Digiturvallisuuden riskikyselyn tuloksia, syksy 2021

DIGI- JA VÄESTÖTIETO-VIRASTO

Tiivistelmä

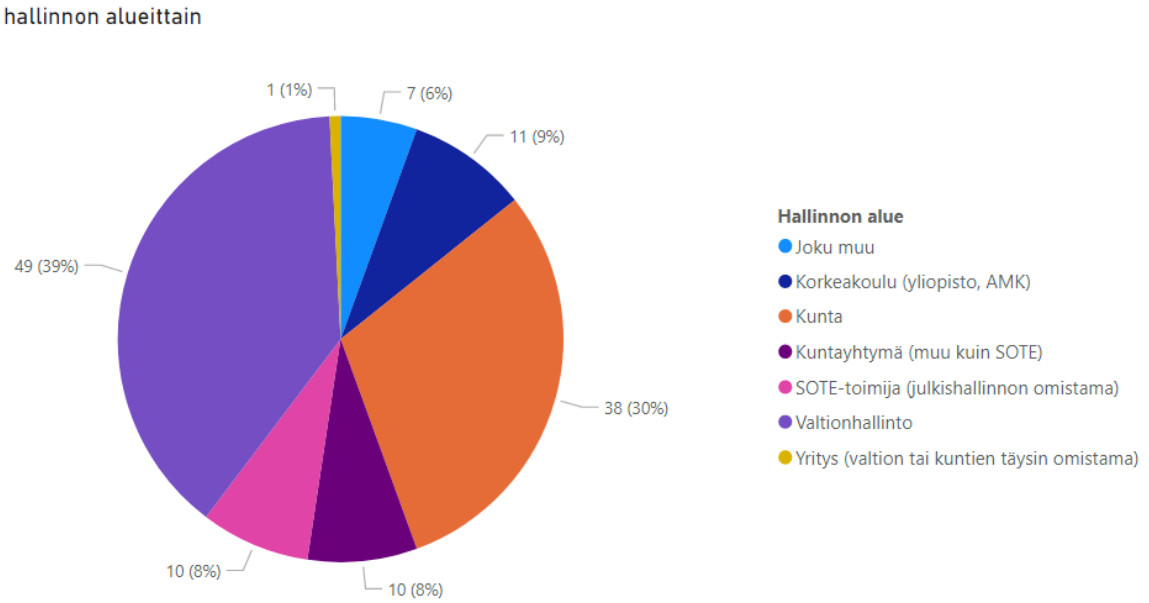
- Julkisen hallinnon toimijoiden näkemyksiä kysyttiin 36 riskiväittämään syyskuun alussa 2021 ja saatu N=126, sisältäen valtionhallintoa 39%, kuntatoimijoita (ml. SOTE) 46%, korkeakouluja 9% sekä muita 6%. Arvioissa pyydettiin näkemystä 3 vuoden aikaikkunassa.
- **Keskeisimmiksi nähdyt riskit koskevat viranomaisten palveluihin sekä niiden takana olevaan infraan kohdistuvia hyökkäyksiä**. Näiden jälkeen on nähtävissä huoli monimutkaisuuden hallittavuudesta sekä resursoinnista. Ensimmäisiin kahteen pyritään vastaamaan informoimalla uhista ja jälkimmäisiin parantamalla mm. digiturvaan liittyvän tiedon hallintaa (ml. löydettävyys) eri muodoissaan, sillä tehostaminen tällä alueella helpottaa myös olemassa olevien resurssien käyttöä.
- Riskilukujen keskiarvot ovat maltilliset ja eri hallinnon kokonaisuuksien välillä ei suuria eroja, mutta tarkemmissa luokitteluissa nähtävissä erilaisia painotuksia mm. eri toiminta-aloilla ja valtion hallinnonaloilla. Näitä voidaan huomioida digiturvatoimien paremmassa kohdentamisessa.
- **Tulokset vahvistavat valtion ja kuntatoimijoiden riskiprofiilien eron**. Kuntien näkymässä painottuu käytännönläheisempi lähestyminen riskeihin sekä huoli digiturvaan asennoitumisesta ja sen huomioimisesta toiminnan suunnittelussa. **Eri kokoisten vastaajaluokkien näkymissä ei ollut merkittäviä eroja, vahvistaen näkemystä, että erilaisilla resursseilla joudutaan vastaamaan samoihin riskeihin** – vain suurimmilla on hieman korkeampi näkemys riskeihin.
- Vähimmin keskeisiksi nähdyt riskit, liittyen mm. tekoälyyn ja vaikuttamiseen, on syytä pitää seurannassa, sillä ne voivat aktivoitua tulevaisuudessa.

Kyselyn toteutus

- DVV ja valtiovarainministeriö selvittivät yhteistyössä syksyn 2021 aikana julkishallinnon digitaalisen turvallisuuden merkittävimmiksi arvioituja riskejä osana julkisen hallinnon digitaalisen turvallisuuden strategisen riskiarviomallin pilotointia.
  - Lähtökohtana olivat aiemman, kunnille 2020 toteutetun riskikyselyn väittämät, joita täydennettiin ja muotoiltiin kyselystä saadun palautteen perusteella.
- Kyselyssä oli 36 riskiväittämää ja mahdollisuus esittää täydentäviä riskiaiheita avoimiin kysymyksiin
  - Väitteet oli otsikoitu OECD:n käyttämän digitaalisen turvallisuuden näkökulman mukaisesti:
    - Kansallinen ja kansainvälinen turvallisuus
    - Lainvalvonta
    - Taloudellinen ja yhteiskunnallinen hyvinvointi
    - Teknologia
  - Riskiväitteet listattu liitteessä 1
- Vastaajia pyydettiin arvioimaan riskiväittämiä neljästä näkökulmasta:
  - Vaikutus talouteen
  - Vaikutus maineeseen
  - Vaikutus palveluiden tuottamiseen
  - Toteutumisen todennäköisyys
- Vastauksissa käytettiin neliportaista asteikkoa (1=epätodennäköinen/vähäinen vaikutus, 4=lähes varma/kriittinen). Näkökulmiin vastaaminen ei ollut pakollista.
- Ensisijaisesti kerätty julkisen hallinnon digiriskeihin liittyvää ohjausta varten. Tulokset on esitelty Digitaalisen turvallisuuden strategiselle johtoryhmälle sekä VAHTI riskienhallinnan kehittämisen työryhmälle 1.12.2021.

Kyselyn tunnusluvut

- Vastausaika 25.8.-21.9.2021
- Kyselyn vastaanottajia 617
- Vastaajia oli 139, joista keskiarvoistamalla laskettiin N=126 kpl eri organisaatiota
  - Vastaajia samasta organisaatiosta
  - Vastaajilla sama Y-tunnus
- Vastaajien jakauma hallinnon kokonaisuuksittain:
  - Kunnat ja kuntayhtymät 58kpl (46%)
  - Valtionhallinto 49kpl (39%)
  - Korkeakoulut 11kpl (9%)
  - Muut 8kpl (6%)



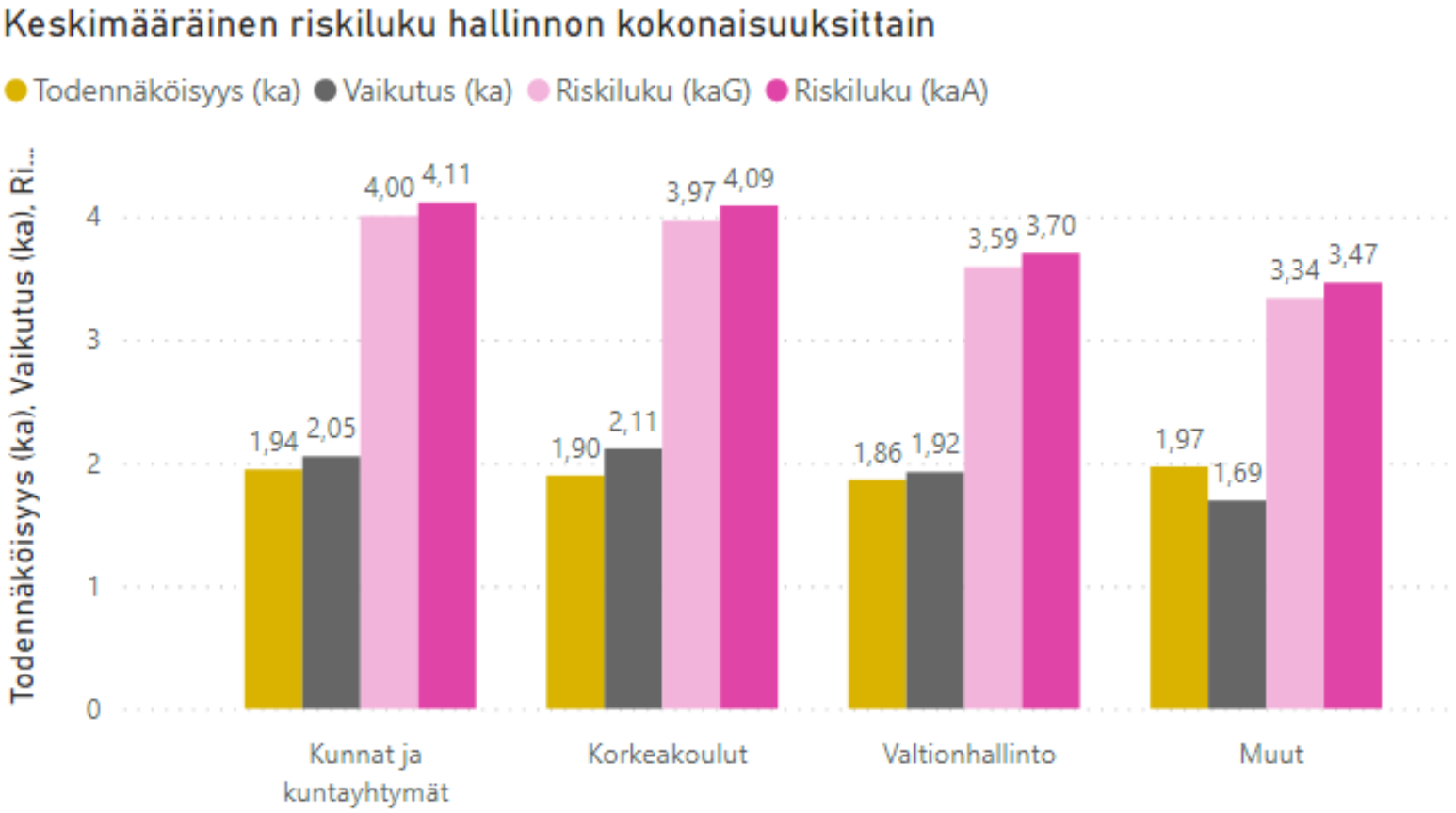
Kyselyn aineiston käsittely

- Koska kysely ei sisältänyt tietojen oikeellisuustarkistuksia, vastausaineistoon tehtiin manuaalisesti y-tunnuksiin liittyviä korjauksia (puuttuvat lisätty, esitysmuoto yhtenäistetty, virheelliset korjattu) sekä täydennettiin puuttuvia organisaatioiden henkilöstömäärätietoja.
- Analyysin tietomalliin tuotiin vastausten lisäksi riskiväittämät luokiteltuina kolmen eri kategorian mukaisesti (OECD, World Economic Forum, digitaalisen turvallisuuden toteutuksessa käytetyt osa-alueet), valtionhallinnon rakenteen kuvauksia sekä kuntien talouteen liittyviä tunnuslukuja.
- Jokaisen vastauksen yksittäiselle riskiväitteelle on laskettu kolmen eri vaikutustekijän aritmeettinen keskiarvo sekä riskiluku, joka on saatu kertomalla keskimääräinen vaikutus todennäköisyydellä. Johtuen laskentatavasta ja pyöristyksistä, esitystä visualisoivien pylväskuvaajien arvot eivät tuota tarkalleen riskiluvun arvoa. Tämä ei vaikuta luokkien vertailtavuuteen.
- Vastausmäärien perusteella syvempiä vertailuita voitiin tehdä vain valtionhallinnon sekä kuntien osalta, mutta nämäkin ovat vain suuntaa-antavia.

Tunnuslukuja

Riskilukukeskiarvot (aritm.) jaoteltuna hallinnon kokonaisuuksittain:

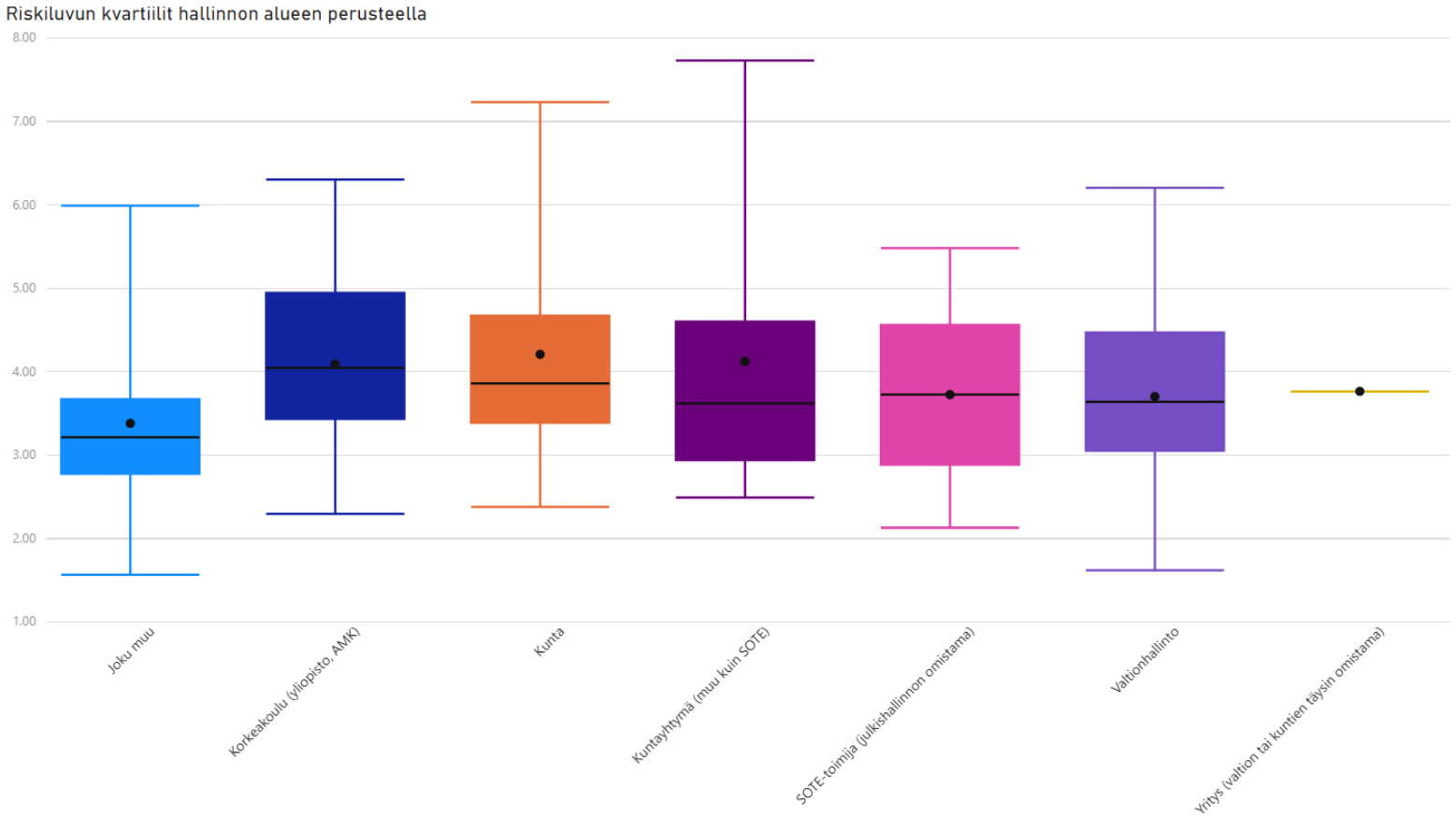
- Kunnat ja kuntayhtymät 4,1
  - Kunnat 4,2
  - Kuntayhtymät 4,1
  - SOTE 3,7
- Korkeakoulut 4,1
- Valtionhallinto 3,7
- Muut 3,5



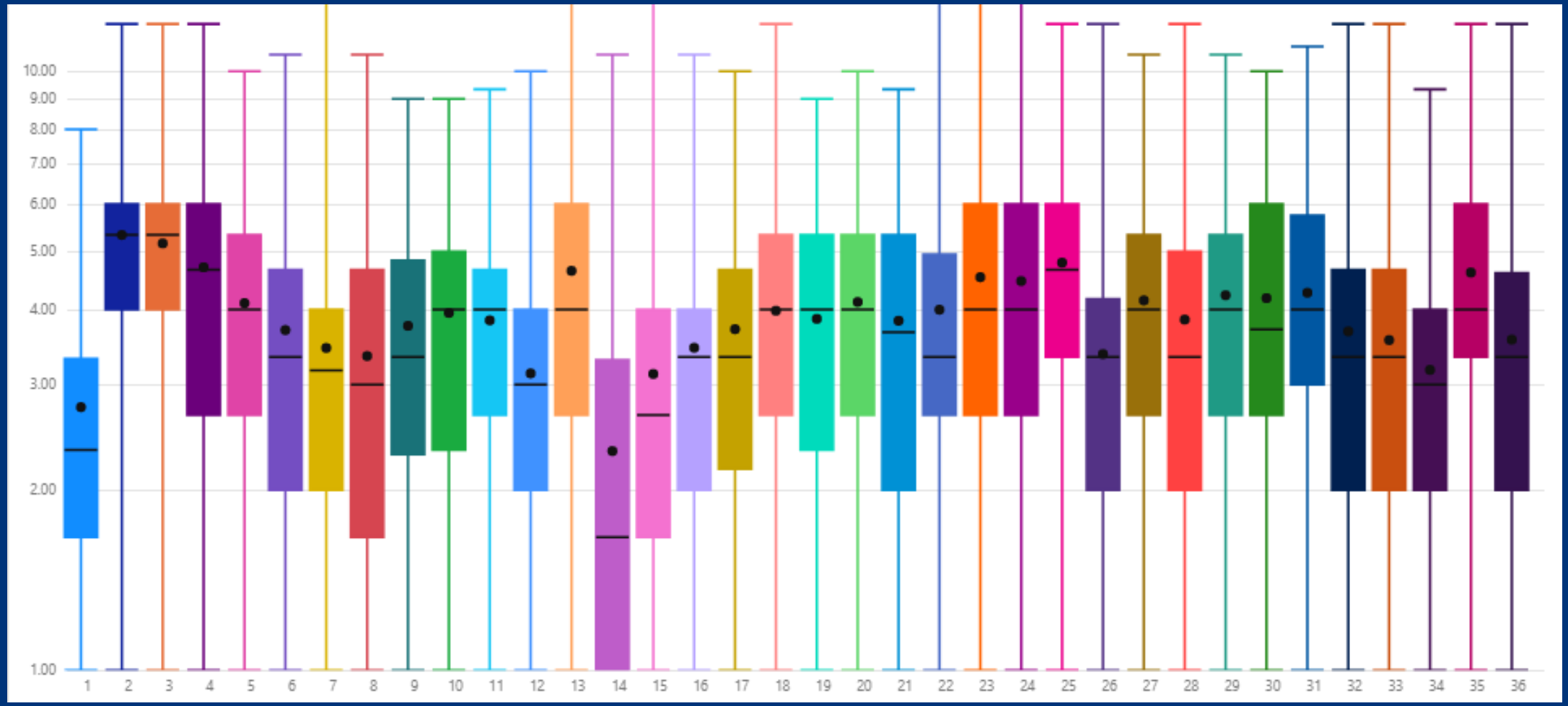
- ➢ Kunnat ja kuntayhtymät sekä korkeakoulut melko tasoissa
- ➢ Valtionhallinnon ja SOTE-alueen arviot alhaisemmat

Tunnuslukujen takana

- Arvioissa voidaan nähdä erilaista käsitystä riskeistä eri alueilla toimivien välillä, mikä ei täysin selity vain riskien erilaisuudella. Tätä tukee vastausten hajonnan erot kokonaisuuksissa, eli kuvaajassa ääripäät sekä keskineljänneksi koko ja sijoittuminen.
  - Valtionhallinnossa selittävinä tekijöinä voi olla parempi jaettu riskinäkymä sekä yhtenäisempi osaaminen.
  - Sote-toimijoilla selitys lienee tarkempi rajaus ja yhtenäisemmät riskit ylipäätään.



Vastausten hajonta, painotuskvartiilit sekä keskiarvot ja mediaanit riskiväittämissä

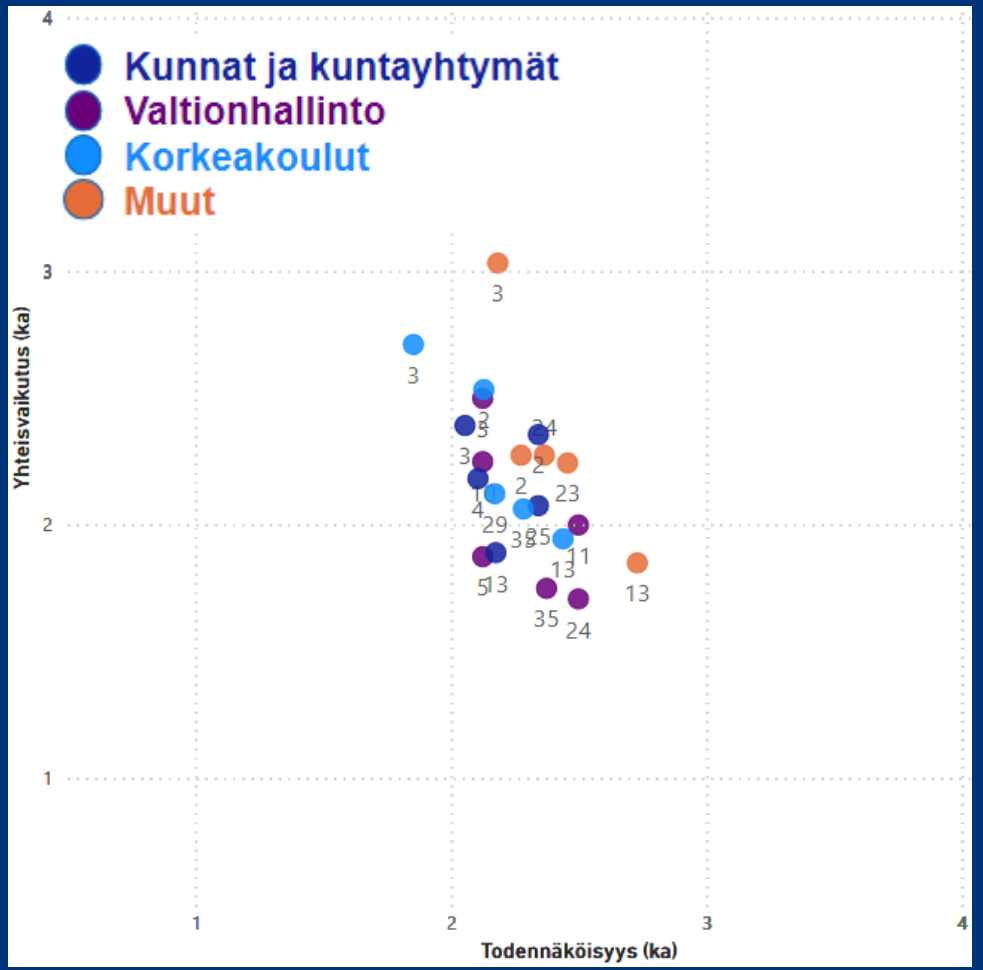


Keskeisinä nähdyt riskit: kaikki vastaajat, top-10

Riskiväitteen numero	Riskiväite	Riskiluku	Todennäköisyys
2	Viranomaisten toimintaan ja palveluihin kohdistuu tahallisia vakavia tietoturvahyökkäyksiä.	**5,3**	2,2
3	Kriittiseen fyysiseen infrastruktuuriin ja tietoverkkoihin kohdistuu vakavia väärinkäytöksiä, haitantekoa, sabotaaseja tai tietoturvahyökkäyksiä.	**5,2**	2,0
25	Tiedonhallintayksikön toimialat ylittävistä prosesseista, ICT-toimittajista, alihankkijoista ja tuotantoympäristöistä koostuvan kompleksisen kokonaisuuden hallinta epäonnistuu, mikä aiheuttaa häiriöitä ja palvelukatkoja.	**4,8**	2,2
4	Tietovarantojen tietoturva vaarantuu merkittävästi, johtuen keskeisesti kiireestä ja resursointivajeesta.	**4,7**	2,0
13	Säädösten, määräysten ja ohjeiden ylimitoitus, ajantasaisuuden puute, virheellisyys, muutosten nopeus tai muut sääntelyn laatuun liittyvät ominaisuudet aiheuttavat kohtuuttomia velvoitteita.	**4,6**	2,3
35	Pilvipalvelujen riskejä ei tunneta riittävästi, jolloin niiden hallintatoimet - joko sopimuksilla tai muilla keinoilla - ovat epäselviä ja tilannekuva puutteellinen.	**4,6**	2,1
23	Digitaaliseen turvallisuuteen ei ole kohdennettu riittävästi taloudellisia resursseja.	**4,5**	2,2
24	Digitaalisen turvallisuuden osaamista ei ole käytettävissä riittävästi.	**4,5**	2,2
31	Häiriötilanteiden jälkeen ei kyetä palauttamaan tietoja käyttöön eli menetetään tietoa, immateriaalioikeuksia tai ohjelmistoja.	**4,3**	1,7
29	Digitaalista turvallisuutta ei ymmärretä, arvosteta tai huomioida toiminnan suunnittelussa.	**4,2**	2,0

Riskilistan tarkastelua

- Riskiväitteet 2 ja 3 nähdään keskeisimpinä
  - *2: Viranomaisten toimintaan ja palveluihin kohdistuu tahallisia vakavia tietoturvahyökkäyksiä.*
  - *3: Kriittiseen fyysiseen infrastruktuuriin ja tietoverkkoihin kohdistuu vakavia väärinkäytöksiä, haitantekoa, sabotaaseja tai tietoturvahyökkäyksiä.*
  - *Painotus siis ulkoisissa uhkatekijöissä*
- Seuraavissa riskeissä korostuu toisaalta hallittavuuden haasteet, selkeyden puute, tiedon saatavuus ja tähän liittyvä laatu sekä toisaalta resurssihaasteet
  - parantamalla hallittavuutta helpotetaan resurssien käyttöä oleelliseen
- Kokonaisuutena riskit arvioidaan melko lähekkäin eri hallinnon kokonaisuuksissa eikä erillisiä klustereita muodostu. Kuvaajassa top-5 riskit
  - Erot näkyvät vasta syvällisemmässä tarkastelussa



Keskeisinä nähdyt riskit: vertailu riskiprofiilien välillä

Keskeisinä nähdyt riskit: vertailu riskiprofiilien välillä (kaksi ylintä)

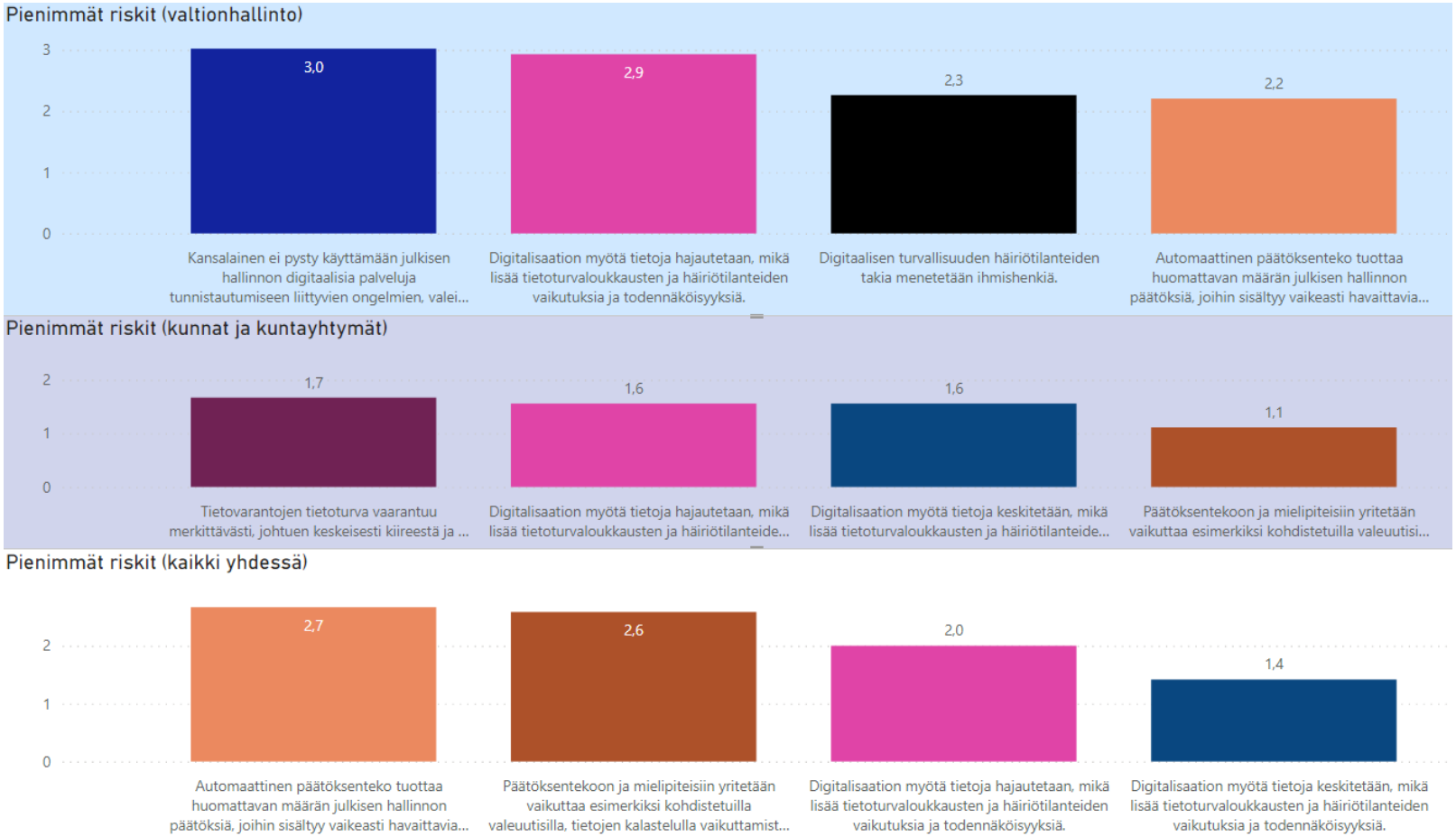
Keskeisinä nähdyt riskit: vertailu riskiprofiilien välillä (eri painotukset)

Vähemmän keskeisinä nähdyt riskit: kaikki vastaajat, bottom-10

Riskiväitteen numero	Riskiväite	Riskiluku	Todennäköisyys
14	Automaattinen päätöksenteko tuottaa huomattavan määrän julkisen hallinnon päätöksiä, joihin sisältyy vaikeasti havaittavia virheitä tai sellaisia painotuksia, jotka tuottavat epäoikeudenmukaisuutta, epätasa-arvoa tai voimistavat eriarvoistumista.	**2,3**	1,3
1	Digitaalisen turvallisuuden häiriötilanteiden takia menetetään ihmishenkiä.	**2,7**	1,3
12	Tiedonhallintayksikkö ei arvioi eikä seuraa digitaalisen turvallisuuden kypsyystasoa.	**3,1**	1,8
15	Tiedonhallintayksiköt eivät voi tietoturva- ja tietosuojavaatimusten tai puutteellisten tiedonsaantioikeuksien vuoksi luovuttaa toisilleen toiminnassa tarvittavia tietoja.	**3,1**	1,9
34	Digitalisaation myötä tietoja hajautetaan, mikä lisää tietoturvaloukkausten ja häiriötilanteiden vaikutuksia ja todennäköisyyksiä.	**3,2**	1,8
8	Valtiolliset tai rikolliset toimijat yrittävät laittomin keinoin hyödyntää julkisen hallinnon tietovarantoja omien poliittisten, sotilaallisten tai taloudellisten tarkoitustensa edistämiseen.	**3,3**	1,7
26	Kansalainen ei pysty käyttämään julkisen hallinnon digitaalisia palveluja tunnistautumiseen liittyvien ongelmien, valeidentiteettien tai identiteettivarkauden takia.	**3,4**	1,9
7	Päätöksentekoon ja mielipiteisiin yritetään vaikuttaa esimerkiksi kohdistetuilla valeuutisilla, tietojen kalastelulla vaikuttamistarkoituksessa tai jopa painostuskampanjalla.	**3,5**	2,0
16	Tiedonhallintayksikössä ei hallita digitaalisen turvallisuuden riskejä osana yleistä riskienhallinnan kokonaisuutta, vaan riskit jäävät yksittäisiksi ja erillisiksi muusta toiminnasta ja sen tavoitteista.	**3,5**	1,9
33	Digitalisaation myötä tietoja keskitetään, mikä lisää tietoturvaloukkausten ja häiriötilanteiden vaikutuksia ja todennäköisyyksiä.	**3,6**	1,8

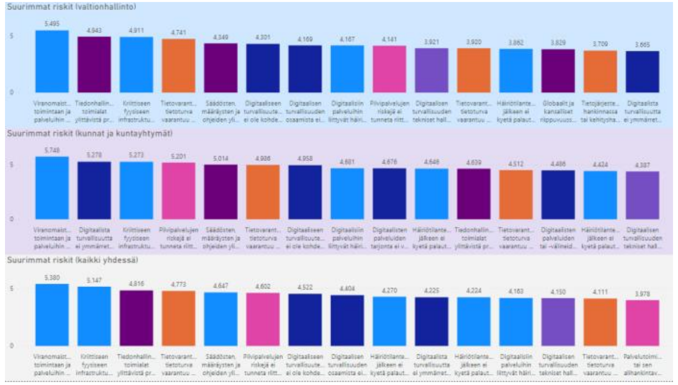
Vähemmän keskeisinä nähdyt riskit: vertailu riskiprofiilien välillä

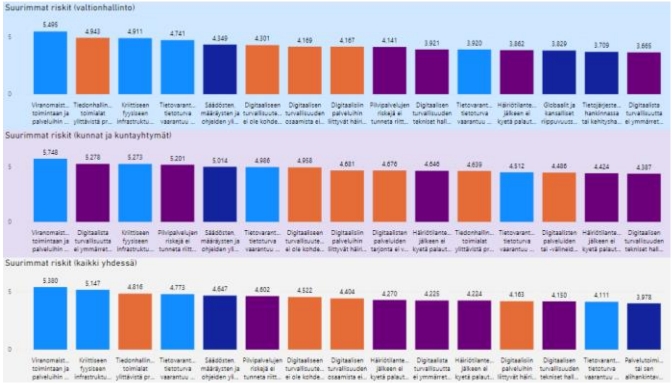
- Profiilien erilaisuus näkyy myös häntäpäässä
- Kunnilla riskilukujen hajonta huomattavasti suurempaa, häntä matalampi
- Keskittämisen ja hajauttamisen välillä ei nähdä eroa
- Kunnat eivät koe vaikuttamista vai eivät tunnista sitä?
- Automaattisen päätöksenteon riskit eivät liene vielä relevantteja (muihin verrattuna)?

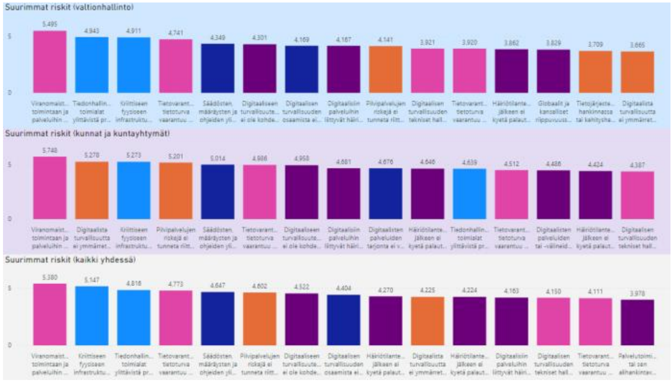


Luokitteluvertailu – erilaisia profiileita

- Top-15 riskien eri luokitteluiden mukaan tehty analyysi näyttää myös erilaisia painotuksia riskiprofiileissa, muttei selkeitä yksinkertaisesti sanoitettavia ilmiöitä. Kehitystä ja sen merkitystä tarkasteltava vuosien aikajänteellä.
  - Kuvaajissa vertailussa ylimpänä valtionhallinto, keskellä kuntakenttä, alhaalla kaikki.
  - Samat riskit väritettynä eri luokkien mukaan. Vasemmalla World Economic Forumin kuusi kategoriaa; keskellä OECD:n neljä luokkaa; oikealla digiturvallisuuden viisi toteutuksen aluetta ja kuudes laajemman katsannon riskiväittämille.

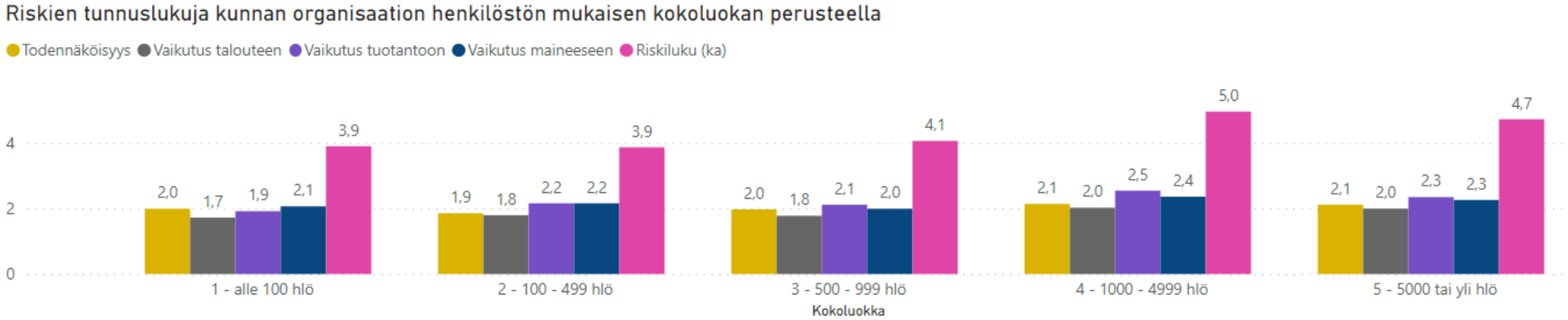






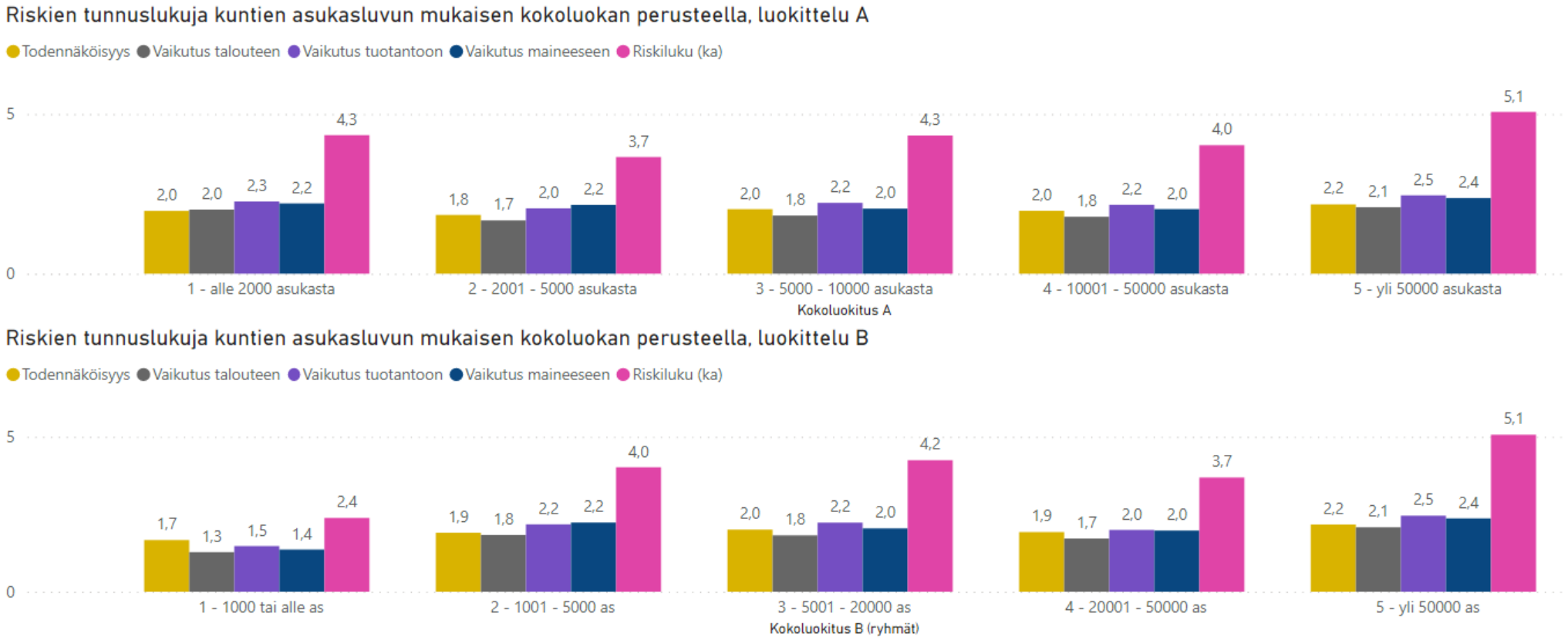
Kuntakenttä

- Vastauksia, riskiluku ja todennäköisyys
- Kuntien riskiluvut ovat melko samanlaiset, riippumatta siitä, mikä niiden koko on asukasluvun tai organisaation henkilöstön määrän mukaan luokiteltuna.
  - Vain suurimpien kohdalla on erotettavissa korkeampia riskilukuja. Selityksenä lienee osallisuus laajempiin toimintoihin (sisältäen mm. laajemmin yhteyksiä lähialueen ulkopuolelle ja komleksisempia vaikutusverkostoja) ja näiden mukana tuleviin riskeihin.
- Vahvistaa ajatusta ”samat riskit kaikilla, mutta eri resurssit vastata niihin”



Vastaajia luokissa (kpl):	3	12	12	5	6

Kuntakentän riskiluvut asukasluvun mukaisissa kokoluokissa (eri raja-arvoin)



Vastaajia (A kpl / B kpl):	5 / 1	9 / 13	5 / 13	12 / 4	7 / 7
Vastaajia max. (2020):	49 / 14	90 / 125	74 / 122	76 / 34	21 / 21

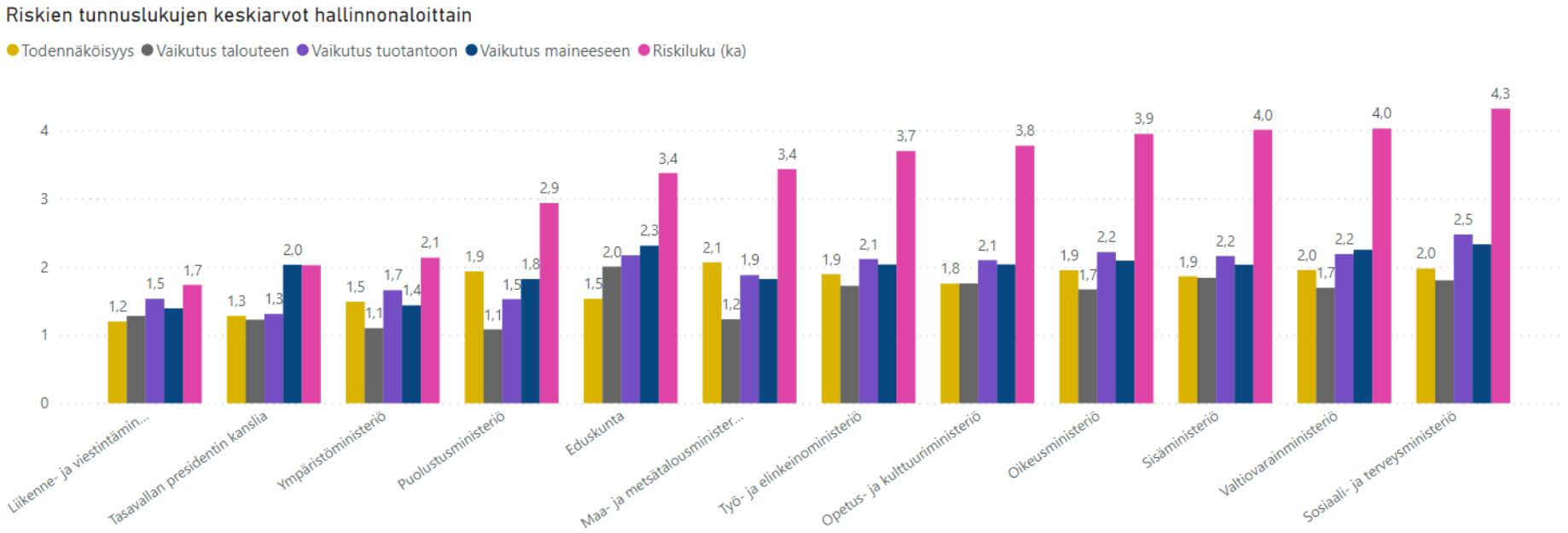
Valtionhallinnon riskinäkymien tunnusluvut

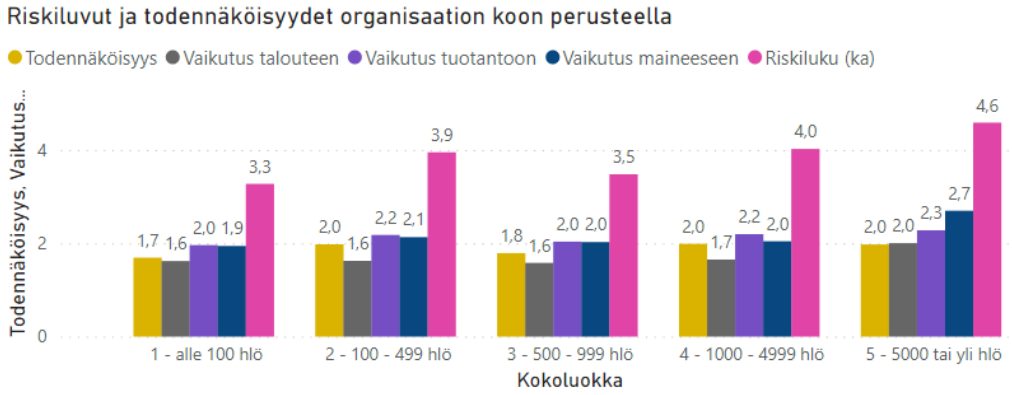
- Vastauksia 49 yksiköltä
- Riskiluvun keskiarvo 3,7
- Todennäköisyyden keskiarvo 1,9
- Digiriskeissä koetut erot näkyvät riskiluvuissa hallinnonaloittain merkittävinä suhteessa toisiinsa
  - Selittävinä tekijöinä mm. omat kyvykkyydet, resurssit ja rakenteet verrattuna sekä suojattaviin kohteisiin ja niiden arvoon että koettuihin uhkiin

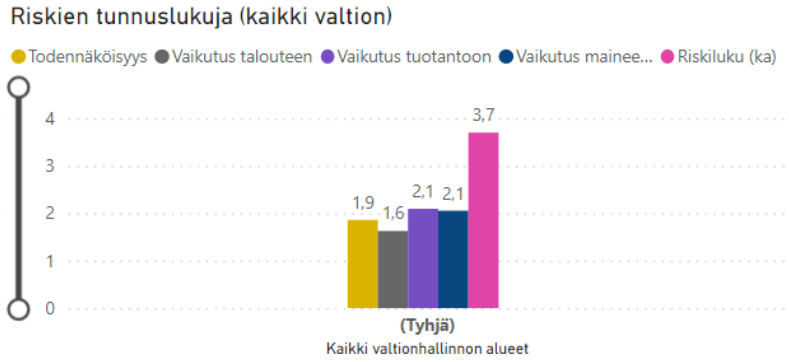
Kokoluokka (henkilöä)	Todennäköisyys (keskiarvo)	Riskiluku (keskiarvo)	Vastanneet (kpl)
Alle 100	1,7	**3,3**	16
100-499	2,0	**3,9**	19
500-999	1,8	**3,5**	6
1000-4999	2,0	**4,0**	7
5000 tai yli	2,0	**4,6**	1

Vastanneet hallinnonalat	Todennäköisyys (keskiarvo)	Riskiluku (keskiarvo)	Vastanneet (kpl)
Liikenne- ja viestintäministeriö	1,2	**1,7**	1
Tasavallan presidentin kanslia	1,3	**2,0**	1
Ympäristöministeriö	1,5	**2,1**	2
Puolustusministeriö	1,9	**2,9**	2
Eduskunta	1,5	**3,4**	1
Maa- ja metsätalousministeriö	2,1	**3,4**	2
Työ- ja elinkeinoministeriö	1,9	**3,7**	5
Opetus- ja kulttuuriministeriö	1,8	**3,8**	5
Oikeusministeriö	1,9	**3,9**	13
Sisäministeriö	1,9	**4,0**	5
Valtiovarainministeriö	2,0	**4,0**	9
Sosiaali- ja terveysministeriö	2,0	**4,3**	3

Valtionhallinnon riskinäkymät kuvaajina







Muita huomioita tuloksista

- Liitteinä olevista riskimatriisien pisteklustereista nähdään, että WEF:n kategorioiden mukaisista luokista digitaalisen infrastruktuurin vakava häiriötilanne sijoitetaan selvästi vaikuttavammaksi kuin vastaavasti keskiarvoa alemmaksi ryhmittyvä teknologinen haitallinen kehitys. Näistä jälkimmäinen sisältää luonteeltaan hitaammin muodostuvia riskejä, joihin vastaaminen on aikaa vievempää ja laaja-alaisempaa, eli painotus on ”välittömämmissä” riskeissä.
- Kehittyneet järjestelmät (tekoäly, algoritmit, koneoppiminen, automatisaatio jne.) saivat vähän huomiota, mutta aihealue muodostunee tulevaisuudessa merkittävämmäksi
  - Syytä tutustua riskeihin etupainotteisesti, sillä alkavat esiintyä tuotteissa
- Vaikuttaminen päätöksentekoon on näyttäytynyt vähäisempänä uhkana
  - Luultavasti painotus on ollut COVID-19 liittyen toisaalla sekä paikallisilla että valtiollisilla toimijoilla ja vaikuttamiseen ollaan ainakin hieman herkempiä nykyisin
  - Varottava, ettei tästä tule sokeaa kohtaa, mikäli uusia vaikuttamisen tapoja ilmaantuu
- Vastaajien ilmoittamien omien riskien ja uusien ilmiöiden merkityksiä ei voitu vertailla, mutta esiin nousi useaan kertaan (eri tavoin muotoiltuna) mm.
  - Sisäisen toimijan tahallinen toiminta
  - Hyvinvointialueet, SOTE-uudistus ja muutokset
  - Kuormitus ja henkilöriski pienissä organisaatioissa
  - Tilanne-, vastuu- ja riskikuvan muodostamisen vaikeus ja tiedonjako, erityisesti yhteisten- ja ulkoisten palveluiden kohdalla
  - Digin turvallisuuden laajemman kuvan unohtaminen, ml. asiakkaat ja prosessit
  - Ilmastovaikutukset, laajat sekä ääriolosuhteet
  - Pitkäaikaisvaikutukset, mm. tiedon säilyttämisen sekä salaamisen suhteen
  - Yhteisten vaatimusten ja ratkaisuiden puute, mutta myös olemassa olevien epätasainen soveltaminen ja tiedon jakaminen

Muuta aiheeseen liittyvää

- Organisaation digiturvakysely (DVV, elokuu 2021)
  - Digiturvallisuuden järjestäminen, ml. riskienhallinnan järjestäminen
    - Riskienhallinnassa selvästi kehitettävää, jäänyt jälkeen muista osa-alueista
    - 18 kehitysehdotusta, joilla vastata mm. riskiväittämiin
- Digiturvabarometri (DVV, lokakuu 2021)
  - Luottamus palveluihin laskussa, useimmat kokeneet mm. tehtävien keskeytyksen
  - Luottamus työnantajiin ja viranomaisiin noin 80%, molemmat lievästi laskussa
- Digitalisaation tilannekuva (VM kesäkuu, lokakuu, joulukuu 2021)
  - Tarkastelee vastaavia strategisia asioita ja riskejä laajemmin, mutta hyvin samalla tavalla ja vastaavan tyyppisiä riskejä
  - Nostoja: sirpaleisuus eri tavoin sekä tiedon hyödyntäminen haasteita laajasti
- Tekoälyn soveltamisen kyber-turvallisuus ja riskienhallinta (Traficom, marraskuu 2021)
  - Yhteen kehittyvään alueeseen kohdistuva näkemys, jossa mukana strategisempia merkityksiä sisältäviä riskejä hyvin erittelevä osuus
- Katsanto myös kyselyn ulkopuolelle: mm. Digiturvaviikkon ohjelma (tallenteet: https://www.mediaserver.fi/live/digiturvaviikko2021), jossa perjantaina aamupäivän tulevaisuuden riskeistä puhuttaessa huomioitiin myös mm. aurinkomyrskyn seuraukset:
  - Suurempaa auringon aktiivisuutta odotetaan ensi vuosikymmenille, minkä lisäksi voi ilmetä erityisen suuri purkaus.
    - Varoitus on korkeintaan 17 tuntia havainnosta.
  - Indusoituvat virrat sähkönjakeluun voivat katkaista globaalit yhteydet. Suomen sähkönsiirto on kuitenkin verrattain häiriösietoisempaa.
    - Digimerkitystä ei ole vielä tarkasti selvitetty täällä eikä maailmalla. Paikalliset verkkohäiriöt häiriöt mahdollisia myös täällä, mutta todennäköisesti ongelmaksi muodostuvat linkittyneet palvelut (etenkin eri maanosiin) → laajoja pitkäkestoisia verkon häiriöitä
      - kyky paikalliseen toimintaan ja omavaraisuuteen korostuu, kuten muissakin kansainvälisten yhteyksien häiriöissä
- EU:n lainsäädäntö on nopeassa kehityksessä digin alueella 2021-2022 ja sen jälkeenkin
  - Datahallinta, tekoäly, digipalvelut, digimarkkinat, sirut, tiedonsiirto…

Hyödyntäminen organisaatioissa: vertailun kautta oman riskinäkemyksen avaamiseen

- Miten oma näkemys organisaation riskeistä vertautuu top-10 listaan?
  - Kattaako oma riskienhallinta kyseiset riskit?
    - Mikäli riskiväitteet eivät tarkalleen osu omaan tilanteeseen, millä muutoksilla niistä tulee relevantteja?
      - Muutos omassa tilanteessa ja toiminnassa (ml. ulkoiset vaatimukset, regulaatio, uudet toiminnot…)
      - Muutos riskin muotoilussa (esim. kohdistaminen tarkemmin tai laajemmin, käytännön toteutukseen sovittaminen)
  - Nämä eivät ole kaikki riskit: miten muut organisaation (digi)riskit vaikuttavat ja suhteutuvat kyselyssä esitettyihin – kumulatiiviset vaikutukset ja dominoefektit
    - Esim. sääntelyn vaatimukset voivat kuormittaa lakipalveluita, mutta tätä kuormitusta voi tulla muualtakin kuin digistä: onko resursointi riittävää ja tarpeeksi syvää
- Miten näihin riskeihin on varauduttu, mitä hallintatoimia pitäisi tehdä?
  - Missä pitäisi olla 2-3 vuoden päästä ja miten sinne päästään?
  - Hallintatoimet eivät ole symmetrisiä laajojen riskien kanssa (kts. seuraava dia)

Organisaatioiden digiturvakyselyn kahdeksan keskeisintä suositusta ja niiden vaikutukset

Täydellinen lista suosituksista organisaatiokyselyn raportin liitteenä DVV:n sivuilla.

Yleinen suositus: riskienhallintaprosessi aktiiviseen käyttöön, sen kehittäminen sekä ulottaminen eri toimijoihin

→ Parantaa yleisesti tilannetta eri riskien suhteen (etenkin: 2, 3, 12, 16, 17, 19, 30, 31, 35)

1. Henkilöstön osaamisen kehittäminen
   → Parantaa yleisesti tilannetta eri riskien suhteen (etenkin: 2, 3, 6, 29)
2. Harjoitustoiminnan kehittäminen ja osallistuminen
   → Parantaa yleisesti tilannetta eri riskien suhteen (etenkin: 2, 3, 9, 11, 30, 31)
3. Raportointi organisaation johdolle ja johto viestii aktiivisesti tilanteesta
   → Parantaa yleisesti tilannetta eri riskien suhteen (etenkin: 16, 17, 23, 29)
4. Etäkäyttöön liittyvien riskien arviointi sekä kattava VPN- ja MFA-käyttöönotto
   → Vähentää mahdollisia todennäköisyyttä ja vaikutuksia (etenkin 2, 3)
5. Varmuuskopiointi, sen testaus ja palautuksen harjoittelu
   → Vähentää mahdollisia vaikutuksia (etenkin 2, 3)
6. Lokitietojen keräämisen varmistaminen ja niiden tehokas hyödyntäminen
   → Vähentää mahdollisia todennäköisyyttä ja vaikutuksia (etenkin 2, 3)
7. Uhkatilanteiden ja toimintaympäristön seuranta sekä riskienhallinta, ml. palvelutuottajien ja kumppaneiden kanssa
   → Vähentää mahdollista todennäköisyyttä (etenkin 2, 3, 5, 9, 11, 27, 28, 29)
8. Palveluiden vikasietoisuuden parantaminen
   → Vähentää mahdollisia vaikutuksia (etenkin 3, 9, 18, 20, 25, 30, 31)

Yhteenveto laajempaa kehittämistä varten

- **Keskeisimmät kehitystehtävät kyselyyn ja riskien listaukseen perustuen**
  - **Riskit 2 ja 3:** Yhtenevän ja jaetun, välittömämpiä uhkia laajemman riskikuvan kehittämistä tulisi edistää. DVV viestii VAHTI-tilaisuuksissa ulkoisen kyberuhkan todellisuudesta ja hallintakeinoista vuoden 2022 aikana.
  - **Riskit 25 ja 13 (ym.):** Yhtenäisen hallittavuuden ja ymmärryksen tukemista eri tasoilla ja tavoilla on tärkeää kehittää. DVV kehittää digiturvallisuuden ohjeistusten löydettävyyttä vuoden 2022 aikana.
  - **Näkymä kuntien riskiprofiiliin syventynyt:** Toimenpiteiden ja tuen kohdentaminen ja muotoilu oikein vaikutusten tehostamiseksi. Pyritään ottamaan huomioon paremmin ja hyödynnetään JUDO-hankkeessa, etenkin Kuntien yhteishankkeessa vuoden 2022 aikana.

Lista riskiväittämistä

Liite 1
Digiturvallisuuden riskikyselyn tulokset, syksy 2021

DIGI- JA VÄESTÖTIETOVIRASTO

Kyselyssä käytetyt riskiväittämät, 1/3

Riski nro	Riskiväite	Risk påstående	OECD	WEF	Digiturva
1	Digitaalisen turvallisuuden häiriötilanteiden takia menetetään ihmishenkiä.	Människoliv går förlorade på grund av störningar i den digitala säkerheten.	Kansallinen ja kansainvälinen turvallisuus	Digitaalisen infrastruktuurin vakava häiriötilanne	Kyberturvallisuus
2	Viranomaisten toimintaan ja palveluihin kohdistuu tahallisia vakavia tietoturvahyökkäyksiä.	Myndigheternas verksamhet och tjänster utsätts avsiktligt för allvarliga datasäkerhetsattacker.	Kansallinen ja kansainvälinen turvallisuus	Digitaalisen infrastruktuurin vakava häiriötilanne	Tietoturva
3	Kriittiseen fyysiseen infrastruktuuriin ja tietoverkkoihin kohdistuu vakavia väärinkäytöksiä, haitantekoa, sabotaaseja tai tietoturvahyökkäyksiä.	Den kritiska fysiska infrastrukturen och datanäten utsätts för allvarligt missbruk, blockering, sabotage eller datasäkerhetsattacker.	Kansallinen ja kansainvälinen turvallisuus	Digitaalisen infrastruktuurin vakava häiriötilanne	Kyberturvallisuus
4	Tietovarantojen tietoturva vaarantuu merkittävästi, johtuen keskeisesti kiireestä ja resursointivajeesta.	Datasäkerheten i datalagren äventyras avsevärt på grund av brådska och resursbrist.	Kansallinen ja kansainvälinen turvallisuus	Digitaalisen turvallisuuden laiminlyönti	Tietoturva
5	Tietovarantojen tietoturva vaarantuu merkittävästi, johtuen keskeisesti monimutkaistuvaan teknologiaan liittyvistä puutteista digitaidoissa.	Datasäkerheten i datalagren äventyras avsevärt på grund av brister i digital kompetens till följd av den allt mer komplicerade tekniken.	Kansallinen ja kansainvälinen turvallisuus	Digitaalisen turvallisuuden laiminlyönti	Tietoturva
6	Tietovarantojen tietoturva vaarantuu merkittävästi. Keskeisenä syynä ovat piittaamattomuus sekä asennoituminen tietoturvan noudattamiseen ja vaatimuksiin.	Datalagrens datasäkerhet äventyras avsevärt. En väsentlig orsak är likgiltighet och attityden till att iaktta datasäkerhet och krav.	Kansallinen ja kansainvälinen turvallisuus	Digitaalisen turvallisuuden laiminlyönti	Tietoturva
7	Päätöksentekoon ja mielipiteisiin yritetään vaikuttaa esimerkiksi kohdistetuilla valeuutisilla, tietojen kalastelulla vaikuttamistarkoituksessa tai jopa painostuskampanjalla.	Man försöker påverka beslutsfattandet och åsikterna till exempel genom riktade falska nyheter, genom nätfiske i syfte att påverka eller till och med genom en påtryckningskampanj.	Kansallinen ja kansainvälinen turvallisuus	Digitaalisten resurssien keskittyminen	Kyberturvallisuus
8	Valtiolliset tai rikolliset toimijat yrittävät laittomin keinoin hyödyntää julkisen hallinnon tietovarantoja omien poliittisten, sotilaallisten tai taloudellisten tarkoitustensa edistämiseen.	Statliga eller kriminella aktörer försöker med olagliga medel utnyttja den offentliga förvaltningens datalager för att främja sina egna politiska, militära eller ekonomiska ändamål.	Kansallinen ja kansainvälinen turvallisuus	Haitallinen teknologinen kehitys	Kyberturvallisuus
9	Globaalit ja kansalliset riippuvuussuhteet tai toimitusverkostojen häiriöt aiheuttavat keskeytyksiä lakisääteisissä tehtävissä.	Globala och nationella beroendeförhållanden eller störningar i leveransnätverken orsakar avbrott i de lagstadgade uppgifterna.	Lainvalvonta	Digitaalisen turvallisuuden ohjauksen epäonnistuminen	Toiminnan jatkuvuus ja varautuminen
10	Tietojärjestelmän hankinnassa tai kehityshankkeessa ei noudateta riittäviä digitaalisen turvallisuuden vaatimuksia.	I upphandling av eller i utvecklingsprojekt gällande datasystem iakttas inte tillräckliga krav på digital säkerhet.	Lainvalvonta	Digitaalisen turvallisuuden laiminlyönti	Riskienhallinta
11	Tietojärjestelmien vaatimustenmukaisuutta ei ole arvioitu tai ei arvioida uudelleen, kun toimintaympäristö muuttuu.	Datasystemens kravenlighet har inte bedömts eller bedöms inte på nytt när verksamhetsmiljön förändras.	Lainvalvonta	Digitaalisen turvallisuuden laiminlyönti	Riskienhallinta
12	Tiedonhallintayksikkö ei arvioi eikä seuraa digitaalisen turvallisuuden kypsyystasoa.	Informationshanteringsenheten varken bedömer eller följer upp den digitala säkerhetens mognadsnivå.	Lainvalvonta	Digitaalisen turvallisuuden ohjauksen epäonnistuminen	Riskienhallinta
13	Säädösten, määräysten ja ohjeiden ylimitoitus, ajantasaisuuden puute, virheellisyys, muutosten nopeus tai muut sääntelyn laatuun liittyvät ominaisuudet aiheuttavat kohtuuttomia velvoitteita.	Överdimensionering av föreskrifter, bestämmelser och anvisningar, brist på aktualitet, felaktighet, snabba förändringar eller andra omständigheter förknippade med regleringens kvalitet resulterar i oskäliga skyldigheter.	Lainvalvonta	Digitaalisen turvallisuuden ohjauksen epäonnistuminen	Muu laajempi digiturvallisuusaihe

Kyselyssä käytetyt riskiväittämät, 2/3

Riski nro	Riskiväite	Risk påstående	OECD	WEF	Digiturva
14	Automaattinen päätöksenteko tuottaa huomattavan määrän julkisen hallinnon päätöksiä, joihin sisältyy vaikeasti havaittavia virheitä tai sellaisia painotuksia, jotka tuottavat epäoikeudenmukaisuutta, epätasa-arvoa tai voimistavat eriarvoistumista.	Automatiskt beslutsfattande ger upphov till ett betydande antal beslut inom den offentliga förvaltningen som innehåller svårupptäckta fel eller fokuseringar som skapar orättvisa och ojämlikhet eller förstärker ojämlikheten.	Lainvalvonta	Haitallinen teknologinen kehitys	Tietosuoja
15	Tiedonhallintayksiköt eivät voi tietoturva- ja tietosuojavaatimusten tai puutteellisten tiedonsaantioikeuksien vuoksi luovuttaa toisilleen toiminnassa tarvittavia tietoja.	Informationshanteringsenheterna kan inte lämna varandra de uppgifter som behövs i verksamheten på grund av datasäkerhets- och datasekretesskrav eller på grund av bristfälliga rättigheter att få information.	Lainvalvonta	Digitaalisen turvallisuuden ohjauksen epäonnistuminen	Tietosuoja
16	Tiedonhallintayksikössä ei hallita digitaalisen turvallisuuden riskejä osana yleistä riskienhallinnan kokonaisuutta, vaan riskit jäävät yksittäisiksi ja erillisiksi muusta toiminnasta ja sen tavoitteista.	Informationshanteringsenheten hanterar inte riskerna inom den digital säkerheten som en del av den allmänna riskhanteringen, utan riskerna förblir enskilda och separata från den övriga verksamheten och dess mål.	Lainvalvonta	Digitaalisen turvallisuuden ohjauksen epäonnistuminen	Riskienhallinta
17	Tiedonhallintayksikön tai toimialan johto ei toteuta riskienhallinnan kautta tunnistettuja, perusteltuja toimenpiteitä.	Ledningen för informationshanteringsenheten eller ett verksamhetsområde genomför inte motiverade åtgärder som identifierats via riskhanteringen.	Lainvalvonta	Digitaalisen turvallisuuden ohjauksen epäonnistuminen	Riskienhallinta
18	Palvelutoimittajan tai sen alihankintaverkostossa olevan toimittajan liiketoimintojen myynti tai päättyminen vaarantaa palvelujen häiriöttömän toiminnan tai palveluissa käytettyjen tietojen turvallisuuden.	Om en tjänsteleverantör eller en leverantör i dennes underleverantörsnätverk säljer eller avslutar sin affärsverksamhet äventyras tjänsternas funktion eller säkerheten i de uppgifter som används i tjänsterna.	Lainvalvonta	Digitaalisten resurssien keskittyminen	Toiminnan jatkuvuus ja varautuminen
19	Digitaalisen turvallisuuden riskienhallinnassa ei huomioida taloudellisia vaikutuksia riittävästi, mistä syntyy merkittäviä ennakoimattomia kustannuksia.	I riskhanteringen av den digitala säkerheten beaktas inte de ekonomiska konsekvenserna tillräckligt, vilket leder till betydande oförutsedda kostnader.	Taloudellinen ja yhteiskunnallinen hyvinvointi	Digitaalisen turvallisuuden ohjauksen epäonnistuminen	Riskienhallinta
20	Digitaalisiin palveluihin liittyvät häiriötilanteet aiheuttavat luottamuksen rapautumista viranomaisiin sekä julkisiin palveluihin.	Störningar i digitala tjänster leder till att förtroendet för myndigheterna och de offentliga tjänsterna raseras.	Taloudellinen ja yhteiskunnallinen hyvinvointi	Digitaalisen infrastruktuurin vakava häiriötilanne	Toiminnan jatkuvuus ja varautuminen
21	Digitaalisten palveluiden tarjonta ei vastaa kansalaisten tarpeita.	Utbudet av digitala tjänster motsvarar inte medborgarnas behov.	Taloudellinen ja yhteiskunnallinen hyvinvointi	Digitaalisen toimintaympäristön epätasa-arvo	Muu laajempi digiturvallisuusaihe
22	Digitaalisten palveluiden tai -välineiden ongelmatilanteisiin ei saa apua riittävän nopeasti tai saatu tuki on puutteellista.	Man får inte hjälp med problem med digitala tjänster eller digitala verktyg tillräckligt snabbt eller stödet är bristfälligt.	Taloudellinen ja yhteiskunnallinen hyvinvointi	Digitaalisen toimintaympäristön epätasa-arvo	Toiminnan jatkuvuus ja varautuminen
23	Digitaaliseen turvallisuuteen ei ole kohdennettu riittävästi taloudellisia resursseja.	Den digitala säkerheten har inte tilldelats tillräckliga ekonomiska resurser.	Taloudellinen ja yhteiskunnallinen hyvinvointi	Digitaalisen toimintaympäristön epätasa-arvo	Toiminnan jatkuvuus ja varautuminen
24	Digitaalisen turvallisuuden osaamista ei ole käytettävissä riittävästi.	Kunskapen om den digitala säkerheten är inte tillräcklig.	Taloudellinen ja yhteiskunnallinen hyvinvointi	Digitaalisen toimintaympäristön epätasa-arvo	Muu laajempi digiturvallisuusaihe
25	Tiedonhallintayksikön toimialat ylittävistä prosesseista, ICT-toimittajista, alihankkijoista ja tuotantoympäristöistä koostuvan kompleksisen kokonaisuuden hallinta epäonnistuu, mikä aiheuttaa häiriöitä ja palvelukatkoja.	Hanteringen av en komplex helhet som består av processer som överskrider informationshanteringsenhetens verksamhetsområden, ICT-leverantörer, underleverantörer och produktionsmiljöer misslyckas, vilket orsakar störningar och serviceavbrott.	Taloudellinen ja yhteiskunnallinen hyvinvointi	Digitaalisen turvallisuuden ohjauksen epäonnistuminen	Kyberturvallisuus

Kyselyssä käytetyt riskiväittämät, 3/3

Riski nro	Riskiväite	Risk påstående	OECD	WEF	Digiturva
26	Kansalainen ei pysty käyttämään julkisen hallinnon digitaalisia palveluja tunnistautumiseen liittyvien ongelmien, valeidentiteettien tai identiteettivarkauden takia.	Medborgaren kan inte använda den offentliga förvaltningens digitala tjänster på grund av problem med identifieringen, falska identiteter eller identitetsstöld.	Taloudellinen ja yhteiskunnallinen hyvinvointi	Haitallinen teknologinen kehitys	Tietosuoja
27	Digitaalisen turvallisuuden tekniset hallintakeinot (mm. työkalut, järjestelmät, asetukset, havainnointi ja suojaus) eivät mukaudu teknologian jatkuvasta muuttumisesta aiheutuviin haasteisiin riittävän nopeasti.	Metoderna för teknisk hantering av digital säkerhet (bl.a. verktyg, system, inställningar, observation och skydd) anpassas inte tillräckligt snabbt till de utmaningar som den kontinuerliga tekniska utvecklingen medför.	Teknologia	Haitallinen teknologinen kehitys	Tietoturva
28	Digitaalisen turvallisuuden hallinnolliset hallintakeinot (mm. päätöksentekotavat, tilannekuvan seuranta, ohjeistus ja osaaminen) eivät mukaudu teknologian jatkuvasta muuttumisesta aiheutuviin haasteisiin riittävän nopeasti.	Metoderna för administrativ hantering av digital säkerhet (bl.a. beslutssätt, uppföljning av lägesbilden, anvisningar och kompetens) anpassas inte tillräckligt snabbt till de utmaningar som den kontinuerliga tekniska utvecklingen medför.	Teknologia	Digitaalisen turvallisuuden ohjauksen epäonnistuminen	Toiminnan jatkuvuus ja varautuminen
29	Digitaalista turvallisuutta ei ymmärretä, arvosteta tai huomioida toiminnan suunnittelussa.	Den digitala säkerheten förstås, uppskattas eller beaktas inte i planeringen av verksamheten.	Teknologia	Digitaalisen toimintaympäristön epätasa-arvo	Riskienhallinta
30	Häiriötilanteiden jälkeen ei kyetä palauttamaan infrastruktuurin hallintaa, eli kokonaisuus on rakennettava käytännössä uudelleen, ja menetetään fyysistä omaisuutta.	Efter störningssituationer kan man inte återställa hanteringen av infrastrukturen, dvs. helheten måste byggas om i praktiken och fysisk egendom går förlorad.	Teknologia	Digitaalisen infrastruktuurin vakava häiriötilanne	Toiminnan jatkuvuus ja varautuminen
31	Häiriötilanteiden jälkeen ei kyetä palauttamaan tietoja käyttöön eli menetetään tietoa, immateriaalioikeuksia tai ohjelmistoja.	Efter störningssituationer kan man inte återställa information, dvs. man förlorar information, immateriella rättigheter eller programvara.	Teknologia	Digitaalisen infrastruktuurin vakava häiriötilanne	Toiminnan jatkuvuus ja varautuminen
32	Prosessien ja tietojärjestelmien välisiä toiminnallisia tai teknisiä riippuvuuksia ei ole tunnistettu riittävällä tarkkuudella ja syvyydellä.	Funktionella eller tekniska beroendeförhållanden mellan processer och informationssystem har inte identifierats med tillräcklig noggrannhet och djup.	Teknologia	Digitaalisen turvallisuuden laiminlyönti	Kyberturvallisuus
33	Digitalisaation myötä tietoja keskitetään, mikä lisää tietoturvaloukkausten ja häiriötilanteiden vaikutuksia ja todennäköisyyksiä.	I och med digitaliseringen centraliseras informationen, vilket ökar sannolikheten för och effekterna av störningar och kränkningar av informationssäkerheten.	Teknologia	Digitaalisten resurssien keskittyminen	Tietoturva
34	Digitalisaation myötä tietoja hajautetaan, mikä lisää tietoturvaloukkausten ja häiriötilanteiden vaikutuksia ja todennäköisyyksiä.	I och med digitaliseringen decentraliseras informationen, vilket ökar sannolikheten för och effekterna av störningar och kränkningar av informationssäkerheten.	Teknologia	Digitaalisten resurssien keskittyminen	Tietoturva
35	Pilvipalvelujen riskejä ei tunneta riittävästi, jolloin niiden hallintatoimet - joko sopimuksilla tai muilla keinoilla - ovat epäselviä ja tilannekuva puutteellinen.	Man känner inte tillräckligt väl till riskerna med molntjänster, vilket innebär att åtgärderna för att hantera dem –antingen genom avtal eller på andra sätt –är oklara och lägesbilden bristfällig.	Teknologia	Digitaalisten resurssien keskittyminen	Riskienhallinta
36	Tietojärjestelmien ja sovellusten sisältämien tietojen sijaintia, liikkumista tai hallintamenettelyjä tietoverkoissa ja -järjestelmissä ei tunneta.	Man känner inte till var uppgifterna i informationssystemen och applikationerna finns, hur de rör sig eller hur de hanteras i datanät och -system.	Teknologia	Haitallinen teknologinen kehitys	Riskienhallinta

World Economic Forumin kategorioiden mukaisesti luokitteltuna, kaikki vastaajat

Liite 2
Digiturvallisuuden riskikyselyn tulokset, syksy 2021

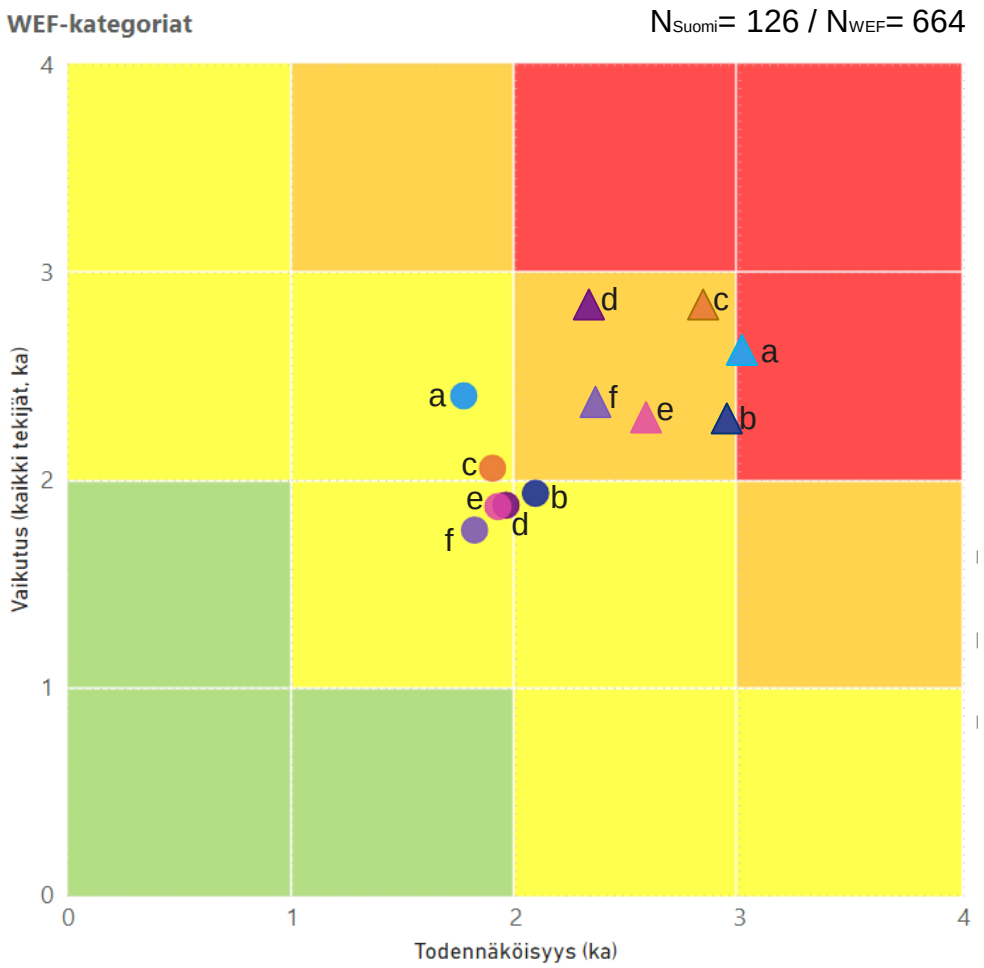
DIGI- JA VÄESTÖTIETOVIRASTO

WEF:n riskikategoriat

	Riskikategoria	Kuvaus
a	Digitaalisten resurssien keskittyminen	Digitaalisten resurssien ja omaisuuden keskittyminen harvojen valtioiden tai yksilöiden käsiin johtaa esimerkiksi harkinnanvaraiseen hinnoitteluun markkinoilla, valvonnan puutteeseen sekä eriarvoiseen asemaan datan hyödyntämisessä.
b	Digitaalisen toimintaympäristön epätasa-arvo	Yksilöiden teknologian käyttö sekä pääsy tietoverkkoihin vaihtelee maittain ja maiden sisällä. Tämä johtuu investointien eriaikaisuudesta, työikäisten osaamisen ja ymmärryksen puutteesta sekä markkinoiden kypsyydestä ja poliittisista rajoituksista.
c	Kyberturvallisuuden laiminlyönti	Vanhentuneet tai päivittämättömät digitaalisen turvallisuuden elementit kotitalouksissa, yrityksissä ja yhteisöissä sekä julkishallinnossa eivät estä hyökkäyksiä. Tämä johtaa merkittäviin kuluihin ja tappioihin sekä aiheuttaa poliittisia jännitteitä ja epävakautta yhteiskunnassa.
d	Digitaalisen infrastruktuurin vakava häiriötilanne	Digitaalisten palvelujen edellyttämän kriittisen infrastruktuurin ja sen ylläpitämiseen liittyvien palveluiden katkos tai heikkeneminen, joka johtuu teknologisesta riippuvuudesta verkkojen tai teknologian osalta: tekoälyä vaativat järjestelmät, Internet, yleishyödylliset palvelut, satelliitit jne
e	Digitaalisen turvallisuuden ohjauksen epäonnistuminen	Maailmanlaajuisten standardien ja viitekehysten puutteesta johtuen valtiot ottavat käyttöön teknologiaa, joka ei ole yhteensopivaa muiden maiden kanssa.
f	Haitallinen teknologinen kehitys	Teknologisen kehityksen tahalliset tai tahattomat negatiiviset seuraukset yksilöille, yrityksille, ekosysteemeille ja/tai taloudelle: tekoäly, aivojen ja tietokoneiden rajapinnat, biotekniikka, geotekniikka, kvanttilaskenta jne.

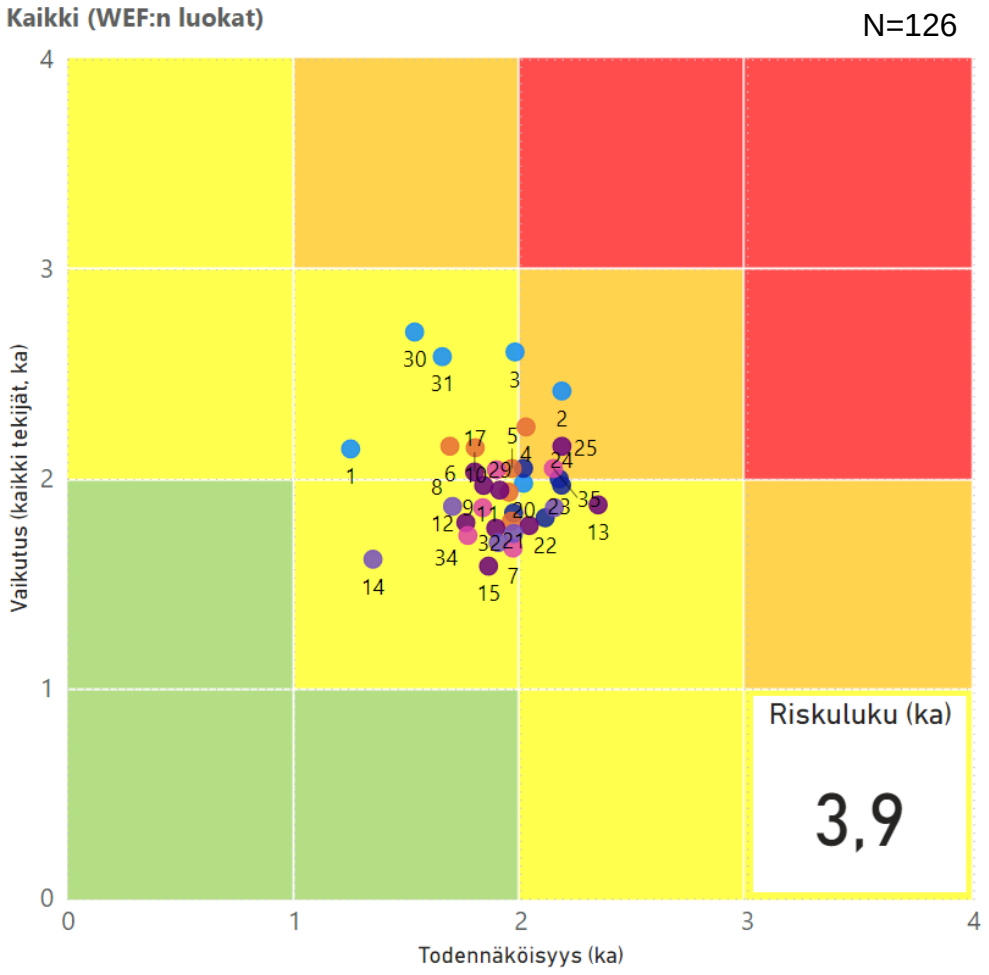
Lähde: https://www.weforum.org/reports/the-global-risks-report-2021 (muun muassa s.89, 11-12, 47, 29-37)

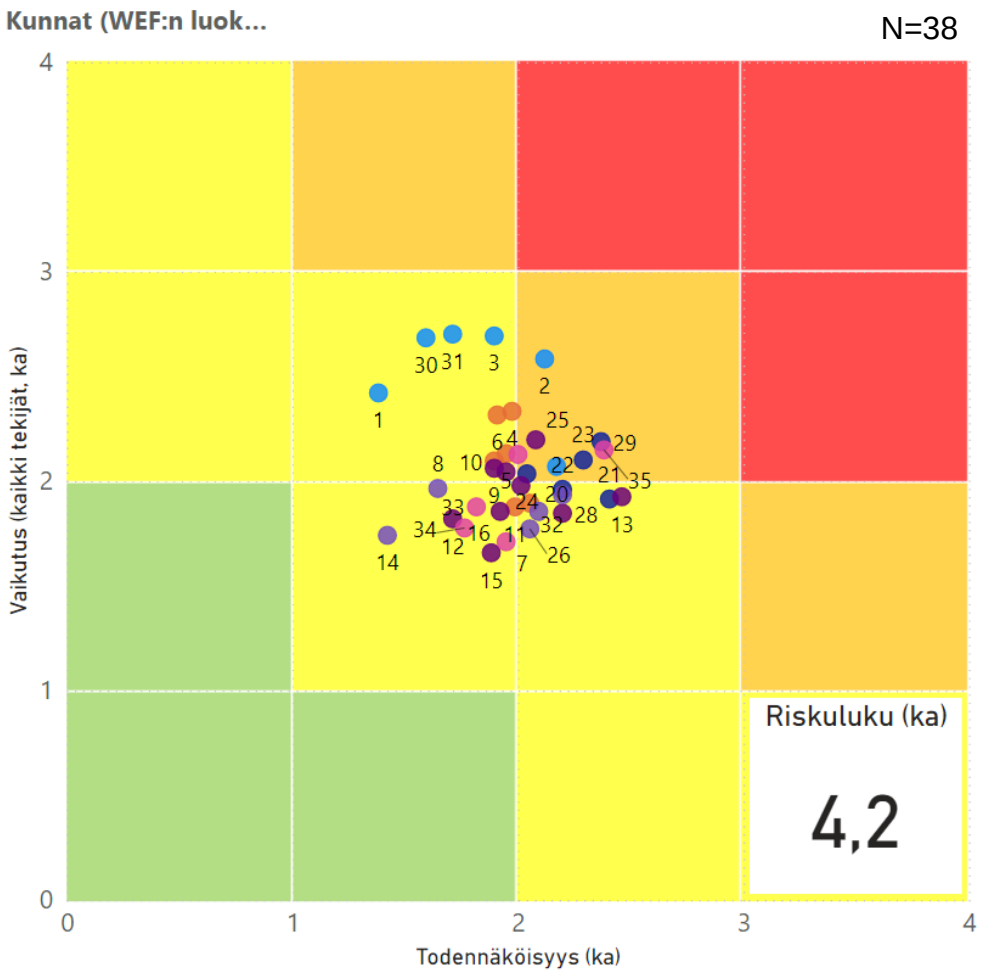
Riskikyselyn tulokset – WEF-kategorioiden välinen vertailu globaaliin näkemykseen



- Vertailu riskikyselyn näkemysten ja World Economic Forumin vastaavan riskimatriisin välillä, jossa arvioidaan globaalia kehitystä 10 vuoden aikaikkunalla (riskikyselyssä kolmen vuoden)
- Riskikyselyn arvot merkitty palloina, WEF:n tutkimuksen arvot kolmioina:
  a. Digitaalisten resurssien keskittyminen
  b. Digitaalisen toimintaympäristön epätasa-arvo
  c. Kyberturvallisuuden laiminlyönti
  d. Digitaalisen infrastruktuurin vakava häiriötilanne
  e. Digitaalisen turvallisuuden ohjauksen epäonnistuminen
  f. Haitallinen teknologinen kehitys
- WEF:n klusterin arvot ovat selvästi suuremmat ja merkittävät erot ovat a ja c kategorioissa verrattuna näkymään Suomessa
- Arvot ovat vain suuntaa-antavia johtuen metodologisista eroista, kuten aikaikkuna
  - WEF:n tutkimus vuodelta 2020, julkaistu raportissa 2021 (s.12)

Riskikyselyn tulokset – WEF-otsikoiden mukainen luokittelu, kaikki ja kunnat vertailu





Kaikki vastaajat
OECD:n digiturvan osa-alueiden luokittelun mukaisesti

Liite 4
Digiturvallisuuden riskikyselyn tulokset, syksy 2021

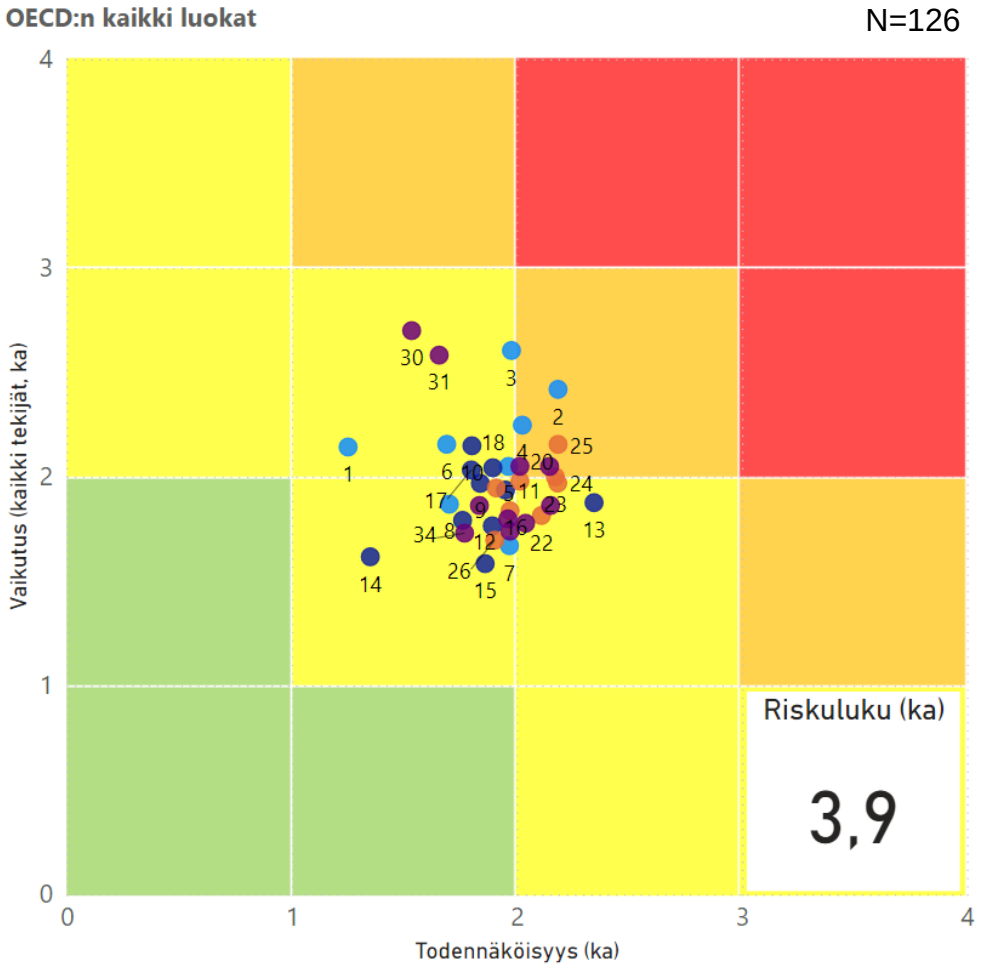
DIGI- JA VÄESTÖTIETOVIRASTO

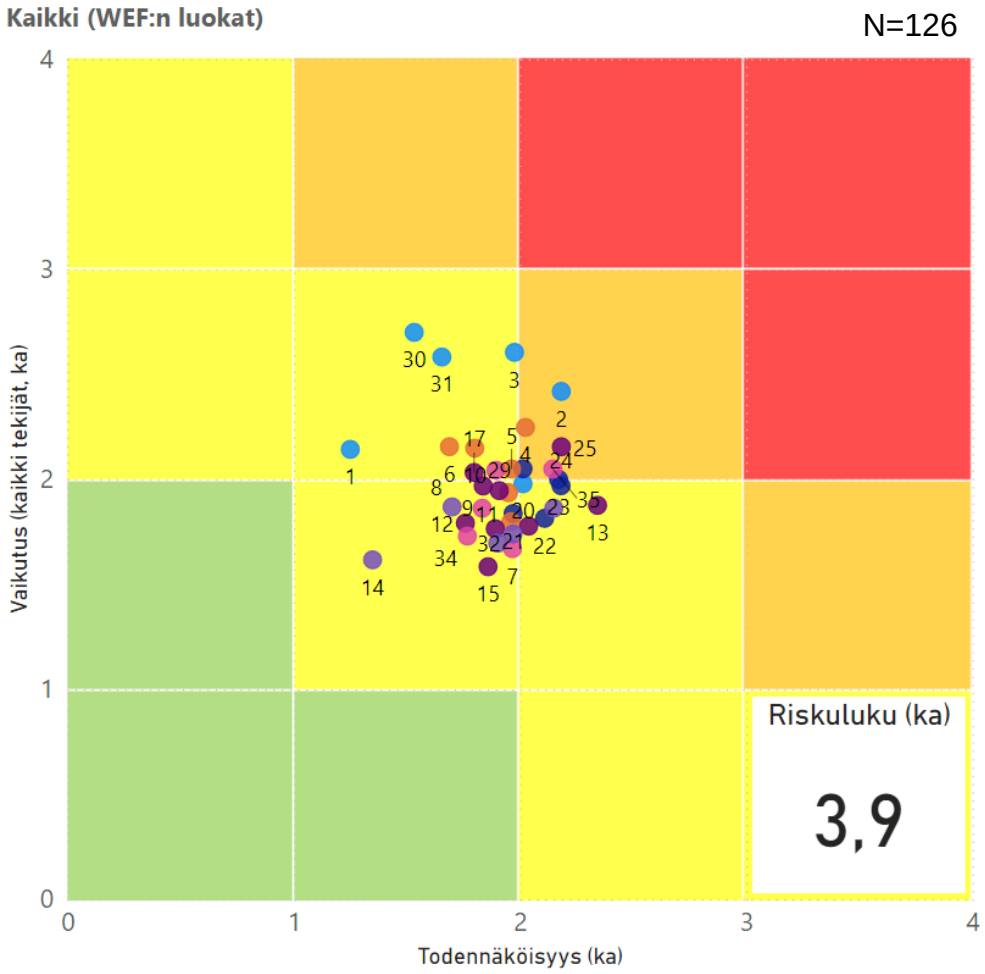
OECD:n luokittelu digiturvan osa-alueista

OECD:n mukaan: *Digitaalista turvallisuutta voidaan lähestyä ainakin neljästä eri näkökulmasta, joista jokainen on lähtöisin omanlaisestaan kulttuurista ja taustasta, vakiintuneista käytännöistä ja tavoitteista:*

- ***teknologia*** *eli keskittyminen digitaalisen ympäristön toimintaan (josta asiantuntijat usein käyttävät sanoja "tietoturvallisuus" tai "verkkoturvallisuus")*
- ***lainvalvonta*** *sekä oikeudelliset näkökohdat laajemminkin (esim. tietoverkkorikollisuus)*
- ***kansallinen ja kansainvälinen turvallisuus*** *käsittäen mm. tieto- ja viestintätekniikoiden roolin tiedustelutoiminnassa, konfliktintorjunnassa, sodankäynnissä jne.*
- ***taloudellinen ja yhteiskunnallinen hyvinvointi****, joka käsittää vaurauden luomisen, innovaatiotoiminnan, kasvun, kilpailukyvyn ja työllisyyden kaikilla talouden osa-alueilla, sekä eri näkökulmat kuten yksilönvapaudet, terveys, koulutus, kulttuuri, demokraattinen osallistuminen, tiede, vapaa-aika ja muut hyvinvoinnin ulottuvuudet, joissa digitaalinen ympäristö toimii kehityksen veturina.*

Riskikyselyn tulokset – OECD ja WEF vertailu, kaikki vastaajat





Kaikki vastaajat Digiturvallisuuden toteutusrakenteen mukaisesti sekä kategoria ”muut”

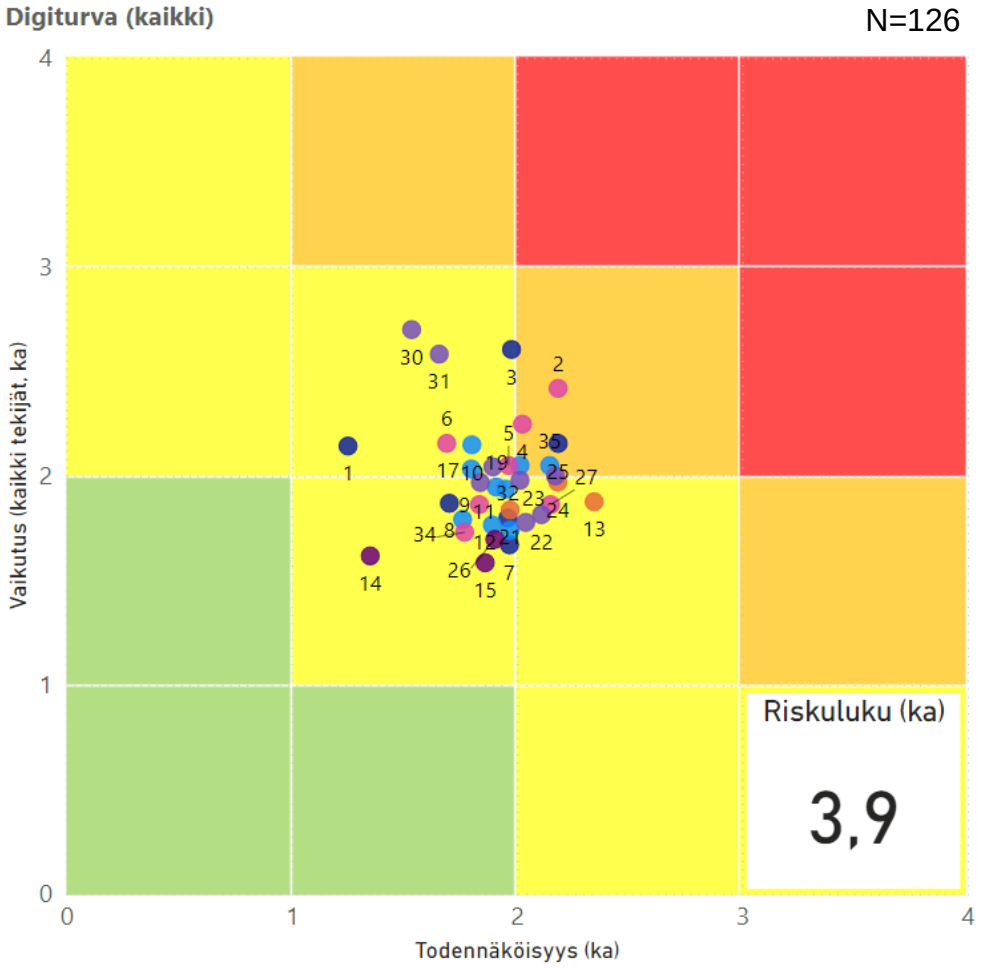
Liite 5
Digiturvallisuuden riskikyselyn tulokset, syksy 2021

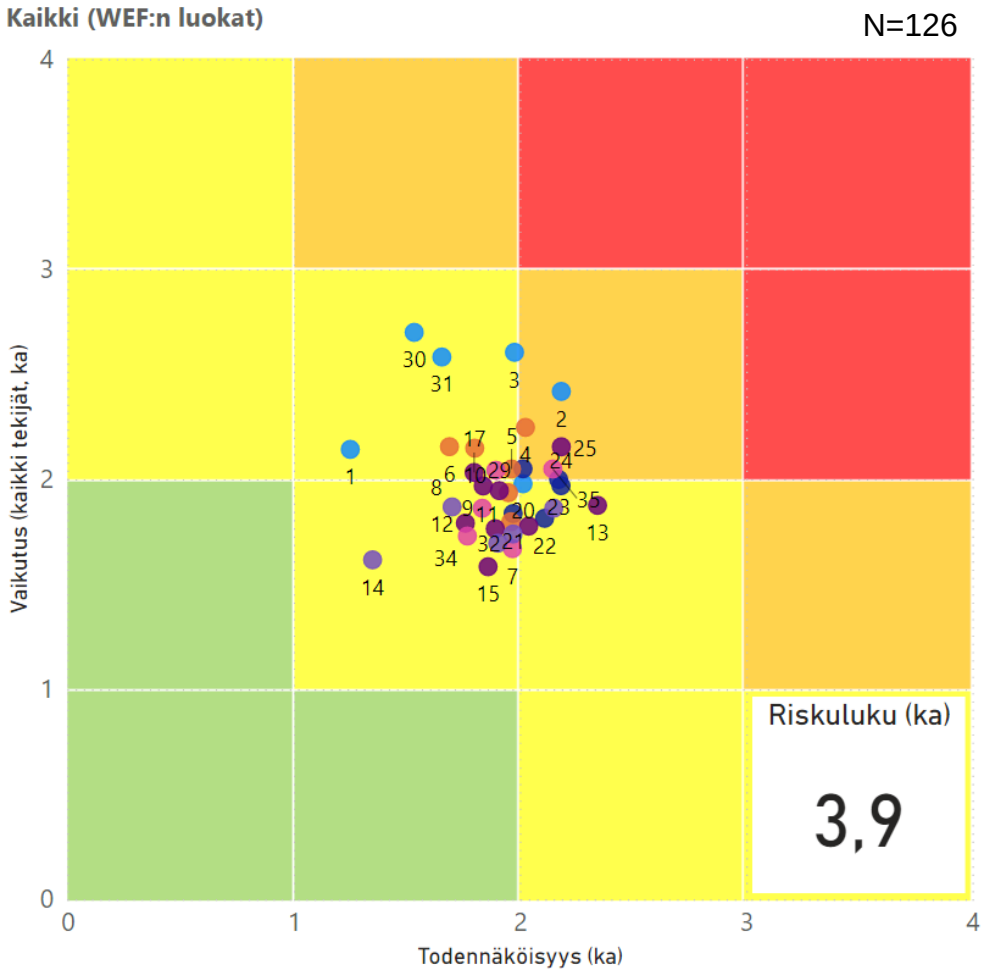
DIGI- JA VÄESTÖTIETOVIRASTO

Digiturvallisuuden toteutusrakenteen osa-alueet luokituksena

1. **Johtaminen ja riskienhallinta**
2. **Tietosuoja**
3. **Tietoturvallisuus**
4. **Jatkuvuudenhallinta**
5. **Kyberturvallisuus**
6. **Muut laajemmat digiturvallisuusaiheet**, sisältäen digitaaliseen turvallisuuteen vaikuttavat asiat, jotka eivät sisälly edellä mainittuihin digiturvan toteuttamisen alueisiin

Riskikyselyn tulokset – Digiturvan rakenteen ja WEF vertailu, kaikki vastaajat





DIGI- JA VÄESTÖTIETOVIRASTO

dvv.fi