

Verohallinto
PL 325
00052 VERO

LAUSUNTO A25/00 00 01/2014

4.8.2014

Lausunto Tietoturvallisuuden arviointiohjeen luonnoksesta 13.06.2014

VM JulkiCT:n lausuntopyyntöön 13.6.2014 Verohallinto vastaa seuraavasti:

Ohjeluonnos antaa hyödyllisen ja kattavan kuvauksen tietoturvallisuuden arvioinnista. Siinä konkretisoidaan käytännön toimien, kuten auditointien, toteuttaminen ja vastuut. Ohjeessa kuvataan selkeästi, mitä hyötyjä saavutetaan tietoturvallisuuden jatkuvalla, oikein kohdistetulla arvioinnilla.

Tietoturvallisuuden arvioinnin taustavaatimukset, arviointiperusteet ja käytännön toteutus erilaisissa käyttötapauksissa kuvataan havainnollisesti. Eri tasojen vaatimukset, ohjeistukset ja toteutuksen aikataulutus esitetään hyvin. Arviointiin osallistujien roolit ja vastuut sekä liittyvä lainsäädäntö ja velvoitteet on koostettu selkeästi ja kattavasti.

Esimerkeillä konkretisoidaan hyvin tiedon käsittelyn, salaamisen ja turvallisuustoimien erityispiirteitä ja -vaatimuksia, kun tietoja siirretään ja käsitellään Suomen rajojen ulkopuolella. Lainsäädännön katsaus on niin hyvä, että se voisi olla oma asiakirjansa, johon viitattaisiin muistakin VAHTI-ohjeista. Luvun tietoturvallisuuden tasovaatimukset kolmas kappale riskien hallintapäätöksistä on tärkeä yksityiskohhta.

Tuomme esiin seuraavia parantamismahdollisuuksia:

- Kappaleissa Tietoturvallisuuden arviointiperusteet ja Katakri voisi olla risti-viittaukset toisiinsa, sillä molemmissa läpikäydään myös kansainvälisen erityissuojattava tietoaineiston käsittelyä. Näiden kappaleiden järjestyksen vaihtaminen keskenään parantaisi luettavuutta.
- Liitteen 2 kohdan Valtori toisella kappaleella voisi olla oma otsikkonsa, esimerkiksi Viranomainen / muuta.
- Osassa tietojärjestelmähankkeiden arviointi (s. 23) olisi hyödyllistä antaa linkit mainittuihin valtionhallinnon yhteiseen arviointikehikkoon ja kustannus-hyötyanalyysin mallipohjaan.
- Käsitteistö kaipaisi täsmennystä. Esimerkiksi sisäisen tarkastuksen ja valvonnan ero ei selviä niiden määritelmistä. Toisena esimerkkinä arviointi ja tarkastus on määritelty itse asiassa synonyymeiksi. Jos ohjeessa tarvitaan vain toista termiä, olisi selvintä käyttää vain sitä johdonmukaisesti.
- Ohjetta olisi mahdollista tiivistää jättämällä pois joitakin itsestään selviä toteamuksia ja fokuoimalla sitä vielä enemmän nimenomaan käsiteltävään aiheeseen.

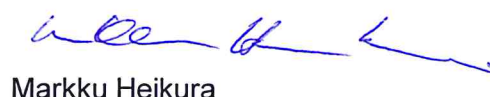
Helsinki 8.8.2014

Pääjohtaja



Pekka Ruuhonen

Tietohallintojohtaja



Markku Heikura