Lausuntoyhteenveto Traficomin suositusluonnoksesta NIS-valvoville viranomaisille NIS2-direktiivin mukaisten kyberturvallisuuden riskienhallinnan toimenpiteiden valvomiseksi

Sisällys

1 Traficomin suositusluonnos

1.1 Lausunnot Traficomin suositusluonnoksesta

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus (jäljempänä "Traficom") pyysi lausuntopalautetta suositusluonnokseen valvoville viranomaisille NIS2-direktiivin mukaisten kyberturvallisuuden riskienhallinnan toimenpiteistä. Suositusluonnos oli lausuntokierroksella lausuntopalvelu.fi -palvelussa suomeksi 8 viikkoa ajalla 5.4.2024 - 31.5.2024 (diaarinumero: Traficom/18410/09.00.02/2023).

Suositusluonnoksesta vastaanotettiin yhteensä 16 lausuntoa.

Lausunnonantajat edustivat lainsäädännön soveltamisalaan kuuluvia valvovia viranomaisia ja toimijoita sekä lainsäädännön soveltamisalaan kuulumattomia tahoja. Suositusluonnoksesta lausuivat seuraavat tahot: Rakennusteollisuus RT ry, Suomen Tunnustuksellinen Luterilainen Kirkko, Maa- ja metsätalousministeriön Tieto- ja tutkimustoimiala, Finnish Information Security Cluster - Kyberala ry, FiCom ry, Suomen Vesilaitosyhdistys ry, Suomen Varustamot ry, Elinkeinoelämän keskusliitto EK, Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira, Suomen Kuntaliitto ry, Ruokavirasto, Energiateollisuus ry, Lääkealan turvallisuus- ja kehittämiskeskus Fimea ja Tiedonhallintalautakunta. Lisäksi Verizon toimitti yleisen kannanoton NIS2-direktiivin yhtenäisestä täytäntöönpanosta jäsenmaissa. Turvallisuus- ja kemikaalivirasto Tukesilla ei ollut lausuttavaa asiaan.

1.2 Tiivistelmä lausunnoista

Lausuntopalautteen mukaan suositusluonnoksen koettiin yleisesti ottaen toimivan valvovan viranomaisen ja toimijan tukena. Suosituksen koettiin konkretisoivan lainsäädännön mukanaan tuomien riskienhallintavelvoitteiden toteuttamista käytännön tasolla. Suositusluonnoksen sisältöä pidettiin lähtökohtaisesti kattavana ja rakennetta selkeänä, koska se noudattaa kyberturvallisuuslain hallituksen esityksen rakennetta vastaavilta osin. Esitystavaksi valittu taulukointi koettiin ymmärrettävyyttä helpottavaksi. Kannatettavana pidettiin sitä, että kukin yksittäinen suositustoimenpide on perusteltu ja sisältää selkeän viittauksen viitekehyksiin.

Toisaalta, kunkin riskienhallintatoimenpiteen tarkastelu yksittäisenä toimenpiteenä muista vaatimuksista erillään koettiin myös haastavana, koska se voi ohjata jokaisen riskin hallintaan samalla intensiteetillä. Lisäksi toivottiin suosituksen sisältämien toimenpiteiden keskinäisen kompensoinnin parempaa huomioimista. Suositus koettiin myös pitkäksi, jonka vuoksi toivottiin tiivistelmää hallintatoimenpiteistä.

Suosituksessa on pyritty tietoisesti esittelemään jokaista riskienhallintatoimenpidettä omana itsenäisenä kokonaisuutenaan ja kuvaamaan hallintatoimen sisältöä, jolloin toteutusesimerkeissä on osittaista päällekkäisyyttä. Suosituksessa esiteltyyn jokaiseen yksittäiseen riskienhallintatoimenpiteeseen sisältyvän perustelutekstin katsottiin toimivan tiivistelmänä.

Suosituksen terminologiaa selkeytettiin ja suosituksessa käytettyjä viitteitä tarkennettiin palautteen mukaisesti. Suosituksen johdantotekstiä täydennettiin ja tarkennettiin siltä osin kuin saatu palaute koski suhteellisuusperiaatetta, johdon vastuuta, riskiperusteisuutta ja suosituksen suhdetta viranomaisten mahdollisesti antamiin tarkentaviin teknisiin määräyksiin. Lisäksi suosituksen lukuohjetta täydennettiin tarkentamalla korkeamman kyberriskin omaavien toimijoiden määritelmää.

Suosituksen sisältämien riskienhallintatoimenpiteiden ja suosituksessa käytettyjen viitekehysten (standardien ja arviointikriteeristöjen) vastaavuus koettiin haasteellisena. Saadun palautteen vuoksi Traficomin laatima ristiinvetodokumentti lisättiin suosituksen liitteeksi mutta suosituksen johdantoa täydennettiin mahdollisten väärinymmärrysten välttämiseksi siitä, että kyseessä olisi yhdenmukaistetut standardit, jotka suoraan täyttäisivät lain vaatimukset.

Suosituksen sisältämiin riskienhallintatoimenpiteisiin lausuttiin sekä yleisissä lausunnoissa että toimenpidekohtaisissa lausunnoissa. Suositus päivitettiin ensisijaisesti vastaamaan muuttunutta kyberturvallisuuslain hallituksen esitystä, jonka jälkeen suosituksen lausuntokierrokselta saadut kyberturvallisuustoimenpiteisiin kohdistuneet lausuntopalautteet huomioitiin mahdollisuuksien mukaan muuttamalla tai tarkentamalla suositusta. Huomiot toimialakohtaisista standardeista ja ohjeista lisättiin suositukseen ehdotusten mukaisesti.

Lisäksi lausuntokierroksen yhteydessä saatiin välittömästi riskienhallintatoimenpiteiden valvontaan ja resursseihin liittyvää palautetta, jota suosituksessa ei voitu ottaa huomioon. Valvontaan ja toimijoiden resursseihin liittyvät palautteet välitetään mahdollisuuksien mukaan valvoville viranomaisille osana Traficomin tulevaa NIS2-direktiivin mukaista tehtävää keskitettynä yhteyspisteenä.

Lausuntopalautteiden mukaan ongelmallisena pidettiin suositusluonnoksen lausuntoajankohtaa ennen kyberturvallisuuslain eduskuntakäsittelyn päättymistä, joka oli myös Traficomin tiedossa. Suositusluonnos tuotiin Traficomin toimesta lausuttavaksi lausuntoajankohdan haasteellisuudesta huolimatta, koska sen katsottiin konkretisoivan keskeneräisenäkin riskienhallintatoimenpiteiden toteutusta ja tuovan apua erityisesti lainsäädännön soveltamisalaan uutena tuleville valvoville viranomaisille ja toimijoille.

2 Yleiset lausunnot suositusluonnoksesta

2.1 Suositus valvovan viranomaisen ja toimijan tukena

Suosituksen koettiin toimivan kokonaisuutena hyvänä lähtökohtana valvonnalle ja tukevan valvovia viranomaisia kansallisen sääntelyn yhdenmukaisessa soveltamisessa yli toimialarajojen. Suositusluonnos yhtenäistää valvontakäytäntöjä eri sektoreilla, jättäen kuitenkin valvovalle viranomaiselle tapauskohtaisen harkinnan mahdollisuuden (Rakennusteollisuus RT ry, Maa- ja metsätalousministeriö, Finnish Information Security Cluster (FISC) – Kyberala ry, Elinkeinoelämän keskusliitto EK, Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira, Suomen Kuntaliitto ry, Lääkealan turvallisuus- ja kehittämiskeskus Fimea, FiCom ry).

Suositusta pidettiin yleisellä tasolla tarpeellisena, koska suositusluonnoksen toteutusesimerkit kattavat NIS2-direktiivin riskienhallinnan toimenpiteet ja niiden koettiin ohjaavan, tukevan sekä yhdenmukaistavan toimijoiden oman riskienhallinnan oikeasuhtaista arviointia ja suunnittelua sekä riskienhallinnan toimeenpanoa (Rakennusteollisuus RT ry, Maa- ja metsätalousministeriö, FiCom ry, Suomen Vesilaitosyhdistys ry, Suomen Varustamot ry, Suomen Kuntaliitto ry).

Kannatettavana pidettiin sitä, että suosituksen sisältämät toteutus- ja todennuskeinot ovat toimijasta ja toimialasta riippuen vaihtelevia esimerkkejä siitä, mitä vaatimukset käytännössä tarkoittavat ja mihin valvonnassa kiinnitetään huomiota vaatimusten noudattamisessa (Tiedonhallintalautakunta, FiCom ry).

Suositus koettiin tervetulleeksi keinoksi ohjauksen optimoimiseksi, koska sen sisältämät riskienhallintatoimenpiteet kohdistuvat viranomaisvalvonnan hajauttamisen aiheuttamaan epävarmuuteen valvonnan ennakoitavuudesta ja johdonmukaisuudesta (Finnish Information Security Cluster (FISC) – Kyberala ry).

Suosituksen hyviä käytänteitä koettiin voitavan hyödyntää myös sellaisten toimijoiden ohjaukseen, jotka eivät kuulu suoraan NIS2-direktiivin täytäntöönpanoa koskevan lainsäädännön soveltamisalaan (Lääkealan turvallisuus- ja kehittämiskeskus Fimea). Toimijoiden katsottiin voivan hyödyntää suositusta soveltuvilta osin myös omien palvelutuottajien ja -sopimusten arvioinnissa (Suomen Kuntaliitto ry).

Positiiviseksi koettiin myös se, että lainsäädännön soveltamisalaan kuuluvat myös monet toimijoille ulkoisia palveluita tarjoavat yhteistyökumppanit (Lääkealan turvallisuus- ja kehittämiskeskus Fimea).

2.2 Suosituksen kattava sisältö ja selkeä rakenne

Suositusluonnos koettiin yleisesti ottaen kattavaksi, selkeäksi, monipuoliseksi ja käytännönläheiseksi (Suomen Kuntaliitto ry, Lääkealan turvallisuus- ja kehittämiskeskus Fimea, Maa- ja metsätalousministeriö). Positiiviseksi katsottiin se, että suositusluonnoksen toteutus- ja todennusesimerkit noudattavat NIS2-direktiivin rakennetta ja ne on esitetty samassa järjestyksessä kuin kyberturvallisuuslain esityksessä (Maa- ja metsätalousministeriö, Ruokavirasto, FiCom ry).

Suosituksen sisällön esitystavaksi valittu taulukointi koettiin suositusluonnoksen ymmärrettävyyttä helpottavaksi (FiCom ry). Myös esitystavan jakaminen toteutusesimerkkeihin, todentamiseen, perusteluihin ja viitteisiin sekä laajennettuun ohjeistukseen koettiin hyväksi (Suomen Varustamot ry). Sekä valvonnan, että toimijoiden kannalta hyvänä pidettiin sitä, että yksittäiset suositukset ovat perusteltuja ja kunkin toimenpiteen kohdalla viitataan selkeästi taustalla oleviin lähteisiin, kuten standardeihin (Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira.

Tärkeäksi koettiin myös toimijoiden jo tunnistamien ja toimeenpanemien riskienhallintakeinojen osalta se, että suositus sisältää kansallisesti laajasti tunnetun Kybermittarin sisältöjä ja viittauksia (Elinkeinoelämän keskusliitto EK). Myös viittaukset muihinkin viitekehyksiin (standardeihin) koettiin hyödyllisiksi (Finnish Information Security Cluster (FISC) – Kyberala ry).

2.3 Riskienhallintatoimenpiteiden yksityiskohtaisuus haasteena - osittaisia tarkennuksia suositukseen

Lausuntopalautteessa myös haastettiin suosituksen rakennetta siitä, että suosituksessa tarkastelleen kutakin yksittäistä kyberturvallisuuslain 9 §:n vaatimusta muista vaatimuksista erillään. Sen sijaan toivottiin riskienhallinnantoimenpiteiden arvioimista kokonaisuutena, jossa huomioidaan toimenpiteiden mahdollinen keskinäinen kompensointi arvioitujen riskien perusteella (Elinkeinoelämän keskusliitto EK). Suosituksessa on pyritty tietoisesti esittelemään jokaista riskienhallintatoimenpidettä omana itsenäisenä kokonaisuutenaan ja esittelemään hallintatoimen sisältöä, jolloin toteutusesimerkeissä on osittaista päällekkäisyyttä.

Suosituksen suuren sivumäärän koettiin heikentävän sisällön omaksumista ja siten ohjauksen tehokkuutta, jonka vuoksi dokumentin alkuun toivottiin tiivistelmää tai yhteenvetoa suosituksista omaksumisen helpottamiseksi (Tiedonhallintalautakunta). Suosituksessa esiteltyyn jokaiseen yksittäiseen riskienhallintatoimenpiteeseen sisältyvän perustelutekstin on katsottu toimivan tiivistelmänä.

Palautetta annettiin myös suositusluonnoksen riskienhallinnan keinovalikoiman puutteellisuudesta siltä osin, kuin kaikkien riskien todennäköisyyttä tai vaikutusta ei voida tai ei

ole järkevää minimoida. Sen sijaan tunnistettu riski voitaisiin hyväksyä perustellusti. Suositus antaa virheellisen kuvan siitä, että kaikki riskit tulisi hallita samalla intensiteetillä (Elinkeinoelämän keskusliitto EK). Liian yksityiskohtainen sääntely sisältää systemaattisen riskin ja riskin toimijoiden rajallisten resurssien kohdentumisesta viranomaisraportointiin (Energiateollisuus ry). Riskien käsittelyä yleisesti ja jäännösriskin hyväksymistä on käsitelty erikseen suosituksen kohdassa 1.5. Yhdessä suosituksen johdantotekstin riskiarviota, harkittua riskienhallintaa ja suhteellisuusperiaatetta koskevien tarkennuksen kanssa palaute katsottiin huomioiduksi.

2.4 Suosituksessa käytettyä terminologiaa selkeytettiin ja viitteitä tarkennettiin

Lausuntopalautteista huomioitiin suositusluonnoksessa käytetyn säädöksen nimen ajantasaistaminen kyberturvallisuuslain hallituksen esitystä (HE 57/2024 vp) vastaavaksi (Finnish Information Security Cluster (FISC) – Kyberala ry, Elinkeinoelämän keskusliitto EK).

Lisäksi huomioitiin tietoturvallisuuteen liittyvän teknisen terminologian uutuus lainsäädännön soveltamisalaan tuleville uusille viranomaisille ja toimijoille lisäämällä tietyt hankalaksi koetut termit (mm. konfigurointi, koventaminen ja luottamattomuusperiaate) suosituksen määritelmiin (Ruokavirasto).

Termien määrittelyn vaihtelevuutta, epäyhtenäisyyttä tai termien puuttumista koskevan palautteen vuoksi suositukseen päätettiin lisätä myös tarkennus siitä, että käsite on määritelty suosituksessa vain, jos sitä ei ole jo määritelty kyberturvallisuuslain määritelmissä (Elinkeinoelämän keskusliitto EK, Energiateollisuus ry, Finnish Information Security Cluster (FISC) – Kyberala ry).

Lisäksi huomioitiin osittain vanhentuneeseen ohjeeseen viittaaminen suosituksessa (ohje turvallisuuskriittisistä hankinnoista (VM2019:7), joka korvattiin päivitetyllä viittauksella (suositus tietoturvallisuudesta hankinnoissa VM2023:57).

Huomioita toimialakohtaisista standardeista ja ohjeista esittivät Tiedonhallintalautakunnan lisäksi Rakennusteollisuusliitto RT ry ja Suomen Tunnustuksellinen Luterilainen Kirkko ja suositusta muutettiin ehdotusten mukaisesti.

2.5 Suosituksen johdantotekstiä täydennettiin ja tarkennettiin - riskiperusteisuus ja suosituksen suhde määräyksiin

Saatujen lausuntopalautteiden perusteella voitiin yleisesti ottaen päätellä, että suositusta saatetaan kohdella lainsäädännöstä ja sen perusteluista irrallisena eikä sääntelykokonaisuutta täydentävänä dokumenttina. Erityisesti tuotiin esiin, että kaikkia suositusluonnoksessa esitettyjä toimenpiteitä ei ole tarpeellista ja resurssitehokasta edellyttää kaikilta toimijoilta tai kaikessa toiminnassa (Elinkeinoelämän keskusliitto EK, Suomen Vesilaitosyhdistys ry). Palautteissa toivottiin myös, että suosituksessa eroteltaisiin selkeämmin, mikä on laista tulevaa vaatimusta ja mikä on perustelutekstiä (Energiateollisuus ry).

Suosituksen johdantotekstissä päätettiin täsmentää sitä, että suositus on luotu ainoastaan kyberturvallisuuslain 9 § ja tiedonhallintalain 18 c § 1-12 kohdissa esitettyjen ja niiden perusteluteksteissä tarkemmin avattujen toimenpiteiden todentamisvaihtoehtojen konkretisoimiseksi. Lisäksi tarkennettiin sitä, että taustalla vaikuttavat kyberturvallisuus- ja tiedonhallintalakien muutkin riskienhallintatoimenpiteisiin läheisesti liittyvät säännökset, kuten toimialaan sidoksissa olevaa riskiarviota sekä toimijan harkittua suhteellisuusperiaatteen huomioivaa riskienhallintaa ja johdon vastuuta koskevat säännökset.

Lausuntopalautteiden mukaan huolta on aiheuttanut se, että suosituksella laajennettaisiin lain vaatimuksia (Elinkeinoelämän keskusliitto EK, Finnish Information Security Cluster (FISC) – Kyberala ry, Energiateollisuus ry). Myös lausuttavana olleen suosituksen suhde valvovien viranomaisten mahdollisesti antamien teknisten määräysten velvoitteisiin koettiin epäselväksi (Elinkeinoelämän keskusliitto EK, Energiateollisuus ry). Suosituksen jalkauttamisen yhteydessä

toivottiin tuotavan esiin se, että suositus ei sido viranomaisia eikä toimijoita (Suomen Vesilaitosyhdistys ry).

Saadun palautteen perusteella suosituksen johdantotekstiä tarkennettiin siltä osin, kuin tekstissä käsitellään suosituksen luonnetta ainoastaan ohjaavana ja avustavana dokumenttina ja suosituksen sisällön suhdetta valvovien viranomaisten mahdollisesti antamiin tarkentaviin teknisiin määräyksiin.

2.6 Suosituksen lukuohjetta täydennettiin ja tarkennettiin - korkeamman kyberriskin omaavat toimijat

Yhdenmukaisten valvontakäytäntöjen luomiseksi suosituksessa toivottiin otettavan kantaa siihen, millaisilta toimijoilta odotetaan korkeampaa kypsyystasoa (Maa- ja metsätalousministeriö). Suosituksen johdantotekstiä tarkennettiin saadun palautteen perusteella.

Suosituksessa esitettyjen viitekehysten käyttöä ei velvoiteta eikä niiden käyttöä ole yleisesti tai toimialakohtaisesti rajoitettu. Näin ollen lausuntopalautteista ei huomioitu pyyntöä täsmentää sitä, minkälaiseen toimintaan kutakin arviointikriteeristöä tulisi soveltaa (Elinkeinoelämän keskusliitto EK).

2.7 Riskienhallintatoimenpiteiden ja viitekehysten vastaavuus haasteena - ristiinviittausdokumentin julkaiseminen suosituksen liitteenä

Lausuntopalautteiden mukaan toimijat ovat kokeneet ongelmalliseksi sen, että suosituksesta ei ole suoraan pääteltävissä, tuottaako suosituksessa viitattujen standardien vaatimuksiin liitetyt kohdat toteuttamalla kyberturvallisuuslain vaatimuksenmukaisuuden vai vaaditaanko jotain lisätoimenpiteitä (Finnish Information Security Cluster (FISC) – Kyberala ry). Tämän vuoksi suositusluonnoksen tuoman lisäarvon arvioitiin jäävän aiottua vähäisemmäksi (Suomen Tunnustuksellinen Luterilainen Kirkko).

Muiden viranomaisten laatimien suositusten hyödyntämisen katsottiin edistävän tiedonhallintalain tarkoitusta mutta esiin tuotiin samalla se, että mm. Julkri-suosituksen kriteeristö ei välttämättä sellaisenaan ole riittävä tapa todentaa lakiin ehdotettuja velvollisuuksia. Näin ollen ehdotettiin lisäviittauksia jo olemassa oleviin tiedonhallintalain tietoturvallisuutta ja tiedonhallintaa koskeviin säännöksiin, joilla voitaisiin luoda kattavuutta vaatimusten täyttämisen todentamiseen (Tiedonhallintalautakunta). Traficom huomioi suosituksessa viitteet jo olemassa oleviin lautakunnan antamiin suosituksiin mutta ei suoria viittauksia tiedonhallintalain jo olemassa oleviin tiedonhallintaa ja tietoturvallisuutta koskeviin pykäliin.

Ristiinviittausten eli viitekehysten täyttämisen ja kyberturvallisuuslain vaatimustenmukaisuuden täyttymisen vastaavuudet toivottiin lisättäväksi suositukseen toimijoiden sekä valvovien viranomaisten tukemiseksi (Finnish Information Security Cluster (FISC) – Kyberala ry, Ruokavirasto, Suomen Tunnustuksellinen Luterilainen Kirkko). Saadun palautteen vuoksi viitekehyksiä koskeva Traficomin laatima ristiinvetodokumentti liitettiin suosituksen liitteeksi mutta väärinymmärrysten välttämiseksi suosituksen johdantoon lisättiin tarkennus siitä, että kyseessä ei ole yhdenmukaistettu standardi, joka täyttäisi vain kyberturvallisuuslain vaatimukset.

2.8 Valvontaan kohdistuneet palautteet - ei muutoksia suositukseen

Viranomaisilta toivottiin tukea siinä, että riskienhallintatoimet tosiasiallisesti johtavat digitaalisten riskien pienemiseen toiminnasta toimijoille aiheutuvan hallinnollisen taakan sijaan. Keskeistä on lainsäädännön mahdollisimman yhdenmukainen soveltaminen jäsenvaltioiden välillä sekä vastaavasti kansallisella tasolla eri sektoreilla (Finnish Information Security Cluster (FISC) – Kyberala ry).

Toiveena oli myös valvovien viranomaisten ennakoiva, joustava, vuorovaikutuksellinen ja pitkäjänteinen yhteistyö ohjauksen, neuvonnan ja tuen muodossa oman toimialansa toimijoiden kanssa toiminnan reunaehtojen määrittämisessä myös sen varmistamiseksi, että toimijat eivät ylimitoita riskienhallintatoimenpiteitä. Myös valvovien viranomaisten koordinaatio ja yhteistyö tulisi voida järjestää valtakunnallisella tasolla siten, että valvonta on tasalaatuista eri toimialojen välillä (Suomen Kuntaliitto ry).

Lausuntopalautteissa tuotiin esiin myös se, että toimijoille asetettu pakottava sääntely ei saa estää sääntelyn toteuttamisesta aiheutuvien kulujen kattamista muun toiminnan kustannuksella (Energiateollisuus ry).

Julkishallinnon valvontatoiminnassa haasteena nähtiin tiedonhallintalain uuden kyberturvallisuusvelvoitteita ja niiden valvontaa koskevan 4 a luvun yhteensopivuus tiedonhallintalaissa jo olemassa olevien tietoturvallisuutta ja tiedonhallintaa koskevien säännösten kanssa niiden osittaisen samansuuntaisuuden kanssa. Myös julkishallintoa valvovan viranomaisen yhteistyö Tiedonhallintalautakunnan kanssa nähtiin merkityksellisenä ohjeistusten ja suositusten yhdenmukaistamiseksi ja valvonnan tehostamiseksi (Tiedonhallintalautakunta).

Lausuntopalautteissa ehdotettiin myös harkittavaksi kansallisesti yhtenäisien sähköisten mallilomakkeiden (esim. tarkastuspöytäkirjapohja tai kysymyspatteristo) lisäämistä suosituksen liitteeksi, joita sektorikohtaiset valvontaviranomaiset voisivat hyödyntää kyberturvallisuuslakia ja suositusta soveltaessaan (Sosiaali- ja terveysalan lupa- ja valvonvirasto Valvira).

Lausuntopalautteissa pyydettiin johdon perehtyneisyyttä koskevan riskienhallintatoimenpiteen tarkentamista määrittelemällä monikansallisen konsernin johto. Palautteen mukaan asiasta tulisi ohjeistaa määritelmällisesti, jotta olisi selvää, milloin konsernijohdon tulee olla perillä kansallisista vaatimuksista (FiCom ry).

Palautteissa pyydettiin kiinnittämään huomiota siihen, että NIS2-soveltamisalamääritelmä toimiala-, koko- ja koosta riippumatta -määritelmien yhdistelmänä koetaan tosiasiallisesti haasteellisena. Vaikka suositusluonnos ei koske lainsäädännön soveltamisalamäärittelyä sellaisenaan, toivottiin valvonnassa ja riskienhallintatoimien tulkinnassa voitavan kiinnittää huomiota toimijan arvioituun tosiasialliseen riskiin. Valvontatoiminnassa toivottiin huomioitavan riskien ymmärrys, jolloin edellytetyt riskienhallintakeinot tosiasiallisesti pienentävät riskin todennäköisyyttä ja vaikutusta (Elinkeinoelämän keskusliitto EK).

Lausuntopalautteissa tuotiin esiin valvonnan soveltamisen tärkeys toimijan koon ja toiminnan mukaisesti sekä huomioiden toimijoiden erilaiset riskit ja tarve käyttää eri riskinhallintamalleja. Valvovan viranomaisen tulisi selventää tarkemmin mitä riskientunnistus, uhka-analyysi ja riskienhallinnan toimintamalli sisältää. Mahdollisen pakollisen turvallisuusjohtamisjärjestelmän sekä olemassa olevien kansainvälisten kyberturvallisuusvaatimusten takia olisi tärkeää, että toimijoiden kyberturvallisuuden toimintamallissa voitaisiin käyttää myös hyväksi jo olemassa olevia järjestelmiä ja järjestelyä päällekkäisyyksien välttämiseksi (Suomen Varustamot ry).

Erityisesti valvonnan näkökulmasta toivottiin riskienhallintatoimenpiteiden käyttöönotolle aikaa sekä vuorovaikutteista ohjausta ja tukea erityisesti rajallisemmilla taloudellisilla, henkilö- ja osaamisresursseilla toimiville toimijoille (Suomen Vesilaitosyhdistys ry).

Edellä mainittuja välittömästi riskienhallintatoimenpiteiden valvontaan liittyviä palautteita ei voitu huomioida suosituksessa mutta ne on mahdollisuuksien mukaan välitetty valvoville viranomaisille osana Traficomin tulevaa NIS2-direktiin mukaista tehtävää keskitettynä yhteyspisteenä.

2.9 Resurssit valvonnan ja toimijoiden haasteena - ei muutoksia suositukseen

Lausuntopalautteista kävi ilmi se, että toimijat kokevat NIS2-direktiivin ja kyberturvallisuuslain minimitoteutuksenkin haasteellisena vallitsevassa julkisen talouden tilassa (Maa- ja metsätalousministeriö). Toimijoiden puolesta esiin tuotiin myös se, että NIS2-toimijoihin

lukeutuu hyvin erilaisin resurssein toimivia toimijoita, joihin uuden lainsäädännön myötä kohdistuu lisävaatimuksia (Suomen Vesilaitosyhdistys ry).

Lausuntopalautteiden mukaan vaatimustenmukaisuuden varmistaminen vaatinee pääosalta sääntelyn soveltamisalaan kuuluvista organisaatioista merkittäviä päivityksiä kyberturvallisuuden ratkaisuihin ja toimintamalleihin, jonka vuoksi tarvitaan nykyistä enemmän osaamista ja resursseja ja lisäksi uudenlaisen turvallisuuskulttuurin rakentamista (Suomen Kuntaliitto ry).

Yleisesti kyberturvallisuuteen liittyvä runsas ja osin päällekkäinen lainsäädäntö aiheuttaa toimijoissa kysymyksiä kyberturvallisuuden tosiasiallisesta parantumisesta sekä huolta kustannustehokkaasta toiminnasta (Energiateollisuus ry).

Edellä mainittuja välittömästi resursseihin liittyviä palautteita ei voitu huomioida suosituksessa mutta toimijoiden palautteet on mahdollisuuksien mukaan välitetty valvoville viranomaisille osana Traficomin tulevaa NIS2-direktiin mukaista tehtävää keskitettynä yhteyspisteenä.

2.10 Yleinen kannanotto NIS2-direktiivin yhtenäisestä täytäntöönpanosta

Lisäksi Verizon toimitti yleisen kannanoton NIS2-direktiivin yhtenäisestä ja muut kyberturvallisuutta koskevat säädökset huomioonottavasta täytäntöönpanosta jäsenmaissa. Kannanotto sisälsi toiveen kyberturvallisuusriskien hallintatoimenpiteitä koskevan 21 artiklan kustannustehokkaasta, teknologianeutraalista, yleiset kansainväliset standardit ja riskiperusteisen lähestymistavan huomioivasta täytäntöönpanosta, jotka on jo huomioitu lausunnoilla olleessa suositusluonnoksessa taustalla vaikuttavina perusperiaatteina.

3 Lausunnot kyberturvallisuuden riskienhallinnan toimenpiteisiin

3.1 Kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja hallintatoimenpiteiden vaikuttavuuden arviointi

Kyberala ry:n ehdottamat lisäykset riskienhallinnan toimintamallin laajemman logiikan selkeyttämisestä toteutettiin suositukseen. Rakennusteollisuusliitto RT ry esitti huomion talotekniikan merkityksestä fyysisen ympäristön ja sen välttämättömien resurssien ja tilaturvallisuuden yhteydessä. Ehdotus huomioitiin 12. toimenpiteessä, joka käsittelee fyysistä turvallisuutta tarkemmin.

Elinkeinoelämän keskusliitto EK lausui riskienhallinnan keinovalikoimasta ja huomautti riskin hyväksymisestä ja seuraamaan jäämisestä oman riskinkantokyvyn puitteissa riskien kokonaisuus huomioiden. Kyseisen kohdan sisältö vastaa lain perustelutekstiä, jonka vuoksi suosituksen tekstiä ei katsottu voitavan muuttaa. Palautetta arvioitiin kuitenkin suosituksen kohdan 1.5. (riskien käsittely) yhteydessä, jonka sisällössä jo huomioidaan myös riskin hyväksymisen mahdollisuus.

3.2 Viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet

FiCom ry:n esittämät palautteet turvallisuutta koskeviin toimintaperiaatteisiin huomioitiin ja pyydetyt muutokset tehtiin todennusmenetelmiin.

3.3 Viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi

FiCom ry huomautti kohdasta 3.2 (hankinnan kohteen turvallisuus), että elinkaaren hallinta on riippuvainen myös aiemmin hankitun teknologian elinkaaresta, joka voi olla huomattavan pitkäkin. Lisäksi FiCom ry huomautti kohdassa 3.8. aikaperustaisen pääsyn rajaamisen

haasteista. Molemmat haasteet on tiedostettu, kun suositusta laadittiin. Suositukseen ei ollut perusteltua tehdä toivottuja muutoksia. Suosituksessa esitetyt toteutukset ovat esimerkinomaisia ja ne on laadittu soveltuvaksi eri toimialoille ja eri kokoisille toimijoille.

Todennusmenetelmää tarkennettiin kohdassa 3.9 FiCom ry:n esittämän huomion pohjalta sopimuksellisista rajoitteista pilvipalvelun penetraatiotestaukselle.

3.4 Toimitusketjun välittömien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt

-

3.5 Omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen

Rakennusteollisuus RT ry:n lausunnon mukaan omaisuudella tarkoitetaan myös toimijan hallussa tai hallinnassa olevia vuokrattuja tiloja, ohjelmistoja ja muita omaisuudenhallinnan piiriin luettavia resursseja. Suositusta täydennettiin Rakennusteollisuus RT ry:n esittämien huomioiden pohjalta.

3.6 Henkilöstöturvallisuus ja kyberturvallisuuskoulutus

Suomen Kuntaliitto ry lausui henkilöiden taustatarkistusmenettelyistä, jotka eivät ole mittavassa määrin käytettävissä kunnissa tai kuntien omistamissa energia-, vesi- ja jätehuollon organisaatioissa ja huomautti mahdollisesta toimeenpanon pullonkaulasta. Suomen Kuntaliitto ry:n huomautuksen ei arvioitu aiheuttavan päivitystarvetta, koska kyseisen hallintakeinon soveltamisen arvio on valvovan viranomaisen toimivallassa.

FiCom ry esitti pyynnön johdon perehtyneisyyttä koskevan kohdan 6.6 tarkentamisesta siltä osin, miten johto määritellään monikansallisessa konsernissa. FiCom ry:n mukaan asiasta tulisi ohjeistaa määritelmällisesti, jotta olisi selvää, milloin konsernijohdon tulee olla perillä kansallisista vaatimuksista. FiCom ry:n pyyntö on nostettu valvontaa koskeviin kommentteihin, jotka pyritään mahdollisuuksien mukaan välittämään valvoville viranomaisille.

3.7 Pääsynhallinnan ja todentamisen menettelyt

-

3.8 Salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttämiseksi

-

3.9 Poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi

FiCom ry esitti palautteen poikkeamien määrittelyn tarkentamisesta. Lausunnoille lähetetyn suositusluonnoksen tekstissä ei selkeästi erotella tietoturvapoikkeamia ja poikkeamia, joilla on tietoturvavaikutuksia. Määrittelyllä on merkitystä kehitettäessä poikkeamien käsittelyn prosesseja sekä arvioitaessa käytännössä kaikkia kohdan sisältämiä alakohtia. Suositusluonnoksessa käytetty määrittely tulee kyberturvallisuuslaista. Suositusluonnoksen johdantokappaleen määritelmiä tullaan tarkentamaan tältä osin ja samalla suosituksesta poistetaan päällekkäisyyden välttämiseksi kyberturvallisuuslaissa jo olevat viittaukset.

FiCom ry:n palautteen perusteella kohdan 9.3 (tapahtumien kirjaaminen ja havainnointi) todennusmenetelmistä muutettiin aikamääritelmän muotoilua, mutta toteutusesimerkissä nykyistä ilmaisua pidettiin perusteltuna, koska se oli konkreettinen ja esimerkinomainen.

3.10 Varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö

Kyberala ry antoi palautetta kohdan 10.2 (varmuuskopiot ja varajärjestelmät) sekä kohdan 10.4 (varaviestintäjärjestelmät) selkeydestä ja jäsentelystä. Toimenpiteiden toivottiin olevan loogisesti jäsenneltyjä ja selkeästi erillisiä. Palautteen pohjalta erityisesti kohdan 10.2 toteutusesimerkkiä täydennettiin. Lisäksi termit "varajärjestelmä" ja "varmuuskopio" lisättiin määritelmiin.

Kyberala ry huomautti suosituksen 10. luvun useissa kohdissa olevan toistoja, mikä tekee dokumentista paikoin tarpeettoman pitkän. Suosituksen nykyistä muotoilua ei päätetty muuttaa. Päällekkäisyys on tarkoituksellista siten, että jokainen taulukko on oma yksittäinen kokonaisuutensa.

3.11 Perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi

Kyberala ry huomautti, että suosituksessa käsitellään samaa asiaa useassa kohdassa ja huomautti tämän haittaavan lukemista. Esimerkkinä mainittiin kohdat 10.3 ja 11.11, jotka käsittelevät varmuuskopioiden tärkeyttä ja testaamista. Suosituksesta tulisi käydä selkeästi ilmi, mitä kohdassa 10.3 tulee tehdä enemmän kohdan 11.11 perustason toimenpiteen lisäksi. Suosituksen perustason tietoturvakäytäntöihin lisättiin viittaukset varsinaiseen toimenpiteeseen. Luvun 11 alakohdista on poistettu sellaiset toteutusesimerkit, jotka ovat selkeästi päällekkäin muissa luvuissa esitettyjen toteutusesimerkkien kanssa.

3.12 Toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi

Rakennusteollisuusliitto RT ry huomautti, että luvussa 12 ja sen alakohdissa ja muissa myöhemmin käsiteltävissä vastaavissa yhteyksissä tulisi mainita toimenpiteiden ulottuvan viestintäverkkojen ja tietojärjestelmien sekä niiden fyysiseen ympäristön lisäksi myös niiden tilaturvallisuuden sekä välttämättömien resurssien järjestelmiin ja palveluihin, joiden osalta rakennusten digitaalisen turvallisuuden ohjeistossa esitetty digitaalisen turvallisuuden taso DT2 vastaa toimitilakiinteistöjen perustasoa. DT1 soveltuu asuinkiinteistöille ja muihin matalan riskin kohteisiin. Kyseiset ohjeistot lisättiin suosituksen viitteisiin, mutta toteutusesimerkkiä ei tarkennettu tältä osin. Fyysisen ympäristön ja sen välttämättömien resurssien sekä tilaturvallisuuteen liittyvät kohdat on tarkistettu siten, että suosituksessa on huomioitu myös talotekniikan merkitys.

Suosituksen luvun 12 kohdan viitteisiin lisättiin Rakennusteollisuusliitto RT ry:n esittämä rakennusten digitaalisen turvallisuuden ohjeisto.