesta syntyy, pisteitä satelee tarkastusosaston laariin. Yhteydenottoja tulee enemmän sisään kuin mitä niitä lähtee tarkastuksen vuosisuunnitelman puitteissa ulos. Asiakas on tyytyväinen. Viime kädessä kivaa on osakkeenomistajilla.

Kyylä vai konsultti?

Sisäisen tarkastuksen painopistealueet riippuvat yleensä yrityksen terveystilanteesta, hallintomallin ja sisäisen valvonnan kypsyysasteista sekä eettisistä arvoista. Kehittyneimmissä organisaatioissa operatiivisia sisäisen valvonnan tehtäviä tehdään yhä enemmän linjaorganisaatiovetoisesti. Näin ollen sisäinen tarkastus voi keskittyä kokonaiskontrolliympäristön varmennukseen ja strategiseen, riskilähtöiseen rooliin.

Perinteisen kyylän – eli väärinkäytösten valvojan – tehtäviä ei voi eikä sovi kokonaan unohtaa vaikka niin olisikin trendikästä tehdä. Jokaisen sisäisen tarkastajan tulisi olla perillä väärinkäytösten riskeistä, indikaattoreista ja tietää, missä kohtaa lisätutkinta on tarpeen. Yritän muistuttaa itseäni siitä, että kukaan pelisääntöjä noudattava ei lähtökohtaisesti pelkää poliisia.

Strategisen sparraajan hattu ja poliisin koppalakki eivät mahdu ainakaan minun päähäni samanaikaisesti. Ne kuitenkin voivat toimia uskottavasti samassa päässä eri aikaan, mikäli vuoropuhelua rooleista, vastuista ja velvoitteista on käyty riittävästi.

Haasteista kiitollinen

Sisäisen tarkastajan työ voi tarjota paljon, jos toimintaympäristö on otollinen ja sisältä kumpuava motivaatio muuntuu kovaksi työksi. Kommelluksilta ja haastavilta kohtaamisilta ei voi valitettavasti välttyä, jos agendalla on ihan oikeasti merkityksellisiä asioita.

Haasteisiin suhtautumistaan ja valmiuksiaan voi onneksi kehittää ja näin kasvaa aina vain paremmaksi yhtiön edun palvelijaksi. Minä olen saanut laadukasta esimiesohjausta sekä sparrausta kokeneemmilta kollegoiltani. Lisäksi olen osallistunut koulutuksiin, kuten IIA Finlandin sisäisen tarkastuksen ammattikurssille (STAK1) sekä CIA-valmennukseen, jotka antavat hyvän pohjan ammatillisen identiteetin kehittymiselle.

Vaikka sisäisen tarkastuksen tehtäviä voi hoitaa hyvin monella eri tasolla ja tavalla, tässä työssä ei voi nähdäkseni olla koskaan liian hyvä. Matka edes ”loistavaksi tarkastajaksi” tuntuu kylmäävän pitkältä.

Ammattikuntansa parhaat sisäiset tarkastajat, joista ei uskoakseni ole ylitarjontaa, ansaitsevat tuntea sisällään suurta ammattiylpeyttä – ylpistymättä kuitenkaan liikaa. ■

Eettinen toimikunta tutuksi

Freeimages.com

Eettinen toimikunta perustettiin aikanaan valvomaan yhdistyksen jäsenten toiminnan eettisyyttä. Siihen tarpeeseen sitä ei koskaan ole varsinaisesti tarvittu. Sitä vastoin tehtävänämme on ollut seurata eettisten asioiden käsittelyä yhteiskunnassa ja auttaa sisäisiä tarkastajia eettisyyden kehittämisessä ja arvioinnissa.

Standardimme edellyttävät sisäisiltä tarkastajilta tässä aihepiirissä kolmea asiaa. Meidän pitää: 1) noudattaa sisäisen tarkastuksen eettisiä periaatteita, 2) arvioida organisaatioidemme etiikkaan liittyvien tavoitteiden ja toimenpiteiden toimivuutta sekä 3) tukea organisaatioitamme etiikan ja arvojen edistämisessä. Kaikkien näiden osalta olemme tehneet eettisessä toimikunnassa työtä.

IIA Globalin presidentti **Richard Chambers** nosti sisäisen tarkastuksen eettisten periaatteiden noudattamisen korkealle omalla agendallaan muutama vuosi sitten ja niin teki myös eettinen toimikunta. Laadimme asiasta artikkeleita alan lehtiin ja olemme käsitelleet niitä seminaareissa ja koulutuksissa. Viime vuonna teimme aihepiiristä videon, joka löytyy Youtubesta hakusanoilla "eettisesti oikein". Linkki videoon on myös yhdistyksen kotisivuilla.

Olemme laatineet useita työkaluja organisaation eettisten tavoitteiden ja toimenpiteiden arviointiin, kuten erilaisia kysymyslistoja ostopalveluihin, rekrytointiprosessiin ja työntekijän poislähtöprosessiin.

Etiikan ja arvojen edistämistä ajatellen olemme laatineet mm. eettisen ohjeen (Code of Conduct) rungon, eettisten asioiden yleisen tarkastuslistan, kyselyrungon tilannearvion tekemiseksi sekä benchmark-tyyppisen listan eettisten asioiden organisoinnista ja järjestämisestä organisaatiossa. Kaikki laatimamme dokumentit ovat jäsenten käytettävissä yhdistyksen kotisivuilla (Sisäinen tarkastus –> Sisäisen tarkastuksen periaatteet ja ohjeet –> Eettiset työohjeet).

Toimikunta on kokoontunut noin kuukauden välein lomakausia lukuun ottamatta ja työssä ovat viime vuonna olleet mukana:

- **Merja Kangas**, sisäinen tarkastaja, LähiTapiola
- **Arja Karkola**, CIA, tarkastusjohtaja, Metsähallitus
- **Eila Koivu**, CIA, CFE, CCSA, Senior Advisor, Tmi Koivu Consulting
- **Taisto Leppänen**, kehittämispäällikkö, Kela
- **Jari Lemetyinen**, tarkastuspäällikkö, Raha-automaattiyhdistys
- **Helka Lukka**, Senior Audit Manager, Microsoft Mobile Oy
- **Outi Nieminen**, CIA, Yrityssuunnittelun asiantuntija, Pohjolan Voima Oy
- **Kari Storckovius**, CIA, CRMA, Audit Manager, Cargotec Oyj
- **Pirjo Tarkkanen**, CIA, CCSA, sisäisen tarkastuksen johtaja, HOK-Elanto
- **Christina Varis**, CIA, sisäinen tarkastaja, UPM-Kymmene Oyj
- **Pirkko Östring**, VP Rating and Collateral Valuation, Danske Bank

Eettisten periaatteiden vastainen toiminta on organisaatiossa aina vakava riskitekijä, ja eettisten toimintatapojen noudattaminen ja edistäminen, sekä niihin liittyvä valvonta onkin siksi tärkeää. Sisäisen tarkastuksen ammattistandardit velvoittavat tarkastusta edistämään organisaationsa eettisiä toimintaperiaatteita ja arvoja arvioimalla johtamis- ja hallintojärjestelmää, sekä antamaan siihen liittyviä suosituksia.

Sisäiset tarkastajat tekevät ratkaisuja usein monimutkaisissa tilanteissa, eikä tarkastajan työssä ole harvinaista joutua ristiriitatilanteisiin, joissa eettiset periaatteet joutuvat koetukselle. Tarkastajien toimintaa ohjaavat ammattistandardien lisäksi monet eri ohjeet, joissa käsitellään ammattietiikkaa ja sisäisen tarkastuksen eettistä toimintaa, mutta miten luovia menestyksekkäästi kaiken ohjeistuksen keskellä? Tähän kysymykseen vastatakseen eettinen toimikunta on koonnut ohjeen "Eettinen toiminta ja sisäinen tarkastus", joka auttaa tarkastajia hahmottamaan "eettisyyden pelikentän" ja tukee oman organisaation toiminnan arvioinnissa. Ohjeessa on tunnistettu mm. asioita, joita organisaatiossa tulee ohjeistaa ja kouluttaa eettisen toiminnan kulttuurin vahvistamiseksi. Voit tutustua ohjeeseen Sisäiset tarkastajat ry:n jäsensivustolla! ■