Nixu Certification Oy
Olli-Pekka Soini
Keilaranta 15B
FI-02150 ESPOO

Valtiovarainministeriö
PL 28
00023 VALTIONEUVOSTO
valtiovarainministerio@vm.fi

Arviomuistio julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeista

Lausuntopyynnön diaarinumero: VN/4400/2021

Lausunto

Kommentit muistion kohtiin

Kiitämme mahdollisuudesta lausua tietojärjestelmäauditointien ja arviointilaitostoiminnan kehittämisestä.

Pitäisimme hyvänä, että valtiovarainministeriö ja Traficom kertoisivat arviointilaitos-toimintaa kehittävien työryhmien toimeksiannosta suoraan arviointilaitoksille, ja pyytäisivät lausuntoa suoraan näiltä.

Työryhmän raportin osuuksia, jotka koskevat tekoälyn hyödyntämistä ja EU-säätelyn vaikutuksia emme ajan puutteen vuoksi kommentoi.

Pidämme hyvänä, että tietoturvan kehittämistä tehdään hallinnonalojen välisenä yhteistyönä.

Nixu Certifícation Oy on osa Nixu-konsernia. Teemme sertifiointiauditointeja ISO 27001, Katakri ja Vahti -auditointikriteeristöjä vasten. Teemme M72 -arviointeja sekä toisiolain perusteella annetun Findatan määräyksen mukaisten käyttöympäristöjen arviointeja.

1) 9.1.1 NLF-asetus ja akkreditointilaki

” NLF-pakettiin liittyvä sääntely (NLF-asetus ja -päätös sekä pakettiin kuuluvat tuotedirektiivisäännökset) lähtee siitä, etteivät kansalliset akkreditointielimet tai ilmoittamisesta vastaavat toimivaltaiset viranomaiset (jollainen myös Liikenne- ja viestintävirasto on esim. radiolaitteiden ja ilmailulaitteiden osalta) saa olla mukana arviointilaitostoiminnassa. Kansalliset akkreditointielimet eivät saa kilpailla vaatimustenmukaisuuden arviointilaitosten kanssa eikä ilmoittamisesta vastaava toimivaltainen viranomainen saa tarjota tai suorittaa mitään toimintoja, joita vaatimustenmukaisuuden arviointilaitokset tekevät.”

Nykytilanteessa arviointien toimivaltainen viranomainen Traficom tarjoaa samoja palveluita kuin arviointilaitokset, jotka se akkreditoi. Jopa yksityisten yritysten arvioinnissa tämä aiheuttaa kilpailutilanteen, mutta etenkin julkishallinnossa tilanne on kilpailu: Traficom tarjoaa samoja TLIV- ja TLIII-arviointeja, joita tekevät myös arviointilaitokset. Viranomaisen hinnoittelu määräytyy maksuperustelain mukaan, ja päivähinta on merkittävästi edullisempi kuin markkinaehtoisten toimijoiden. Suurin osa arvioinneista tehdään julkishallintoon.

Traficom on ilmaissut halunsa luopua TLIV-auditoinneista, ja antaa ne arviointilaitosten tehtäväksi.

Katsomme, että Traficomin ei tulisi tehdä arviointeja, kuin milloin sen hankkiminen arviointilaitokselta ei lainsäädännöstä johtuen ole mahdotonta.

2) 9.1.2 Arviointilain ja arviointilaitoslain mukainen arviointi ja todistus

” Arviointilain mukaan valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain kyseisessä laissa tarkoitettua menettelyä (Liikenne- ja viestintäviraston suorittama arviointi) taikka sellaista arviointilaitosta, joka on saanut Liikenne- ja viestintäviraston hyväksynnän tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011, arviointilaitoslaki) mukaan.”

Arviointilaissa on selkeästi kielletty muiden kuin laissa mainittujen käyttäminen tietojärjestelmien arviointiin. Määräys on käytännössä kuollut kirjain: viranomaiset tilaavat erilaisia arviointeja muiltakin, ei vain arviointilaitoksilta, eikä niissä käytetä ns. arviointilaitosmenetelmiä.

Katsomme, että joko vaatimusta käyttää ainoastaan laissa mainittuja aletaan noudattaa, tai säädös muutetaan vastaaman todellisuutta, jossa arviointeja tekevät muutkin. Vaihtoehtoisesti voidaan rajata tietyn tyyppiset auditoinnit arviointilaitoksille, ja sallia muiden käyttö muissa tapauksissa, esimerkiksi kun tietojärjestelmässä ei käsitellä salassa pidettävää aineistoa.

3) 9.1.2 Arviointilain ja arviointilaitoslain mukainen arviointi ja todistus ja 9.2.3 Arviointilaitosten hyväksyminen, hyväksyjä ja valvonta

”Arviointilaitoslaissa säädetyt edellytykset arviointilaitoksen hyväksymiselle ovat hyvin yleisluontoiset. Tämä on johtanut siihen, että hyväksyntä perustuu suurelta osin Liikenne- ja viestintäviraston antamaan ohjeeseen tietoturvallisuuden arviointilaitoksille (Ohje 210/2016 O) – eli ei sitovaan normistoon.”

Arviointilaitoksen hyväksyntä eli akkreditointi perustuu osin mainittuun Arviointilaitosohjeeseen, mutta vain ylätasolla. Käytännön työssä hyväksynnän saamisen vaatimat työt eivät ilmene Arviointilaitosohjeesta, vaan ne saadaan suullisesti, sähköpostilla ja vaihtelevilla tavoilla. Todennusmenetelmien tekeminen, näyttöauditointi ja ns. kotitehtävät ovat esimerkkejä pätevyyden osoittamiseen käytetyistä keinoista, jotka ovat sinällään hyvät, mutta pätevyyttä haluavalle arvioitilaitoskandidaatille nämä selviävät matkan varrella, vähitellen, ei ensimmäisessä kokouksessa saadun määräyksen tai ohjeen perusteella. Akkreditoinnin tulisi olla yhtä lailla määrämuotoinen prosessi kuin on auditointi.

” Arviointilaitosten hyväksymistä koskevat vaatimukset on arviointilaitoslaissa säädetty yleisellä tasolla siten, ettei niiden perusteella voida muodostaa selkeää kokonaiskäsitystä siitä, mitkä ovat konkreettisia vaatimuksia arviointilaitoksille. Tältä osin sääntelyä voidaan pitää epätäsmällisenä, tulkinnanvaraisena ja puutteellisena. Sääntely jättää harkintavaltaa arviointilaitoksen hyväksyvälle viranomaiselle, jolloin tällaisten vaatimusten täyttämistä koskevat soveltamisohjeet voivat sisältää konkreettisia vaatimuksia, joiden tulisi olla lakitasoisia.

Toisaalta tietojärjestelmien arvioinnissa vaatimuksenmukaisuuden todentaminen kohdentuu arvioinnin tekevän tarkastajan tai muun asiantuntijan ammatilliseen pätevyyteen, jolloin arvioinnin tekijän kelpoisuutta ei voida kohdentaa pelkästään yleisesti organisaatioon, vaan myös tosiasiassa arviointeja tekeviin henkilöihin.”

Arviointilaitokseksi hakeutuvalla on epäselvä kuva siitä, mitä kaikkea hakemuksen hyväksyminen edellyttää, ja raportin ehdotus tämän selkeyttämisestä on kannatettava. On lisättävä, että vaatimukset ovat varsin kovat, jotta auditointitoiminnan laatu pysyy hyvänä. Emme näe perustetta vaatimusten lieventämiselle.

Vaatimusten asettaminen on tehtävä normihierarkiassa riittävän alhaisella tasolla, jotta muuttuvassa maailmassa tarpeellinen joustavuus säilyy.

4) 9.1.2 Arviointilain ja arviointilaitoslain mukainen arviointi ja todistus

” Lisäksi nykytilanteen eräänä haasteena on, että arviointilaitosten osaamisalueet eivät täysin vastaa viranomaisarvioinnilta (eli Liikenne- ja viestintäviraston tekemältä arvioinnilta) vaadittavaa sisältöä, ja arviointilaitosten pätevyysalueita on jouduttu hyväksymään osittaisina. Arviointilaitosten pätevyysalueet eivät kata esimerkiksi salausratkaisujen, yhdyskäytäväratkaisujen tai hajasäteilysuojausten riittävyyden arviointia kuin osittaisina ja rajauksin”

Arviointilaitosten pätevyysalueen laajentaminen on pitkä ja vaativa työ, ja se edellyttää runsaasti työtä. Luultavasti enemmän kuin nykyiset arviointilaitokset ovat arviointilaitoksiksi hakeutuessaan kuvitelleet.

Katsomme, että vaikka on kaikkien edun mukaista pitää arviointilaitosten vaatimustaso korkeana, on turhaa pätevyyden osoittamista syytä välttää esimerkiksi tapauksissa, joissa vaatimusten sisältö ei ole muuttunut, mutta niiden paikka standardissa on.

Pätevyysalueita rajaa paitsi osaaminen ja pätevyyden hankkimisen kustannukset myös kysynnän määrä: vaikka kryptopätevyys olisi ammatillisesti kuinka kiinnostavaa, on arviointilaitoksen arvioitava, onko kysyntää riittävästi, jotta pätevyyden saamisen kustannukset kyetään kohtuullisessa ajassa kattamaan. Tämä pätee erityisesti hajasäteilymittaukseen. Kryptoarvioinnissa tilanne saattaa olla toinen, mutta tietoa arviointien määrästä emme ole saaneet.

Katsomme, että Traficomin ja muiden toimijoiden on kerrottava realistinen arvio auditointien määrästä pätevyysaluittain, jotta päätös niihin hakeutumisesta voidaan tehdä myös taloudellisin perustein. Näin voidaan saada aikaan tarjontaa – jos sille on riittävästi kysyntää.

5) 9.1.2 Arviointilain ja arviointilaitoslain mukainen arviointi ja todistus

”Arviointilain mukaista arviointia ei ole kansallisella tasolla säädetty pakolliseksi, eikä valtion hallinnon viranomaisella ole velvollisuutta hankkia arviointilaissa tarkoitettua todistusta siitä, että tietojärjestelmä täyttää vaatimukset”

Tilanne on kuvatun kaltainen. Arviointilakia sekä vuoden 2010 asetusta valtionhallinnon tietoturvallisuudesta säädettäessä uskoimme arviointien tulevan pakolliseksi, mutta näin ei käynyt.

On mielestämme perusteltua sanoa, että kansalaisen perusoikeuksiin kuuluu hänen asiansa tietoturvallinen käsittely viranomaisessa. On vaikea kuvitella tilannetta, jossa asianmukainen käsittely voisi olla tietoturvaton.

Katsomme, että ainakin turvaluokiteltujen tietojärjestelmien arviointi on säädettävä pakolliseksi lailla tai asetuksella. Lain olisi koskettava myös kuntia, joissa tilanne edistyneempiä kuntia lukuun ottamatta on valtionhallintoa heikompi.

Raportissa esitetty ” kevyempi, konsultoiva tietojärjestelmien tarkastus” on eräs vaihtoehto, mutta on varottava tilannetta, jossa hyvin kevyt tarkastus täyttää lain vaatimukset. Miksi vaatia asiaa, joka ei varmuudella kerro paljoakaan? Kevyet tarkastukset ja omavalvonta ovat käytössä sotejärjestelmien arvioinneissa, ja meidän mielestämme ne eivät ole riittäviä huomioiden tiedon kriittisyys. Konsultoinnin ja auditoinnin erottaminen on myös keskeinen periaate tällä toimialalla.

Kun valtionhallinnossa tehdään uusia arviointikriteeristöjä, kuten Pitukri ja JulKri, toivomme, että niissä noudatetaan arviointilakia.

6) 9.1.2 Arviointilain ja arviointilaitoslain mukainen arviointi ja todistus

” Arviointilain 8 a §:n mukaan asetuksella voidaan säätää, että valtionhallinnon viranomaisten on hankittava todistus tietojärjestelmistä tai tietoliikennejärjestelyistä, joissa käsitellään tietoja, joiden turvallisuusluokka on TL I tai TL II. ”

Missään laissa ei ilmeisesti ole säädetty pakolliseksi TLI ja TLII todistusta. On syytä harkita auditointien tai todistukseen tähtäävien auditointien tekemistä pakolliseksi yleislainsäädännössä, jos erityislainsäädäntöön ei ole tullut näitä pykäliä.

7) 9.1.7. Erityislainsäädännön arviointivaatimuksista

”Yleislainsäädännössä ei ole säädetty viranomaisille velvollisuutta hankkia todistusta tietojärjestelmän vaatimuksenmukaisuudesta taikka pyytää Liikenne- ja viestintävirastolta tai arviointilaitokselta tietojärjestelmänsä vaatimuksenmukaisuuden arviointia. ”

Auditointinen ja todistukseen tähtäävien auditointien määrä valtionhallinnossa on jäänyt odottamaamme vähäisemmäksi. Erityislainsäädännön (kuten toisiolaki ja M72A/2018) pakolliseksi tekemiä auditointeja on vastaavasti kohtuullisen paljon.

Katsomme, että tietoyhteiskunnassa ei julkishallinnon hyvän hallinnon velvoite voi täyttyä ilman tietoturvan asianmukaista todentamista todistuksella, ja katsomme, että auditointivelvoite olisi otettava yleiseen hallintolainsäädäntöön riittävän pitkällä ja vaiheittaisella siirtymäajalla.

8) 9.2.1. Tietojärjestelmien vaatimuksenmukaisuuden arviointia koskevan sääntelyn soveltamisala

” Tästä syystä kehittämiskohteena voidaan nähdä vaatimustenmukaisuuden arviointia koskevien lakien (arviointilaki ja arviointilaitoslaki) ulottaminen koskemaan nykyistä laajemmin tietojärjestelmiin kohdistuvien vaatimusten mukaisuuden arviointia.”

Kannatamme esitystä, että arviointivelvoite ulotetaan koskemaan nykyistä laajemmin. Itse asiassa yleistä velvoitetta ei tietääksemme ole lainkaan. Arviointien pakollisuus on syytä aloittaa korkeimman suojaustason järjestelmistä, ja uusista suunnitteilla olevista.

”Tässä yhteydessä – erityisesti, jos arviointi säädetään joissain tilanteissa pakolliseksi – on myös arvioitava sitä, mikä lisäarvo järjestelmän päätöksentekosääntöjen ja lain mukaisen toimintalogiikan vaatimusten täyttymistä koskevalla ulkopuolisen tahon hyväksynnällä on.”

Ulkopuolisen tekemä toimintalogiikan testaus AI-ratkaisuissa voi olla tarpeen, mutta kuten raportissa todetaan, tämän tekeminen edellyttää käsiteltävän hallintoasian tuntemista, ei tietototurva-osaamista. Arvioinnin edistäminen on hyvä asia, mutta nykyiset arviointilaitokset eivät nykyisellään ole siihen valmiita.

”*Liikenne- ja viestintäviraston tehtäväksi tietoturvallisuuden arviointiviranomaisena voitaisiin nykykäytäntöä vastaavasti säätää turvallisuusluokiteltujen (TL IV-TL I) tietojen käsittelyyn käytettyjen tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnin lisäksi (tai siihen sisältyvänä) myös toiminnan jatkuvuuden ja varautumisen vaatimustenmukaisuuden arviointi. Liikenne- ja viestintävirasto on ehdottanut, että sen arvioinnit sisältäisivät lisäksi arvioitavaan tietojärjestelmään liittyvän turvallisuusjohtamisen (hallinnollinen turvallisuus ja henkilöstöturvallisuus) arvioinnin.”*

Nykyisellään arvioinneissa tavallisesti käytetty Katakri ei juuri sisällä jatkuvuusvaatimuksia, sillä kriteeristö on laadittu nimenomaan luottamuksellisuuden suojaamiseen. Tämä linjaus päti uusimmassa Katakri 2020 -kehitystyössä. Käytännön auditointityössä tästä seuraa eriskummallisia tilanteita: esimerkiksi konesaliin häiriökestävyys voi olla olematon, mutta Katakri-todistuksen myöntämisen edellytykset täyttyvä, kun tietojen luottamuksellisuus ja eheys on turvattu. Periaatteessa on mahdollinen tilanne, jossa korkeaa käytettävyyttä valtionhallintoon myyvä konesali on toimimaton, mutta edelleen Katakrin mukainen. Tilanne on arkijärjellä ajatelleen outo.

Katsomme, että suomalaisen tietoyhteiskunnan kehitys tarvitsee aivan välttämättä jatkuvuudenhallinnan kehittämistä, ja tämän auditointia.

Katakrin perusajatus on – hieman kärjistäen – että kerran turvallinen järjestelmä on turvallinen tulevat vuodet, ja että auditointi voidaan tehdä vain I-osasta. Kannatamme vahvasti Liikenne- ja viestintäviraston ehdotusta arviointien laajuuden kasvattamisesta kattamaan turvallisuusjohtamisen, joka luo tiettyä turvaa muuttuvassa maailmassa.

Kannatamme lisäksi pakollisia vuosiauditointeja kaikissa auditoinneissa, jotka myönnetään määräajaksi.

9) 9.2.3 Arviointilaitosten hyväksyminen, hyväksyjä ja valvonta

” *Edellä esitetyistä syistä arviointilaitoslakia tulisi muuttaa siten, että siinä asetetaan sekä arviointilaitokselle että sen palveluksessa olevalle arvioitsijalle yksilöidyt vaatimukset, joita voidaan lakitasoiseen sääntelyyn perustuen valvoa. Lisäksi arviointilaitoslakia tulisi muuttaa siten, että eri viranomaistoimijoilla on selkeä ja perusteltu toimivalta päättää arviointilaitoksen hyväksynnästä ja suorittaa kelpoisuusvaatimusten noudattamista koskevaa valvontaa.”*

Nykyisessä mallissa arviointilaitokset itse asettavat kelpoisuusvaatimukset henkilöilleen, aivan kuten ISO 17021 mukaisen sertifiointielimen kuuluu. Vaatimusten sisällyttäminen vaatimuksiin ei olennaisesti muuta asioita, mutta nykyisessä mallissa emme näe ongelmaa.

Jos pätevyysvaatimukset henkilöille asetetaan, on muistettava, että liian tiukat vaatimukset vaikeuttavat henkilöiden rekrytointia arviointilaitokseen, mikä ei ole aivan helppoa nytkään. Samat vaatimukset koskisivat ilmeisesti myös Traficomin auditointeja tekevää henkilöstöä. On myös hyvä harkita, olisi ehdotettu systeemi henkilökohtaisen pätevyyden osoittava sertifikaatti.

Pätevyysvaatimusten tekeminen ja ylläpito eri auditointien osa-alueille (kuten tietoliikenneturvallisuus, turvallisuusjohtaminen, käyttöturvallisuus, pääsynhallintajärjestelmät) lienee liian mutkikas, ja vaatisi Traficomilta lisäresursseja. Koska riittämätön osaaminen ei mielestämme ole ongelma, emme kannata nykyjärjestelyn muuttamista.

10) 9.2.3 Arviointilaitosten hyväksyminen, hyväksyjä ja valvonta

”Niin ikään arviointikohde on täsmennettävä siten, että viranomainen ei voisi ulkoistaa tietojärjestelmiensä kelpoisuuden arviointia kokonaisuudessaan yksityiselle, koska sillä on merkittävä vaikutus julkisen vallan käyttöön tietojärjestelmän toiminnallisuuksia

käytettäessä esimerkiksi hallintoasiaan liittyvässä päätöksenteossa. ”

Emme voi suoraan ottaa kantaa, onko viranomaisen tietojärjestelmien vaatimuksenmukaisuuden toteaminen sellaista merkittävää julkisen vallan käyttöä, ettei sitä perustuslain mukaan voi siirtää yksityiselle, joka toimii virkavastuulla ja viranomaisen valvonnassa. Toteamme kuitenkin, että mikäli näin on, on epäjohdonmukaista, että näiden järjestelmien tietoturvallisuudelle ja tietoturvan auditoinnille ei ole laissa velvoitetta viranomaiselle, mutta jos vaatimuksenmukaisuus halutaan todeta, sen voi tehdä vain viranomainen.

Mikäli nykyinen malli, jossa arviointilaitokset toimivat virkavastuulla on perustuslain vastainen, on tästä tietenkin luovuttava, mutta samalla on pidettävä mielessä, että hyväksynnän tekeminen viranomaisessa hidastaa tietoturva-auditointien tekemistä.

11) 9.2.3 Arviointilaitosten hyväksyminen, hyväksyjä ja valvonta

” Nykyiselle sääntelylle vaihtoehto voisi olla, että arviointilaitosten hyväksymistehtävä siirrettäisiin FINAS:lle.”

Nykyisessä mallissa sekä FINAS että Traficom osallistuvat hyväksymiseen. Vaikka mallissa on joitain käytännön heikkouksia, on muistettava, että valtionhallinnon paras tietoturva-auditointiosaaminen on Traficomissa. Katsomme, että Traficomin roolia ei saa heikentää auditointitoiminnan laadun takaamiseksi.

Mikäli ehdotus tarkoittaa vain akkreditointielimen muuttamista, jotta ristiriita Traficomin tarjoamien auditointien osalta poistuisi, emme näy tälle estettä, mutta järjestely ei poista sitä tosiasiallista päällekkäisen tarjonnan tilannetta viraston ja arviointilaitosten kesken.

Traficomin vahva rooli akkreditoinnista lähtien edesauttaa viraston arviointilaitoksiin tekemää valvontaa.

12) 9.2.3 Arviointilaitosten hyväksyminen, hyväksyjä ja valvonta

”Viranomaisiin kohdistuvasta arviointilaitosjärjestelmästä luopuminen voi olla vaihtoehtoinen tapa lähestyä arviointilainsäädännön uudistamista. Tällöin viranomaisten tietojärjestelmien arvioinnit tehtäisiin (arviointilain mukaisena) viranomaistoimintana, jossa arviointiviranomainen voisi käyttää arvioinnissa apunaan yksityisiä määritetyn ammattipätevyyden täyttäviä arvioijia….Tällaisessa mallissa kuitenkin rajautuisi arviointisääntelyn ulkopuolelle puhtaasti yksityisten yritysten tarpeet tietoturvallisuuden arvioinnille. Näitä arviointeja voitaisiin tehdä arviointilaitoslain perusteella.”

Arviointilaitosten perustamisen syy oli riittävien resurssien saaminen valtionhallinnon tietojärjestelmien arviointiin, vaikka henkilöt eivät työskentelisi virka- tai työsuhteessa valtionhallintoon. Katsomme, ettei esitys palaamisesta kymmenen vuoden takaiseen aikaan ole käytännössä mahdollinen.

Suurin osa arviointilaitosten Katakri- ja VAHTI-auditoinneista tehdään viranomaisten tietojärjestelmissä. Arviointilaitokset ovat tehneet merkittäviä investointeja päästäkseen auditoimana näitä arviointilaitoksena, emmekä pidä hyvänä, että hallintopäätöksellä suurin osa näistä auditoinneista loppuisi, ja ne siirrettäisiin

Traficomille, jolla tuskin on resursseja niiden tekemiseen, eikä resurssien hankkiminenkaan ole helppo ja nopea tie.

Katsomme, että auditointien siirto takaisin viranomaiselle heikentäisi merkittävästi valtionhallinnon muiden, pitkäjänteisyyttä vaativien Public-Private Partnership (PPP) hankkeiden onnistumisen edellytyksiä, kun julkisen toimijan sitoutumiseen ei voisi luottaa.

13) 9.2.5 Tietoturvallisuutta ja tietojärjestelmiä (ja tietoliikennejärjestelyjä) koskevat vaatimukset (ja ns. arviointikriteeristöt)

”Tietojärjestelmien tietoturvallisuuden vaatimustenmukaisuuden arvioinnissa hyödynnetään ”epävirallisia” kriteeristöjä, kuten kansallisen turvallisuusviranomaisen Katakri-kriteeristö, jonka Liikenne- ja viestintävirasto on arvioinut soveltuvan myös kansallisten tietoturvallisuusvaatimusten arviointiin. Katakri on kansainvälisistä tietoturvavelvoitteista annettua lakia täsmentävä. Sitä käytetään nykyisin myös turvallisuusselvityslain mukaisissa kansallisissa ja kansainvälisissä arvioinneissa sekä turvallisuusluokiteltavia tietoja käsittelevien kansallisten tietojärjestelmien ja tietoliikenneratkaisujen arviointilain mukaisissa arvioinneissa. Kuitenkaan Katakri-kriteeristöä ei ole laadittu kansallisen tietoturvallisuusvaatimusten näkökulmasta eikä sen laadinnasta ole vastannut toimivaltainen viranomainen. Siten sitä ei voida pitää lähtökohtana tietoturvallisuusarvioinnille muissa kuin alkuperäisessä käyttökontekstissaan. Se ei sisällä salassa pidettävien tietojen eikä toiminnan jatkuvuuden hallinnan ja varautumisen arviointikriteerejä.

Arviointikriteereinä on käytetty myös VAHTI-ohjeita, joita ei ole enää päivitetty ja jotka eivät ole ajantasaisia. VAHTI-ohjeet eivät myöskään muodosta yhtenäistä kokonaisuutta, jonka varaan luotettava ja asianmukainen tietoturvallisuuden arviointi voitaisiin perustaa. VAHTI-ohjeet olivat pääosin valtionhallinnon käyttöön tarkoitettuja. Vanhentuneita VAHTI-ohjeita ja aiempia Katakri-versioita käytetään kuitenkin edelleen arvioinnissa. Asiaintilaa ei voida pitää tällä hetkellä hyvän hallinnon kannalta katsottuna asianmukaisena. Katakri-kriteeristön ja Vahti-ohjeiden soveltuvuus koko julkisen hallinnon käyttöön on rajallinen, koska kuntasektorilla turvallisuusluokittelua ei käytetä eikä Katakrin käytöstä kansallisten turvallisuusluokiteltujen tietojen käsittelyn vaatimusten arvioinnissa ole säädetty.”

Katakri on tiukasti tulkiten ”epävirallinen”, mutta sen asema on siksi vakiintunut, että kriteeristö muodostaa ns. Soft Law:ta: sitä noudattamalla voi perustellusti olettaa yrittäneensä huolehtia huolellisuusvelvoitteesta. Niistä tuskin voi tehdä virallisia SFS-standardeja (koska Katakrin T-osa olisi vastaava kuin ISO 27001), mutta aseman virallistaminen esim. määräyksellä on harkittavissa. Tämä kuitenkin hidastasi sen päivittämistä (määräyksen päivittäminen on ohjetta hankalampaa), ja tarve on aivan päinvastainen.

On erittäin voimakkaasti korostettava, että Katakri-auditointikriteeristön aseman virallistaminen ei yksin riitä, vaan auditointien tekoon liittyy monia standardin ulkopuolisia asioita, jotka on ehdottomasti virallistettava myös. Esimerkiksi poikkeamien luokat ja todistuksen myöntämisen edellytykset eli saako todistuksen myöntää, jos on yksi pieni poikkeama. Nykytilanteessa todistuksen myöntämisen edellytykset Katakrissa (eli ei yhtään pientäkään poikkeamaa sallita) ei perustu määräykseen tai muuhunkaan normiin. Kyse on vain vallitsevasta käytännöstä

Traficomissa. Tässä ei sinällään ole mitään vikaa, mutta normiperustetta asialle ei tietääksemme ole, ja toisissa auditoinneissa (esim. ISO 27001), todistuksen myöntämisen edellytykset ovat toiset.

Tämä on ongelma, joka on tullut vahvasti esiin toisiolain mukaisten käyttöympäristöjen auditoinnissa Findatan määräyksen mukaan.

VAHTI-ohjeiden päivittämättömyys on jonkin asteinen ongelma. Iso osa niistä on ohjeita, eivätkä tarkoitettu auditointiin. Toiset ovat käyttökelpoisia vuosikymmenen jälkeen. Uudet asiat, kuten pilvipalvelut, ovat jääneet vaille VAHTI-ohjetta, joita ei ole julkaistu vuoden 2017 jälkeen, kun Tiedonhallintalautakunta otti vastatakseen tietoturvan kehittämisen. Tiedonhallintalain ja sitä tukevan VAHTI100-kriteeristön odotettiin aloittavan uuden aikakauden VAHTI:n historiassa, mutta näin ei ainakaan arviointilaitoksen vinkkelistä ole tapahtunut, eikä enää tule tapahtumaan.

Suhtaudumme varauksella siihen, että julkishallinnossa kehitetään uusi arviointikriteeristö. Pidämme parempana nykyisten laajentamista ja kehittämistä kattamaan ei-turvaluokiteltu tieto ja jatkuvuuden hallinta.

Arviomuistion keskeinen viesti on normiperusta, lainmukaisuus. Tämä on hyvä asia, mutta olemme törmänneet tilanteeseen, jossa aivan keskeisestä asiasta olemme saaneet eri tahoilta erilaista kantaa. Kysyimme: saako turvaluokiteltua (TL-tietoa) tallentaa ulkomailla olevassa pilvipalvelussa, ja jos ei, niin mihin säädökseen kielto perustuu. Vastaus oli, että yleistä hyväksyntää (siis todistusta) ei tiedolle voi myöntää, ja että asia on niin itsestään selvä, että sitä ei ole kirjattu lakiin. Myöhemmin olemme saaneet toisenlaisia kantoja: asiaa ei ole säädöksellä kielletty, joten se on sallittu.

Arviointilaitos ei voisi myöntää Pitukri-todistusta ulkomaiselle pilvipalvelulle, jos todistukseen tähtääviä auditointeja voisi ylipäätään tehdä. Toivomme, että asiantilaan tulee selkeä pykälä.

14) 9.2.5 Tietoturvallisuutta ja tietojärjestelmiä (ja tietoliikennejärjestelyjä) koskevat vaatimukset (ja ns. arviointikriteeristöt)

”*Nykytilanteessa tietoturvallisuuden vaatimukset/arviointiperusteet koetaan tulkinnanvaraisiksi. Sekä arviointilaitokset että arvioinnin kohteet ovat pyytäneet Liikenne- ja viestintävirastolta Katakri-kriteeristön tulkintoja. Liikenne- ja viestintävirastolle ei kuitenkaan ole säädetty ohjaus- tai valvontatoimivaltaa viranomaisia koskevien kansallisten tietoturvallisuusvaatimusten osalta. Toimintaympäristön muutosten takia nämä arviointiperusteiden tulkintaa tai toteutusten teknisiä yksityiskohtia koskevat linjaukset ja tulkinnat ovat myös olleet vain osin vakiintuneita. Henkilöiden vaihtuvuuden takia tulkinnoissa on myös henkilöriippuvuutta ja että yksittäiset arvioinnit hidastuvat, kun tulkintasuosituksia ei ole saatavilla riittävän nopeasti.*

Tulkintapyyntöjen on koettu hidastavan merkittävästi niin arviointilaitosten kuin arviointeja tilaavien viranomaisten ja yhteisöjen toimintaa. Palvelujen tuottajille ja käyttäjille arviointien venyminen jopa vuoden mittaiseksi voi aiheuttaa kohtuuttomia haittoja. Muuttuvien tulkintojen takia tietojärjestelmiin joudutaan myös tekemään teknisiä ja toiminnallisia muutoksia ja muutosten takia aiemmin tehdyt arvioinnin osat saatetaan joutua uusimaan.”

Kohdassa on esitetty oikea ongelma, sekä erittäin harhaanjohtava päätelmä. Arviointilaitokset ovat kysyneet Traficomin kantaa linjausta vaativissa suurissa asioissa, jotta kaikki tekisivät yhdenmukaisen päätöksen omissa auditoinneissaan. On aivan totta, että toisten tulkintojen saaminen on yleensä hyvin nopeaa, toisten hyvin hidasta. Emme ota kantaa, onko tämä henkilöitynyt vai ei, mutta on totta, että vastausajan ja kysymyksen kohdistuminen tiettyyn Katakrin kohtaan ennustaa vastausaikaa. Katakri F-osan tulkinnat tulevat yleensä joutuisasti.

Muistiossa esitetään, että tulkintojen saaminen on viivästyttänyt pitkään, jopa vuodella, tulkintoja odotettaessa. Emme ole havainneet tätä omissa auditoinneissamme. Tulkintojen odottaminen on viivästyttänyt, mutta vain vähän. Viivästymiset johtuva pääasiassa kohteesta johtuvista seikoista, kuten korjausten hitaasta etenemisestä.

Traficom on ohjeistanut arviointilaitoksia tekemään enemmän itsenäisiä tulkintoja senkin uhalla, että yhden arviointilaitoksen tulkinta poikkea Traficomin linjasta. Tästä olisi hyvä saada ohje tai määräys, sillä olemme itse pitäneet yhtenäistä linjaa tulkinnoista tärkeänä. Toimimme luonnollisesti viraston ohjeiden mukaan.

15) 9.2.5 Tietoturvallisuutta ja tietojärjestelmiä (ja tietoliikennejärjestelyjä) koskevat vaatimukset (ja ns. arviointikriteeristöt)

”*Arviointia voi käytännössä olla haastavaa suorittaa yksinomaan säädöksiin sisältyvien melko yleisten vaatimusten perusteella – varsinkin, jollei ole toimivaltaisen viranomaisen yksityiskohtaisempia tulkintoja säännösten sisällöstä. Jotta päästäisiin eroon epävirallisten kriteeristöjen käytöstä vaatimustenmukaisuuden arvioinnissa, tiedonhallintalautakunta valmistelee parhaillaan julkisen hallinnon tietoturvallisuuden arviointikriteeristöä ottaen huomioon myös toiminnan varautumisen ja jatkuvuudenhallinnanasettamat vaatimukset. Tällainen arviointikriteeristö ei ole kuitenkaan sitova eikä sitä voida myöskään arviointien kautta muuttaa ikään kuin se olisi sitova esimerkiksi erilaisia kelpoisuuksia määriteltäessä tai todistuksia annettaessa.*”

Arvioinnin tekeminen säädökseen liittyvien yleisten vaatimusten pohjalta ei ole haastavaa, se on erittäin vaikeaa, ellei mahdotonta. Määräystä on tuettava alemman asteen normeilla, kuten määräyksillä. Näin on menetelty toisiolain- ja eIDAS-auditoinneissa.

Voi olla tarpeen tehdä vielä yksi kriteeristä lisää, jotta niiden virallisuuden puute saadaan ratkaistua, mutta näkisimme huomattavasti parempana tapana jonkin nykyisen kriteeristön kehittämisen ja virallistamisen. Nämä ovat puutteistaan huolimatta koeteltuja, ja niiden tapana on tulkintatraditio, mikä uudelta puuttuu.

16) 9.2.5 Tietoturvallisuutta ja tietojärjestelmiä (ja tietoliikennejärjestelyjä) koskevat vaatimukset (ja ns. arviointikriteeristöt)

”*Vai pitäisikö ennemminkin vaatimusten ja kriteeristöjen itsessään olla riskiarviointiin perustuen joustavia.*”

Auditointikriteeristöjen maailmassa riskipohjaisuuden merkitys on kasvanut, ja trendin voi olettaa jatkuvan. Katsomme, että tähän suuntaan on hyvä edetä.

Numeroidut kommentit

1) Kommenttinne arviomuistiossa tehdystä nykytilan kuvauksesta

   Nykytila on kuvattu tietojärjestelmän arviointien osalta pääosin hyvin, mutta monissa yksityiskohdissa kuvaus ei vastaa tilannetta niin kuin me sen koemme.

2) Kommenttinne tietojärjestelmistä sääntelykohteena

   Tietojärjestelmä on reaalimaailman ilmiö, jolla on merkittävä vaikutus julkishallintoon, ja se on sääntelyn kohteena aivan mahdollinen. On kuitenkin syytä huomata, että perinteiset määritelmät tietojärjestelmästä eivät aina sovellu pilvipalveluihin: ne ovat palveluita, joiden takan on järjestelmä, mutta eivät järjestelmä perinteisessä mielessä.

3) Millaisia yleisiä vaatimuksia tietojärjestelmien toiminnallisuuksille pitäisi lainsäädännöllä asettaa?

   Järjestelmä toimii aiotulla tavalla, sen käytettävyys ja vikasietoisuus ovat hyvät, ja se on tietoturvallinen, noudattaa järjestelmässä käsiteltävien tietojen käsittelyä sääteleviä lakeja.

4) Millaisia olennaisia teknisiä vaatimuksia hallintoasioita käsitteleville tietojärjestelmille pitäisi lainsäädännöllä säätää?

   a) Käytettävyys
   b) Tietoturvallisuus ja sen jatkuva ylläpito (vuosiauditoinnit)
   c) Ylläpidettävyys
   d) Siirrettävyys
   e) Järjestelmää koskevien lakien tunnistaminen ja niiden noudattaminen

5) Millaisia vaatimuksia, kuten dokumentointivaatimuksia, tietojärjestelmien kehittämiselle pitäisi lainsäädännöllä säätää?

   Hyvä käytäntö tietojärjestelmähankkeissa on kuvattuna useissa standardeissa. Joku näistä tulisi valita, ja täydentää kansallisilla asioilla. Lisäksi järjestelmän käsittelemän tiedon korkein tietoturvaluokka, tietoja koskevien lakien lista sekä yleinen tietoturvakuvaus, jossa mm. jatkuvan auditoinnin suunnitelma

6) Miten lainsäädännöllä tulisi varmistua virkavastuun toteutumisesta ja kohdistumisesta, mitä tulee tietojärjestelmien kehittämiseen, käyttöönottoon ja käyttöön, sekä tietovarantojen käyttöön?

   Ei kantaa.

7) Mitä edellytyksiä tietovarannoille, niiden laadulle tai niiden käytölle tulisi lainsäädännössä asettaa, jotta niitä voidaan käyttää osin tai täysin automaattisessa päätöksenteossa?

   Tietojen käsittelyn turvallisuus, etenkin niiltä osin kuin pilvipalveluissa hyödynnetään pilvipalvelutoimittajan AI-toiminnallisuutta. On huolehdittava, että henkilötietojen käsittely tapahtuu asianmukaisesti (anonyymisti) ja EU:n alueella.

   Tilanne, jossa saamamme tiedon mukaan todistusta ei voi myöntää pilvipalvelulle, joka toimii ulkomailla, on outo, koska meille on kerrottu, että asia ei perustu lakiin, vaan on itsestään selvä. Haluaisimme lain, esimerkiksi pilvipalvelulain.

   Tarve säädellä tekoälyn käyttöä on olemassa, mutta paljon akuutimpi tarve on pilvipalveluiden säätelyssä, ja niiden todistukseen tähtäävien auditointien tekemisessä mahdolliseksi (nyt niitä ei saa tehdä, kunnes Traficom toisin ohjeistaa).

8) Miten tietoturvallisuuden arviointia ja arviointijärjestelmää koskevaa lainsäädäntöä tulisi kehittää? Entä erityisesti viranomaisten tietojärjestelmien arvioinnin osalta?

   Vastaus annettu edellä. Tärkeimmät kohdat ovat
   1) Auditointien tekeminen pakollisiksi ja säännöllisiksi (vuosiauditoinnit)
   2) Riittävän resurssoinnin takaaminen niin, että julkishallinto hyödyntää arviointilaitoksia auditoinneissa mahdollisimman laajasti, ja selvittää näiden pätevyysalueen laajentaminen esim. kv-tietojärjestelmin, TLII-järjestelmiin ja kryptohyväksyntään.
   3) Traficomin asiantuntijaroolin vahvistamisella ja valvontaroolin pitämisenä pääosin nykyisellään (ei siirtoa muille viranomaisille).

9) Kommenttinne muistiossa todetuista sääntelytarpeista yleensä.

   Otamme kantaa vain tietojärjestelmäauditointien säätelytarpeeseen.

10) Muut yleiset kommentit arviomuistiosta

    Nixu Certification Oy olisi mielellään kuullut valmistelutyöstä, ja tullut haastatelluksi sen aikana.

Olli-Pekka Soini
Lead Auditor
CISSP, CISA, CISM, CRISC
ISO 27001 Lead Auditor
Nixu Certification Oy

Mobile : +358 40 5098456
olli-pekka.soini@nixu.com
www.nixu.com
Keilaranta 15,
FI-02150 Espoo,
Finland