Digiturvan kokonaiskuvapalvelu: Hyvät käytännöt

DIGI- JA VÄESTÖTIETO-VIRASTO

Sisällysluettelo

Mikä on digiturvan kokonaiskuvapalvelu?

Mikä on digiturvan kokonaiskuvapalvelu?

Digiturvan kokonaiskuvapalvelu on työkalu, jolla organisaatio voi itse arvioida ja kehittää digitaalista turvallisuuttaan. Palvelu on maksuton.

Palvelun avulla organisaatio voi kustannustehokkaasti:

- Arvioida ja raportoida digitaalisen turvallisuuden tilannekuvaa organisaation johdolle
- Tunnistaa kehityskohteita ja suunnitella toimenpiteitä digitaalisen turvallisuuden kehittämiseksi
- Verrata omaa digiturvan tilaa muihin samantyyppisiin organisaatioihin
- Toteuttaa lakisääteisiä vaatimuksia

Palvelun hyödyntäminen edistää tehokkaasti organisaation digitaalisen turvallisuuden jatkuvaa strategista seurantaa ja raportointia.

Palvelu on teknisesti tarkastettu, edellyttää vahvan tunnistautumisen, ja vain DVV:n rajattu pääkäyttäjätiimi näkee yksityiskohtaiset vastaukset.

Kokonaiskuvapalvelulla on keskeinen merkitys myös Suomen kyberturvallisuusstrategian toteuttamisessa. Palvelun tuottaman tiedon avulla organisaation tiedot tulevat osaksi samankaltaisia organisaatioita joiden tuloksia verrataan, seurataan ja raportoidaan joukkona. Samalla voidaan seurata digitaalisen turvallisuuden tilannetta ja kohdistaa toimenpiteet ja resurssit keskeisiin kehityskohteisiin.

Mikä on organisaatiomme digiturvan tila tällä hetkellä?

Millainen on digiturvamme tila verrattuna muihin samanlaisiin organisaatioihin?

Mitä meidän pitää tehdä digiturvamme kehittämiseksi?

Miten voimme helposti ja kustannustehokkaasti seurata digiturvan kehittämistä?

Miten vastaan kokonaiskuvapalvelussa?

Kokonaiskuvapalvelun rakenne

Kokonaiskuvapalvelun ensimmäisessä osiossa täytetään organisaation **Taustatiedot** eli esimerkiksi digiturvallisuuteen liittyvät kustannukset ja henkilöstömäärä.

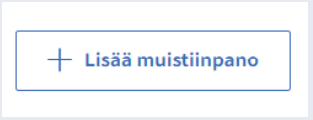
Toinen osio on **Havainnointi** eli edellisen kalenterivuoden aikana tapahtuneiden tietoturvaloukkausten, hyökkäysten ja vastaavien tapahtumien lukumäärät.

Varsinainen digiturvakysely kattaa kuusi aihealuetta:

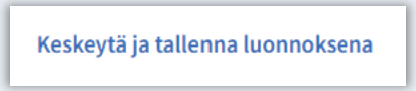
- **Johtaminen**
- **Riskienhallinta**
- **Toiminnan jatkuvuus ja varautuminen**
- **Tietoturvallisuus**
- **Tietosuoja**
- **Kyberturvallisuus**

Jokaisella aihealueella esitetään väittämiä, jotka tarkastelevat digitaalisen turvallisuuden toteutumista käytännössä. Väittämiin vastaamalla muodostetaan digiturvan kokonaiskuva.

VINKKI
Palvelun ensimmäisellä sivulla voit ladata kaikki väittämät Excel-tiedostona. Tiedostoon voi esimerkiksi kerätä tarvittavia tietoja ennen kuin ryhtyy täyttämään kyselyä.



VINKKI
Jokaisen väittämän yhteydessä on mahdollisuus lisätä oma muistiinpano. Muistiinpanot ovat käytössä myös seuraavilla kerroilla.



VINKKI
Voit tallentaa vastauksesi luonnoksena ja jatkaa vastaamista myöhemmin.

Vastausvaihtoehdot

- **Ei koske meitä / Ei voi soveltaa**

  Olemme arvioineet, että väittämä ei koske meidän organisaatiotamme, tai sitä ei voi kohdallamme soveltaa.
  Huomio: Tätä vaihtoehtoa voi käyttää vain hyvin rajatuissa tilanteissa.

- **Ei**

  Emme ole tunnistaneet toimenpiteitä, tai emme aio kehittää asiaa.

- **Osittain: Tunnistettu kehityskohteet**

  Olemme tunnistaneet, että asia on merkityksellinen organisaatiomme digiturvalle, mutta emme ole vielä aloittaneet toimenpiteitä.

- **Osittain: Käynnissä**

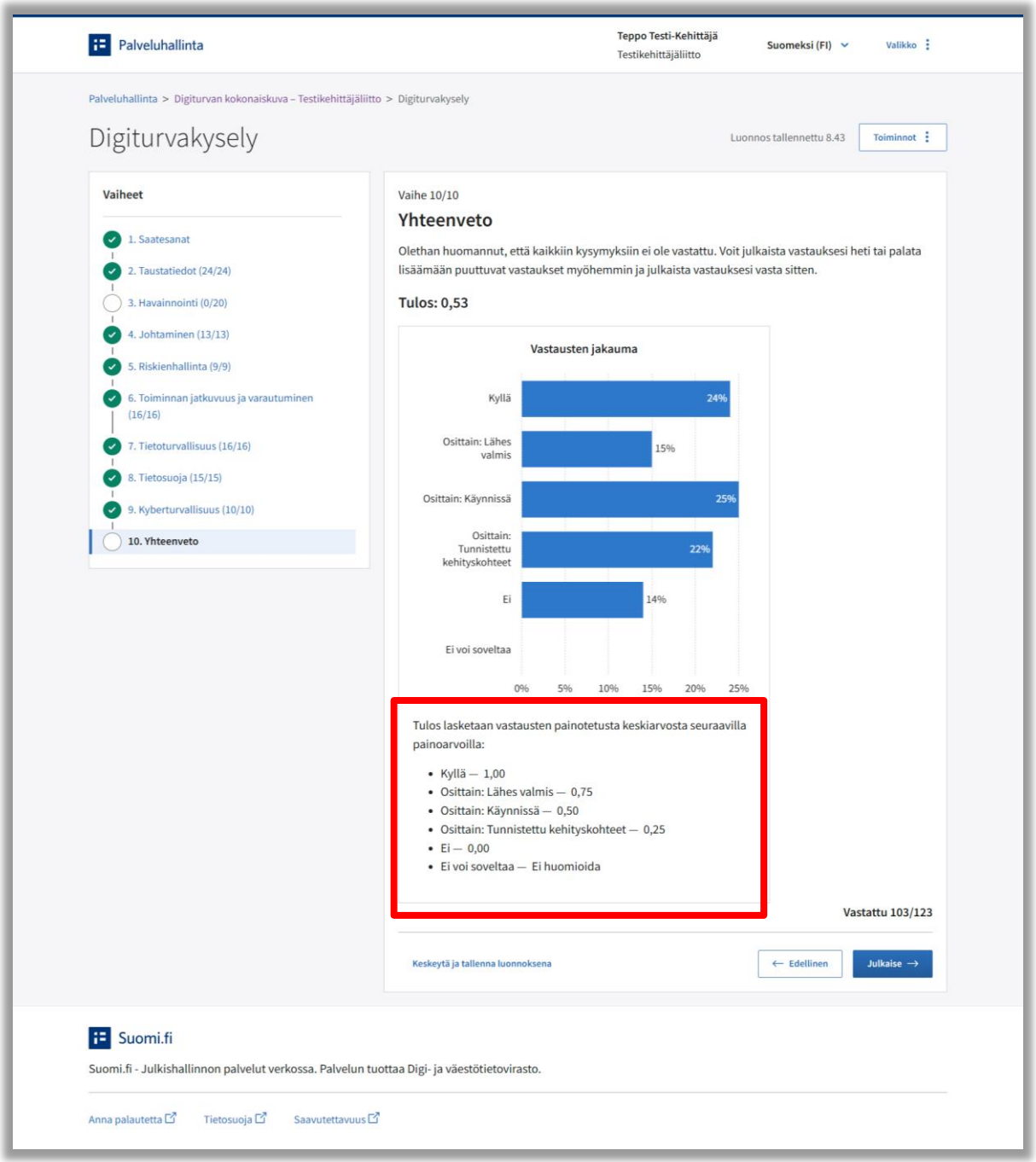
  Olemme määritelleet tavoitetason ja suunnitelleet tarvittavat toimenpiteet.

- **Osittain: Lähes valmis**

  Olemme tehneet lähes kaikki tarvittavat toimenpiteet asian kehittämiseksi riittävälle tasolle.

- **Kyllä**

  Olemme toteuttaneet tarvittavat toimenpiteet riittävälle tasolle.



Vastausten yhteenveto

Viimeisessä osiossa näytetään yhteenveto vastauksista, eli kuinka suuri prosenttiosuus kaikista väittämistä on arvioitu eri kehitysasteille.

On hyvä huomata, että lopullinen tulos lasketaan siten, että eri vastausvaihtoehtoja painotetaan eri tavoin. Kyllä-vastaus saa suurimman painoarvon, ja Osittain-vastauksia painotetaan sitä enemmän, mitä lähempänä valmista ne ovat.

Varsinaiset tulokset näytetään Julkaise-painikkeen painamisen jälkeen ja organisaation vastaus liittyy osaksi ryhmän vertailtavaa tulosta.

Miten voit hyödyntää kokonaiskuvapalvelun tuloksia?

Esimerkki: Tyrskylän kunta

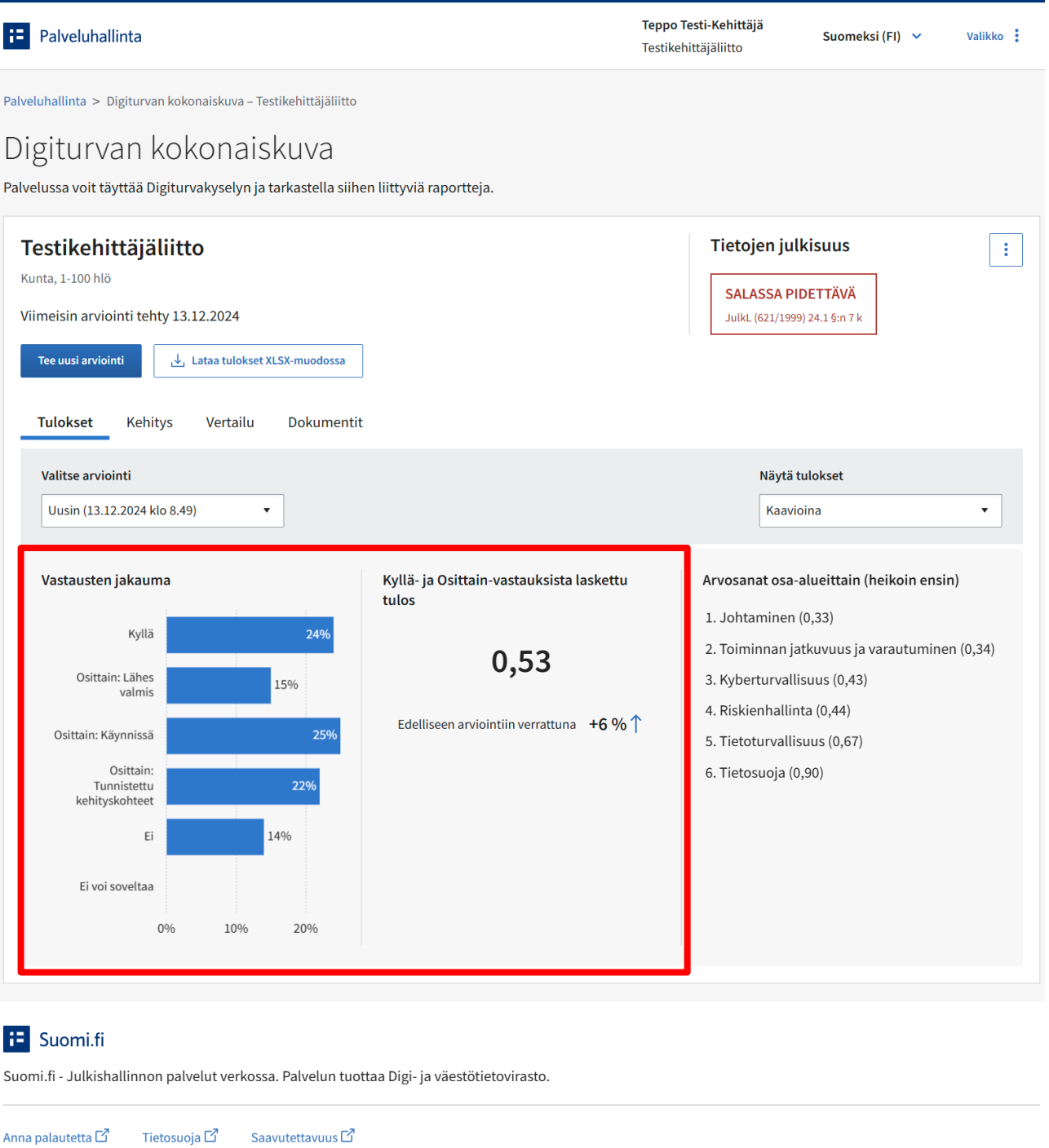
ESIMERKKI:

Tyrskylän kunta

Tyrskylän kunta sijaitsee Kaakkois-Suomessa meren rannalla. Tämä 5879 asukkaan kunta pitää sisällään useampia korkean teknologian yrityksiä sekä sataman, jota kautta kulkee 2,42% Suomen meriliikenteen kautta tapahtuvasta ulkomaankaupasta. Kunnassa toimii myös kansainvälisen merkittävän pilvipalvelutoimittajan nykyaikainen konesalikokonaisuus.

Tyrskylän kunnassa on vasta aloittanut työnsä Tanja Tietoturvapäällikkö. Ensi töikseen Tanjan on saatava kattava tilannekuva digitaalisesta turvallisuudesta, koska kunnassa on huomattavia kriittisen infrastruktuurin kohteita. Hän haluaa päästä matalalla kynnyksellä ja hyvin rajallisella budjetilla arvioimaan digiturvan nykytilannetta ja kehittämään sitä vahvemmaksi.

Tanja tietää, että DVV:n tarjoama kokonaiskuvapalvelu on kattava ja selkeä perustyökalu; se sopii Tyrskylän kunnan tarpeisiin täydellisesti!

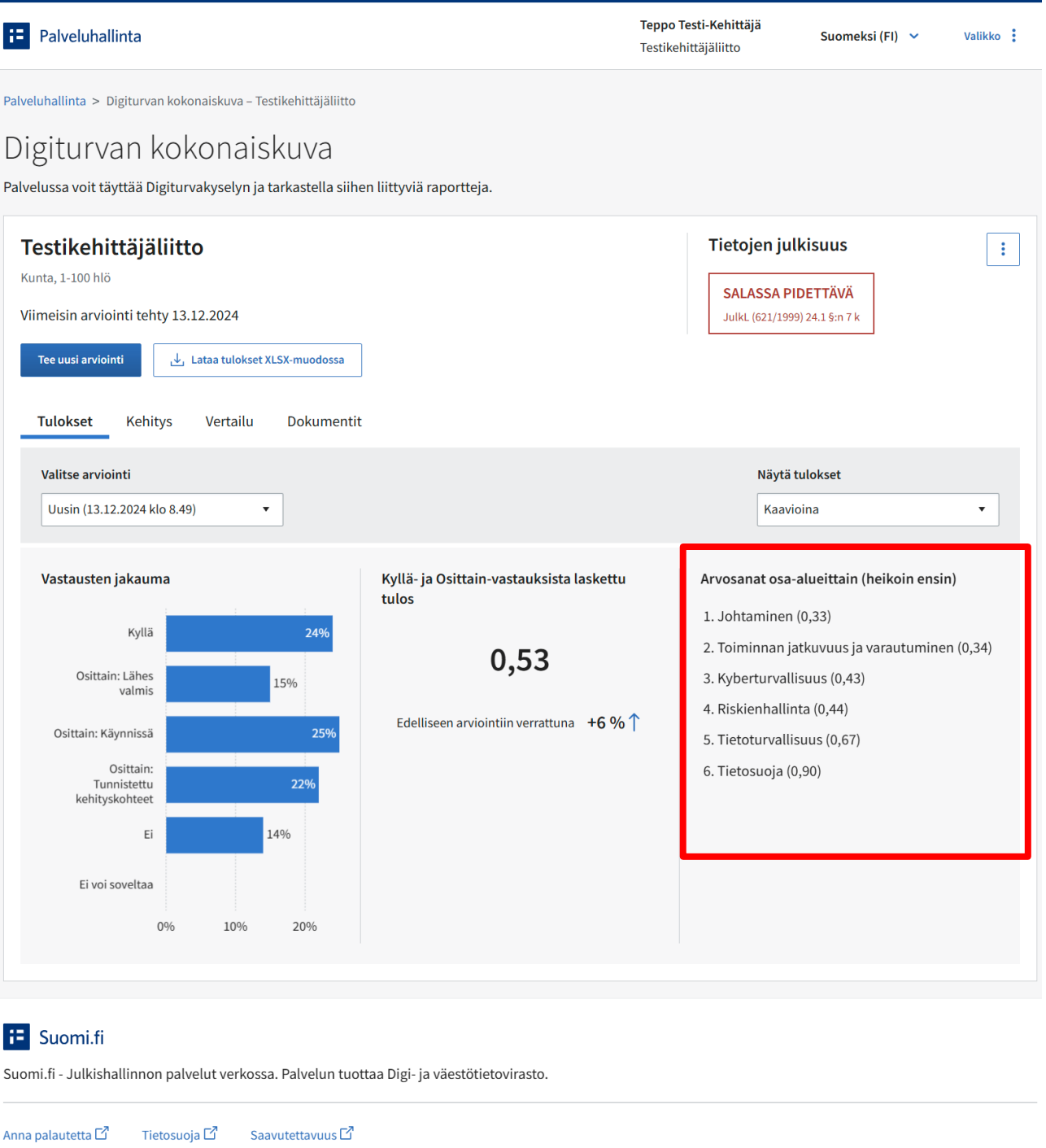


“Mikä on digiturvan tilanne Tyrskylässä tällä hetkellä?”

Tyrskylässä Tanja Tietoturvapäällikkö on täyttänyt digiturvan kokonaiskuvapalvelun digiturvakyselyn. Julkaise-painikkeen painamisen jälkeen hän saa näkyviin tulokset. Ne kertovat selkeästi ja visuaalisesti digiturvan tilanteen Tyrskylässä tällä hetkellä. Tanja ottaa kuvakaappauksen tuloksista ja liittää sen esitykseen kunnan johdolle.

Tanja kiteyttää tilannekuvan esityksessään:

- 24% vastauksista on Kyllä eli niissä ollaan jo tavoitetasolla.
- Digiturvan kehittämistoimenpiteet etenevät: yhteensä 62% arvioiduista asioista ovat ainakin osittain tavoitetasolla (Osittain-vastaukset yhteensä)
- Painotettu yhteistulos Kyllä- ja Osittain-vastauksista on 0,53, joka on selvästi parempi kuin edellisessä arvioinnissa.



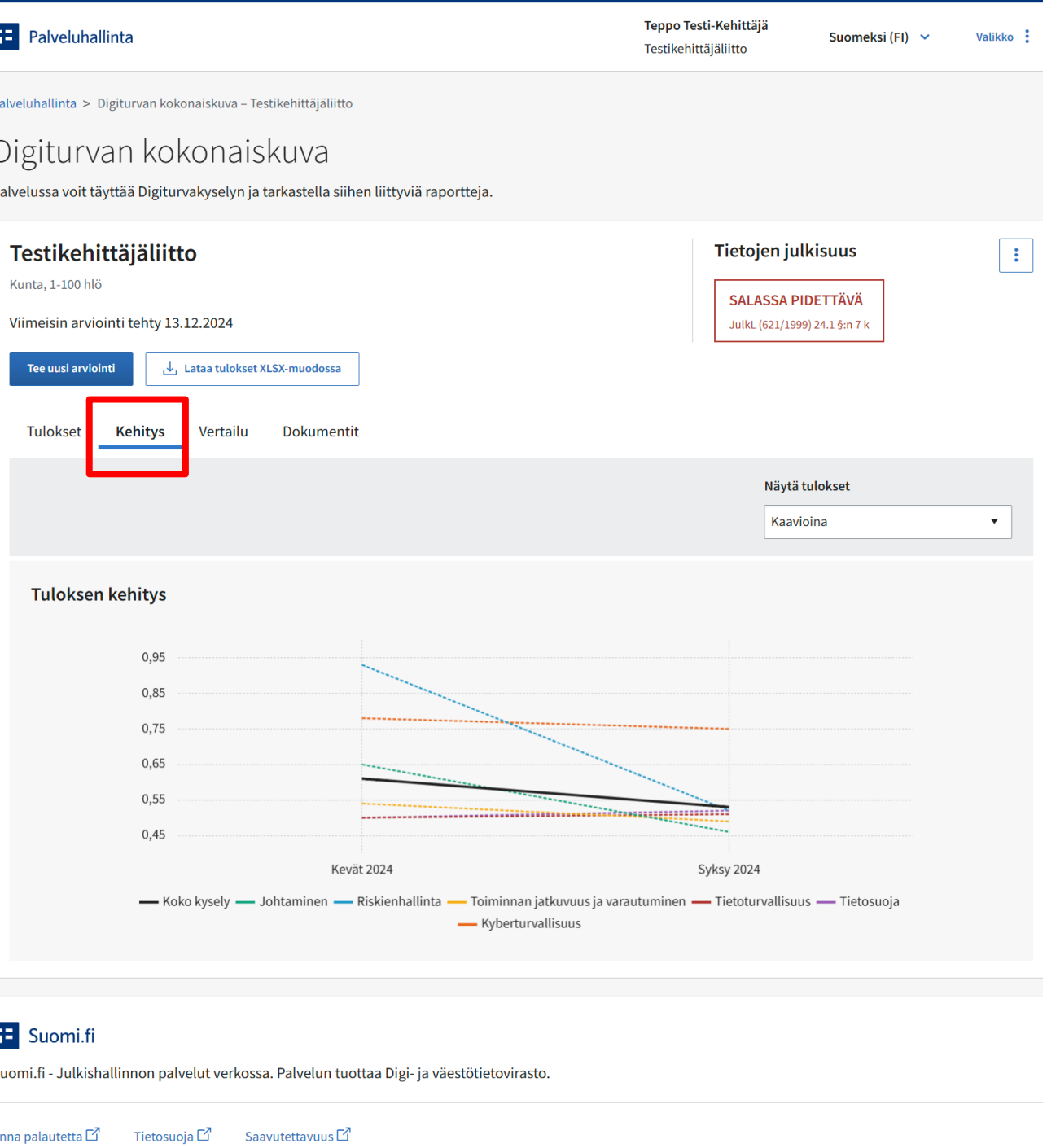
“Mitkä ovat tärkeimmät toimet digiturvan kehittämiseksi Tyrskylässä?”

Tanja Tietoturvapäällikkö kiinnittää huomionsa arvosanoihin eri osa-alueilla. Tanja ilahtuu huomatessaan tuloksista, että tietosuoja on Tyrskylän digiturvan vahvin osa-alue. Sen kehittämiseen ollaankin panostettu paljon, ja se näkyy tuloksissa.

Hän huomaa myös, että heikoimmat osa-alueet ovat:

1. Johtaminen
2. Toiminnan jatkuvuus ja varautuminen
3. Kyberturvallisuus
4. Riskienhallinta

Näihin osa-alueisiin on kiinnitettävä jatkossa enemmän huomiota. Tanja etsii lisätietoa Digiturvan tietopankista ja myös sieltä löytyvästä digiturvan palveluhakemistosta ohjeita osa-alueiden kehittämiseen. Tietopankista löytyy myös tukimateriaalia kuten kehitys – ja osaamispolkuja, joiden avulla voidaan kehittää kunnan digiturvallisuutta ja myös henkilöstön osaamista.



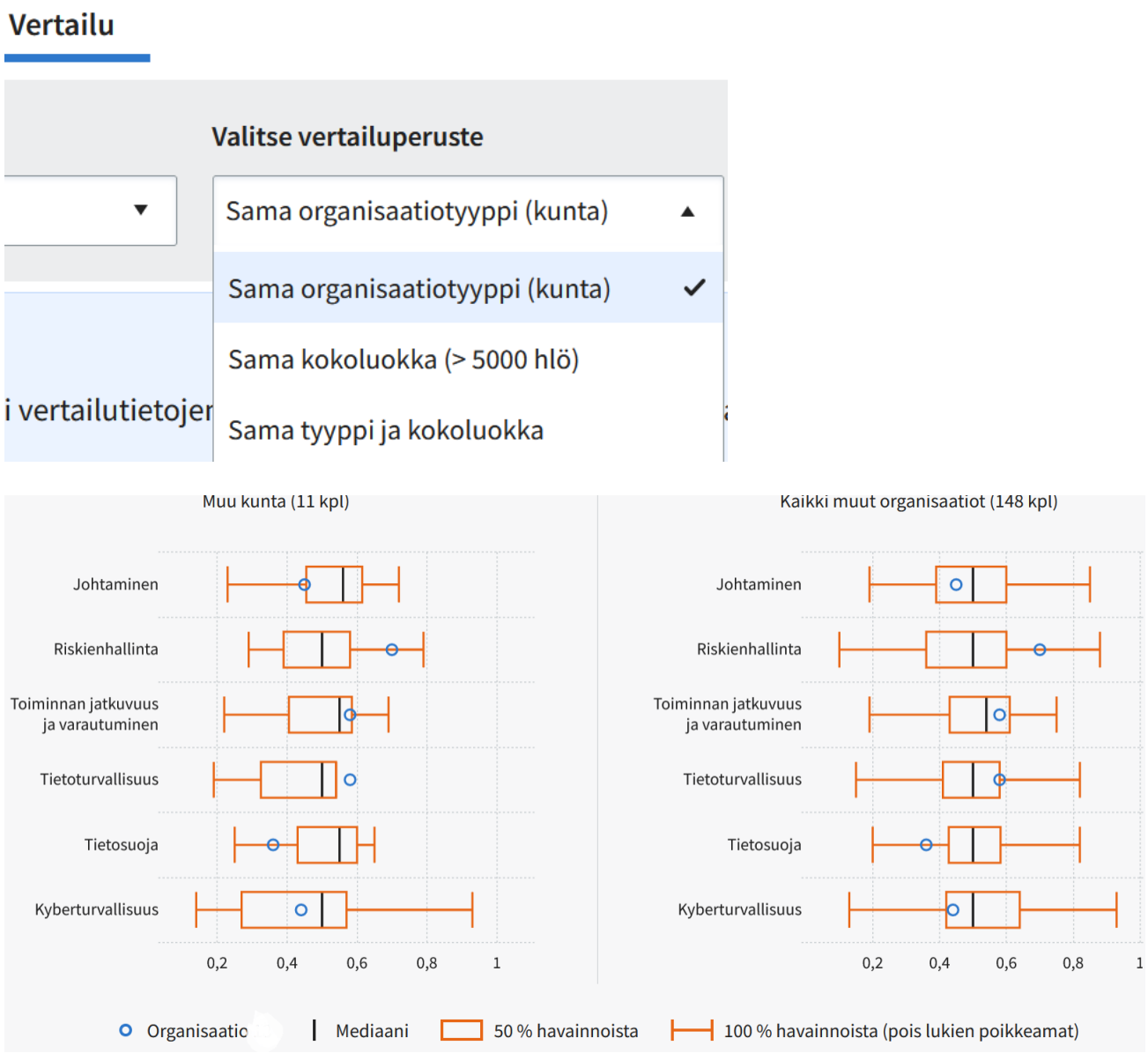
“Miten hyvin olemme onnistuneet kehittämään digiturvaamme viime vuosina?”

Tyrskylän kunnan johto haluaa tietää, miten digitaalinen turvallisuus on kehittynyt vuoden aikana. Tanja Tietoturvapäällikkö ottaa kokonaiskuvapalvelun tuloksissa esille Kehitys-osion.

Graafisesta kuvaajasta johto näkee nopeasti, minkälainen kehitystrendi on ollut. Useimpien osa-alueiden osalta kehitys on ollut melko vakaata.

Riskienhallinta on heikkommalla tasolla kuin aiemmin. Tanja ryhtyy selvittämään, mistä tämä johtuu ja ottaa kehityssuunnan korjaamisen erityiseen seurantaan. Riskienhallintahan on kansallisestikin se digitaalisen turvallisuuden osa-alue, joka on noussut keskeisenä esille mm. DVV:n viestinnässä.

Tilannekuvan havainnollistaminen havahduttaa Tyrskylän kunnan johdon parantamaan digiturvallisuuden resursointia, jotta mahdollistetaan digiturvan kokonaisvaltainen kehittäminen.



“Mikä on digiturvan tilanne samantyyppisissä organisaatiossa verrattuna meihin?”

Tyrskylän kunnan johto haluaa myös tietää, miten hyvä tai huono digitaalisen turvallisuuden tilanne on verrattuna muihin saman kokoisiin kuntiin.

Tanja Tietoturvapäällikkö ottaa esiin kokonaiskuvapalvelun tulosten Vertailu-osion. Siellä hän voi valita erilaisia vertailuperusteita, esimerkiksi samantyyppiset ja/tai samankokoiset organisaatiot.

Tanja raportoi kunnan johdolle vertailudataa. Sen perusteella johto määrittelee Tyrskylälle tavoitetason digiturvallisuudelle, jotta se pärjää vertailuissa jatkossa entistä paremmin.

Organisaatioiden vertailua tulee tehdä säännöllisesti aina kun uusi arviointi kokonaiskuvapalveluun on tehty.

“Miten kehittämistä jatketaan ja miten sitä mitataan?”

Tanja kokoaa tulosten ja vertailun perusteella digiturvallisuuden seuraavan vuoden kehittämistoimet johdon asettaman tavoitetason mukaan.

Tanja ehdottaa johdolle päätettäväksi, että Tyrskylän tiedot kokonaiskuvapalvelussa päivitetään kunnan digiturvan vuosikellon mukaan jatkossa aina alkuvuodesta, jonka jälkeen tuloksista tunnistetaan kehityskohteet. Kehityskohteet kirjataan myös vuosittaiseen tietotilinpäätökseen.

Johto päättää kehityskohteiden edistämisestä ja edellyttää, että Tanja raportoi johdolle kehittämisen edistymisestä syksyllä samana vuonna.

Jälleen seuraavan vuoden alkuvuodesta tiedot päivitetään taas kokonaiskuvapalveluun, josta Tanja jälleen raportoi johdolle tulokset ja ehdottaa seuraavat kehityskohteet, jotka johto edelleen päättää.

Näin kokonaiskuvapalvelua hyödynnetään

Esimerkki: Hyvinvointialueet

ESIMERKKI:

Digiturvaa hyvinvointialueille

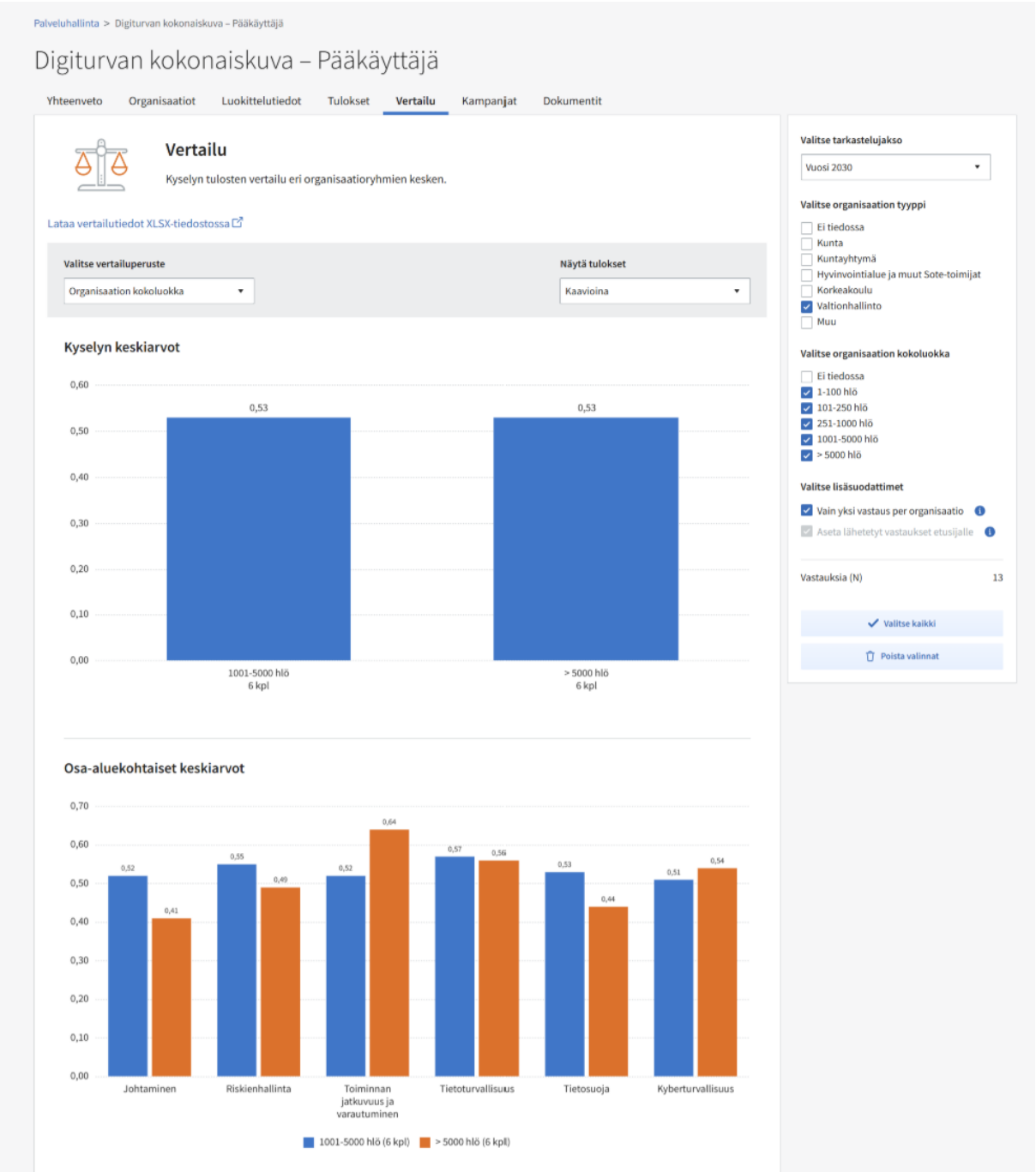
Kokonaiskuvapalvelu on monipuolinen työkalu, joka tukee hyvinvointialueiden digitaalisen turvallisuuden hallintaa ja kehittämistä tehokkaasti:

- **Tilannekuvan saaminen**: Palvelu tarjoaa kattavan ja ajantasaisen tilannekuvan organisaation digitaalisesta turvallisuudesta, mikä auttaa tunnistamaan vahvuudet ja kehityskohteet.
- **Vertailtavuus**: Kaikki hyvinvointialueet käyttävät samaa mittaristoa, mikä mahdollistaa vertailun muiden alueiden kanssa. Tämä auttaa ymmärtämään, missä oma alue sijoittuu suhteessa muihin ja mihin kannattaa panostaa.
- **Raportointi**: Palvelun raportointiominaisuudet ovat hyödyllisiä johdon raportoinnissa ja päätöksenteossa. Alueellinen raportointi auttaa myös kohdentamaan toimenpiteitä ja resursseja tehokkaammin.
- **Rahoituksen perustelu**: Tilannekuvan avulla voidaan tuoda esiin rahoitustarpeita ja perustella niitä konkreettisilla tiedoilla, mikä voi helpottaa rahoituksen saamista.
- **Kehityksen seuranta**: Palvelu mahdollistaa digitaalisen turvallisuuden kehityksen seurannan säännöllisesti, mikä auttaa pitämään kehityksen oikealla tiellä ja tekemään tarvittavia korjausliikkeitä ajoissa.
- **Yhteistyö**: Palvelu tukee yhteistyötä eri organisaatioiden välillä, sillä se tarjoaa yhteisen kielen ja mittariston digitaalisen turvallisuuden arviointiin ja kehittämiseen.
- **Käytännön hyödyt**: Organisaatio saa konkreettisia työkaluja ja tietoa, joiden avulla voidaan parantaa digitaalista turvallisuutta ja varautumista erilaisiin uhkiin.

Teksti työstetty Microsoft Copilotin avulla perustuen STM:n erityisasiantuntija, tietoturvapäällikkö Andrei Laurénin haastatteluun 29.11.2024

Näin kokonaiskuvapalvelua hyödynnetään

Esimerkki: Työ- ja elinkeinoministeriö



ESIMERKKI:

Tilannekuva työ- ja elinkeinoministeriölle koko hallinnonalalta

Työ- ja elinkeinoministeriö (TEM) on ottamassa käyttöön digiturvan kokonaiskuvapalvelua kaikissa ohjauksessaan olevissa virastoissa. Useilla virastoilla kokonaiskuvapalvelu onkin jo käytössä, mutta jatkossa käyttö on systemaattista ja ministeriön ohjauksessa.

Tähän saakka kerättyjen käyttökokemusten pohjalta kokonaiskuvapalvelu sopii tarkoitukseensa hyvin. Tärkeää on kuitenkin huomioida, että tilanteet pienten ja suurten organisaatioiden välillä eroavat suuresti. Käyttöönotto tulee ohjeistaa hyvin, jotta vältytään erilaisilta tulkinnoilta.

TEM saa käyttöönsä tietoa digiturvan tilanteesta ja voi hyödyntää palvelun tuloksia johdolle viestinnässä sekä tulossuunnittelun tukena.

Pidemmällä tähtäimellä TEMin toiveena on, että kokonaiskuvapalvelu tarjoaa raportointia myös virastotasolla. Se mahdollistaa paremman tilannekuvan.

Näin kokonaiskuvapalvelua hyödynnetään

Esimerkki: Suomi

Kokonaiskuvapalvelu tukee kansallista kyberturvallisuusstrategiaa

Kokonaiskuvapalvelun on kehittänyt ja sitä ylläpitää Digi- ja väestötietovirasto (DVV). Palvelun avulla DVV ja digitaalisen turvallisuuden kehittämisestä vastaava valtiovarainministeriö (VM) saavat tietoa julkisen hallinnon digitaalisen turvallisuuden tilanteesta. Kokonaiskuva auttaa ministeriötä digitaalisen turvallisuuden kehittämisessä ja ohjaamisessa sekä DVV:tä kehittämistoimenpiteiden kohdentamisessa oikeille osa-alueille.

Digiturvan kokonaiskuvapalvelu tukee tehokkaasti Suomen kansallisen kyberturvallisuusstrategian tavoitteiden saavuttamista ja parantaa koko yhteiskunnan kyberturvallisuutta.

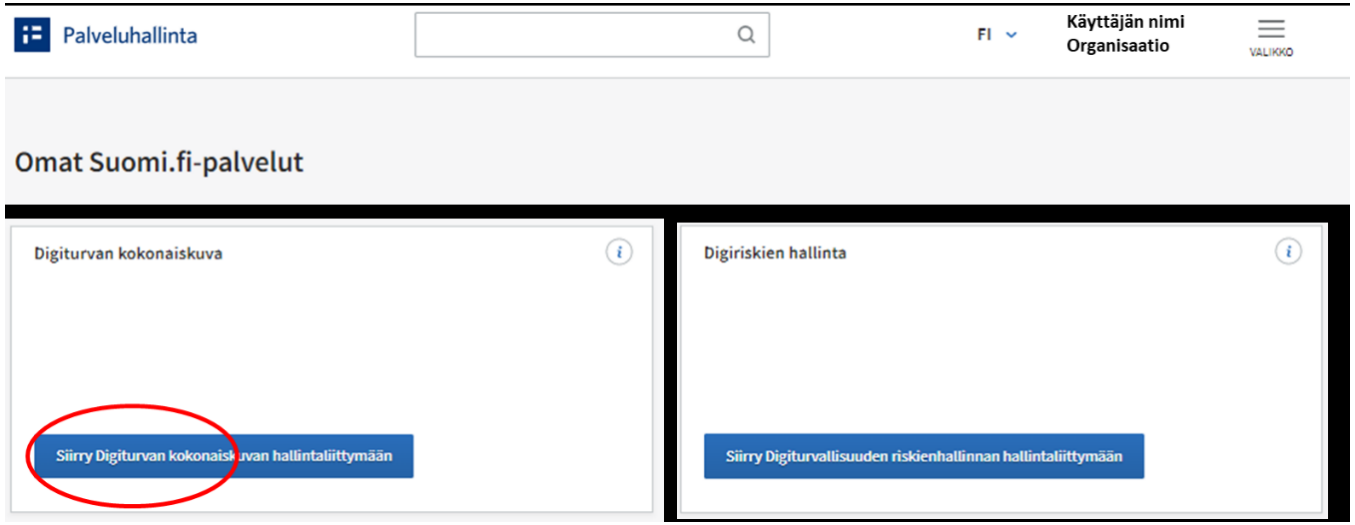
- **Tilannekuvan ylläpito**: Palvelu auttaa julkisen hallinnon organisaatioita arvioimaan, seuraamaan ja raportoimaan digitaalisen turvallisuuden tilaansa. Tämä jatkuva tilannekuva on keskeinen osa kyberturvallisuusstrategian toteuttamista, sillä se mahdollistaa ajantasaisen tiedon keräämisen ja analysoinnin.
- **Riskienhallinta:** Digiturvan kokonaiskuvapalvelu tarjoaa työkaluja digitaalisen turvallisuuden riskien arviointiin ja hallintaan. Tämä tukee strategian tavoitteita parantaa yhteiskunnan kyberresilienssiä ja toimintavarmuutta.
- **Vertailutieto**: Palvelun avulla organisaatiot voivat saada vertailutietoa toimialansa ja kokoluokkansa organisaatioista sekä koko julkisen hallinnon tilanteesta. Tämä vertailutieto auttaa tunnistamaan kehityskohteita ja parhaita käytäntöjä, mikä on tärkeää strategian tavoitteiden saavuttamiseksi.
- **Strateginen suunnittelu**: Digiturvan kokonaiskuvapalvelu tukee organisaatioiden strategista suunnittelua ja päätöksentekoa tarjoamalla ajantasaista tietoa digitaalisen turvallisuuden tilasta. Tämä auttaa kohdentamaan kehittämistoimet tehokkaasti ja varmistamaan, että ne vastaavat kansallisen kyberturvallisuusstrategian tavoitteita
- **Yhteistyö ja tiedonvaihto**: Palvelu edistää julkisen hallinnon organisaatioiden välistä yhteistyötä ja tiedonvaihtoa, mikä on keskeistä kansallisen ja kansainvälisen kyberyhteistyön vahvistamiseksi.

Liite 1

Miten otan kokonaiskuvapalvelun käyttöön?

Näin saat kokonaiskuvapalvelun käyttöön

1. Ota selvää, kuka on organisaatiosi Suomi.fi -Palveluhallinnan pääkäyttäjä.
2. Pyydä pääkäyttäjää myöntämään sinulle Ylläpitäjä-oikeudet Digiturvan kokonaiskuvapalveluun.
3. Digiturvan kokonaiskuvapalvelu löytyy Suomi.fi-palveluhallinnan etusivulta kohdasta Omat Suomi.fi-palvelut.



Liite 2

Täydentäviä tietoja kokonaiskuvapalvelun aihealueista ja väittämistä

OSIO:

Taustatiedot

Taustatiedot-osiossa kartoitetaan organisaation digiturvallisuuteen vaikuttavia tekijöitä edellisen kalenterivuoden ajalta:

- Henkilöstön määrä
- Tietoturvapoikkeamien, -hyökkäysten ja –loukkausten aiheuttamat kustannukset
- Digiturvallisuuden kehittämis- ja ylläpitokustannukset
- Kriittisten ja ei-kriittisten tietoturvapoikkeamien lukumäärät
- Henkilötyövuodet, jotka kohdistuvat riskienhallintaan, jatkuvuuteen ja varautumiseen, tietoturvallisuuteen, tietosuojaan sekä kyberturvallisuuteen
- Henkilötyövuodet ja niihin liittyvät kustannukset, jos ostetaan digiturvan asiantuntijapalveluita palveluntuottajalta
- Oman digiturvahenkilöstön kustannukset
- Digiturvallisuuden koulutus henkilöstölle keskimäärin (tuntia/hlö)
- Prosenttiosuus henkilöstöstä, joka osallistui digiturvallisuuden koulutukseen
- Osallistuminen digiturvallisuuden harjoituksiin ja/tai DVV:n Taisto-harjoitukseen
- Oman organisaation järjestämien kyber- ja digiturvaharjoitusten lukumäärä

VINKKI

Edellisessä kokonaiskuva-arvioinnissa annetut vastaukset on tallennettu, joten seuraavilla vastauskerroilla tarvitsee vain päivittää vuoden aikana tapahtuneet muutokset.

OSIO:

Havainnointi

Havainnointi-osiossa raportoidaan digiturvallisuutta vaarantaneiden tapahtumien lukumäärä edellisen kalenterivuoden ajalta:

- Organisaation itse tuottamiin palveluihin kohdistuneet onnistuneet hyökkäykset sekä ICT-palvelutoimittajan ilmoitukset hyökkäyksistä, jotka ovat aiheuttaneet tietomurron, tietovuodon tai henkilötietojen tietoturvaloukkauksen
- Salassa pidettäviä tietoja tai henkilötietoja on käsitelty ohjeiden vastaisesti luvattomilla laitteilla (esim. työntekijän henkilökohtaisella päätelaitteella) tai luvattomissa palveluissa (esim. pilvipalveluissa)
- Henkilötietojen tietoturvaloukkaus, joka on edellyttänyt ilmoitusta valvontaviranomaiselle ja/tai rekisteröidyille
- Kriittisissä palveluissa olleet tekniset (eli ei tieto- tai kyberturvallisuuteen liittyvät) häiriöt, jotka ovat haitanneet organisaation toimintaa jonkin verran tai merkittävästi
- Päätelaitteeseen ja/tai palveluun päässeet haittaohjelmat
- Palvelunestohyökkäykset, jotka ovat haitanneet organisaation toimintaa jonkin verran ja/tai merkittävästi
- Päätelaite on varastettu
- Julkiseen verkkoon näkyvässä tietojärjestelmässä tai verkossa on ollut kriittinen ja hyödynnettävissä ollut tietoturvahaavoittuvuus

OSIO:

Havainnointi (jatkuu)

- Organisaation työntekijä on tietoisesti luvattomasti käsitellyt salassa pidettäviä tietoja tai henkilötietoja, esim. ilman lupaa, liiallisessa laajuudessa tai ilman työhön liittyvää perustetta
- Organisaation kriittisiä tai lakisääteisesti säilytettäviä tietoja on korruptoitunut tai tuhoutunut lopullisesti (eli tietoja ei ole saatu palautettua varmistuksilta)
- Organisaation nimissä on lähetetty huijausviestejä, joissa yritetään urkkia asiakkaiden tai muiden henkilöiden tietoja, esim. käyttäjätunnuksia, salasanoja, pankki- tai muihin palveluihin liittyviä tietoja
- Organisaation palveluita tuottava toimittaja, alihankkija tai kumppani on toiminut vastoin sovittuja tietoturva- tai tietosuojakäytäntöjä
- Organisaation web- tai sosiaalisen median kanaviin on yritetty vaikuttaa bottien, trollitilien tai vastaavien avulla tai muilla keinoilla
- Organisaation henkilöstöön tai toimintaan on yritetty vaikuttaa informaatiovaikuttamisen keinoin, esim. painostamalla tai muilla mielipidevaikuttamisen keinoilla, jotka ovat organisaation arvojen vastaisia
- Organisaatio on ollut räätälöidyn, kohdistetun tietoturva- tai kyberhyökkäyksen kohteena

AIHEALUE:

Johtaminen

Johtaminen on avainasemassa digiturvallisuuden edellytysten ja digiturvallisuuskulttuurin luomisessa.

Johtamiseen kuuluu digiturvallisuuden tavoitteiden ja vastuiden selkeä määrittely sekä sidosryhmien vaatimusten huomioiminen. Johdon sitoutuminen ja viestintä luovat pitkälti organisaatioon sen digiturvallisuuskulttuurin.

Säännöllinen raportointi pitää johdon tietoisena digiturvallisuuden tilanteesta ja mahdollistaa tarvittaessa uusien toimenpiteiden käynnistämisen turvallisuuden parantamiseksi.

Jatkuva digiturvallisuuden kehittäminen puolestaan pitää digiturvan ajantasaisena ja henkilöstön toistuva koulutus huolehtii turvallisuuden viemisestä jokapäiväiseen käytännön työhön.

Aihealueeseen sisältyy 13 väittämää:

1. Organisaation digitaalisen turvallisuuden tehtävät ja vastuut on tunnistettu ja kuvattu selkeästi.
2. Organisaatio on kartoittanut sen digitaalista turvallisuutta ohjaavan lainsäädännön ja tunnistanut siitä aiheutuvat velvoitteet.
   Lisätiedot: Kattaa kaikki digitaalisen turvallisuuden osa-alueet
   Selvennys: Tietojen luottamuksellisuus, eheys, saatavuus ja kiistämättömyys, tietosuoja, riskienhallinta ja varautuminen
3. Organisaatio on kartoittanut keskeiset sidos- ja asiakasryhmät sekä niiltä tulevat digiturvavaatimukset.
   Lisätiedot: Lainsäädännölliset ja sopimukselliset velvoitteet
4. Organisaatiossa on riittävästi osaavaa henkilöstöä digiturvallisuuden eri osa-alueilla. **Lisätiedot**: Digiturvallisuudesta vastaavia henkilöitä on riittävästi ja heillä on riittävä osaaminen
   Selvennys: Mahdollistaa digiturvan tason asteittaisen parantamisen.
5. Organisaatiolla on riittävä budjetti digiturvallisuuden ylläpitoon sekä kehittämiseen.
   Selvennys: Mahdollistaa digiturvan tason asteittaisen parantamisen.
6. Organisaation johto on sitoutunut digitaalisen turvallisuuden kehittämiseen.
   Lisätiedot:
   - Organisaation johto on viestinyt ja osoittanut riittävässä määrin tukevansa digitaalisen turvallisuuden toteuttamista ja kehittämistä.
   - Johto viestii sisäisesti digitaalisen turvallisuuden pääkohdista
   - Strategiadokumentista löytyy digitaalisen turvallisuuden tavoitteita
   - Toiminnan suunnittelusta ja tavoitteista löytyy digitaalisen turvallisuuden osuuksia
   - Johto seuraa suunnitelmien ja tavoitteiden toteutumista järjestelmällisesti raportoinnin kautta

AIHEALUE:

Johtaminen (jatkuu)

7. Organisaation digitaalisen turvallisuuden osa-alueita kehitetään järjestelmällisesti hyödyntäen yhtä tai useampaa selkeää prosessia tai hallintamallia.
   Lisätiedot: Järjestelmällinen kehittäminen toteutuu esimerkiksi digitaalisen turvallisuuden hallintamallia, kehittämissuunnitelmia ja –arkkitehtuuria noudattamalla

8. Henkilöstölle on olemassa riittävä ohjeistus digitaalisesta turvallisuudesta.
   Lisätiedot:
   - mm. hyväksyttävän käytön periaatteet ja tarkempi ohjeistus, tietoaineistojen käsittelyohjeet sisältäen esimerkiksi ohjeet henkilötietojen ja salassa pidettävien tietojen käsittelystä eri palveluissa, toimitilojen tietoturvallisuutta koskevat ohjeet; tietosuojaperiaatteet
   - Onko ohjeistus ja prosessit jalkautettu ja miten se pystytään osoittamaan?
   - Henkilöstölle viestitään digiturvallisuuden ajankohtaisista asioista

   Selvennys: Ohjeistus löytyy keskeisiltä osin, mukaan lukien yllä olevat esimerkit

9. Henkilöstölle annetaan säännöllisesti koulutusta digitaalisesta turvallisuudesta.
   Lisätiedot:
   - onko digitaalinen turvallisuus huomioitu henkilöstön perehdytyksessä?
   - onko henkilöstön säännöllistä koulutusta digitaalisesta turvallisuudesta?
   - onko otettu huomioon eri rooleihin ja työtehtäviin liittyvät erityistarpeet?
   - onko osaamisen ylläpitäminen säännönmukaista toimintaa?
   - Koulutussuunnitelma
   - koulutus- ja perehdytysmateriaalit

   Selvennys: Digitaalisen turvallisuuden koulutus ja kompetenssikehitystarpeet huomioidaan vuosittaisessa suunnittelussa sekä organisaation tasolla että henkilötasolla (tarvepohjaisesti).

10. Organisaatiolla on olemassa prosessi väärinkäytöksiin reagoimiseksi.
    Lisätiedot: Kuvattu prosessi, vastuut ja seuraamukset

11. Digitaaliseen turvallisuuteen liittyvät mittarit on määritelty.
    Lisätiedot:
    - Mittarit on määritelty (tavoitteiden pohjalta) ja niihin liittyvää data kerätään jatkuvasti
    - Mitattavat osa-alueet on pääosin tunnistettu ja dokumentoitu
    - Tavoitteet on pääosin määritelty, dokumentoitu ja ylimmän johdon hyväksymiä
    - Mittarit on pääosin määritelty ja dokumentoitu
    - Mittareihin liittyvää dataa kerätään järjestelmällisesti

12. Digitaalisen turvallisuuden tilaa seurataan jatkuvasti.
    Lisätiedot:
    - Kattaa sekä hallinnollisen että teknisen seurannan
    - Seurattavat osa-alueet on pääosin tunnistettu ja dokumentoitu
    - Seurannan menetelmät on pääosin määritelty ja dokumentoitu
    - Seurantaa tapahtuu kattavasti, järjestelmällisesti ja säännönmukaisesti sekä toimintaa kehitetään mittareiden seurannan perusteella

13. Digitaalisen turvallisuuden kokonaistilanteesta raportoidaan säännöllisesti organisaation johdolle.
    Lisätiedot: Vähintään kerran vuodessa

AIHEALUE:

Riskienhallinta

Riskienhallinta on tärkeä osa digiturvallisuutta, ja sen tarkoituksena on tunnistaa, arvioida ja hallita organisaation kohtaamia riskejä.

Keskeiset riskienhallinnan osuudet sisältävät johdon hyväksymät riskienhallintalinjaukset, selkeät vastuut sekä riskienhallintaa ohjaavan prosessin.

Tehokas riskienhallinta edistää organisaation kykyä rakentaa digipuolustustaan, tehostaa varautumistaan ja jatkuvuudenhallintaansa ja se parantaa myös organisaation reagointikyvykkyyttä.

Lisäksi se luo pohjan kustannustehokkaan ja oikein mitoitetun digiturvallisuuden rakentamiselle.

Aihealueeseen sisältyy 9 väittämää:

14. Organisaatiolla on johdon hyväksymät, toimintaan sovitetut riskienhallinnan linjaukset, vastuut ja prosessi.
Lisätiedot: Riskienhallintapolitiikka tai vastaava

15. Organisaatio tekee digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt, toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen.
Lisätiedot: Prosessi ja vastuut kuvattuna, ja näyttöä prosessin toimivuudesta

16. Organisaatiossa viestitään digiturvallisuuden riskitilanteesta ja uusista riskeistä koko organisaation laajuisesti.
Lisätiedot: Digiturvasta vastaavien ja viestinnän yhteistyönä

17. Organisaatiossa raportoidaan riskitilanteesta johdolle säännöllisesti.
Lisätiedot: Vähintään kerran vuodessa

18. Kriittisistä, organisaation toimintaa uhkaavista riskeistä raportoidaan johdolle välittömästi.
Lisätiedot: Prosessi kuvattuna ja näyttöä sen toimivuudesta

19. Organisaatio seuraa riskien ja niiden hallintatoimenpiteiden tilannetta säännöllisesti.
Lisätiedot: Kuvattu menettely ja näyttöä sen toimivuudesta

20. Organisaation ylin johto sekä organisaation hallitus (tai vastaava) seuraa merkittävien riskien ja niiden hallintatoimenpiteiden tilannetta säännöllisesti.

21. Organisaatiossa arvioidaan jäännösriskejä riskienhallintatoimenpiteiden toteuttamisen jälkeen ja jäännösriskit käsitellään asianmukaisella tasolla.
Lisätiedot: johto tai ko. toiminnon/riskin omistaja tekee tarvittavat päätökset

22. Organisaatiossa kehitetään riskienhallintaprosessia saatujen riskienhallinnan tavoitteiden tai saatujen kokemusten perusteella.

AIHEALUE:

Toiminnan jatkuvuus ja varautuminen

Toiminnan jatkuvuussuunnittelun ja varautumisen tarkoituksena on varmistaa, että organisaatio pystyy ylläpitämään keskeiset toiminnot ja palvelut myös poikkeustilanteissa ja häiriötilanteissa sekä palautumaan niistä nopeasti.

Toiminnan jatkuvuus kattaa mm. valmiussuunnitelmat, kriittisten toimintojen tunnistamisen ja suojauksen sekä poikkeamien hallintaprosessit.

Aihealueeseen sisältyy 16 väittämää:

23. Organisaation tehtävät ja vastuut ovat selkeät myös poikkeustilanteissa ja poikkeusoloissa.
Lisätiedot: kuvattu esim. valmiussuunnitelmassa

24. Organisaatiolla on prosessi ja valmiudet nopeaan ja tehokkaaseen digiturvallisuuden häiriöiden, uhkien ja poikkeamien käsittelyyn.
Lisätiedot: poikkeamanhallintaprosessi ja vastuut kuvattuina

25. Organisaatio on kuvannut jatkuvuuden hallinnan periaatteet, tavoitteet, organisoinnin ja vastuut.
Lisätiedot: jatkuvuudenhallinnan periaatteet tai vastaava

26. Organisaatio on tunnistanut ja dokumentoinut suojattavat kohteet.
Lisätiedot:
   - mm. henkilöstö, tilat, tietojärjestelmät, laitteet jne.
   - Organisaation käytössä olevat järjestelmät, palvelut ja laitteet (sisäiset ja ulkoiset) sekä niiden turvallisuuteen vaikuttavat asiat.
   - Organisaation tietovarannot, niiden kuvaukset, tiedonkäsittelyprosessit, vastuut, riskit ja suojaustoimet.

   Selvennys: Ainakin pääosin

27. Suojattavien kohteiden tunnistamiseen ja kriittisyyden määrittelyyn on dokumentoitu ja hyväksytty menetelmä.
Lisätiedot: Kriittisyyden määrittelyyn on olemassa kuvattu menetelmä

28. Organisaatio on määritellyt kuinka pitkiä toimintakatkoksia kriittiset toiminnot sietävät organisaation toiminnan häiriintymättä.
Lisätiedot:
   - Organisaatio tuntee lainsäädännön vaatimukset liittyen sen järjestelmien, rekistereiden ja palveluiden saatavuuteen.
   - Organisaatio tuntee oman toiminnan ja sidosryhmien vaatimukset.

AIHEALUE:

Toiminnan jatkuvuus ja varautuminen (jatkuu)

29. Toiminnan jatkuvuuden edellyttämät palvelutasovaatimukset ovat osa hankintavaatimuksia ja sopimuksia.
Lisätiedot: mm. SLA, RPO, RTO

30. Jatkuvuuteen liittyviä riskejä ja riskitilanteen muutosta arvioidaan säännöllisesti.
Lisätiedot: mm. SLA, RPO, RTO

31. Organisaatiolle ja sen kriittisille toiminnoille/palveluille on laadittu jatkuvuussuunnitelmat, jotka perustuvat tunnistettuihin riskeihin.
Lisätiedot: prosessi kuvattuna ja näyttöä sen toimivuudesta

32. Kriittisille tietojärjestelmille on laadittu toipumissuunnitelmat.
Lisätiedot: Sisältää mm. häiriötilanteen johtamiseen liittyvät menettelyt ja vaihtoehtoiset toimintatavat

33. Organisaatiolla on häiriö- ja kriisitilanteiden viestintäsuunnitelma.
Lisätiedot:
    - Viestinnän kohderyhmät, välineet, vastuut ja pääviestit
    - Myös suunnitelma vaihtoehtoisten viestintätapojen käytöstä, kun puhelin ja viestintäverkot eivät ole käytettävissä organisaatiossa tai sen sidosryhmillä ja asiakkailla

34. Suunnitelmien sisältö on koulutettu häiriötilanteiden hallintaan osallistuville henkilöille.

35. Organisaatiossa on luotu yhteydet ja verkostot tarvittavien sidosryhmien väliseen viestintään poikkeamatilanteissa.
Lisätiedot: yhteystahot ja menettelyt kuvattu

36. Organisaatiolla on olemassa menettely sen toimintaa kohdistuvien häiriöiden, hyökkäysten ja loukkausten ilmoittamiseksi keskeisille viranomaisille.
Lisätiedot: mm. Poliisi, Tietosuojavaltuutetun toimisto, Kyberturvallisuuskeskus

37. Organisaatio harjoittelee säännöllisesti sen toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista.
Lisätiedot:
    - vähintään kerran vuodessa (valitun osa-alueen osalta)
    - dokumentaatio harjoitusten toteutumisesta ja havainnoista

38. Jatkuvuus-, toipumis- ja viestintäsuunnitelmia päivitetään harjoitusten tai toteutuneiden häiriötilanteiden perusteella
Lisätiedot: näyttö päivityksestä

AIHEALUE:

Tietoturvallisuus

Tietoturvallisuus on olennainen osa digiturvallisuutta, keskittyen tietojen, järjestelmien ja verkkojen suojaamiseen.

Tietoturvallisuus kattaa mm. tietoturvapolitiikat, käyttövaltuuksien hallinnan, monivaiheisen tunnistautumisen, varmuuskopioinnin sekä haittaohjelmien torjunnan.

Tietoturvallisuuden tavoitteena on varmistaa tietojen luottamuksellisuus, eheys ja saatavuus, sekä lakisääteisten velvoitteiden täyttäminen.

Aihealueeseen sisältyy 16 väittämää:

39. Organisaatiolla on johdon hyväksymä tietoturvapolitiikka tai vastaava tietoturvallisuuden toteuttamista ohjaava asiakirja.
Lisätiedot: mm. tavoitteet, periaatteet, organisointi, vastuut

40. Organisaatiolla on olemassa henkilöiden taustatarkistuksiin liittyvä menettely, joka kattaa oman ja palvelutoimittajien henkilöstön.
Lisätiedot: kuvattu menettely ja näyttöä sen toimivuudesta

41. Organisaatiolla on olemassa käyttövaltuuspolitiikka ja prosessi käyttövaltuuksien hallintaan.
Lisätiedot: dokumentoitu prosessi

42. Käyttövaltuuksien ajantasaisuus varmistetaan säännöllisesti.
Lisätiedot: menettelyt kuvattu, tarkistus vähintään vuosittain

43. Organisaatio on määrittänyt fyysisesti suojatut turvallisuusalueet asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi.
Lisätiedot: dokumentaatio ja ohjeistus

44. Organisaation tietojärjestelmät ja laitteet ovat kattavasti järjestelmänhallinnan piirissä.
Lisätiedot: mm. prosessit automaattisiin päivityksiin

45. Organisaatiolla on käytössä monivaiheinen tunnistus etäkäytössä.
Lisätiedot: MFA, Multi-Factor Authentication tai vastaava

46. Toimitilojen ulkopuolella työskenneltäessä yhteydet organisaation ICT-palveluihin sallitaan vain VPN-yhteydellä.

AIHEALUE:

Tietoturvallisuus (jatkuu)

47. Organisaatiolla on olemassa tarvittavat tekniset ratkaisut ja menettelyt haittaohjelmien tunnistamiseen ja estämiseen.
Lisätiedot: toteutus yhdyskäytävä- ja työasematasolla sekä tarvittava ohjeistus henkilöstölle
Selvennys:
    - Ainakin Windows -tietokoneissa on haittaohjelmien tunnistus- ja esto-ohjelmat.
    - Sisääntulevat sähköpostiviestit tarkistetaan automaattisesti haittaohjelmien tunnistus- ja esto-ohjelmalla

48. Organisaation tiedoista ja järjestelmistä otetaan säännöllisesti varmuuskopiot.
Lisätiedot: kuvattu menettely ja näyttöä sen toimivuudesta

49. Varmuuskopioiden palautusta testataan säännöllisesti
Lisätiedot: ainakin kriittisten palveluiden osalta

50. Tietojärjestelmien käytöstä ja tietojen luovutuksista kerätään riittävät lokitiedot.
Lisätiedot:
    - lainsäädännön ja toiminnan vaatimukset on selvitetty ja toteutettu lokitus niiden mukaisesti
    - Huomioitava Tiedonhallintalaki 17 § ja siitä annettu suositus

    Selvennys:
    - Lainsäädännön vaatimukset on selvitetty kattavasti
    - Tiedonhallintalain 17§ ja siitä annettu suoritus on huomioitu
    - Lokitus on lainsäädännön mukaista
    - Lokitietoa kerätään järjestelmällisesti ja kattavasti

51. Käytössä olevien tietojärjestelmien teknisiin haavoittuvuuksiin liittyviä tiedotteita seurataan ja niihin reagoidaan.
Lisätiedot: olemassa oleva menettely ja näyttöä sen toimivuudesta
Selvennys:
    - Tiedotteiden lähteet on tunnistettu (esimerkiksi Traficom)
    - Tiedotteiden seurantaa tehdään ja se on säännöllistä
    - Organisaatiolle tietojärjestelmiin liittyvät oleelliset tekniset uhat tunnistetaan tietolähteiden seurannassa ja niihin reagoidaan

52. Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti.
Lisätiedot:
    - sisältää hallinnolliset ja tekniset auditoinnit
    - järjestelmiin vähintään käyttöönottovaiheessa sekä kriittisyyden mukaan säännöllisesti

53. Tietoturva- ja tietosuojavaatimukset ovat osa hankintavaatimuksia ja sopimuksia.
Lisätiedot: ovat hankinnoissa ns. pakollisia vaatimuksia

54. Tietoturva- ja tietosuojavaatimukset otetaan huomioon myös järjestelmien ja palveluiden kehittämisessä sekä ylläpidossa.
Lisätiedot: kuvattu menettely ja näyttöä sen toimivuudesta

AIHEALUE:

Tietosuoja

Tietosuoja keskittyy henkilötietojen asianmukaiseen käsittelyyn ja suojaukseen.

Tietosuoja kattaa henkilötietojen keräämisen, tallentamisen, käsittelyn ja jakamisen, sekä näihin liittyvät roolit ja vastuut organisaatioissa.

Vahva tietosuoja ei ainoastaan suojaa yksilöitä, vaan vaikuttaa myös organisaation maineeseen.

Aihealueeseen sisältyy 15 väittämää:

55. Organisaatiolla on tiedossa, millaisia henkilötietoja se käsittelee (TsA 4 art. 1 kohta)
Lisätiedot:
- nimi, osoite, sähköpostiosoite, puhelinnumero jne.
- hetu (TSL 29 §)
- erityiset henkilötietoryhmät (TsA 9 art. TSL 6 §)
- rikostuomioihin ja rikkomuksiin liittyvät henkilötiedot (TsA 10 art., TSL 7 §)
- Turvakiellon alaiset henkilötiedot
- Henkilöstön (TtsL), asiakkaiden, vierailijoiden, sidosryhmien henkilötiedot

56. Henkilötietojen käsittelyn oikeusperusteet on tunnistettu (TsA 6, 9 ja 10 art. TsL 6 ja 29 §, TtsL 2, 3, 5 ja 6 luku)
Lisätiedot:
- Suostumus
- Sopimus
- lakisääteinen velvoite (edellyttää säännöksen yksilöintiä)
- elintärkeä etu
- yleinen etu ja julkinen valta (edellyttää säännösten yksilöintiä, yleisenedun yksilöintiä ja julkisen vallan säädösperustaa)
- oikeutettu etu
- Käsittelyn erityisedellytykset on huomioitu mm. seuraavissa tapauksissa
  - erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyperusteet
  - rikostuomioihin ja rikkomuksiin liittyvä käsittely
  - henkilötunnuksen käsittely
  - henkilötietojen käsittely työsuhteen yhteydessä

AIHEALUE:

Tietosuoja (jatkuu)

57. Organisaatio on tunnistanut, milloin se toimii rekisterinpitäjänä ja milloin se toimii käsittelijänä (TsA 4 art. 7-8 kohta)
Lisätiedot: On olemassa prosessi tai ohjeistus rekisterinpitäjän ja käsittelijän tunnistamiseksi

58. Sopimukset henkilötietojen käsittelystä on tehty ja sopimusten hallinta on kunnossa (TsA 28 art)
Lisätiedot:
- Onko tietosuoja sisäänrakennettu hankintaprosessiin?
- Onko henkilötietojen käsittelyn vaatimukset ja ehdot huomioitu henkilötietojen käsittelijöiden kanssa tehdyissä sopimuksissa?
- Onko sopimusten hallintamalli laadittu?
- Onko siirrot 3. maihin otettu huomioon?

59. Yhteisrekisterinpitäjyystilanteet tunnistetaan ja yhteisrekisterinpitäjyyttä koskevista vastuista on sovittu? (TsA 26 art., huom. myös EDPB:n ohje)
Lisätiedot:
- Tunnistetaanko tilanteet, joissa on kyse yhteisrekisterinpitäjyydestä?
- Onko yhteisrekisterinpitäjien vastuunjaosta sovittu tiedon keräämisestä sen hävittämiseen/arkistointiin?
- Ovatko roolit ja vastuut selkeitä ja läpinäkyviä rekisteröidyille?
- ohje tai prosessi, joka auttaa tunnistamaan yhteisrekisterinpitäjyyden ja siihen liittyvät roolit
- Sopimukset
- viestintä rooleista ja vastuunjaosta rekisteröidylle

60. Henkilötietojen käsittelyyn liittyvät oman organisaation sisäiset roolit ja vastuut on tunnistettu ja vahvistettu (TihL 4.2. §, TsA 37 art.)
Lisätiedot:
- rekisterien omistajat / vastuuhenkilöt
- johdon vastuut
- Esimiehet
- Henkilöstö
- Valvonta
- Tietosuojavastaava
- muut roolit (tiedonhallinta, tietosuoja, tietoturva, riskienhallinta, tilaturvallisuus)

61. Tietosuojavastaavan asema ja rooli on määritelty (TsA 37 – 39 art.)
Lisätiedot:
- tarve tietosuojavastaavan nimeämiseen on selvitetty
- Tietosuojavastaavan sijaisjärjestelyt kunnossa, yhteydenotot poissaolon aikana
- tietosuojavastaavan tehtävät ja asema ovat laissa säädetyn mukaiset
- päätös tietosuojavastaavan nimeämisestä
- esim. asema määritelty hallintosäännössä, työjärjestyksessä tms.
- tehtävänkuvaus

62. Seloste käsittelytoimista on laadittu (TsA 30 art.)
Lisätiedot:
- Sisältääkö vaaditut tiedot?
- Toteutuvatko tietosuojaperiaatteet organisaatiosi toiminnassa? (TsA 5 art.)
- lainmukaisuus, kohtuullisuus, läpinäkyvyys
- Käyttötarkoitussidonnaisuus
- tietojen minimointi
- Täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus

AIHEALUE:

Tietosuoja (jatkuu)

63. Organisaatiolla on tiedossa missä tietojärjestelmissä henkilötietoja käsitellään
Lisätiedot:
- tietojärjestelmäsalkku/rekisteri
- Tietovirtakuvaukset
- aputiedostot/listaukset

64. Rakenteeton tieto on tunnistettu ja sen hallinta on kuvattu
Lisätiedot:
- Satunnaisten, ei-jäsenneltyjen sähköisten tietojen tunnistaminen ja hallinta
- Tietoa käsitellään sellaisissa ympäristöissä, joissa tiedon elinkaarta ei pystytä metatietojen avulla hallitsemaan.
- esim. sähköpostiviestit, verkkolevyllä olevat tiedostot, Teams-tiimien tiedostot, Skype-/Teams-keskusteluhistoria

Selvennys:
- Rakenteeton tieto on pääosin tunnistettu
- Hallintatapa on ainakin pääosin dokumentoitu

65. Informointikäytännöt on määritelty ja niitä noudatetaan (TsA 12-14 art. Laki digitaalisten palveluiden tarjoamisesta (306/2019)
Lisätiedot:
- Otetaan huomioon informoinnin kohderyhmä sekä käsittelyn laajuus ja luonne valittaessa informointikäytäntöä.
- Pystyttävä osoittamaan, että rekisteröity on saanut informaation
- onko informaatio ymmärrettävää ja saavutettavaa

66. Organisaatiolla on olemassa prosessi vaikutustenarvioinnin tarpeen tunnistamiseksi (TsA 35 (1) art.)
Lisätiedot:
- onko tunnistettu, milloin tulee suorittaa vaikutustenarviointi tai ennakkokuuleminen?
- onko vakioitu prosessi kriteerien tunnistamiseksi olemassa?

67. Organisaatiolla on olemassa henkilötietojen tietoturvaloukkausten hallintaprosessi (TsA 33-34 art.)
Lisätiedot:
- vakioitu prosessi olemassa loukkausten käsittelemiseksi ja dokumentoimiseksi?
- ilmoituskanavan määrittäminen ja vastuuhenkilöt ilmoitusten käsittelyyn
- viranomaisilmoitusten tekeminen, päätöksentekovastuu ilmoituksista
- rekisteröidyille ilmoittaminen
- Miten varmistetaan henkilöstön kyvykkyys tunnistaa tietoturvaloukkauksia?
- kuvaus prosessista

68. Jos henkilötietoja siirretään kolmansiin maihin, organisaatio on selvittänyt siirron edellytykset? (TsA 5 luku)
Lisätiedot:
- Onko ymmärretty, mitä tarkoitetaan siirrolla kolmansiin maihin (esim. pääsy tietoihin kolmannesta maasta)?
- Onko tunnistettu ne tilanteet, joissa tapahtuu siirtoja kolmansiin maihin?
- Onko vaatimusmäärittelyssä huomioitu ne tilanteet, joissa siirrot kolmansiin maihin ei ole mahdollista?
- Onko huomioitu siirrot kolmansiin maihin koko alihankintaketjussa?
- Sopimuksen kolmansiin maihin siirtoja koskevat ehdot

69. Organisaatiossa tietosuojasta huolehtiminen on muuttunut toiminnaksi, kulttuuriksi ja asenteeksi (TSA 5 art.)
Lisätiedot:
- Mieti, miten kykenet arvioimaan toiminnan, kulttuurin ja asenteen muuttumista organisaatiossasi.
- esim. johdolle ja henkilöstölle kohdennetut kyselytutkimukset
- palvelulupaus tietosuojan huomioonottamisesta organisaationtoiminnassa
- Tietosuojapolitiikka
- vuosikello
- osaamisen mittaaminen

AIHEALUE:

Kyberturvallisuus

Kyberturvallisuus suojaa tietojärjestelmiä, verkkoja ja dataa luvattomalta käytöltä, vahingoittumiselta ja häiriöiltä, kattaen laajasti erilaiset tekniset ja hallinnolliset toimenpiteet.

Siihen liittyvät kiinteästi yhteiskunnan kannalta kriittisten palveluiden tunnistaminen, suojaaminen ja toimintakyvyn varmistaminen poikkeustilanteissakin.

Tämä edellyttää riittävien resurssien ja osaamisen varmistamista sekä jatkuvaa yhteistyötä sidosryhmien kanssa.

Aihealueeseen sisältyy 10 väittämää:

70. Organisaatio on huomioinut digitaalisen turvallisuuden osana kokonaisarkkitehtuuria.
Lisätiedot: ainakin tietoturvallisuus
Selvennys: Digitaalinen turvallisuus on ainakin pääosin osana kokonaisarkkitehtuurin kuvausta.

71. Organisaatiolla on riittävät resurssit ja osaaminen digitaalisen turvallisuuden kehittämiseen osana kokonaisarkkitehtuuria.
Lisätiedot: nimetty vastuuhenkilö ja aikaa tehtäviin
Selvennys:
    - Digitaalisen turvallisuuden kehittämiseen liittyvät vastuut on kuvattu, dokumentoitu ja ylimmän johdon hyväksymiä
    - Henkilöt ovat kattavasti ja dokumentoidusti nimetty
    - Henkilöiden osaamista kehitetään järjestelmällisesti ja se on ainakin pääosin resursoitu
    - Digiturvallisuudesta vastuussa olevan henkilöstön osaaminen sekä työaika, jonka he pystyvät käyttämään digitaalisen turvallisuuden kehittämiseen tarkistetaan ja päivitetään määräajoin
    - Toimiva varahenkilöjärjestely on ainakin pääosin olemassa

AIHEALUE:

Kyberturvallisuus (jatkuu)

72. Organisaatio on tunnistanut oman roolinsa YTS:n mukaisissa tehtävissä sekä globaalissa näkökulmassa
Lisätiedot:
    - Miten riippuvainen yhteiskunta on organisaation tuottamista palveluista?
    - Riski hybridi- / informaatiovaikuttamiseen sekä siihen varautuminen
73. Organisaatiossa on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten organisaatioiden tai yhteiskunnan toimintaan.
Lisätiedot: palvelut, joista muiden organisaatioiden operatiivinen toiminta on riippuvainen
74. Organisaatiossa on kattavasti tunnistettu kriittisten palveluiden riippuvuudet ulkoisista palvelutoimittajista.
Lisätiedot: kriittisten palveluiden toimittajat ja niiden häiriöiden vaikutukset organisaation toimintaan
75. Organisaation kriittisten palveluiden palveluntuottajien kanssa yhteistyössä arvioidaan ja hallitaan riskejä säännöllisesti.
Lisätiedot: kuvattu menettely ja näyttöä sen toimivuudesta
76. Kriittisten toimittajien ja alihankkijoiden kanssa käsitellään digiturvallisuutta säännöllisesti toimittaja/palvelunhallintakokouksissa.
Lisätiedot: kuvattu menettely ja näyttöä sen toimivuudesta
77. Organisaatio on varautunut ja laatinut suunnitelman siihen kohdistuvan mustamaalaus- tai vaikuttamiskampanjan varalta.
Lisätiedot: toimintatavat kuvattu
78. Organisaatio seuraa säännöllisesti toimintaympäristönsä digitaalisen turvallisuuden tilannekuvaa.
Lisätiedot: Esimerkiksi toimintatavat toimintaympäristössä tapahtuvien ilmiöiden seurantaan sekä ilmiöiden vaikutusten arviointiin.
79. Organisaatiolla on toiminnalliset ja tekniset menettelyt tietojenkäsittely-ympäristönsä digitaalisen turvallisuuden valvontaan ja havainnointiin.
Lisätiedot: esimerkiksi digitaalisen turvallisuuden poikkeamia havainnoivat automatisoidut valvontatyökalut ja tietoturvavalvomo

DIGI- JA VÄESTÖTIETOVIRASTO

dvv.fi