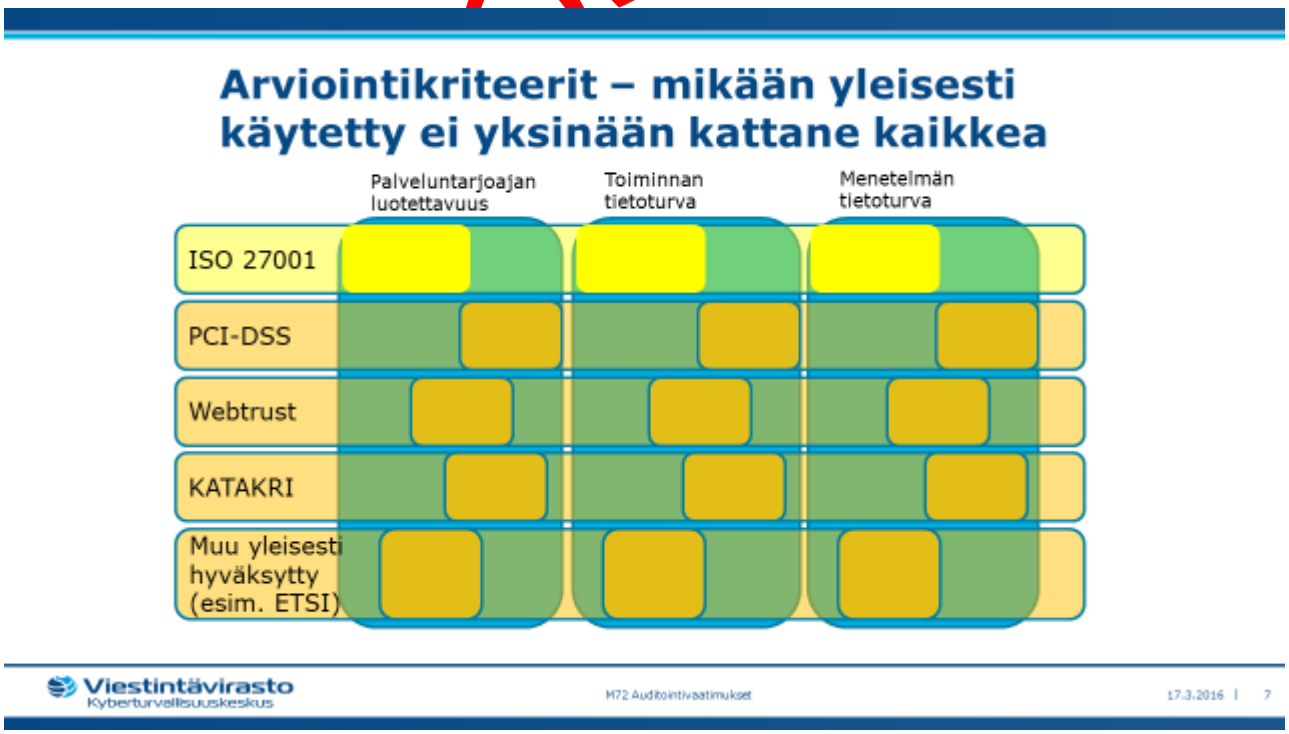
M72 valmistelumuistio 2021: tunnistuspalvelun arviointikriteerit ja arviointielimen vaatimukset

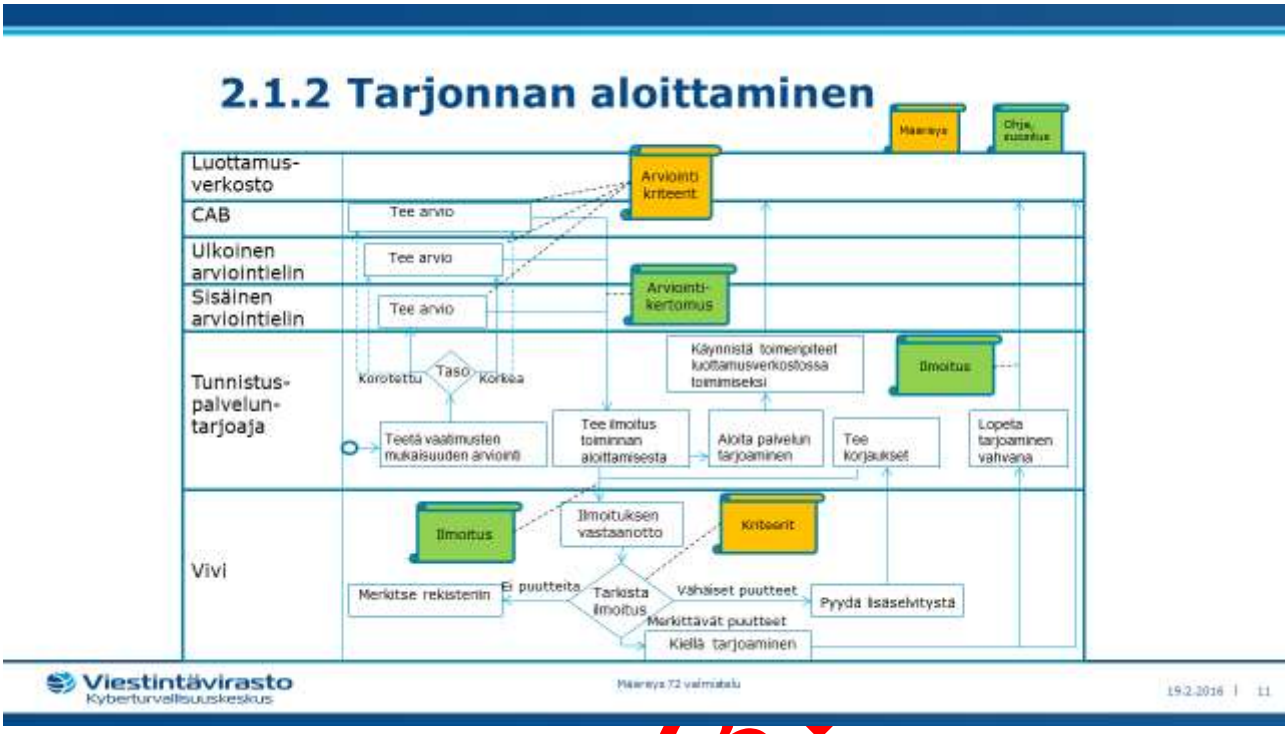
Contents

1 Kuva

Kuva: Kalvo vuoden 2016 määräysvalmistelusta



Kuva: kalvo vuoden 2016 määräysvalmistelusta



2 Säännös ja perustelut

Tähän on koottu voimassa olevasta määräyksestä **Viestintävirasto 72/2018 M sähköisistä tunnistus- ja luottamuspalveluista** säännökset, joiden muutostarvetta muistiossa arvioidaan.

Tähän on koottu myös säännösten perustelut ja soveltamisohjeet **perustelumuistiosta MPS72.** Perustelumuistion 14.5.2018 päivätyssä versiossa ovat mukana vuoden 2016 perustelut ja 2018 osittaismuutoksen perustelut. Perustelut päivitetään muutoksen yhteydessä.

Koko määräys ja perustelumuistio Finlexissä https://www.finlex.fi/fi/viranomaisnormi/480001/42947

2.1 Säännös 15 § *Arviointikriteerit*

15 § Arviointikriteerit

Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat

1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän)
a) tietoturvallisuuden hallintaan
b) tietojen säilyttämiseen
c) tiloihin ja henkilökuntaan
d) teknisiin toimenpiteisiin

2) tunnistusmenetelmään eli tunnistusvälineen
a) hakemiseen ja rekisteröintiin
b) hakijan henkilöllisyyden todistamiseen ja varmentamiseen

c) tunnistamisen menetelmän ominaispiirteisiin ja laatimiseen
d) myöntämiseen, toimittamiseen ja aktivointiin
e) voimassaolon keskeyttämiseen, peruuttamiseen ja uudelleen aktivointiin
f) uusimiseen ja korvaamiseen
g) todentamismekanismeihin

Edellä 1 momentissa mainittujen osa-alueiden arvioinnin on perustuttava tunnistus- ja luottamuspalvelulain ja tämän määräyksen vaatimuksiin, EU:n tai muun kansainvälisen toimielimen antamiin säännöksiin tai ohjeisiin, julkaistuihin ja yleisesti tai alueellisesti sovellettuihin tietoturvallisuutta koskeviin ohjeisiin tai yleisesti käytettyihin tietoturvallisuus-standardeihin tai menettelyihin.

2.1.1 Perustelumuistio

Pykälän 1 momentissa luetellaan ne tunnistuspalvelun toteutuksen ja tarjonnan osa-alueet, joiden osalta säädännön vaatimusten täyttyminen täytyy osoittaa joko ulkoisella tai sisäisellä arvioinnilla. Arviointikriteerit perustuvat säädösten vaatimuksiin, erityisesti EU:n varmuustasoasetuksen [2] vaatimuksiin. Tietoturvavaatimuksia tarkennetaan myös tämän määräyksen 2 luvussa.

Tunnistuspalveluntarjoaja voi täyttää säännöksessä määrätyt arvioinnin vaatimukset yhdellä tai useammalla valitsemallaan arvioinnilla. Esimerkkejä kansainvälisistä tai kansallisesti yleisesti käytetyistä standardeista, joihin perustuvia arviointeja toimijat voivat tietyin edellytyksin hyödyntää, luetellaan jäljempänä arviointielimen pätevyyttä koskevan 18 §:n kohdalla.

Pykälän 2 momentissa säädetään siitä, mitä vaatimuksia vasten arviointi on tehtävä. Vaatimukset, jotka tunnistusjärjestelmän on täytettävä, säädetään tunnistus- ja luottamuspalvelulaissa, EU:n varmuustasoasetuksessa ja niitä tarkennetaan tässä määräyksessä. Arvioinnissa voidaan lisäksi ottaa huomioon myös muita lähteitä, kuten tietoturvallisuusstandardeja, jotka tarkentavat hyviä tietoturvakäytäntöjä ja konkretisoivat arvioinnissa huomionarvoisia yksityiskohtia.

Arviointielimen pätevyysvaatimuksista säädetään tunnistus- ja luottamuspalvelulain 33 §:ssä ja vaatimuksia tarkennetaan tämän määräyksen 18 §:ssä.

Arvioinnin hankkivan tunnistuspalveluntarjoajan on huolehdittava sitä, että arvioinnissa otetaan huomioon myös nimenomaisesti tunnistusjärjestelmään ja tunnistusmenetelmään kohdistuvat vaatimukset, vaikka palvelun tuotanto- ja hallintaympäristö usein on vain osa muuta tuotanto- ja hallintaympäristöä ja vaikka arviointi kohdistuisi kokonaisuutena tähän laajempaan kokonaisuuteen.

<u>Soveltaminen, Viestintäviraston ohjeet 211/2016 O ja 215/2016 O</u>

Viestintävirasto julkaisee ohjeena 211/2016 O tunnistuspalvelun arvioinnin mallikriteeristön [25], jota käyttämällä kaikki määräyksessä vaaditut osa-alueet tulevat huomioiduksi. Mallikriteeristö perustuu pääosin tietoturvallisuuden hallinnan standardiin ISO/IEC 27001 [8]. Mallikriteeristössä on viittaukset vaatimuksia koskeviin säännöksiin.

Viestintävirasto julkaisee myös ohjeen 215/2016 O sähköisten tunnistus- ja luottamuspalveluiden tarkastuskertomuksista [7]. Ohjeessa selvitetään, mitä tietoja arviointielimen laatimassa tarkastuskertomuksessa täytyy olla. Tarkastuskertomus täytyy tunnistus- ja luottamuspalvelulain 10 §:n mukaan toimittaa Viestintävirastolle.

2.2 Säännös 16 § Selvitys muiden vaatimusten täyttämisestä

16 § Selvitys muiden vaatimusten täyttämisestä

Tunnistuspalveluntarjoajan on osoitettava omalla kirjallisella selvityksellään tai edellä 15 §:ssä tarkoitetulla arvioinnilla seuraavien tunnistuspalveluntarjoajan luotettavuuteen ja tunnistuspalvelusta annettaviin tietoihin liittyvien vaatimusten täyttyminen:

1) julkaistut ilmoitukset ja käyttäjätiedot, kuten tunnistusperiaatteet, sopimusehdot ja hinnastot
2) vakiintunut organisaatio
3) valmius ottaa vahinkoriskejä
4) riittävät taloudelliset varat
5) vastuu alihankkijoista
6) suunnitelma toiminnan päättämisen varalta

2.2.1 Perustelumuistio

Perustelut

Pykälään on koottu ne tunnistuspalveluntarjoajan luotettavuutta koskevat osa-alueet, jotka eivät liity erityisesti tunnistusjärjestelmään vaan yleisemmin toimijan luotettavaan toimintakykyyn ja vastuullisuuteen. Näiden vaatimusten täyttämisen voi osoittaa yrityksen omalla selvityksellä Viestintävirastolle aloitus- tai muutosilmoituksen yhteydessä.

Vaatimusten täyttämisen voi osoittaa myös soveltuvalla arvioinnilla. Määräyksen valmistelussa ei ole tullut toimialalta ehdotuksia tällaisista yleisiä luotettavuusvaatimuksia koskevista standardeista, joten tässä ei esitetä esimerkkejä.

Soveltaminen, Viestintäviraston ohje 214/2016 O

Viestintäviraston ohjeessa 214/2016 O tunnistus- ja luottamuspalveluiden ilmoituksista käsitellään joiltain osin tietoja tai liitteitä, joita Viestintävirastolle on toimitettava. Tiedoista ei kuitenkaan ole laadittu yksityiskohtaisia soveltamisohjeita, vaan tarvittavia tietosisältöjä arvioidaan mm. tunnistus- ja luottamuspalvelulain perustelujen avulla.

Ks. tuoreempi neuvontakooste tunnistuspalvelun tarjoajan vaatimuksista

2.3 Säännös 17 § Kansallisen solmupisteen arviointiperusteet

17 § Kansallisen solmupisteen arviointiperusteet

Kansallisen solmupisteen tietoturvallisuuden arvioinnin tulee perustua ISO/IEC 27001 -standardiin ja Euroopan komission täytäntöönpanoasetukseen (EU) 2015/1501[1].

2.3.1 Perustelumuistio

Säännös on lähinnä informatiivinen. Komission täytäntöönpanoasetuksessa (EU) 2015/1501 [23] mainitaan oletuksena standardiin ISO/IEC 27001 perustuva tietoturvallisuuden hallinta. Määräyksessä vahvistetaan tämä olettama, koska tämä on myös käytännössä Väestörekisterikeskuksen toimintaan soveltuva ratkaisu. Komission täytäntöönpanopäätöksessä säädetään joitain vaatimuksia solmupisteen toiminnalle.

[1] Komission täytäntöönpanoasetus yhteentoimivuusjärjestelmän vahvistamisesta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 12 artiklan 8 kohdan mukaisesti

2.4 Säännös 18 § Tunnistuspalvelun ulkoisen arviointielimen vaatimukset

18 § Tunnistuspalvelun ulkoisen arviointielimen vaatimukset

Tunnistus- ja luottamuspalvelulain 33 §:ssä arviointielimelle säädettyjen riippumattomuus- ja pätevyysvaatimusten täyttymisen voi osoittaa

1) *ISO/IEC 27001 -standardiin perustuvalla akkreditoinnilla tai osoittamalla muutoin pätevyys standardin mukaiseen arviointiin;*
2) *Webtrust -säännöstöön perustuvalla kansainvälisesti tunnetun itsesääntelyjärjestelyn mukaisesti osoitetulla pätevyydellä;*
3) *PCI DSS - maksukorttistandardiin perustuvalla akkreditoinnilla tai osoittamalla muutoin pätevyys standardin mukaiseen arviointiin;*
4) *ISACA:n standardien ja tietojärjestelmien valvontakehikon mukaisesti osoitetulla pätevyydellä; tai*
5) *muiden edellisiin rinnastettavien yleiseen tietoturvallisuuden hallintaan taikka sektorikohtaiseen sääntelyyn tai standardointiin liittyvien säännösten, ohjeiden tai standardien edellyttämän pätevyyden osoittamisella tai noudattamisella.*

Pätevyyden osoittaminen tunnistusjärjestelmän arviointiin edellyttää sitä, että osoitetaan myös, miten ja miltä osin edellä 1 momentissa tarkoitetut säännökset, ohjeet tai standardit kohdistuvat tunnistusjärjestelmään.

2.4.1 Perustelumuistio

Viestintävirastolle tunnistus- ja luottamuspalvelulain 10 §:n mukaisesti annettavassa aloitus- tai muutosilmoituksessa ja sen liitteissä annetaan valvovalle viranomaiselle tiedot riippumattomasta arvioinnista. Lisäksi on annettava selvitys, jonka perusteella voidaan arvioida, että arvioinnin tekijä täyttää tunnistus- ja luottamuspalvelulain 33 §:n vaatimukset arviointielimen riippumattomuudelle ja pätevyydelle.

Pykälän tarkoitus on selkeyttää arviointielimen riippumattomuuden ja pätevyyden määrittelyn perusteita ennakoitavasti. Tarkoitus on selkeyttää myös sitä, että arviointielimen riippumattomuus ja pätevyys eivät voi perustua toimijan omiin säännöstöihin tai omaan arvioon, vaan niiden on oltava objektiivisesti perusteluja.

Pykälän 1 momentissa luetellaan esimerkkejä sellaisista kansainvälisistä standardeista tai sääntely- tai itsesääntelykehyksistä, joihin arviointielimen riippumattomuus ja pätevyys voi perustua. Luettelo ei ole tyhjentävä ja 5 kohdassa todetaan yleisesti edellytykset sille riippumattomuuden ja pätevyyden osoittamiselle. Tarkoitus on, että toimijat voisivat tukeutua mahdollisimman joustavasti erilaisiin jo muutoinkin käyttämiinsä arviointeihin.

Esimerkkejä mahdollisista arviointielimistä ovat akkreditoitu ISO 27001 tarkastuslaitos, muu ulkoinen ISO 27001-auditoija tai vastaavat muihin relevantteihin standardeihin perustuvat arvioijat.

Pykälän 2 momentista ilmenee, että edellytyksenä eri standardien tai säännöstöjen käyttämiselle riippumattomaan ja pätevään tunnistusjärjestelmän arviointiin on se, että arviointi todella kohdistuu tunnistusjärjestelmän vaatimuksiin. On tunnistuspalvelun tarjoajan vastuulla huolehtia siitä, että näin todella on ja että arviointi kattaa kaikki tässä määräyksessä määritellyt osa-alueet. Tarkastuskertomuksesta on ilmettävä selkeästi auditoinnin kohdistuminen tosiasiassa tunnistusjärjestelmän vaatimuksiin.

<u>Soveltaminen</u>

Auditoinnin tekevä arviointielin voi tunnistus- ja luottamuspalvelulain 29 §:n mukaisesti olla joko sisäinen tarkastuslaitos, muu ulkoinen arviointilaitos tai akkreditoitu vaatimustenmukaisuuden arviointilaitos.

Viestintävirasto julkaisee ohjeen 215/2016 O sähköisten tunnistus- ja luottamuspalveluiden tarkastuskertomuksista [7]. Ohjeessa selvitetään, mitä tietoja arviointielimen laatimassa tarkastuskertomuksessa täytyy olla.

Seuraavassa on suuntaa-antava ja informatiivinen lista standardeista tai muista lähteistä, joiden mukaisia arviointeja Viestintäviraston tunnistuspalvelurekisteriin merkityt toimijat käyttävät kyselyn perusteella ja jotka voivat soveltua myös tunnistusjärjestelmän arviointiin. Tässä ei ole erityisesti eritelty riippumattomuuden ja pätevyyden perusteita tai arvioitu, miltä osin lähteet soveltuisivat tunnistusjärjestelmän vaatimusten arviointiin. Esimerkkilista voi myös soveltua seuraavassa pykälässä käsiteltyjen sisäisten tarkastuslaitosten pätevyyden arviointiin:

- *ISO 27001*
- *PCI DSS, PCI/QSA*
- *Webtrustin Trust Services Principles and Criteria for Certification Authorities ja Webtrust for Certification Authorities - SSL Baseline Requirements Audit Criteria*
- *Information Security Forumin (ISF) "Standard of Good Practice"*
- *ISF:n IRAM-kriteeristö (Information Risk Analysis Methodology)*
- *ETSI TS 101456 (CA policy) [25]*
- *ISRS 4400 ja ISAE 3000*
- *Katakri*
- *Vahti*
- *Euroopan keskuspankin tai FIVA:n määräykset tai ohjeet*
- *FIVA:n määräys ja ohje 2.4 "Asiakkaan tunteminen - rahanpesun ja terrorismin rahoittamisen estäminen"*
- *Euroopan keskuspankin Cybersecurity questionnary 2015*
- *BISin (Bank for International Settlements) ohje External audits of banks [26]*

2.5 Säännös 19 § *Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset*

19 § Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset

Tunnistus- ja luottamuspalvelulain 33 §:ssä sisäiselle tarkastuslaitokselle säädettyjen riippumattomuusvaatimusten täyttymisen voi osoittaa:

1) *IIA:n ammattistandardien (sisäisen tarkastuksen riippumattomuus ja objektiivisuus, ml. organisatorinen riippumattomuus) noudattamisella;*
2) *ISACA:n standardien ja tietojärjestelmien valvonnan kehikoiden noudattamisella;*
3) *BIS:in (Bank for International Settlements) sisäistä tarkastusta koskevien ohjeiden noudattamisella;*
4) *Finanssivalvonnan määräys- ja ohjekokoelman sisäistä tarkastusta koskevien ohjeiden noudattamisella;*
5) *muiden ETA-alueen jäsenvaltioiden vastaavien valvontaviranomaisten antamien ohjeiden tai määräysten noudattamisella; tai*
6) *muilla edellisiin rinnastettavilla viranomaissääntelyyn tai yleiseen riippumattoman sisäisen tarkastuksen hallintaan liittyvien standardien noudattamisella.*

Pätevyyden osoittaminen tunnistusjärjestelmän arviointiin edellyttää sitä, että osoitetaan myös, miten ja miltä osin 1 momentissa tarkoitettujen säännösten, ohjeiden tai standardien mukaisesti organisoitu sisäinen tarkastus kohdistuu tunnistusjärjestelmään.

2.5.1 Perustelumuistio

Pykälän perustelut ovat samat kuin perustelut 18 §:lle. Myöskään sisäisen tarkastuslaitoksen riippumattomuus ja pätevyys eivät voi perustua toimijan omiin säännöstöihin tai omaan arvioon, vaan niiden on oltava objektiivisesti perusteluja ja sovelluttava perustellusti tunnistusjärjestelmän vaatimusten arviointiin.

Asiaa käsitellään vaikutusarvioinnin (ks. A osa) luvussa 3.2.5.

Soveltaminen

Pykälän 2 momentissa esimerkkinä mainittuja sisäisen tarkastuksen säännöstöjä löytyy esimerkiksi seuraavista lähteistä

- *Finanssivalvonnan määräys- ja ohjekokoelma [27]*
  - *Luotettava hallinto ja toiminnan järjestäminen Kappale 5.6. Sisäinen tarkastus*
- *BIS: The internal audit function in banks [26]*

3 Lähteet vaikutusarviointiin

3.1 Yleiskuvaus lähtötilanteesta, viraston arvio kyselyssä 2020

3.1.1 Arviointielimistä

Tunnistus- ja luottamuspalvelulain ja eIDAS-asetuksen mukaan tunnistuspalveluiden vaatimustenmukaisuuden arviointi on pakollista ja siitä täytyy toimittaa valvovalle viranomaiselle arviointi- tai tarkastuskertomus. Arvioija voi palvelusta riippuen olla FINASin akkreditoima vaatimustenmukaisuuden arviointilaitos, muu ulkoinen arviointilaitos tai sisäinen tarkastuslaitos.

Määräyksessä määritellään ne kriteerit, joiden perusteella vaatimustenmukaisuuden arvioijan riippumattomuus ja pätevyys arvioidaan objektiivisesti. Kriteerit perustuvat pääasiassa kansainvälisesti tai kansallisesti yleisesti käytettyihin standardeihin, säännöksiin tai ohjeisiin.

Määräyksen 18 §:ssä ja 19 §:ssä määritellään esimerkkejä sellaisista kansainvälisistä standardeista tai sääntely- tai itsesääntelykehyksistä, joihin arviointielimen riippumattomuus ja pätevyys voi perustua. Luettelot eivät ole tyhjentäviä, vaan jokin vastaava objektiivinen standardi tai säännöstö voi osoittaa pätevyyden.

3.1.2 Arviointikriteereistä

Virasto on laatinut yhteistyössä toimialan kanssa tunnistuspalveluiden arviointiohjeen 211/2019. Sillä päivitettiin aikaisempia ohjeita 211/2016 auditointikriteeristöstä ja 215/2016 sähköisten tunnistus- ja luottamuspalveluiden tarkastuskertomuksista.

Viraston käsitys on, että määräyksen 15 §:n ja päivitetty tunnistuspalvelun arviointiohje 211/2019 muodostavat nyt toimivan kokonaisuuden, jonka puitteissa on edelleen mahdollista hyödyntää muista syistä tehtyjä tietoturva-arviointeja. Virasto arvioi myös, että ei ole tarkoituksenmukaista muuttaa tätä yhdistelmää olennaisesti, jotta kahden vuoden välien tehtävässä arvioinnissa päästäisiin vakiinnuttamana käytäntöjä.

3.2 Vuonna 2016 ja 2018 vaikutusarvioinneissa linjatut asiat

3.2.1 Tunnistuspalvelun arvioinnin kattavuusvaatimukset

MPS2016 kohta 3.2.2

Arvioitava kysymys: Onko arvioinnin katettava kaikki vaatimusten osa-alueet, joista säädetään tunnistus- ja luottamuspalvelulaissa ja EU:n varmuustasoasetuksessa, johon laissa viitataan?

Vaikutusarvioinnin lähtökohdat

EU:n varmuustasoasetuksen mukaan määräajoin tehtävän auditoinnin täytyy kattaa kaikki palvelujen kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

Merkitykselliset toimintalohkot voidaan jaotella karkeasti kolmeen osa-alueeseen, joita ovat palveluntarjoajan luotettavuus, tunnistusjärjestelmän luotettavuus ja tunnistusmenetelmän luotettavuus. Näistä kaksi jälkimmäistä liittyvät tietoturvallisuuden hallintaan ja toteuttamiseen, joihin tietoturvallisuusauditoinnit yleensäkin kohdistuvat.

Vaatimusten täytyy kohdistua tasapuolisesti kaikkiin toimijoihin ja tästä syystä arvioitavien osa-alueiden täytyy olla kaikilla toimijoilla samat sen sijaan, että toimijat voisivat itse valita jossain rajoissa, mitkä osa-alueet arvioidaan riippumattomasti ja minkä osa-alueiden vaatimustenmukaisuudesta toimija antaa selvityksen itse. Yhteismitallisten raporttien valvonta on myös viranomaisen kannalta tehokasta.

Linjaukset

Arvioinnin ei tarvitse kattaa palveluntarjoajan yleistä luotettavuutta tai käyttäjille ja luottaville osapuolille tarjottavia tietoja palvelusta (tunnistusperiaatteet, sopimusehdot, hinnastot). Näistä riittää toimijan oma selvitys.

Arvioinnin täytyy kattaa kaikki tunnistuspalvelun tarjontaan vaikuttavan toiminnan tietoturvan ja tunnistusmenetelmän tietoturvan osa-alueet.

Arvioinnin voi koota useamman auditoijan tai arviointielimen useisiin kriteeristöihin perustuvista auditoinneista.

Määräyksen 15 § ja 16 § on laadittu näiden linjausten mukaisesti.

Määräykselle vaihtoehtoiset ohjauskeinot

Suositus/ohje. *Suosituksella voidaan helpottaa toimijoita hahmottamaan, miten nykyisistä auditoinneista saa koottua tarvittavan kokonaisuuden ja mitä mahdollisesti tarvitaan lisää. Viestintävirasto julkaisee ohjeen 211/2016 O tunnistuspalveluntarjoajan auditoinnin mallikriteeristö [6].*

Yhteissääntely. *Ei relevantti. Tunnistuspalveluntarjoajien luottamusverkoston tekeillä olevat käytännesäännöt vastaavat velvoittavuudeltaan Viestintäviraston suositusta. Auditointien kattavuuden määrittely liittyy siihen, missä määrin arviointityö on Viestintäviraston valvonnan varassa ja miltä osin vaatimustenmukaisuuden varmistamista tukee säännöllinen riippumaton ja pätevä auditointi.*

Informaatio-ohjaus. *Vaihtoehtona voisi tarkastella sitä, että tiedot toimijoiden auditointien kattavuudesta julkaistaisiin. On kuitenkin vaikea nähdä, miten tämä kannustaisi siihen, ettei osaa asioista olisi jätetty Viestintäviraston arvioitavaksi, mikä olisi epätasapuolista ottaen huomioon sen, että rekisteröinti- ja valvontamaksu on kaikille toimijoille sama. Auditointien kattavuutta koskevien tietojen julkaiseminen sellaisenaan voi olla ongelmallista myös liikesalaisuuksien näkökulmasta.*

3.2.2 Tunnistuspalvelun arviointikriteeristön tarkkuustaso määräyksessä

MPS2016 kohta 3.2.3

Arvioitava kysymys: Millä tarkkuudella tunnistuspalvelun arviointivaatimukset eli auditointikriteeristö laaditaan määräykseen? Vaihtoehdot ovat yksityiskohtainen yhdenmukainen kriteeristö tai yleistason kriteeristö, jota täydennetään soveltamissuosituksella.

Vaikutusarvioinnin lähtökohdat

Yleisesti arviointikriteeristön määrittely määräyksessä edistää kilpailun tasapuolisuutta, kun kaikki joutuvat panostamaan arviointiin yhtäläisellä tasolla.

Edelleen arviointien vähimmäistason määrittely määräyksessä edistää tietoturvallisuuden ylläpitoa. Sen arvioidaan sinänsä olevan keskimäärin hyvällä tasolla, mutta vähimmäistasolla on merkitystä alalle tulijoiden toiminnan tason kannalta. Luottamusverkoston toiminnan kannalta on oleellista, että sen jäsenet voivat luottaa varmuudella myös alalla aiemmin toimimattomien palveluntarjoajien täyttävän tietoturvallisuudelta vaaditun vähimmäistason.

Viestintäviraston on helpompi arvioida tasapuolisesti yhdenmukaisten arviointiraporttien (laissa tarkastuskertomusten) pohjalta sitä, että toimija täyttää tunnistus- ja luottamuspalvelulaissa tai eIDAS-asetuksessa sille asetetut vaatimukset myös uusien toimijoiden osalta. Sääntelyssä varaudutaan siihen, että markkinoille tulee uusia toimijoita erityisesti tunnistusvälityspalvelun, mutta myös tunnistusvälineiden tarjoajaksi.

Vaihtoehto 1, tarkka kriteeristö määräyksessä.

Yhdenmukainen toteutus ja ohjaus vähentäisivät viranomaistoiminnan kustannuksia, joita aiheutuisi yrityskohtaisesta vaatimusten selvittämisestä ja tulkinnasta sekä vähentäisivät riskiä siitä, että valvova viranomainen ei pitäisi yrityksen tulkintaa riittävänä.

Yhdenmukainen kriteeristö on myös hyvä työkalu esimerkiksi sisäistä tarkastusta tekeville. Tunnistuspalvelu on tyypillisesti vain pieni osa tarkastettavaa tuotantokokonaisuutta eikä sisäinen tarkastus välttämättä pysty aivan helposti tunnistamaan kaikkia siihen liittyviä erityiskysymyksiä. Kriteeristö olisi siten hyvä tuki tähänkin.

Tarkka arviointikriteeristö on kuitenkin vaikea määritellä riittävän joustavaksi. Toimijoiden saattaa olla hankalaa sovittaa tarkka kriteeristö täysmittaisesti käytössään oleviin auditointeihin. Tarkkaan kriteeristöön tarvitaan myös todennäköisesti muutoksia useammin kuin yleispiirteiseen kriteeristöön. Tällä on vaikutusta myös Viestintäviraston työmäärään.

Vaihtoehto 2, yleispiirteinen kriteeristö määräyksessä

Yleispiirteinen kriteeristö on joustava siinä mielessä, että sen voi täyttää monenlaisilla arvioinneilla. Se myös kestää aikaa paremmin kuin tarkka kriteeristö.

Toisaalta arvioinnin suunnitteluvaihe voi tässä vaihtoehdossa olla toimijalle työläämpi, koska täytyy varmistaa, että toimijan omassa käytössä olevien kriteeristöt kattavat kaikki vaatimukset. Tätä soveltamista voidaan tukea määräyksen yleistä kriteeristöä selittävällä suosituksella.

Virastolle toimitettavan arviointiraportin (laissa tarkastuskertomuksen) voi koostaa useammista tehdyistä auditoinneista. Kun yleinen jaottelu on yhdenmukainen, raporttien valvonta on helpompaa.

Linjaus

Määräyksen luettelo asioista, jotka arvioinnin täytyy kattaa, laaditaan yleisellä tasolla ja siinä tukeudutaan EU:n varmuustasoasetuksen mukaiseen vaatimusten ryhmittelyyn.

Tällöin toimijat voivat hyödyntää joustavasti arviointikriteeristöjä, joita ne muutoinkin jo käyttävät. Toisaalta toimijoiden täytyy arvioida ja varmistaa, että niiden käyttämät eri standardeihin perustuvat kriteeristöt todella kattavat kaikki vaaditut tunnistusjärjestelmän arvioinnin osa-alueet. Viestintävirasto joutuu myös tarkastuskertomuksia valvoessaan arvioimaan, että tämä toteutuu.

Määräyksen 15 § on laadittu näiden linjausten mukaisesti.

Määräykselle vaihtoehtoiset ohjauskeinot

***Suositus/ohje**. Laaditaan Viestintäviraston ohjeena 211/2016 O määräyksen yleistason vaatimuksia tarkentava auditointikriteeristö, jonka läpikäymällä ainakin täyttää arviointivaatimukset. Laaditaan Viestintäviraston ohje 215/2016 O sähköisten tunnistus- ja luottamuspalveluiden tarkastuskertomuksista [7], joka helpottaa arvioinnin valmistelua ja hankintaa.*

***Yhteissääntely**. Valmistelussa ei ole havaittu, että luottamusverkoston tekeillä oleviin käytännesääntöihin olisi tarvetta ottaa arviointiin liittyviä vaatimuksia. Alalle tulon kynnyksen ja mahdollisten kilpailuoikeudellisten kysymysten kannalta on myös parempi, että viranomainen vastaa vähimmäisvaatimusten*

asettamisesta. Tiedonvaihto erilaisten kriteeristöjen hyödyntämisestä ja tulkintakysymyksistä voi toki soveltua yhteissääntelyn piiriin.

***Informaatio-ohjaus.** Valmistelussa on harkittu vaihtoehtona sitä, että tietoa toimijoiden käyttämistä auditointikriteeristöistä julkaistaisiin Viestintäviraston verkkosivuilla olevassa rekisterissä. Tietoturvallisuuden ylläpito on kuitenkin perusvaatimus, jonka vähimmäistasoa ei voida pitää kilpailuasiana.*

Vuonna 2016 arvioitiin määräysvalmistelussa seuraavia asioita:

Millä tarkkuudella tunnistuspalvelun arviointivaatimukset eli auditointikriteeristö laaditaan määräykseen? Vaihtoehdot olivat yksityiskohtainen yhdenmukainen kriteeristö tai yleistason kriteeristö, jota täydennetään soveltamissuosituksella.

Määräyksen 15 §:ään otettiin vaikutusarvioinnin perusteella otsikkotason luettelo asioista, jotka arvioinnin täytyy kattaa. Luettelossa tukeudutaan EU:n varmuustasoasetuksen mukaiseen vaatimusten ryhmittelyyn.

Tarkoitus on, että toimijat voivat hyödyntää joustavasti arviointikriteeristöjä, joita ne muutoinkin jo käyttävät. Toisaalta toimijoiden täytyy arvioida ja varmistaa, että niiden käyttämät eri standardeihin perustuvat kriteeristöt todella kattavat kaikki vaaditut tunnistusjärjestelmän arvioinnin osa-alueet. Virasto joutuu myös tarkastuskertomuksia valvoessaan arvioimaan, että tämä toteutuu.

3.2.3 Tunnistuspalveluntarjoajan sisäisen tarkastuslaitoksen riippumattomuus ja pätevyys

Arvioitava kysymys: Miten tunnistuspalvelun sisäisen tarkastuksen vaatimukset määritellään ennakoitavasti ja yleispätevästi siten, että ne takaavat objektiivisesti luotettavan, riippumattoman ja pätevän arvioinnin ja samalla mahdollistavat esim. muuhun sektorikohtaiseen, kuten finanssialan säädäntöön, perustuvat tarkastuskehykset?

Näkökohtia vaikutusarviointiin

Tunnistus- ja luottamuspalvelulain 33 §:n yleiset riippumattomuus- ja pätevyysvaatimukset koskevat myös sisäistä tarkastusta. Viestintävirasto voi määrätä arviointielimen pätevyysvaatimuksista ja tunnistuspalvelun vaatimustenmukaisuuden arvioinnissa käytettävistä arviointiperusteista. Arviointiperusteiksi voidaan määrätä säädösten lisäksi Euroopan unionin tai muun kansainvälisen toimielimen antamia säännöksiä tai ohjeita, julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta koskevia ohjeita ja yleisesti käytettyjä tietoturvallisuusstandardeja tai menettelyjä.

Määräyksen vaatimusten tarkoitus on turvata sitä, että sisäisen tarkastuksen pätevyysvaatimukset ovat yleispäteviä, tasapuolisia ja ennakoitavia. Tavoitteena on ollut koota esimerkkiviitteitä sellaisiin säännöstöihin, joihin sisäisen tarkastuksen riippumattomuus ja pätevyys voi objektiivisesti arvioiden perustua sen sijaan, että se perustuisi vain toimijan omaan arvioon ja toimintatapaan.

Sisäisen tarkastuksen pätevyysvaatimusten valmistelussa on pyritty selvittämään erityisesti pankkien sisäisen tarkastuksen sääntelyperustaa, koska sisäinen tarkastus on alalla vakiintuneesti käytössä ja sitä säännellään mm. Finanssivalvonnan määräyksillä ja ohjeilla.

Työryhmältä ei saatu määräyksen valmistelun yhteydessä tietoa sisäisen tarkastuksen sääntelystä, standardeista tai ohjeistuksesta muilla aloilla.

EU:n varmuustasoasetuksen epävirallisessa soveltamisohjeessa [10] todetaan seuraavaa: Standardissa EN ISO 19011 on johtamisjärjestelmien auditointia koskevia ohjeita, mukaan lukien sisäisen ja ulkopuolisen tarkastuksen periaatteet sekä ohjeita siitä, miten tarkastusprosessiin osallistuvien henkilöiden osaamista voidaan arvioida. Valmistelussa kyseinen standardi on kuitenkin arvioitu varsin yleispiirteiseksi.

Lisäksi valmistelussa on saatu tietoturvallisuuden arviointisektorilta tieto, että sisäisestä auditoinnista on olemassa IIA-standardeja. Näihin ei ole valmistelussa perehdytty, eikä mikään nykyisistä toimijoista ole todennut käyttävänsä niitä, mutta ne on huomioitu määräyksessä.

Linjaukset

Määräyksen vaatimukset sisäiselle tarkastukselle laaditaan siten, että esimerkit antavat selvän käsityksen sitä, millaisiin säännöksiin, standardeihin tai ohjeisiin riippumattomuus ja pätevyys voi perustua.

Tavoitteena on, että erityisesti pankit voivat hyödyntää sektorikohtaiseen sääntelyyn perustuvia tarkastuksiaan. Edellytyksenä on, että nämä tarkastukset kohdistuvat muun ohessa myös tunnistusjärjestelmään.

Määräyksen 19 § on laadittu näiden linjausten mukaan.

Määräykselle vaihtoehtoiset ohjauskeinot

***Suositus/ohje.** Viestintävirasto on arvioinut valmistelussa, että vaatimukset on tarpeen määritellä ennakoitavasti pakottavalla säännöksellä, jotta on tarvittaessa myös perusteet hylätä toimijan subjektiiviseen näkemykseen tukeutuvat sisäiset arvioinnit.*

***Yhteissääntely.** Ei ole tarkasteltu.*

***Informaatio-ohjaus.** Ei ole tarkasteltu erikseen vertailukelpoisen tiedon tuottamista sisäisen tarkastuksen laadun ohjauskeinona. Muutoin valmistelussa on todettu, että tietoturvallisuus ja sen hallinta on perusvaatimus, jonka vähimmäistaso ei ole kilpailutekijä.*

3.2.4 Tunnistuspalveluiden arviointivaatimusten taloudelliset vaikutukset

MPS2016 kohta 3.3

Viestintävirasto on koonnut valmistelun aikana tietoja nykyisten tunnistuspalveluntarjoajien teettämistä auditoinneista määräystyön tueksi. Kyselyn tavoitteena oli saada kattavasti tietoa jo tehdyistä auditoinneista ja toisaalta muodostaa arvio siitä, mitä lisätyötä määräyksessä asetettavat auditointivaatimukset mahdollisesti aiheuttaisivat toimijoille.

Toimijoille tehdystä kyselystä ja EU:n varmuustasoasetuksen soveltamisohjeesta on kerätty listaa esimerkkistandardeista, joiden perusteella tunnistuspalvelun arviointeja tehdään.

Selvityksen perusteella päädyttiin siihen, että tunnistuspalveluiden käyttämien ulkoisten ja sisäisten arviointielinten vaatimukset määritellään neutraalisti, jotta toimijat voivat hyödyntää mahdollisimman laajasti tällä hetkellä jo käyttämiään auditointikehyksiä.

Ratkaisulla pyritään pitämään toimijoille tunnistuspalveluiden auditointivaatimuksista aiheutuvat kustannukset mahdollisimman maltillisina. Selvityksessä esille tulleet standardit on huomioitu määräyksessä vaihtoehtoina auditoijien riippumattomuuden ja pätevyyden osoittamisessa, jotta toimijat voisivat hyödyntää mahdollisimman paljon nykyisiä auditointejaan.

Vaatimusten osa-alueita, joilta edellytetään riippumatonta arviointia, on myös rajattu edellä kohdassa 3.2.2 kuvatulla tavalla.

3.2.5 Tunnistus- ja luottamuspalveluiden arviointitoiminnan kilpailun edistäminen

MPS2016 kohta 3.7

Arvioitava kysymys: Voidaanko määräyksen vaatimuksilla edistää arviointielinten tarjontaa tai kilpailua?

Arvioinnin lähtökohdat

Perusvaatimukset arviointielinten käyttämisestä ja vaatimuksista säädetään eIDAS-asetuksessa ja tunnistus- ja luottamuspalvelulaissa. Määräyksen vaikutusarvioinnissa ei arvioida eIDAS-asetuksen tai lain vaikutuksia, vaan niiden tavoitteet ovat myös määräyksellä edistettäviä tavoitteita.

Vaatimustenmukaisuuden arviointilaitosten vaatimukset perustuvat EU-tason säännöksiin ja standardointiin, joten Viestintävirasto pystyy vaikuttamaan laitosten syntymiseen sujuvalla prosessilla ja yhteistyöllä FINASin kanssa. Tästä on saatu hyvää kokemusta tietoturvallisuuden arviointilaitosten perustamisen yhteydessä.

Tunnistuspalveluiden käyttämien ulkoisten arviointielinten suhteen EU:n varmuustasoasetuksen ja tunnistus- ja luottamuspalvelulain vaatimukset ovat yleisluonteisemmat kuin luottamuspalveluiden vaatimustenmukaisuuden arviointilaitoksille. Määräyksen antamisessa on pidettävä huolta siitä, että vaatimukset määritellään mahdollisimman neutraalisti.

Kilpailun ja tarjonnan syntyminen on kiinni ennen kaikkea kysynnästä.

Linjaus

Arviointipalvelujen tarjontaa voidaan edistää lähinnä huolehtimalla siitä, että säännösympäristö on selkeä ja kansainvälisesti yhdenmukainen. Määräyksessä viitataan siksi (vain) kansainvälisiin standardeihin, joiden asema ei muutoin ole oikeudellisesti selvä.

Määräykselle vaihtoehtoiset ohjauskeinot

Suositus/ohje. *Ohjeet 211/2106 O tunnistuspalvelun arvioinnin mallikriteeristöstä ja 215/2016 O sähköisten tunnistus- ja luottamuspalveluiden tarkastuskertomuksista helpottavat tunnistuspalveluiden arviointielimien kilpailuttamista.*

Yhteissääntely. *Tätä voidaan tarkastella siinä vaiheessa, kun arviointitoimintaa syntyy.*

Informaatio-ohjaus*. Tässä vaiheessa ei ole olemassa vertailevaa tietoa, jonka julkaisemisella voitaisiin edistää kilpailua.*

3.3 Lähteet/referenssit/standardit

MPS2016 viitteitä ja teknisten vaatimusten valmistelumuistion viitteitä.

[4] FINAS (Finnish Accreditation Service) Turvallisuus- ja kemikaaliviraston (Tukes) akkreditointiyksikkö https://www.finas.fi/Sivut/default.aspx

[23] Komission täytäntöönpanoasetus (EU) 2015/1501 **yhteentoimivuusjärjestelmän vahvistamisesta sähköisestä tunnistamisesta** ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 12 artiklan 8 kohdan mukaisesti

[26] BIS, Bank for International Settlements: External audits of banks - http://www.bis.org/publ/bcbs280.htm, The internal audit function in banks http://www.bis.org/publ/bcbs223.htm

[27] Finanssivalvonnan määräys- ja ohjekokoelma http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Uusi/Documents/4.1.std5.pdf

- [1] Laki vahvasta sähköisestä tunnistamisesta ja sähköistä luottamuspalveluista (617/2009 muutoksineen, tunnistus- ja luottamuspalvelulaki)
- [3] * EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (nk. eIDAS-asetus)
- [2] EU:n komission täytäntöönpanoasetus (EU) 2015/1502 (nk. varmuustasoasetus) teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti
- [10] ”LOA guidance” EU:n varmuustasoasetuksen epävirallinen soveltamisohje
  - https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents
  - Suomennos https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf

- ISO/IEC 27001:2013 Information security management (tai uudempi)
- Häiriönhallinnan ISO/IEC (myös SFS) [tarkenna]
    - x
- Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta (SFS-ISO/IEC 27005)
- ETSI
    - varmennestandardit tunnistusvarmenteen kannalta
- [18] NISTin (National Institute of Standards and Technology) FIPS-standardit (Federal Information Processing Standards) www.nist.gov
- [19] SANS (The SANS Institute) www.sans.org
- [15] KATAKRI 2020, Tietoturvallisuuden auditointityökalu viranomaisille
    - https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille
- Pilvipalveluiden turvallisuuden arviointikriteeristö, PiTuKri
    - https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

3.4 Toimialakysely 2020 muutostarpeista

Seuraavaan on koottu viraston elokuussa 2020 tekemästä muutostarvekyselystä aiheeseen liittyviä kysymyksiä ja vastauksia. Vastauksia on tässä koosteessa osittain niputettu ja anonymisoitu.

3.4.1 Kysymykset arviointielimistä

61) Arviointielinten vaatimukset. Ovatko määräyksen 18 §:n ja 19 §:n standardi- ja määräysluettelot ajan tasalla? Ovatko listatut lähteet relevantteja? Puuttuuko jotain?

- Nämä kohdat ovat riittävät.
- Erityisesti 18 §:n ja 19 §:n alakohtien mahdollistamat muut kriteeristöt ovat mahdollisia ja niiden soveltaminen näytetään tarvittaessa arvioinnin yhteydessä.
- jos palveluntarjoaja tarjoaa luottamuspalveluita, esimerkiksi tähän liittyvään ETSI-kriteeristön arviointiin on mahdollista viitata, samoin kuin yleiseen ISO/IEC 27001 -standardiin tunnistuspalvelun arvioinnissa.

62) Arviointielinten vaatimukset. Mitä listatuista itse hyödynnätte/käyttämänne arviointielin hyödyntää?

- Ruotsin Finansinspektionin (FFFS) ja Suomen Finanssivalvonnan määräyksiä ja ohjeita koskien sisäisen tarkastuksen organisointia ja toimintaa (mm Fiva)
- kansainvälisen kattojärjestön IIA:n ohjeita, sääntöjä ja tarkastusperiaatteita (The Institute of Internal Auditors, www.theiia.fi).
- pätevyys toimia eIDAS-arviointeja toteuttavana perustuu ISO27001-akkreditointiin, sekä asemaan Traficomin hyväksymänä arviointilaitoksena.
- ISO/IEC 27001- ja ETSI-kriteeristöjä

- ETSI-kriteeristöjä

63) Arvioinnin vaatimukset. Ovatko määräyksen perustelumuistion lähteet relevantteja? Puuttuuko jotain?

- Lähdeluettelo on kattava.

64) Arvioinnin vaatimukset. Mitä listatuista itse hyödynnätte/käyttämänne arviointielin hyödyntää?

- ISO 27001 standardia
- osittain sisäisiä tarkastusohjelmia ja tarkastuskäsikirjaa (Global Audiot Manual)
- IIA:n ammatillista ohjeistusta sekä eri osa-alueiden tarkastamisen parhaita käytänteitä (best practices)
- fyysisen turvallisuuden osalta valtiohallinnon Katakri auditointityökalu

65) Arviointiohje. Olisiko arvioinnin esimerkkistandardit ja lähteet tarkoituksenmukaisempaa siirtää perustelumuistiosta arviointiohjeeseen 211/2019?

- Ne on tarkoituksenmukaista sisällyttää molempiin, huomioiden myös määräyksen ja ohjeen eritasoinen sitovuus.

3.4.2 Kysymykset arviointikriteereistä ja muista vaatimuksista

66) Arviointikriteerit. Onko määräyksen 15 §:n tarkkuustaso arvioitavista asioista mielestänne tarkoituksenmukainen?

- On, huomioiden, että perustelumuistiossa todetun mukaisesti pykälässä luetellut osa-alueet ja arviointikriteerit perustuvat eri säädösten vaatimuksiin, erityisesti EU:n varmuustasoasetuksen vaatimuksiin.

67) Arviointikriteerit. Olisiko kriteereitä tai arviointiperusteita tarkasteltava määräysvalmistelussa? Olisiko niitä tarkennettava joltain osin?

- Kriteereitä ja arviointiperusteita on käsitelty yksityiskohtaisemmin arviointiohjeessa, viittaus arviointiohjeeseen perustelumuistiossa on riittävä ja perusteltu.
- Määräyksen 15 §:n sisältöä tukee myös perustelumuistion viittaus tarkastuskertomusohjeeseen.

68) Tunnistusjärjestelmä ja alihankkijat. Onko määräysvalmistelussa tarpeen tarkastella tunnistusjärjestelmän arkkitehtuuriin ja alihankintaan liittyviä kysymyksiä?

- Arkkitehtuurilla ja alihankkijoilla on yhteys palvelutoteutuksiin ja palveluntarjonnassa käytettävään henkilökuntaan, minkä yksityiskohtaisempi tarkastelu arviointiohjeen ja tarkastuskertomusohjeen yhteydessä on riittävää.

69) Arviointiohje. Onko arviointiohje toimiva vai olisiko siinä jotain korjaustarpeita?

- *Arviointiohje on varsin kattava ja yksityiskohtainen.*
- *Määräyksen tueksi on laadittu auditointeja tukevaa materiaalia, kuten auditointikriteeristöjä. Tämä on erittäin tärkeää.*
- *Ensisijaisesti mallikriteeristön ja muun materiaalin tulee noudattaa samaa rakennetta kuin M72 tai muu normi, johon se liittyy. Materiaalin tehtävänä on vaatimuksen auditoinnin tukeminen. Tällä on merkitystä niin auditoinnin suunnittelussa kuin löydösten raportoinnissa*

- *Toissijaisesti on mallikriteeristössä tai muussa materiaalissa noudatettava tunnettuja kansainvälisiä tai kansallisia auditointikriteeristöjä. ISO 27001, OWASP ja Katakri ovat esimerkkejä näistä. PCI DSS on tuttu monille.*
- *Mallikriteeristössä suuri ei ole kaunista. On tärkeämpää auditoida tärkeät kohdat perusteellisesti kuin yrittää auditoida kaikkia asioista ihan pikkuisen.*
- *Kriteeristön kääntäminen englanniksi on tärkeää.*
- *Mobiiliratkaisujen auditoinnissa on tukeuduttu OWASP.n auditointikriteeristöön, mikä on hyvä asia. Näin on syytä menetellä myös jatkossa ja pitää mobiiliauditointikriteeristö ajan tasalla.*
- *Vaikka ISO 27001:n mukainen tietoturvan johtamisjärjestelmä oikein tehtynä täyttää M72A vaatimukset, on muistettava, että näitä johtamisjärjestelmiä perustavat, hallinnoivat ja auditoivat ihmiset. Olisi erittäin suotavaa, että ennen edes sertifioidun johtamisjärjestelmän hyväksilukua siitä tarkastettaisiin seuraavat kohdat:*
    - *Sertifikaatin voimassaolo. Siitä vireillä olevien valitusten, erikoisauditointien tai muiden sertifikaatin uskottavuutta vaarantavien asioiden selvittäminen sertifiointielimeltä olisi hyvä asia, mutta ei välttämätöntä*
    - *Johtamisjärjestelmän kohdissa 4.2b (”the requirements of these interested parties relevant to information security.”) ja A.18 Compliance M72 ja eIDAS on otettu huomioon.*
    - *Johtamisjärjestelmän auditointiraportissa ei ole esitetty merkittävää poikkeamaa, joka on korjaamatta ja joka koskee em. kohtia. Muiden vakavien poikkeamien arviointi on tapauskohtaista, mutta on perusteltua lähteä olettamasta, ettei näillä ole vaikutusta 4 § täyttymisen osalta, jos ISO 27001 sertifikaatti on voimassa.*
    - *ISO 27001 sertifikaatti on voimassa kolme vuotta (audit cycle), jonka aikana on vuosittaiset seuranta-auditoinnit. eIDAS-sykli on kaksi vuotta, joten on perusteltua linkittää nämä toisiinsa. Esimerkiksi niin, että eIDAS-auditoinnissa edellytetään ISO-sertifioinnin olevan voimassa yhden vuoden auditoinnin päättymisen jälkeen. Vaikka sertifioinnista luovuttaisiin, on mahdollista, että johtamisjärjestelmä on edelleen standardia noudattava, joten on perusteltua antaa yhden vuoden siirtymäaika (eli seuraavaan eIDAS-auditointiin saakka).*
- *Traficomin olisi hyvä antaa ohjeistus, mitkä auditoinnit ja näihin liittyvät todistukset voidaan lukea hyväksi (ISO 27001:n lisäksi) näyttönä M72 noudattamisesta.*

70) Tunnistuspalveluntarjoajan muut vaatimukset. Onko määräyksessä tai ilmoitusohjeessa muutostarpeita, joita pitäisi tarkastella määräysvalmistelun yhteydessä?

- *Emme ole tällä hetkellä havainneet muutostarpeita.*

4 Muutosvaihtoehdot ja vaikutusarviointi 2021

4.1 Arviointikriteeristö (15 § selkeytys, ml. tietoturvallisuuden hallinnan arvioinnin ja vaatimustenmukaisuuden hallinnan arvioinnin suhde)

4.1.1 Säännösluonnos arviointikriteerit ja -kriteeristöt

15 kohta ~~§~~ Arviointikriteerit

15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioinnin osa-alueet

Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat

1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän)
a) tietoturvallisuuden hallintaan
b) tietojen säilyttämiseen
c) tiloihin ja henkilökuntaan
d) teknisiin toimenpiteisiin

2) tunnistusmenetelmään eli tunnistusvälineen
a) hakemiseen ja rekisteröintiin
b) hakijan henkilöllisyyden todistamiseen ja varmentamiseen
c) tunnistamisen menetelmän ominaispiirteisiin ja laatimiseen
d) myöntämiseen, toimittamiseen ja aktivointiin
e) voimassaolon keskeyttämiseen, peruuttamiseen ja uudelleen aktivointiin
f) uusimiseen ja korvaamiseen
g) todentamismekanismeihin

15.2 Arviointikriteeristöt

1. Edellä 15.1 kohdassa ~~momentissa~~ mainittujen osa-alueiden arvioinnin on kattettava kaikki ~~perustuttava~~ tunnistus- ja luottamuspalvelulain ja tämän määräyksen vaatimukset.

2. Arviointi voi perustua Liikenne- ja viestintäviraston arviointiohjeeseen tai ~~iin,~~ EU:n tai muun kansainvälisen toimielimen antamiin säännöksiin tai ohjeisiin, julkaistuihin ja yleisesti tai alueellisesti sovellettuihin tietoturvallisuutta koskeviin ohjeisiin tai yleisesti käytettyihin tietoturvallisuusstandardeihin tai menettelyihin. Arviointi voi perustua usean edellä mainitun lähteen yhdistelmään.

4.1.2 Perustelut ja soveltaminen

Säännöksen sanamuotoa on selkeytetty. Vaatimusten sisältö ei ole muuttunut.

MPS2016:

Lakia tarkentavien arviointivaatimusten vaihtoehtojen ja vaikutusten arviointi on määräyksen valmistelun tärkein osa-alue tietoturvallisuuden, toimijoiden tasapuolisen kohtelun, toimijoille aiheutuvien taloudellisten vaikutusten ja viranomaistoiminnan resursoinnin kannalta.

4.1.3 Tietoturvallisuuden hallinnan arviointi ja koko vaatimustenmukaisuuden arviointi

15.2.1

On syytä huomata, että tietoturvallisuuden ja riskien hallinta ei riitä täyttämään tunnistusjärjestelmän vaatimuksia, vaan tunnistusjärjestelmän on kaikilta osin täytettävä tekniset vaatimukset, joista säädetään tunnistuslaissa ja muualla tässä määräyksessä.

Vaatimustenmukaisuuden arvioinnin kannalta tämä tarkoittaa sitä, että pelkkä tietoturvallisuuden hallinnan arviointi ei riitä osoittamaan säädettyjen vaatimusten täyttämistä, vaan on nimenomaisesti arvioitava, täyttääkö järjestelmä esimerkiksi tietoliikenteen salausvaatimukset.

Vrt. LOA guidance

Riskienhallinnassa yleisenä periaatteena on, että organisaation on itsensä valittava, minkä tasoista riskiä se pitää hyväksyttävänä. Kohdan 2.4 vaatimuksella muutetaan tätä yleistä

periaatetta, sillä sen mukaan organisaation turvatoimenpiteiden on oltava suhteutettuja riskeihin kulloisellakin tasolla.

4.1.4 Perustelujen esimerkkilistan päivittämistarve

15.2.2

Määräyksen perustelumuistioon koottiin 2016 määräysvalmistelussa työryhmältä esimerkkejä standardeista tai muista lähteistä, joiden mukaisia arviointeja tunnistuspalvelurekisteriin merkityt toimijat kyselyn perusteella käyttävät. Valmistelussa tai perustelumuistiossa ei ole eritelty riippumattomuuden ja pätevyyden perusteita tai arvioitu, miltä osin lähteet soveltuisivat tunnistusjärjestelmän vaatimusten arviointiin.

Standardit tai lähteet voivat soveltua myös tunnistusjärjestelmän arviointiin.

Esimerkkilista
- ISO 27001
- PCI DSS, PCI/QSA
- Webtrustin Trust Services Principles and Criteria for Certification Authorities ja Webtrust for Certification Authorities - SSL Baseline Requirements Audit Criteria
- Information Security Forumin (ISF) "Standard of Good Practice"
- ISF:n IRAM-kriteeristö (Information Risk Analysis Methodology)
- ETSI TS 101456 (CA policy)
- ISRS 4400 ja ISAE 3000
- Katakri
- Vahti
- Euroopan keskuspankin tai FIVA:n määräykset tai ohjeet
- FIVA:n määräys ja ohje 2.4 "Asiakkaan tunteminen - rahanpesun ja terrorismin rahoittamisen estäminen"
- Euroopan keskuspankin Cybersecurity questionnary 2015
- BISin (Bank for International Settlements) ohje External audits of banks

Onko määräyksen perusteluissa oleva lista informatiivinen, hyödyllinen ja ajan tasalla?

4.1.5 Muut ohjauskeinot

Ohje. Liikenne- ja viestintäviraston arviointiohje 211/2019 O kattaa kaikki 15.1 ja 15.2.1 kohdassa tarkoitetut vaatimukset.
Suositus. Ei huomioita.
Yhteissääntely. Ei huomioita.
Informaatiolla ohjaaminen. Ei huomioita.

4.2 Arviointielimen riippumattomuus ja pätevyys (18 § ja 19 §)

Arvioitava kysymys:
Ovatko 18 § ja 19 §:n viittaukset soveltuvia ja ajan tasalla
Onko perustelumuistion esimerkkistandardilista arvioinnille soveltuva, ajan tasalla ja hyödyllinen

4.2.1 Säännös 18, ulkoinen arviointielin

18 kohta ~~§~~ Tunnistuspalvelun ulkoisen arviointielimen vaatimukset

Tunnistus- ja luottamuspalvelulain 33 §:ssä arviointielimelle säädettyjen riippumattomuus- ja pätevyysvaatimusten täyttymisen voi osoittaa

6) ISO/IEC 27001 -standardiin perustuvalla akkreditoinnilla tai osoittamalla muutoin pätevyys standardin mukaiseen arviointiin;
7) Webtrust -säännöstöön perustuvalla kansainvälisesti tunnetun itsesääntelyjärjestelyn mukaisesti osoitetulla pätevyydellä;
8) PCI DSS - maksukorttistandardiin perustuvalla akkreditoinnilla tai osoittamalla muutoin pätevyys standardin mukaiseen arviointiin;
9) ISACA:n standardien ja tietojärjestelmien valvontakehikon mukaisesti osoitetulla pätevyydellä; tai
10) muiden edellisiin rinnastettavien yleiseen tietoturvallisuuden hallintaan taikka sektorikohtaiseen sääntelyyn tai standardointiin liittyvien säännösten, ohjeiden tai standardien edellyttämän pätevyyden osoittamisella tai noudattamisella.

Pätevyyden osoittaminen tunnistusjärjestelmän arviointiin edellyttää sitä, että osoitetaan myös, miten ja miltä osin edellä 1 momentissa tarkoitetut säännökset, ohjeet tai standardit kohdistuvat tunnistusjärjestelmään.

Viraston arvion mukaan esimerkkilistassa ei ole muutostarpeita.

4.2.2 Säännös 19, sisäinen arviointielin

19 kohta ~~§~~ Tunnistuspalvelun sisäisen tarkastuslaitoksen vaatimukset

Tunnistus- ja luottamuspalvelulain 33 §:ssä sisäiselle tarkastuslaitokselle säädettyjen riippumattomuusvaatimusten täyttymisen voi osoittaa:

7) IIA:n ammattistandardien (sisäisen tarkastuksen riippumattomuus ja objektiivisuus, ml. organisatorinen riippumattomuus) noudattamisella;
8) ISACA:n standardien ja tietojärjestelmien valvonnan kehikoiden noudattamisella;
9) BIS:in (Bank for International Settlements) sisäistä tarkastusta koskevien ohjeiden noudattamisella;
10) Finanssivalvonnan määräys- ja ohjekokoelman sisäistä tarkastusta koskevien ohjeiden noudattamisella;
11) muiden ETA-alueen jäsenvaltioiden vastaavien valvontaviranomaisten antamien ohjeiden tai määräysten noudattamisella; tai
12) muilla edellisiin rinnastettavilla viranomaissääntelyyn tai yleiseen riippumattoman sisäisen tarkastuksen hallintaan liittyvien standardien noudattamisella.

Pätevyyden osoittaminen tunnistusjärjestelmän arviointiin edellyttää sitä, että osoitetaan myös, miten ja miltä osin 1 momentissa tarkoitettujen säännösten, ohjeiden tai standardien mukaisesti organisoitu sisäinen tarkastus kohdistuu tunnistusjärjestelmään.

Viraston arvion mukaan esimerkkilistassa ei ole muutostarpeita.

4.2.3 Muut ohjauskeinot

Ohje.
Suositus.

Yhteissääntely.
Informaatiolla ohjaaminen.

4.3 Solmupisteen tietoturvallisuuden arviointi

Arvioitava kysymys: Onko solmupisteen tietoturvallisuuden arvioinnin perusteita arvioitava määräysvalmistelussa? DVV toivonut arviointia ja komission eIDAS-työryhmässä ollaan selvittämässä asiaa.

Liikenne- ja viestintävirasto käsittelee säännöksen erikseen DVV:n kanssa.

5 Säädäntö

5.1 Määräyksen antamisen perusta

Viestintävirastolla on tunnistuslain 42 §:ssä määräysvaltuus tunnistuspalvelun vaatimustenmukaisuuden arviointiperusteista ja arviointielinten pätevyysvaatimuksista.

5.2 Asiaan liittyvät säännökset

Tunnistus- ja luottamuspalvelulaissa edellytetään, että tunnistuspalveluntarjoaja hankkii vaatimustenmukaisuuden arvioinnin.

Arvioinnin voi lain 29 §:n mukaan tehdä vaatimustenmukaisuuden arviointilaitos, muu ulkoinen arviointilaitos tai sisäinen tarkastuslaitos.

Arvioinnin täytyy EU:n varmuustasoasetuksen liitteen 1 kohdan 2.4.7 mukaan kattaa kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot. Viittaus varmuustasoasetukseen on tunnistuslain 8.1 §:n 5 alakohdassa, joka koskee tietoturvallisuuden hallintaa.

Arviointielimen riippumattomuus- ja pätevyysvaatimuksista säädetään lain 33 §:ssä.

EU:n komission varmuustasoasetus ja soveltamisohje

2.4.7 Noudattaminen ja tarkastus

MATALA

Määräajoin tehdään sisäisiä tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

OHJE:

Tarkastuksissa huomioidaan järjestelmään/järjestelmän osiin liittyvä riskitaso. Tämä tarkoittaa, että tarkastuksen perinpohjaisuus saattaa eri varmuustasoilla olla hyvinkin erilainen.

Sisäistä tarkastusta koskeva vaatimus voidaan täyttää myös käyttämällä ulkopuoliselta hankittua tarkastusta. Tasolla ”matala” ei vaadita riippumatonta tarkastusta (riippumattoman määritelmästä tarkemmin jäljempänä).

Tietoturvallisuuden hallintajärjestelmää koskevassa tarkastuksessa tavanomaisena menettelynä on, että kaikki järjestelmän osat käydään läpi kolmen vuoden aikana, mihin sisältyvät myös vuosittain toistuvat valvontatarkastukset.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohdan A.18 "Compliance" (vertaa kohta A.18.2, "Information security review") mukaisia turvatoimenpiteitä.

5.3 Muu sääntely