

**Nixu Certification Oy:n lausunto VAHTI:n ohjeesta 3/2016
Tietoturvapoikkeamatilanteiden hallinta**

Nixu Certification Oy sai tiedon VAHTI:n Tietoturvapoikkeamatilanteiden hallinnan ohjeen lausuntopyynnöstä 10.10.2016 vain muutamia tunteja ennen määräajan umpeutumista. Emme tällä aikataululla pysty kommentoimaan ohjeen sisältöä tai sen vaatimusten auditoitavuutta.

Jotta tilanne ei toistuisi, esitämme että VAHTI pyytää automaattisesti kommentteja Viestintäviraston hyväksymiltä arviointilaitoksilta, mikäli näiden pätevyysalueeseen kuuluu VAHTI-tarkastukset.

Ottamatta mitään kantaa yksittäisessä ohjeessa esitettyihin vaatimuksiin, haluamme tuoda esiin VAHTI:n tietoturvavaatimusten suuren määrän ja tästä seuraavan auditoinnin suuren koon. Tämä asia on Valtionhallinnon tietoturvallisuuden ohjaukseen kuuluva, ei yksittäisen ohjeen laatineen työryhmän.

Tietoturvapoikkeamatilanteiden hallinnan ohjeen tultua hyväksytyksi on luontevaa, että se sisällytetään arviointilaitosten VAHTI-pätevyysalueeseen. Tämä nostaa auditoitavissa olevien VAHTI-vaatimusten määrän noin 1300:n. Näitä on kolmelle tietoturvasolulle, jolloin taso-vaatimus -yhdistelmiä on suunnilleen 3900. Yksittäisen vaatimuksen velvoittavuudelle on aina vähintään kolme vaihtoehtoa (pakollinen, vahva suositus ja suositus), jolloin vaatimus-taso-velvoittavuus -kohtia on n. 11700. Yksittäiset ohjeet käyttävät useita muita velvoittavuuden asteita, joten kokonaismäärä on suurempi. Vertailukohtana mainittakoon, että mikäli organisaatio on valinnut kaikki ISO 27001 Liite A:n kontrollit, on auditoitavia kohtia varsinaisessa standardissa ja Liitteessä A yhteensä noin 250.

Niki Klaus
Toimitusjohtaja

Olli-Pekka Soini
Päätarkastaja