Elinkeino-, liikenne- ja ympäristökeskus

Etelä-Savo, ELY tietohallinto

Lausunto

13.8.2014 ESAELY/757/2014

Valtiovarainministeriö
valtiovarainministerio@vm.fi

Lausuntopyyntö Tietoturvallisuuden arviointiohje,VM047:21/2007, 1862/00.01.00.01/2012

Elinkeino-, liikenne ja ympäristökeskuksen lausunto Tietoturvallisuuden arviointiohjeesta

Ohje on sinänsä kovin tarpeellinen ja pääpiirteisään hyvä. Ohjeesta on toisaalta välillä vaikea saada konkreettisia työkaluja johtuen ohjeen ajoittaisesta ympäripyöreydestä. Ohjeessa on paljon viittauksia muihin Vahti-ohjeisiin, mutta varsinaista kokoavaa otetta joutuu välillä etsimään.

Muita kommentteja:

- olisiko hyödyllistä tuoda vielä voimakkaammin esiin arvioinnin kehittävä näkökulma muuallakin kuin kohdassa arvioinnin hyödyt? Lisäksi olisi syytä kiinnittää enemmän huomiota arvioinnin jälkeiseen kehittämistoimintaan. Koska arviointi toistuu vuosittain, niin vaarana on, että kehittämisestä luistetaan ja se kuitataan vain jollakin vastineella.

- Lainsäädäntöosio on hyvä kooste toimintaa ohjaavasta lainsäädännöstä ja tarkastavista viranomaisista/laitoksista. Tätä osaa voisi tiivistää. Käytännön arvioinnin suunnittelijalla voisi olla enemmän hyötyä taulukkomaisesta esitystavasta, jossa olisi kuvattu viittauksin kutakin toimintaa ohjaava lainsäädäntö (lainsäädännön tarkastuslista). Osittain tämä on tehtykin VAHTI- ohjeistuksen osalta.

- **Arviointiperusteet/perusteiden yhteensovittaminen:** Tietoturva-asetus, ISO27001 – standardi, KATAKRI, vahti- ohjeet on kuvattu kattavasti. Ohjeluonnoksessa ei ole käsitelty yksityiskohtaisesti eri kriteereiden yhteensovittamista. Tämä tarve on ainakin ELY-keskuksilla, joita velvoittaa toisaalta tietoturva-asetuksen vaatimukset ja toisaalta virastolle delegoitujen maksatustehtävien tietoturvavaatimukset, jotka perustuvat ISO27001- standardiin. Samoja tietoturvavaatimuksia arvioidaan tästä johtuen erillisinä prosesseina , mikä sitoo virastojen entisestään supistuvia voimavaroja tietoturvallisuuden hallinnan osalta. Valtori on julkaissut työkaluja, joiden avulla voidaan yhteen sovittaa eri arviointivaatimuksia. Niistä voisi olla maininta ja viittaukset tässäkin ohjeessa.

- **Toimeksiantosuhteen arviointi s 17**: Viittaukset muihin Vahti-ohjeisiin (Vahti 3/2011, 2/3013) ok. Tässäkin voisi mainita Valtorin tarjoamat hankintojen apuvälineet, joita on päivitetty vastikään tänä keväänä. Selkeä jaottelu hankintojen tietoturvavaatimuksista hankintaosapuolien edustamien tahojen osalta.

- **Arvioinnin suorittaminen:** arviointiprosessin kulku kuvattu selkeästi s. 26- 30.

Kommentteja ely- keskuksista

- 1. Sivu 13: perustaso on esitetty liitteessä 4, ei liitteessä 3, kuten tekstissä väitetään (sama virhe muuallakin).
-
- 2. Yleiskommentti: Tietoturvan suunnittelun, hallinnan ja arvioinnin näkökulmasta ohjeet ovat varsin asialliset sellaisen valtion viraston näkökulmasta, jolla on kaikki langat omissa käsissään.
- Kun ko. ohjetta (ja vastaavia ohjeita) lukee yksittäisen ELY-keskuksen näkökulmasta, tulee sellainen vaikutelma, että meillä ei ole näkyvyyttä moneen tietoturvaan liittyvään asiaan (esim. tekninen tietoturva vs. AHTI).
- Toki tämä ei yksin ohjeen vika, vaan liittyy laajemmin organisaatiorakenteisiin, palvelukeskusrakenteisiin ja vastuiden jakoon.
-
- 3. Sivu 34: "Perustason täyttyminen todennetaan ulkoisella arvioinnilla.". Ymmärtääkseni kaikkia ELY-keskuksia ei auditoida eikä kaikille suoriteta ulkoista arviointia, vaan kun muutama ELY on auditoitu ja/tai arvioitu, oletetaan niiden edustavan riittävän hyvin koko joukkoa (voi olla, että olemme ymmärtäneet tämän väärin). Jos näin on, pitäisikö tämä "otoksen perusteella arviointi samankaltaisten virastojen kohdalla" ottaa huomioon tekstissä?
-
- 4. Liite 1: Benchmarkingin määrittely: voi olla hiusten halkomista, mutta oman kokemukseni mukaan benchmakingissa ei haeta pelkästään parhaita käytäntöjä, vaan joissain tapauksissa myös ns. "epäonnistuneita caseja", joiden kohdalla opetus on tyyppiä "älä tee ainakaan näin".
- Netistä ja kirjallisuudesta löytyykin jonkun verran "benchmarking worst practices"-tyyppisiä lähteitä, esim:
- http://www.ideaconnection.com/right-brain-workouts/00245-benchmarking-worst-practices.html

Liitteenä Hämeen ELY- keskuksen lausunto kokonaisuudessaan.

Johtaja Mika Koskinen

Tietoturva-asiantuntija Päivö Lappalainen

Tiedoksi ESELY kirjaamo, ELY – keskukset
Liitteet Hämeen ELY- keskuksen lausunto

Elinkeino-, liikenne- ja ympäristökeskus

Lausunto HAMELY/1036/2014

Häme 7.7.2014

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