Päivö Lappalainen
paivo.lappalainen@ely-keskus.fi
ELY tietohallintoyksikkö

VM:n lausuntopyyntö VAHTI- arviointiohjeen luonnoksesta

LAUSUNTO TIETOTURVALLISUUDEN ARVIOINTIOHJELUONNOKSESTA

Arviointiohjeluonnoksen mukaan viranomaisten tietoturvallisuuden arviointi jakautuu hallinnollisen tietoturvallisuuden ja viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden arviointiin. Hallinnollisissa arvioinneissa tarkastellaan viranomaisten tietoturvallisuuden hallintajärjestelmän kattavuutta ja toimivuutta, ja ne kohdistuvat toimintaprosesseihin ja menettelytapoihin. Ohjeessa todetaan, että arvioinnissa täytyy aina olla jokin viitekehys tai vaatimuskokonaisuus, jonka pohjalta arviointi toteutetaan. Hallinnollisissa arvioinneissa viitekehys voi olla esimerkiksi sopimus tai tietoturvastandardi tai valtionhallinnon viitekehys, kuten tietoturvataso. Arviointitapoina ohjeessa tuodaan esiin itsearviointi, sisäinen arviointi tai tarkastus, vertaisarviointi tai ulkoinen arviointi. Ohjeessa pidetään tietoturvallisuuden jatkuvan kehittämisen kannalta suositeltavana sitä, että hallinnollista arviointia tehtäisiin itsearviointina säännöllisin väliajoin.

Hämeen ELY-keskus pitää tärkeänä sitä, että hallinnollisen tietoturvallisuuden arvioinnissa ja kehittämisessä otettaisiin käyttöön menettelyt, jotka nykyistä tiiviimmin osallistaisivat hallinnollisen organisaation johtajat, päälliköt ja tiiminvetäjät tietoturvallisuuden edistämiseen ja kehittämiseen omissa toimintayksiköissään ja tiimeissään. ELY-keskus ehdottaa, että tietoturvallisuuden arviointi liitettäisiin suunnitelmallisesti osaksi ELY-keskusten ja TE-toimistojen säännöllisesti toistuvia sisäisen valvonnan ja riskienhallinnan tilaa seuraavia COSO-ERM-kyselyitä ja toiminnan kehittämisen yleisenä viitekehyksenä käytettyä CAF-kuvausta ja -arviointia.

COSO-ERM-kysely

Organisaation sisäisen valvonnan ja riskienhallinnan tilaa ja kehittämistarpeita kartoittava COSO-ERM-kysely tehdään joka toinen vuosi. Kysely tehdään sähköisesti, ja sen organisoi keskitetysti ELY-keskusten talous- ja henkilöstöhallintoyksikössä toimiva sisäinen tarkastus yhteistyössä kunkin ELY-keskuksen (ja TE-toimiston) sisäisen valvonnan yhteyshenkilön kanssa. Yhteyshenkilö organisoi kyselyn omassa organisaatiossaan, kokoaa sen tulokset ja valmistelee niiden pohjalta organisaation johdon hyväksyttäväksi kaksivuotisen sisäisen valvonnan ja ris-

kienhallinnan toimintasuunnitelman, jossa todetaan organisaation keskeiset kehittämiskohteet ja jonka toteutumista seurataan säännöllisesti.

Tietoturvakysymykset ovat olennainen ja luonteva osa organisaation sisäisen valvonnan ja riskienhallinnan kokonaisuutta, ja tietoturvallisuuden toimintaprosessien ja menettelytapojen tilan ja niiden kehittämistarpeiden kartoittaminen voitaisiin hyvin sisällyttää organisaation sisäisen valvonnan itsearviointiin. **COSO-ERM-kyselyä tulisi kehittää niin, että siihen sisällytettäisiin nykyistä järjestelmällisemmin myös organisaation tietoturvallisuutta ja sen kehittämistarpeita kartoittavia kysymyksiä.** Organisaation sisäisen valvonnan yhdyshenkilö ja tietoturvavastaava voisivat käsitellä yhdessä tietoturvallisuutta koskevat kyselyvastaukset ja valmistella kehittämisehdotukset, ja ne voitaisiin käsitellä myös organisaation sisäisen valvonnan ja riskienhallinnan ohjausryhmän ja tietoturvallisuusryhmän yhteisessä kokouksessa ja sisällyttää sisäisen valvonnan ja riskienhallinnan toimintasuunnitelmaan, joka viedään johdon hyväksyttäväksi.

CAF-kuvaus ja -arviointi Vuorovuosin COSO-ERM-kyselyn kanssa ELY-keskuksissa ja TE-toimistoissa laaditaan organisaation CAF-mallin mukainen kuvaus ja tehdään CAF-itsearviointi. Myös CAF-kuvauksiin sopii hyvin sisällyttää organisaation tietoturvallisuutta koskevia seikkoja. CAF-arviointimallin mukaan erityisesti arviointialueella 4 (Kumppanuudet ja resurssit) on arviointikohtia, joihin voisi liittää nykyistä järjestelmällisemmin tietoturvallisuuteen liittyviä seikkoja: CAF-mallin arviointikohdissa 4.4.–4.6 kysytään, kuinka organisaatio johtaa tietoa, teknologiaa ja toimitiloja. Arviointialueella 5 (Prosessit) voisi ehkä tarkastella myös prosessien tietoturvallisuuteen liittyviä näkökohtia. **Koko CAF-arviointimalli tulisi käydä läpi siitä näkökulmasta, kuinka eri arviointialueiden kuvaukseen voitaisiin ottaa mukaan myös tietoturvallisuutta koskevia näkökulmia**, ja asia tulisi ottaa mukaan ohjaavalta taholta (tai tulevalta KEHAlta) saatavaan ohjeistukseen CAF-kuvausten ja -arviointien tekemisestä. CAF-arviointi voidaan toteuttaa myös vertaisarviointina, joka on myös tietoturvallisuuden arviointiohjeessa mainittu arviointitapa.

Ylijohtajan sijainen,
johtaja Tommi Muilu

Yksikön päällikkö Riitta Turunen