DIGI- JA VÄESTÖTIETO-VIRASTO

Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta

Yleinen riskitilannekatsaus, kevät 2023

29.05.2023

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

DTYT / Reivo Juho (DVV)

29.5.2023

Sisällysluettelo

DTYT / Reivo Juho (DVV)

29.5.2023

1 JHDTSRH – yleinen riskitilannekatsaus, kevät 2023

Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta (JHDTSRH) tarkastelee sekä riskejä, että myös riskienhallinnan tilaa. Tarkastelu perustuu tätä varten kuvattuun malliin[1], minkä avulla pyritään kehittyvään riskienhallintaan ja laadukkaaseen tuotettuun tietoon päätöksentekoa varten. Vuosittain tuotettava tietotuote on julkisen hallinnon laajuisen strategisen tason ennakoiva näkymä digiturvallisuuden riskeihin ja riskienhallintaan. Tehtävä perustuu lakiin Digi- ja väestötietovirastosta (304/2019) §3.

Raportti sisältää turvallisuuteen liittyvää materiaalia, jota tulee käsitellä asianmukaista huolellisuutta noudattaen, huomioiden tarvittavilta osin laki viranomaisten toiminnan julkisuudesta (621/1999) sekä laki julkisen hallinnon tiedonhallinnasta (906/2019). Tarkasteltavat riskit sekä niistä tuotettava tilastollinen tieto on pyritty suunnittelemaan siten, että käsittely ei sisällä tai ole tarkkuudeltaan turvallisuutta heikentävää, jotta tiedonvaihto julkishallinnossa mahdollistuu. Raporttista tuotetaan erillinen versio kyselyyn osallistuneille.

Digi- ja väestötietoviraston digiturvallisuusryhmä tuottaa tarvittaessa tarkasteluita ja vertailutietoa digiturvallisuuden kokonaisuuden ja osa-alueiden tilanteesta, ml. riskienhallinnasta: digiturva@dvv.fi

1.1 Julkisen hallinnon digitaalisen turvallisuuden riskienhallinta

Organisaatiot toteuttavat riskienhallintaa kukin omista lähtökohdistaan ja omaan toimintaansa keskittyen, kuten on riskienhallinnassa standardin mukaista. Erikseen tietyistä toimenpiteistä, joiden voidaan katsoa liittyvän riskiprosessiin, vastaavat toimivaltaiset viranomaiset. Riskienhallinnan tulee heijastaa organisaation (tai muun tarkasteltavan kohteen tai kokonaisuuden) toimintaa ja näkemystä itsestään sekä suhdettaan ympäröivään toimintaympäristöön. Nykyaikainen riskienhallinta ja modernien, etenkin digiriskien, hahmottaminen vaativat laaja-alaisempaa tarkastelua myös yli omien siilojen rajojen, esimerkiksi asiakkaille ja sidosryhmille muodostuviin riskeihin.

1.1.1 Riskienhallintaprosessin toteuttaminen

Riskienhallintamallin erityinen tarkoitus on mahdollistaa poikkihallinnollisten ja laajojen jaettujen riskien tunnistaminen (tässä kontekstissa) hajautettuun rakennemalliin vertautuvasta julkishallinnosta, arviointi ja käsittelyyn ohjaus sekä hallintatoimien tehostaminen yhteiseksi hyväksi. Strategiseen riskikuvaan tunnistetaan useista kansallisista ja kansainvälisistä tietolähteistä sellaisia riskejä, jotka toteutuessaan aiheuttaisivat laajasti vakavia haittoja niin valtionhallintoon kuin muillekin julkisen hallinnon toimijoille, sijoittuen kuitenkin kontekstina kansallisen riskinarvion alapuolelle ja tarkastellen digiturvallisuuteen vaikuttavia asioita sitä laajemmin.

Julkisen hallinnon digitaalisen turvallisuuden strategisen riskienhallinnan malli (JHDTSRH-malli) koostuu kattavasta, systemaattisesta, toistettavasta ja kehittyvästä prosessista sekä siihen liittyvistä tehtävistä. Se näyttäytyy hieman erilaisena eri organisaatioille, riippuen niiden osallisuudesta oman riskienhallintansa ulkopuolisiin toimenpiteisiin, kuten hallintatoimien kehittämiseen. Useimmille prosessi toimii tiedon kerääjänä omaa riskienhallintaprosessia varten. Julkishallinnossa on tärkeää, että

[1] https://dvv.fi/documents/16079645/110183105/Julkisen+hallinnon+digitaalisen+turvallisuuden+strategi-nen+riskienhallinta+-+riskienhallintamallin+rakenne.pdf/

prosessissa on tuotu esiin hyvän hallintotavan vaatimuksena päätöksenteko, jolloin tietoon perustuva ja riskiperustainen päätöksenteko tehdään näkyväksi.

Kuva 1: Yksinkertaistettu esitys julkisen hallinnon toteuttamasta riskienhallinnan prosessista.

Raportoinnin sisältöä muotoa, valittuja lähteitä, analyysiä ja ulkoasua tullaan jatkossa kehittämään eteenpäin. Sekä mallissa kuvattuja laajempia rakenteita, että kyselyn sisältöä tulee arvioida kokonaisuutena, sillä vain toisen tarkastelu voi tuottaa vinoutuneen kuvan tavoitteista ja painotuksista. Raportissa nyt esitettyjen huomioiden ja poimintojen tukena on myös asiantuntijanäkemyksiä sekä ulkopuolista raportointia sisällön laadun vahvistamiseksi. Riskienhallintamallin mukaisen toiminnan maturiteetin kasvattaminen kaikilla prosessin osa-alueilla toivottavalle tasolle tulee viemään vuosia, mm. trendi- eli kehitysdatan keräämisen vuoksi. On nähtävissä, että tarve tiedolle ja sen keräämiselle tulee kasvamaan. Pelkän datan sijaan halutaan laadukkaampaa ja syvällisempää analyysiä, mihin tarvitaan eri kontekstien asiantuntijoiden osaamista, mitä pitää joukkoistaa, sillä haasteet ovat entistä monitahoisempia – mitä riskiväitteet kyselyssä osaltaan heijastavat. Riskitiedon käsittely ja siitä viestiminen vaativat riittävää resursointia ja ovat välttämättömiä nykyaikaisessa turvallisuusyhteistyössä. Tiedonkeruusta koettu haastavuus ilmaisee, että keräystavoissa ja -kanavissa on kehitettävää, suhteessa tarpeeseen, sillä nykyiset järjestelmät eivät ole riittävän automatisoituja, kyvykkäitä ja yhteensopivia prosessin merkittäväksi tehostamiseksi – asia, jota tulisi kehittää laajemmassa toiminnan ohjauksessa.

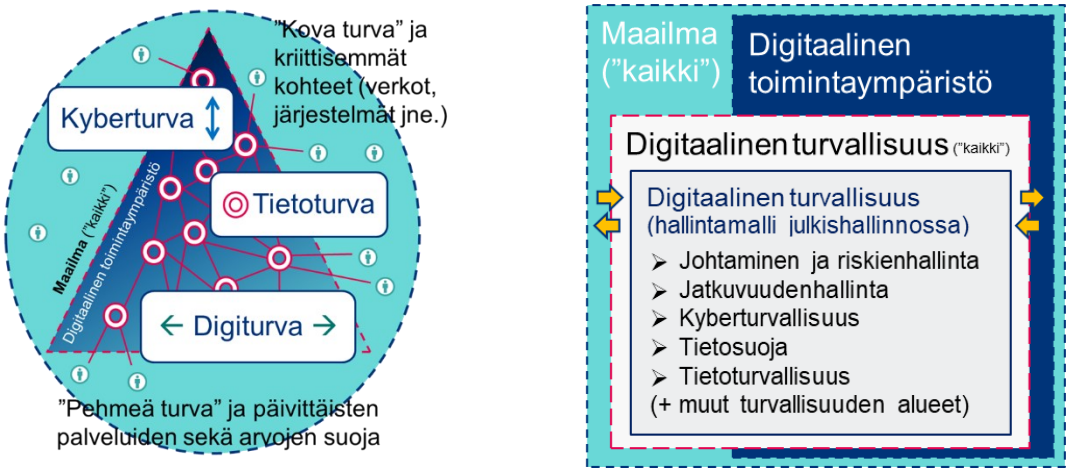
1.1.2 Huomautuksia tarkastelun joistain rajauksista

Julkisen hallinnon digitaalisen turvallisuuden strategisen riskienhallinnan mallissa on kuvattu tarkemmin tarkasteluun liittyviä rajauksia. Tämän raportin taustoittamiseksi avataan tässä niistä muutamaa. Keskeisten termien, kuten digitaalisen turvallisuuden, määrittelyä on tehty VAHTI-riskienhallintasanastossa2, jossa on luotu

[2] https://dvv.fi/documents/16079645/110183105/VAHTI-riskienhallintasanasto+digitaaliseen+toimintaymp%C3%A4rist%C3%B6%C3%B6n.pdf/6d71d86f-c7bc-6683-9b36-c55d16d4c1f0/VAHTI-riskienhallintasanasto+digitaaliseen+toimintaymp%C3%A4rist%C3%B6%C3%B6n.pdf

systemaattista kokonaisuutta käsitteille. Yleisesti ottaen digiturvasta keskusteltaessa käytössä on tunnistettavissa kaksi päädiskurssia:

- *Laajennus tai erotus kyberturvallisuudesta* (OECD 2015/2016, 2022)[3,4], tarkoittaen (pääosin) normaaliolojen turvallisuusulottuvuutta, joka huomioi mm. talouden, arvot, sosiaaliset ulottuvuudet sekä mahdollisuudet ja mahdollistamisen
  - Vastaten, miten kyberturvallisuus on rajattu esimerkiksi: *Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa* (Sisäministeriö, VN 2023:31)[5]
- ”Kokoava yleistermi” (VN periaatepäätös VM/2022/47)[6], missä digiturva ei ole itse mitään, vaan se toimii *yhdistävänä ja kattavana hallinnon viitekehyksenä* (tietynlaisena ”minimi” kokoonpanona) turvallisuuden eri osa-alueille.
  - ”Useita turvallisuuksia”: johtaminen ja riskienhallinta, jatkuvuudenhallinta, kyberturvallisuus, tietosuoja, tietoturvallisuus (sekä mahdolliset organisaation toimintaan ja tarpeisiin liittyvät muut turvallisuuden toteutusalueet).
  - Vastaava analogia ei-digitaalisesta turvallisuudesta ovat ”turvallisuuden” sisältämät eri osa-alueet, kuten esimerkiksi logistiikan turvallisuus, toimitilaturvallisuus, henkilöstöturvallisuus, työturvallisuus tai ympäristöturvallisuus.



Kuva 2a ja 2b: Tarkastelu riskeistä keskittyy tietylle alueelle, jonka rajaukseen vaikuttavat eri näkemykset. Vasen ympyrä pyrkii havainnollistamaan suurempien pääkäsitteiden välistä diskurssia ja oikeanpuoleinen digiturvallisuuden sekä digiturvallisuuden hallintamallin sijoittumista.

Tarkastelu JHDTSRH-mallissa on tarkoitus kohdistaa noin 2-5 vuoden aikajänteelle, jotta julkisessa hallinnossa kyetään valmistelemaan ja tuottamaan osana normaaleja prosesseja tarvittuja hallintatoimia. Tässä raportissa käytetyssä kyselyssä on pyydetty tekemään arviot noin 1-3 vuoden aikajänteelle, jolloin tämänhetkiset tilanteet ovat todennäköisesti jo muuttuneet ja seuraavat muutokset voivat olla tulollaan.

Käytännön esimerkkeinä mallin eri kohdistusten tunnistetuista rajoitteista tuotakoon esiin muutama esimerkki. Vaikka yksittäisen tekoälytekniikan tarkastelu on nykyisin liian lähellä ennakoivalle arvioinnille, on laajempi tekoälykehitys hyvinkin merkittävää.

[3] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75412/OECD_julkaisu_NETTI.pdf?sequence=1&isAllowed=y
[4] https://www.oecd.org/publications/oecd-policy-framework-on-digital-security-a69df866-en.htm
[5] http://urn.fi/URN:ISBN:978-952-383-542-9
[6] https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f806928f5

Toiseen suuntaan katsottuna, kvanttiteknologian (sen huomioimisen puutteiden) riskit saatetaan tunnistaa vasta liian myöhään, sillä ”kvanttiaikakauden” oletetaan edelleen alkavan varteenotettavasti 2030-luvulla, mikä ylittää tämän riskienhallintatarkastelun aikaikkunan – mikä on valitettavaa, sillä aiheeseen liittyvä ”aikasiirtymä” (tallennetun salatun tiedon murtaminen myöhemmin) on jo tietyssä mielessä realisoitunut riski (vaikutukset havaitaan viiveellä), jota ei pystytä käsittelemään reaktiivisesti, vasta kun se tulee eteen. Kyberturvallisuutta – ja siihen sisältyviä kansallisen turvallisuuden alueelle kohdistuvia riskejä – on tarkoituksellisesti suhteutettu vain kahdella laajemmalla riskiväitteellä, jotta yhteys näihin säilyy, sekä jotta vältetään tässä yhteydessä kohtuuttomasta turvallisuustiedosta aiheutuvat riskit ja haasteet tiedon jakamiselle.

1.2 Käytetyt kyselyt ja niiden taustatiedot

Digiturvan riskienhallintatietoa keräävän palvelun riskinäkemyskyselyn on osa julkisen hallinnon digitaalisen turvallisuuden strategisten riskien hallintaa, jota on pilotoitu 2020-2022 ja siitä on siksi osittaista vertailutietoa. Vastaukset kerättiin välillä maaliskuu-huhtikuu, sillä pyydetyn vastausajan (8.3.-4.4.2022) ulkopuolelta pystyttiin sisällyttämään jälkivastaajia. 17 vastaajaa vähintäänkin loi käyttäjäprofiilin Digiturvallisuuden riskienhallintatiedon palveluun, muttei tallettanut vastauksiaan.

Kutsu riskinäkemyskyselyyn lähetettiin 670 julkisen hallinnon organisaatioon. Kyselyyn vastanneita oli 105 organisaatioita, joista 102:n vastauksia käytettiin tilastoinnissa (N=102). Tilastoinnissa käytetään poikkeavien vastausten suodatusta (Tukey's fences -kaava) pienten vertailuryhmien tulosten vinoutumisen ehkäisemiseksi. Koko kyselyn osalta, jossa käytössä oli julkisen hallinnon riskienarvioinnin asteikko (1-4), annetut tulokset pääsääntöisesti keskittyivät - odotetusti - arvon 2 tienoille. Riskiluku on todennäköisyyden (1-4) ja vaikutusten keskiarvon (1-4) tulo. Vastausten määrä tuo esiin eroja sekä yksittäisten riskiväittämien että käytettyjen luokittelumallien sisällä. Vastanneiden organisaatioiden määrää voidaan pitää riittävänä suuntaa-antavan luotettavuuden saavuttamiseksi kaikki sisältävissä sekä laajoissa ryhmittelyissä. Vastaajista 51 organisaatiota eli 50%, oli kuntia ja kaupunkeja, edustaen noin 16,5% koko kuntakentästä (2023 oli 309 kuntaa). Valtionhallinnosta vastaajia oli 35 organisaatiota, mikä kattaa yksilöllisen y-tunnuksen omaavat kirjanpitoyksiköistä noin 55%, joita oli 64 vuonna 2023 (näiden ”sisällä” 104 tulosohjattua virastoa, joiden alla 184 työnantajavirastoa). Kokonaistuloksissa kuntien näkemykset siis hieman korostuvat, vaikka valtio on suhteessa laajemmin edustettuna pienyksiköistä ministeriöihin.

Riskien tarkastelu koostuu julkisen hallinnon organisaatioiden asiantuntijoille tehdystä 100 riskiväitteen kyselystä, mikä on laajentunut aiemmista 36 ja 40 riskistä. Määrä ja sisältö ovat kompromissi halutun kattavuuden ja käytännöllisyyden suhteen. Nämä on rajattu digitaalisen turvallisuuden tulokulmaan (erotuksena mm. kyberturvallisuuden laajempaan kansalliseen turvallisuuteen liittyvästä painotuksesta) ja muodostamisessa on huomioitu tietotarpeiden lisäksi turvallisuusmerkitykset ja jatkohyödyntäminen (jaettavuus). Tarkemmalle ja laajemmalle tiedonkeräykselle on kasvava tarve, mutta toistaiseksi organisaatiot eivät kykene automaattisesti tuottamaan kontekstisidonnaista harkintaa sisältävää laadukasta tietoa tai keräämään sitä järjestelmistä. Tämän takia tarvitaan asiantuntijoiden osallistumista. Kokonaisvaltaista julkisen hallinnon riskienhallintaa varten, minkä on tarkoitus hyödyttää kaikkia organisaatioita, on tärkeää, että organisaatioissa on kohdennettu riittävästi resursseja myös uhka- ja riskitiedoista viestimiseen ja asiantuntijuuden jakoon kaikissa verkostoissa. Digitaalisen

turvallisuuden eri osa-alueiden (ja siten myös riskienhallinnan) tiedon keräyksen automatisointi ja tehostaminen ovat osa kyselyssä luodattuja hallinnollisia, yhteistoimintaan liittyviä sekä osin kompleksisuuden riskiaiheita.

Avoimissa vastauksissa tuotiin esiin muutamia riskejä, jotka eivät kuitenkaan sisälly kyselyn rajaukseen, sekä yksi mahdollisesti täydennettävä riski, liittyen roolitusten ja vastuiden selkeyteen. Palautetta varten käytössä oli erillinen lomake, johon saatiin kymmenkunta vastausta. Sisällön rakennetta pidettiin kokonaisuutena pääosin loogisena. Käytettävyys, kattavuus ja vertailtavuus jakoivat mielipiteitä. Avoimissa palautteissa oli huomioita erityisesti laajuudesta suhteessa organisaation asiantuntijan tai asiantuntijoiden resursseihin (huomioiden, että vastaajaorganisaatiot ovat hyvin eri kokoisia) sekä havaittuihin puutteisiin. Palautteet pyritään ottamaan huomioon jatkokehityksessä, siten kun palvelulle asetetut tavoitteet ja käytettävissä olevat järjestelmät ne sallivat.

Riskitietoa täydentävä tieto riskienhallinnan tilasta julkisen hallinnon organisaatioissa on peräisin digiturvallisuuden kokonaiskuvakyselystä organisaatioille. Kyselyssä luodataan laajasti digitaalisen turvallisuuden eri osa-alueille kohdistuvien toimien toteuttamista. Siinä vastauksia on otettu vastaan tammi-maaliskuussa 2023. Vastaajia (N) tässä kyselyssä oli 195 organisaatiosta tarkasteluhetkellä. Vastaajista 104organisaatiota, noin 53%, oli kuntia ja kaupunkeja, edustaen noin 34% koko kuntakentästä (309 vuonna 2022). Valtionhallinnosta vastaajia oli 37 organisaatiota.

DTYT / Reivo Juho (DVV)

29.5.2023

2 Yleisnäkemykset riskien kehityksestä

Koko kyselyn osalta kaikkien erilaisten riskien riskilukujen keskiarvot eivät ole erityisen hyvä indikaattori riskitasosta sinänsä, mutta niiden muutosten voidaan katsoa heijastelevan yleistä tilannetta, näkemystä siitä, miten niiden odotetaan kehittyvän. Tätä hieman selkeämpinä indikaattoreina voidaan pitää vaikutusten ja todennäköisyyksien arvoja. Johtuen muuttuneesta kyselyn laajuudesta ja sisällöstä, kehitystrendejä on käsitelty vain rajatusti tämän vuotisessa katsauksessa.

Kahden aiemman kyselyn (syksy 2021 - syksy 2022) välisessä vertailussa merkittävimpänä pidettävä turvallisuusympäristöä laajasti koskettaneen muutoksen (Venäjän hyökkäys Ukrainaan ja siihen liittynyt kyberaktiviteetti) voidaan olettaa heijastuneen myös digitaalisen turvallisuuden näkymiin, vaikka tulokset heijastelivat luottamusta digiturvan tilanteeseen Suomessa. Myös tämänkertaisessa vertailussa (syksy 2022 – kevät 2023) merkittävin, myös digitaaliseen toimintaympäristöön ja digiturvaan vaikuttava yksittäinen tapahtuma, on kansainväliseen turvallisuuteen liittyvä (NATO-ratifiointi), jolla voisi mahdollisesti olla vaikutus tulevaisuuden näkymiin. Näiden, puhtaammin kyberturvallisuuteen kuuluvien tapahtumien, saaman huomion ei kuitenkaan tulisi peittää alleen muita lukuisia teknologian, talouden ja sääntelyn kehityssuuntia, joilla on merkitystä digitaalisen turvallisuuden kehitykselle.

Riskiluvun keskiarvo koko kyselylle oli 3,78. Tarkasteltaessa vain aiemmassa kyselyssä tarkasteltuja riskejä (40 riskiväitettä), näiden osalta riskiluvun keskiarvo oli noin 3,98 laskien aikaisemmasta (2022: 4,23) Riskien sekä niihin kohdistuvien hallintatoimien nähdään yleisesti kehittyvän suotuisaan suuntaan. Näin yleisen tunnusluvun kohdalla on kuitenkin syytä huomioida sen sisältämä usea riski ja osin vaihtunut vastaajakunta. Kyselyiden välillä on 54 samaa vastaajaorganisaatiota, jakautuen 26 samaa kuntaa ja 20 samaa valtion organisaatiota.

Julkisen hallinnon digitaalisen turvallisuuden riskien todennäköisyyden keskiarvo oli kaikkien (100 riskiväitettä) osalta 1,87. Aiemman suppeamman kyselyn riskien (40 riskiväitettä) osalta kokonaisriskiluku oli noin 1,88 (2022: 1,94). Muutos on pieni, mutta indikoi yleistä luottamusta digitaalisen toimintaympäristön vakauteen Suomessa. Tämä on myös linjassa esimerkiksi SUPO:n esittämän kyberturvallisuuden arvion kanssa[7]. Kokonaisuuden sisällä on kuitenkin huomattavissa toisenlainen nykähdys vastakkaiseen suuntaan, liittyen jatkuvuudenhallintaan sekä haitalliseen teknologiseen kehitykseen, joihin liittyvien riskien todennäköisyyksien nähtiin yleisesti hienokseltaan kasvavan.

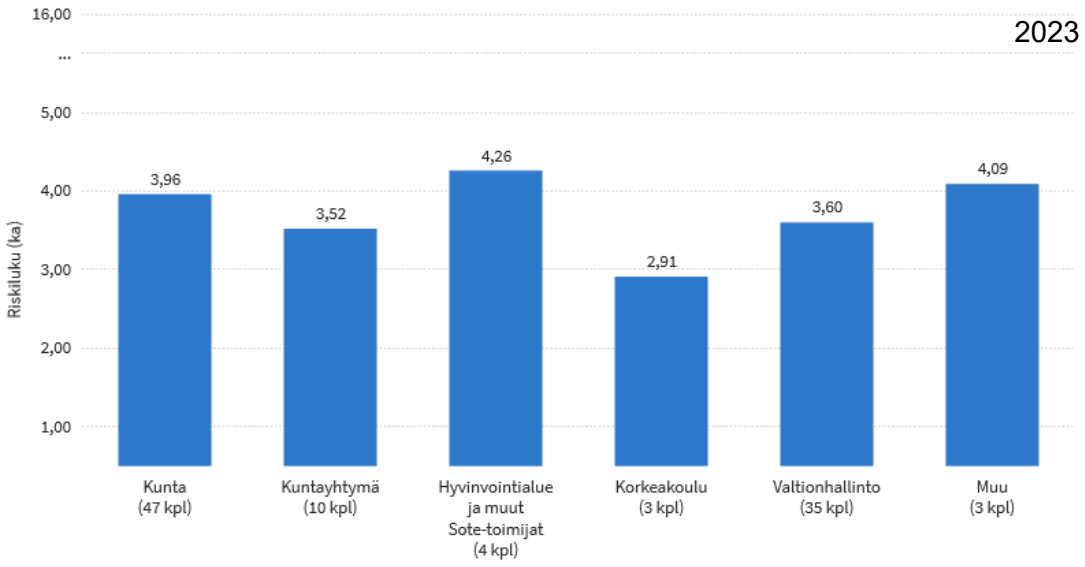
Vaikutuksen keskiarvo oli kaikkien (100 riskiväitettä) osalta 1,94. Tämän sisällä, aiemman suppeamman kyselyn riskien (40 riskiväitettä) osalta se oli 2,05 tänä vuonna (2022: 2,10). Näkemys tulevasta kehityksestä vaikutusten osalta on siis hieman lieventynyt aiempien kyselyiden välisestä noususta. Vaikutuksen keskiarvon kehityksessä on kuitenkin huomattavissa merkittäviä eroja eri vastaajaryhmien välillä, mitä tarkastellaan erikseen.

[7] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-uhkataso-pysynyt-kohonneena-kohdistettujen-hyokkaysten-maara

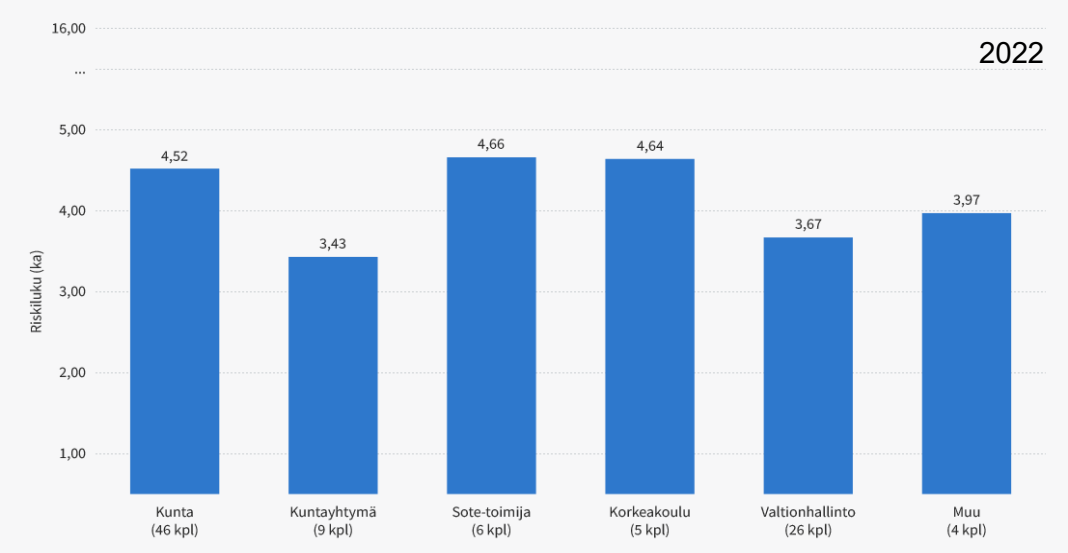
2.1 Vastaajaryhmien erot ovat korostuvat edelleen, mutta normalisoituvat

Aiemmassa raportissa nostettiin esiin, miten eri vastaajaryhmien erot korostuivat selkeästi. Tuoreemmassa vertailussa keskeisin havainto on, miten nämä erot ovat joiltain osin tasoittumassa. Lievät muutokset sekä tasoittuminen tilastointiin liittyvistä syistä on odotettua ja toivottua. Yhteinen jaettu näkemys riskeistä ja niiden arvotusten painotuksista eri muuttujien osalta muodostuu jaetusta vertailutiedosta sekä muusta riskeihin liittyvästä viestinnästä ja keskustelusta. Vaikka jokainen tekee arvioinnin perustuen oman organisaationsa lähtökohtiin, arvioinnin kalibrointiin vaikuttaa käsitys viiteryhmien arvioinnista. Tämän positiivinen puoli on, että jaettu riskikäsitys tukee realistisempaa ja tehokkaampaa yhteistoimintaa yleisesti, mutta myös rajatumpien kohderyhmien sisällä.

Eri organisaatiotyyppien mukaisessa ryhmittelyssä on nähtävissä kaksi kehityssuuntaa edelliseen kyselyyn nähden, joiden tarkkaa merkitystä tai kestoa ei vielä voida kunnolla arvioida. Ensimmäinen kokonaisuus liittyy mahdollisesti hyvinvointialueiden (HVA) perustamisestä johtuviin muutoksiin ja niiden seurausten selkeytymiseen muutoksen jälkeen. Kuntien ja hyvinvointialueiden riskinäkymät ovat selkeästi parantuneet syksyn 2022 vastauksista, verrattuna valtionhallintoon, mikä on pysynyt stabiilina. Toinen liittyy vaikutusten kehityksen vastakkaisiin näkemyksiin kuntien ja valtion toimijoiden välillä, mikä voi liittyä osin edellä mainittuun HVA-muutokseen, mutta myös toisistaan poikkeavien riskikäsitysten lähentymiseen, johon on kiinnitetty huomiota aiemmissa raportoinneissa. Näitä tulkintoja, vaikkakin selkeitä kerätyn datan perusteella, tulisi pitää lähinnä heikkoina signaaleina tässä vaiheessa – vasta tulevien vuosien uusintakyselyt voivat vahvistaa tulkinnat, kun laajennettua kyselyä toistetaan.

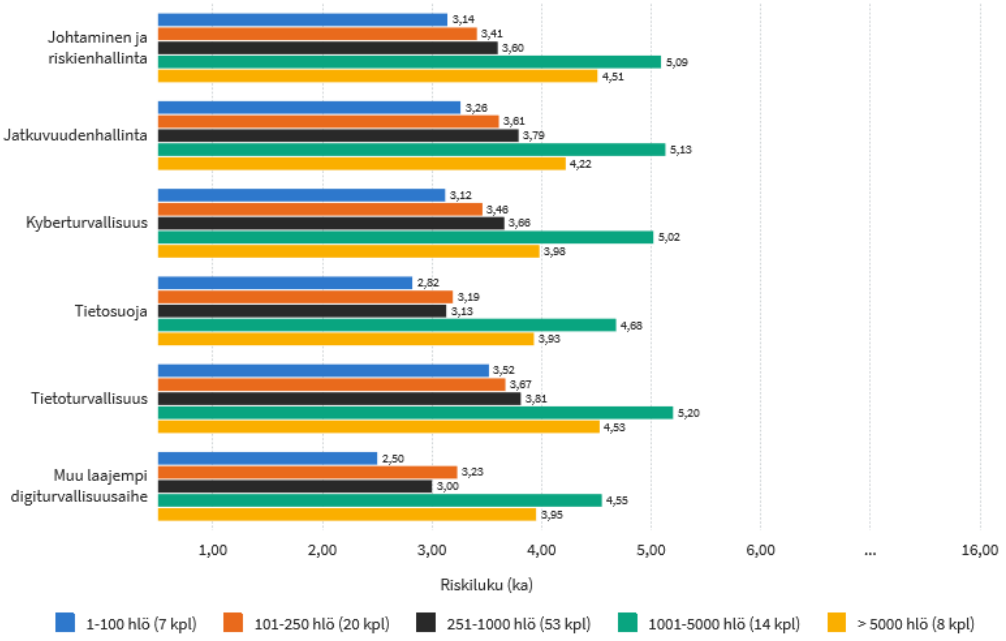


Kuva 3a: Vuoden 2023 riskilukujen keskiarvot vastaajaorganisaatioiden hallinnon alueiden mukaisesti. Suurempi luku viittaa korkeampaan yleistettyyn riskinäkymään.



Kuva 3b: Vuoden 2022 riskilukujen keskiarvot vastaajaorganisaatioiden hallinnon alueiden mukaisesti. Suurempi luku viittaa korkeampaan yleistettyyn riskinäkymään.

Eri kokoluokkien vastaajien välillä on nähtävissä selkeät erot riskilukujen perusteella. Pienten ja keskisuurten vastaajien näkemykset riskeihin olivat selvästi alhaisemmat kuin suurten (1001-5000hlö) ja hyvin suurten (>5000hlö) organisaatioiden. Suurten toimijoiden riskien suuruuteen voi ilmiönä liittyä merkittävä uhkien, suojattavien asioiden sekä suojautumisjärjestelyiden hallinnan kompleksisuuden kasvu skaalautuessa. Aiemmat vertailut ovat antaneet hyvin samansuuntaisen näkymän, joka nyt korostuu enemmän. Erityisen huomattavaa nyt on suurten (1001-5000hlö) yksiköiden korostuminen. Vastaajasegmenttien pienuus kuitenkin rajoittaa vertailun luotettavuutta.



Kuva 4: Digiturvan osa-alueiden riskilukujen keskiarvot vastaajaorganisaatioiden kokoluokan mukaisesti.

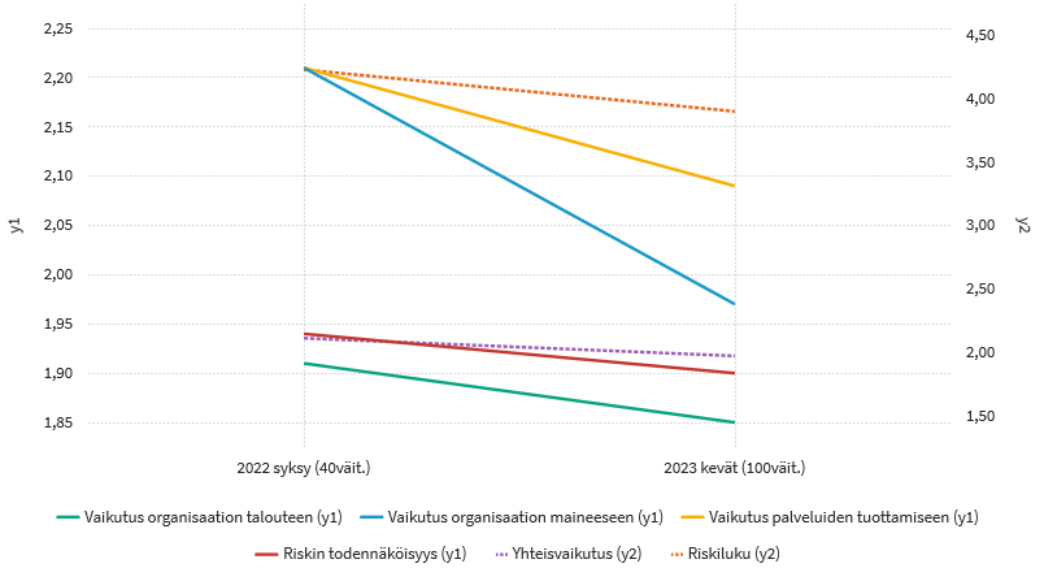
DTYT / Reivo Juho (DVV)

29.5.2023

3 Digiturvan riskit ovat pääosin lievässä laskusuunnassa

Riskien vaikutusta tarkastellaan jakamalla se kolmeen osaan: vaikutus talouteen, vaikutus maineeseen sekä vaikutus palveluiden tuottamiseen [eli toimintakykyyn]. Edellisessä raportissa kiinnitettiin huomiota taloudellisten vaikutusten korostumiseen aiemmasta vuodesta: 1,76 (2021) nousi 1,88:aan (2022) suppeammassa kyselyssä. Maineen ja palveluiden tuottamisen osalta muutos oli maltillisempi.

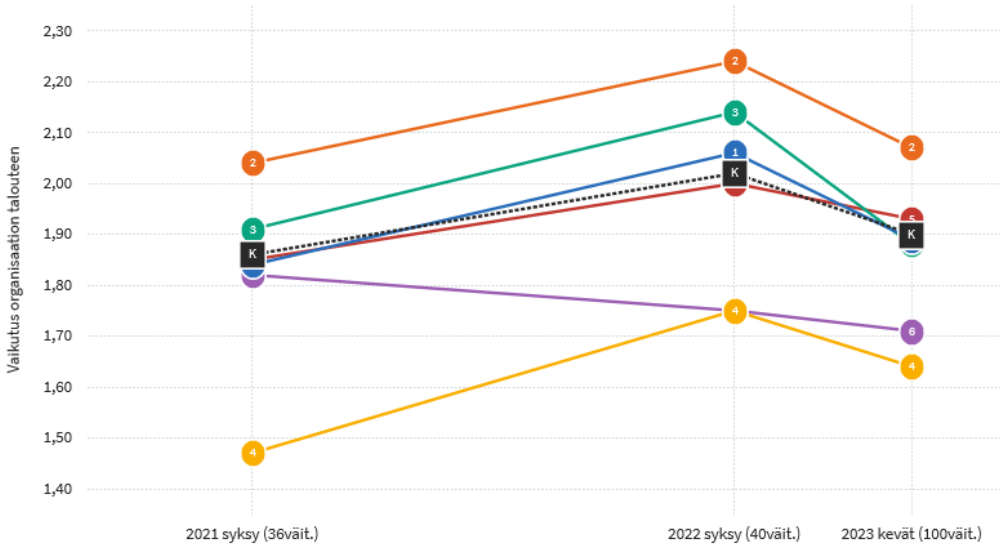
Kaikki keskeiset indikaattorit olivat uudessa laajennetussa kyselyssä laskusuunnassa, mutta tätä ei voida pitää uskottavana tuloksena, huomioiden aiemman kyselyn erilaisuuden. Taloudellisten vaikutusten keskiarvo oli 1,83. Vaikutus organisaation maineeseen oli 1,97. Myös palveluiden tuotantokyky (ja siten organisaation kyky toimia) laski, ollen nyt 2,09. Näiden lisäksi myös riskien todennäköisyyksien keskiarvo oli lievästi laskenut, ollen nyt 1,90. Yhteisvaikutuksesta sekä todennäköisyydestä johtuen kyselyn kokonaisriskiluku oli 3,90.



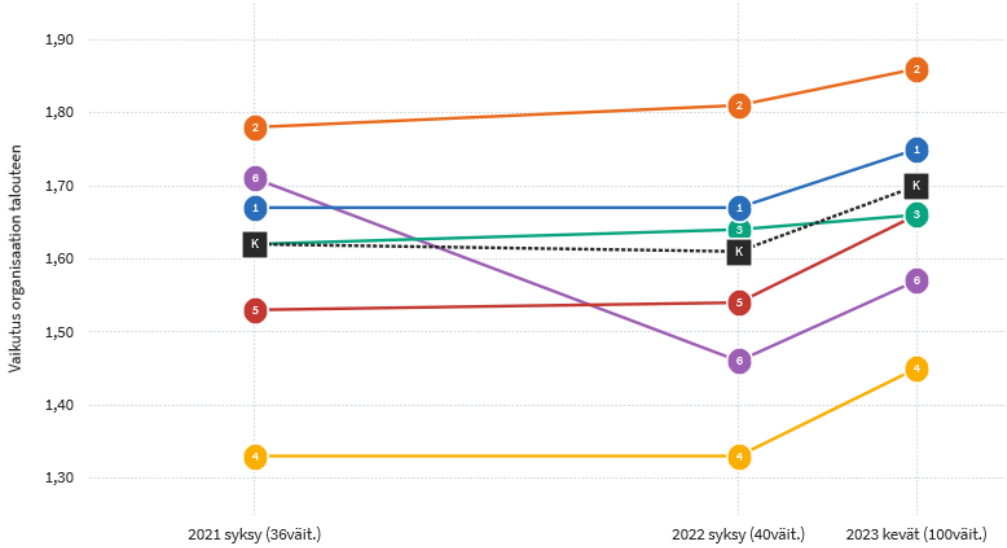
Kuva 5: Riskien keskeisten tunnuslukujen muutos edelliseen kyselyyn verrattuna. Kyselyiden hyvin erilaisen kattavuuden johdosta muutostrendejä ei voida uskottavasti tulkita.

Edellisessä raportissa esitetty päätelmä, että digitaalisen turvallisuuden yhteys julkisen hallinnon organisaatioiden talouteen nähdään saavan enemmän merkitystä tulevaisuudessa, on edelleen pätevä, huomioiden sitä tukevat näkemykset yleisestä taloudellisesta kehityksestä sekä digitaalisen toimintaympäristön uhkien määrän ja vakavuuden kasvu. Vaikka uusi data yhteiskeskiarvoissa on laskusuuntaista, pääosin useimmissa luokitteluissa, tarkemmassa tarkastelussa on nähtävissä vastakkaista kehitystä. Siinä, missä kunnat ja kaupungit näkevät tulevaisuudessa digitaalisen turvallisuuden taloudellisten vaikutusten laskevan, valtionhallinnossa niiden nähdään edelleen nousevan. Näiden kahden vastaajasegmentin näkemykset ovat kuitenkin vielä hyvin eri tasoilla, vaikka ne näin lähentyvätkin. Lähentymistä selittää osin HVA-muutoksen vaikutusten selkeytyminen kuntien osalta, mutta laajemmassa tarkastelussa myös mahdollisesti riskikäsitysten lievä yhteneminen. Tarkastelun kannalta

merkityksellistä tulevaisuudessa lienee, miten valtion talouden linjaukset[8] ja digitaalisuuden painopisteet asettuvat. Muutoksia on jatkossa mahdollisuus seurata.



Kuva 6a: Kuntien vastaajien (N=47) näkemyksen kehitys digiturvan riskien taloudellisten vaikutusten osalta. Sininen 1: johtaminen ja riskienhallinta; oranssi 2: jatkuvuudenhallinta; vihreä 3: kyberturvallisuus; keltainen 4: tietosuoja; punainen 5: tietoturvallisuus; violetti 6: muu laajempi digiturvallisuusaihe.



Kuva 6b: Valtionhallinnon vastaajien (N=35) näkemyksen kehitys digiturvan riskien taloudellisten vaikutusten osalta. Sininen 1: johtaminen ja riskienhallinta; oranssi 2: jatkuvuudenhallinta; vihreä 3: kyberturvallisuus; keltainen 4: tietosuoja; punainen 5: tietoturvallisuus; violetti 6: muu laajempi digiturvallisuusaihe.

[8] https://vm.fi/talouden-ennusteet

Yleisten talousennusteiden mukaan kustannukset tulevat kasvamaan eri tavoin[9] ja indikaattorien mukaan tämä tulee kestämään seuraavat kaksi tai kolme vuotta. Vakuutusten merkitys julkishallinnossa on vähäinen, mutta ne voivat tulla esiin välillisesti digiturvallisuuteenkin liittyen, esimerkiksi palveluntuottajien kautta. Vakuuttamiseen nojaava riskin siirto esimerkiksi suurista vahingoista tai toiminnan keskeytyksistä voi kohdata ongelmia, sillä markkinoista johtuen tarvittavaa jälleenvakuutuspääomaa ei tule olemaan käytettävissä vastaavia määriä, kuin aiemmin. Tämä voi sekä nostaa vakuutuskuluja tai tehdä jopa suurista vakuuttamisista mahdotonta. Tiukentunutta rahoitusriskiä pienentääkseen voi eteen tulla vaatimuksia digiriskeihin liittyen, että näihin liittyvät hallintatoimet ja kontrollit on asianmukaisesti hoidettu, ja että tämä pystytään osoittamaan esimerkiksi standardinmukaisuudella. Tämä voi aiheuttaa ylimääräistä rasitusta, mutta laajemmassa kuvassa lisävaatimuksia voidaan pitää myös positiivisena sivuvaikutuksena digiturvallisuuden kehittämisessä.

Erityinen kustannusten nousuun vaikuttava ilmiö kryptaamishyökkäyksissä on niissä havaittu pyrkimys ehkäistä palautumistoimia ja käytännössä tuhota järjestelmiä[10]. Tämän tyyppisten hyökkäysten määrän voidaan myös odottaa kasvavan, mikä lisää todennäköisyyttä onnistuneiden hyökkäysten määrästä, lisäten kokonaiskustannuksia julkiselle hallinnolle. Kyselystä on nähtävissä tässä oleellisiin palauttamiseen ja varmuuskopiointiin liittyen, että sekä infran että tiedon osalta nämä ovat taloudellisilta vaikutuksiltaan merkittävimpiä riskejä organisaatioille. Julkisen hallinnon kokonaiskuvassa muutamat muut riskit voivat voisivat muodostua näitä kalliimmiksi, mikäli ne monistuvat ja leviävät vaikuttamaan laajemmin.

3.1 Osa-aluekohtaiset näkemykset

Tarkastelun vastausten analysoinnissa käytettiin erilaisia luokitteluita, joiden sisällä vastaukset toimivat indikaattoreina eri otsikoinneille. Toisiinsa suhteutetut luokittelujen otsikot auttavat yksin ja erikseen tunnistamaan laajempia strategisia aiheita, joille mahdollisesti tulisi suunnata erityistä huomiota. Tämä on merkityksellistä, sillä hallintatoimet harvoin ovat täysin symmetrisiä koettuihin uhkiin nähden ja samalle alueelle kohdistuviin haasteisiin voidaan tehokkaammin kohdistaa kattavia toimenpiteitä. Käytännön hallintatoimien toteuttamiseksi nämä strategisen tason näkemykset voidaan muuttaa esimerkiksi ISO27001 tai NISC CSF -mallien osa-alueiksi ja kontrolleiksi.

Käytetyt luokittelut ja niiden ryhmittelevät otsikoinnit olivat:

- Organisation for Economic Co-operation and Development eli OECD (*Kansallinen ja kansainvälinen turvallisuus, Lainvalvonta, Taloudellinen ja yhteiskunnallinen hyvinvointi*)
- World Economic Forum eli WEF (*Haitallinen teknologinen kehitys, Digitaalisen infrastruktuurin vakava häiriötilanne, Digitaalisen turvallisuuden laiminlyönti, Digitaalisten resurssien keskittyminen, Digitaalisen turvallisuuden ohjauksen epäonnistuminen, Digitaalisen toimintaympäristön epätasa-arvo, Informaatioturvallisuus [uutena 2023, Sosiaalisen alaluokka Misinformation and disinformation]*)
- Digitaalisen turvallisuuden hallintamalli[11] (*Johtaminen ja riskienhallinta, Jatkuvuudenhallinta, Kyberturvallisuus, Tietosuoja, Tietoturvallisuus, Muu laajempi digiturvallisuusaihe*)

[9] https://www.enisa.europa.eu/news/cybersecurity-investments-in-the-eu-is-the-money-enough-to-meet-the-new-cybersecurity-standards
[10] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv
[11] https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f806928f5

- Aihealueiden mukainen jaottelu, perustuen asiantuntijanäkemykseen merkityksellisiksi katsottavista digiturvallisuuteen vaikuttavista osa-alueista, teknologioista, toimintarakenteista sekä kiinnostuksenkohteista, joita riskiväitteistä on tunnistettavissa. Samoja indikaattoreita voi sisältyä useampaan aihealueeseen (*Hallinnollinen turvallisuus, Riskienhallinta ja ennakointi, Säädäntö ja ohjeet, Kaupalliset toimijat, Hankinta, Talous ja resurssit, Yhteistoiminta, Vakavat uhat, Informaatioturvallisuus, Järjestelmien toimintakyky, Palvelut ja toiminta, Tekoäly ja automaatio, Pilvipalvelut, Kompleksisuus, Osaaminen ja kulttuuri, Toiminnan kehittäminen*).

Tarkasteltaessa trendejä ja muutoksia edellisvuoteen kussakin luokittelussa, ja huomioiden myös vaikutusten osa-alueet, voidaan havaita muutamia yksittäisiä poikkeamia. Merkittävää näissä muutoksissa ovat toisistaan erottuvat ja eroavasti käyttäytyvät luokitteluiden otsikkoalueet. Niiden tulkinnassa on kuitenkin huomioitava, etteivät vuosien 2021 ja 2022 kyselyt olleet täysin identtiset ja vuosien 2022 ja 2023 välillä muutos oli vielä merkittävämpi, kun luokkiin lisättiin uusia riskiaiheita. Tästä johtuen kehitystrendien seurantaa ei sisällytetä raporttiin erillisiä huomioita laajemmin.

3.1.1 Aiheluokissa todennäköisimpinä riskeinä kompleksisuus ja informaatioturvallisuus

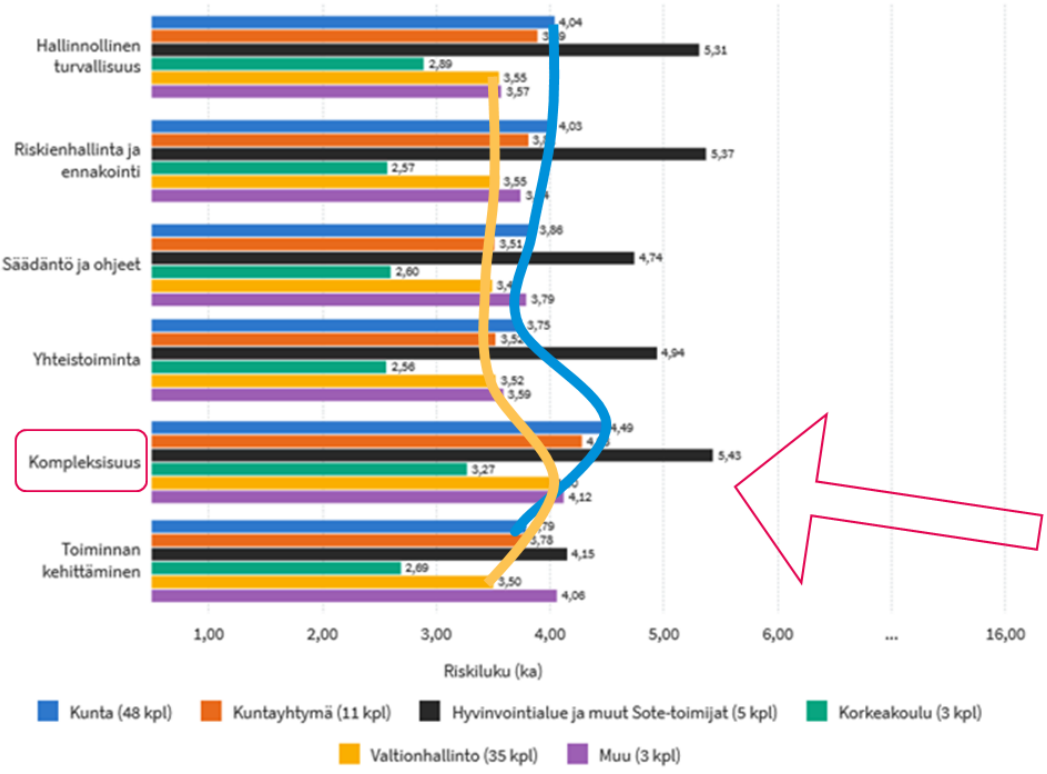
Vaikutuksen ja todennäköisyyden hajonta eri luokitteluilla näyttää pääosin vain pieniä eroja, mutta toisaalta myös miten muutama otsikko erottuu kustakin joukosta, vaikka käytetty vastausmetodiikka ja luokittelut tuottavat odotetusti kasaantumista vastauksissa. Erityisesti tässä tarkastelussa esiin tulevat aihealueet ovat luonteeltaan erilaisia ja eri syistä merkille pantavia (nähtävissä kuvassa 7):

- *Vakavat uhat* vaikuttavimpana (mutta epätodennäköisenä) riskiaiheena
- *Kompleksisuus* todennäköisimpänä riskiaiheena
- *Informaatioturvallisuus* toiseksi todennäköisimpänä riskiaiheena

Vakavat uhat liittyvät ymmärrettävästi kyberturvallisuuden alueelle painottuviin uhkiin ja niiden seurauksiin. Vaikka tältä alueelta ei (tarkoituksellisesti) tarkastella tarkkoja riskejä, voidaan yleisluonteisemmista riskiväitteistä tulkita yleistä käsitystä, luottamusta ja aiheen kehityssuuntaa. Vastausten perusteella aiheeseen liittyvien riskien mahdolliset vaikutukset tunnistetaan siinä määrin, että ne eroavat selvästi muista riskeistä. Niiden todennäköisyyttä pidetään kuitenkin tulevaisuudessakin selvästi pienempänä kuin useimpien muiden digiturvan riskien.

Kompleksisuus on todennäköisimpänä nähty riskiaihe. Se on laaja kokonaisuus, joka vaikuttaa kaikille alueille, myös turvallisuuskontekstin ulkopuolelle, ja yksinkertaistettuna ajatuksena kuvaa maailmamme vaikutusverkostojen hahmottamisen haasteellisuutta. Digitaalisessa turvallisuudessa se liittyy keskeisesti hallittavuuteen ja hahmottamiseen, millä on yhteys toiminnan tehokkuuteen – puhutaan sitten uhkien ja niiden vaikutusten tunnistamisesta, riskitiedon käsittelystä ja jakamisesta, tai hallintatoimien suunnittelusta ja toteuttamisesta. Se on kuitenkin erillinen käytännöllisemmistä hallinnasta ja johtamisesta. Sen merkittävin ero toiseen todennäköiseen uhkaan, informaatioturvallisuuteen, on sen hidas, pitkäaikainen ja abstrakti luonne riskinä. Se myös kohdistuu kaikkiin toimijoihin, riippumatta näiden toiminnasta tai varautumisesta. Se on osa modernia maailmaa, joten sitä ei voida poistaa riskinä, vaan sen määrää ja laatua on hallittava. Siihen ei voida kohdistaa käytännöllistä hallintatoimea, vaan sen käsittely tulisi huomioida osana jokaista hallintatoimea, tiedonkäsittelyä, järjestelmää, käytettävyyttä, ohjaavaa mallia ja aiheeseen liittyvää viestintää.

Informaatioturvallisuuden riskit (eritasoinen vaikuttaminen ja tältä suojaavat järjestelyt) sen sijaan, vaikka voivatkin olla yleisiä, sisältävät pääsääntöisesti kohdistusta mm. yleisön, ajan, paikan, toimijan ja tavoitteen muodossa. Siinä voidaan erottaa pitkän aikavälin vaikuttaminen, mutta digiturvan kontekstissa merkittävämpää on lyhyemmän aikavälin vaikuttaminen ja sen yhdistäminen muihin uhkiin. Huoltovarmuuskeskus on käynnistänyt informaatioturvallisuuden osaamiskeskuksesta pilotin[12]. Informaatiovaikuttaminen julkistenpalvelujen yhteydessä on toimenpiteenä seuraavan hallituskauden hanke-ehdotuksessa (VM). Hybridiosaamiskeskus on julkaissut mallin (DISARM)[13] vaikuttamistoimien yhdenmukaisen analyysin ja luokittelun tekemiseksi sekä yhdessä EU:n (JRC) kanssa laajemman hybridivaikuttamisen hallintarakenteen (CORE model)[14], mitkä tukevat ilmiön ymmärtämistä, tiedonjakoa ja hallintaa.



Kuva 7: Valikoitujen hallintaan liittyvien riskiaiheiden joukossa kompleksisuus nousee esiin sekä kuntien että valtionhallinnon vastaajien kohdalla, riskinäkemysten muuten ollessa hyvin yhtenevät. Myös muissa vastaajaryhmissä tämä korostuu, mutta näiden vastaajamäärät ovat selvästi pienemmät.

3.1.2 Resursointi merkittävä huoli, erityisesti asiantuntijoiden määrä organisaatioissa

Riskinäkemyskyselyssä ja digitaalisen turvallisuuden kokonaiskuvan kyselyssä on nähtävissä viitteitä taloudellisessa resursoinnin puutteisiin digiturvassa, nyt ja tulevaisuudessa. Riskinäkemyskyselyssä resursointiin liittyvät riskit ovat selvästi korkeammalla kuin

[12] https://www.huoltovarmuuskeskus.fi/a/huoltovarmuuskeskus-rakentaa-kykya-torjua-informaatiovaikuttamista
[13] https://www.hybridcoe.fi/wp-content/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf
[14] https://publications.jrc.ec.europa.eu/repository/handle/JRC129019

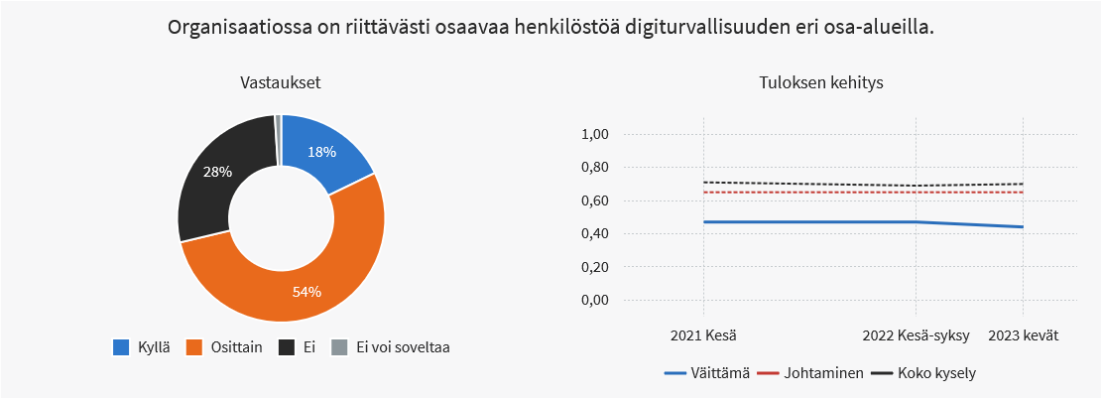
kyselyn riskien keskiarvo. Taloudellista panostusta merkittävämpänä puutteena ennakoidaan olevan palkattujen asiantuntijoiden määrä, mikä heijastuu kaikessa toiminnassa.

Väittämä	2021 syksy (36väit.)	2022 syksy (40väit.)	2023 kevät (100väit.)
K = Koko kysely	3,92	4,12	3,82
O = Talous ja resurssit	4,36	4,39	4,05
30. Tietovarantojen tietoturva vaarantuu merkittävästi, johtuen keskeisesti kiireestä ja resursointivajeesta.	4,66	4,57	4,98

Kuva 8: Riskinäkemyskyselyssä erityisesti asiantuntijoiden resursoinnin puutteet korostuvat riskinä. Kyseinen riski on kehittynyt voimakkaasti (noussut 4,98) muihin riskeihin nähden (keskiarvo laskenut 3,82).

Kuten edellisessäkin raportissa todettiin, kokonaiskuvakyselyssä puolet vastanneista piti budjetointia vaillinaisena joiltain osin ja enemmän kuin joka kymmenes selvästi riittämättömänä. Tämä on huolestuttavaa, sillä ennakkoon toteutetut riskienhallintatoimet ovat pitkässä juoksussa taloudellisempia ja ehkäisevät myös muita vaikutuksia. Luonnollisesti kyse on myös priorisoinneista sekä digiturvan, digitaalisen toiminnan, mutta myös organisaatioiden kokonaisbudjettien sisällä. Näiden välillä tulisikin tehdä riittävät keskinäiset vertailut osana riskienhallintaa, jotta kohdentaminen on perusteltua ja digiturvallisuuteen priorisoidaan riittävästi. Riskiväite ”*muut tarpeet priorisoituvat suhteettomasti digitaalista turvallisuutta tärkeämmiksi*”, sai kuitenkin vastauksissa korkean arvon (4,38), mikä tulisi ottaa esiin organisaatioiden taloussuunnittelussa.

Eri tavat tehostaa resurssien käyttöä, esimerkiksi yhteiskäytöllä tai -hankinnoissa, tulisi selvittää ja harkita. Julkisen hallinnon yhteisiin toimiin ei näkemysten perusteella panosteta riittävästi tuleviin tarpeisiin nähden, sillä sen nähdään olevan todennäköisin yhteistoiminnan aihealueen tarkasteltu riski. Tämän sivuvaikutuksena, ne yhteiset hallintatoimet, joihin on varaa, jäävät pistemäisiksi, mikä osaltaan voi heikentää hallittavuutta ja ruokkia kompleksisuuteen liittyviä riskejä, mikä puolestaan luo systeemistä heikkoutta.



Kuva 9: Digiturvallisuuden kokonaiskuvakyselyssä tilanne julkisessa hallinnossa henkilöstön osalta ei ole parantunut edelliseen kyselyyn verrattuna.