DIGI- JA VÄESTÖTIETO-VIRASTO

Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta

Yleinen riskitilannekatsaus, syksy 2022

23.1.2023

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

DTYT / Reivo Juho (DVV)

23.1.2023

Sisällysluettelo

DTYT / Reivo Juho (DVV)

23.1.2023

1 JHDTSRH – ennakoiva riskitilannekatsaus, syksy 2022

Julkisen hallinnon digitaalisen turvallisuuden strateginen riskienhallinta (JHDTSRH) tarkastelee sekä riskejä että sen myötä myös riskienhallinnan tilaa. Tarkastelu perustuu tätä varten kuvattuun malliin, jossa on eritelty eri toimijoiden ja tarkastelutasojen prosesseja, minkä avulla pyritään kehittyvään riskienhallintaan ja laadukkaaseen tuotettuun tietoon, kun toiminnan maturiteettitaso kehittyy eri osa-alueilla. Keskeinen tuotettava tietotuote on julkisen hallinnon laajuisen strategisen tason ennakoiva näkymä digiturvallisuuden riskeihin ja riskienhallintaan. Tämä dokumentti on ote siitä. Laajempi versio on ladattavissa kyselyyn osallistuville organisaatioille Digiturvan riskitieto -alustalla.

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). Mahdollinen tarkempi luokittelu on merkittynä kansilehdellä.

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.

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

DTYT / Reivo Juho (DVV)

23.1.2023

Kuva 1: Yksinkertaistettu esitys julkisen hallinnon toteuttamasta riskienhallinnan prosessista.

Riskienhallintamallin mukaisen toiminnan maturiteetin kasvattaminen kaikilla prosessin osa-alueilla toivottavalle tasolle tulee viemään vuosia, mm. trendi- eli kehitysdatan keräämisen vuoksi. Raportissa nyt esitettyjen huomioiden ja poimintojen tukena on myös asiantuntijanäkemyksiä sekä ulkopuolista raportointia sisällön laadun vahvistamiseksi. Raportoinnin sisältöä muotoa, valittuja lähteitä ja ulkoasua tullaan jatkossa kehittämään eteenpäin.

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 mahdollisesti jo muuttuneet ja seuraavat muutokset voivat olla tulollaan.

1.2 Käytetyt kyselyt

Digiturvan riskienhallintatietoa keräävän palvelun riskinäkemyskyselyn on osa julkisen hallinnon digitaalisen turvallisuuden strategisten riskien hallintaa, jota on pilotoitu edeltävinä vuosina ja siitä on siksi osittaista vertailutietoa. Nyt sen tarkastelu koostuu julkisen hallinnon organisaatioiden asiantuntijoille tehdystä 40 riskiväitteen kyselystä.

Vastaukset kerättiin välillä toukokuu-marraskuu, sillä varsinaisen vastausajan (21.9.-11.10.2022) ulkopuolelta pystyttiin sisällyttämään ennakkoon vastanneiden testiorganisaatioiden vastauksia sekä erikseen sovittuja jälkivastaajia. Kymmeniä vastaajia aloitti vastaamisen luomalla vähintäänkin käyttäjäprofiilin Digiturvallisuuden riskienhallintatiedon palveluun, muttei lopulta tallettanut vastauksiaan.

Kutsu riskinäkemyskyselyyn lähetettiin 540 julkisen hallinnon organisaatioon. Kyselyyn vastanneita organisaatioita oli 97kpl, joista 96:n vastauksia käytettiin tilastoinnissa (N=96). 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.

Vastausten määrä kuitenkin tuo esiin eroja sekä yksittäisten riskiväittämien että käytettyjen luokittelumallien sisällä. Vastaajista 46kpl, noin 48%, oli kuntia ja kaupunkeja, edustaen noin 15% kuntakentästä (309kpl vuonna 2022).

Riskitietoa täydentävä tieto riskienhallinnan tilasta on digiturvallisuuden kokonaiskuvakyselystä organisaatioille. Se toteutettiin välillä 21.6.-24.8.2022. Kutsu kyselyyn lähetettiin 612 julkisen hallinnon organisaatioon. Vastaajia (N) tässä kyselyssä oli 116 organisaatiota. Kyselyssä tarkasteltiin laajasti digitaalisen turvallisuuden eri osa-alueille kohdistuvien toimien toteuttamista. Vastaajista 57kpl, noin 49%, oli kuntia ja kaupunkeja, edustaen noin 18% koko kuntakentästä (309kpl vuonna 2022).

1.3 Tiivistelmä riskinäkymän keskeisistä kohdista

Raportti käyttää lähteenään kahta kyselyä, joissa vastaajia on ollut noin sadasta julkisen hallinnon organisaatiosta. Riskejä (40kpl) on pyydetty tarkastelemaan 1-3 vuoden päähän tulevaisuuteen. Kyselyt on toistettu alku syksyinä 2021 ja 2022. Tuloksia voidaan pitää suuntaa antavina ja **raportointia tullaan kehittämään** edelleen.

Kokonaisuutena **riskien todennäköisyyksien ei nähdä merkittävästi kasvaneen** tarkasteluajankohtien välillä. Sama koskee myös suurimmiksi riskeiksi nähtyjä hyökkäyksiä viranomaisten digitaalisen turvallisuuden infraan ja palveluihin. Tämän katsotaan heijastelevan luottamusta kansalliseen osaamiseen ja varautumiseen.

Riskien vaikutusalueista **taloudellisten vaikutusten nähdään yleisesti kasvavan**. Erityisesti taloudelliset vaikutukset korostuvat häiriöistä palautumisen riskeihin liittyen, vaikka niiden todennäköisyys pysyy melko maltillisena. Huoli palautumisen epäonnistumisesta, niin laitteistojen kuin tietopääomankin suhteen, koskee sekä ennakkovarautumisen että jälkihoidon kustannuksia. Erityisesti **hyökkäyksen jälkihoidon kustannusten voidaan odottaa kasvava**, sillä pääosassa näistä on havaittu pyrkimys vahingoittaa varmuuskopioita, jolloin järjestelmien palautus ei onnistu suunnitellusti.

Todennäköisimpänä riskinä nähdään säädösten, määräysten ja ohjeiden hajanaisuus ja laatu. Tämä voi luoda heikkouksia ja välillisesti luoda tai pahentaa haavoittuvuuksia. Kokonaiskuvan ja ohjauksen hallinnan selkeyttämiseksi tehdään jo toimia, mutta tämän tiedon hallintaan on panostettava myös organisaatioissa, sillä niiden tulisi tuntea omaan toimintaansa vaikuttava sääntely ja ohjaus vastuiden kokonaiskuvan hahmottamiseksi.

Digiturvallisuuden **riskienhallinta on vielä heikkoa julkisessa hallinnossa verrattuna sen muihin osa-alueisiin**. Tilanne on lievästi parantunut, mutta vain noin neljännes organisaatioista tekee sitä säännöllisesti ja kattavasti, miltei viidennes ei ollenkaan. Suojattavat kohteet on tunnistanut vain kolmasosa ja kriittiset kohteet vain noin puolet. Suurin osa kuitenkin kertoo kehittävänsä riskienhallintaansa järjestelmällisesti ja useimmat viestivät digiturvallisuuden riskeistä koko organisaatioonsa.

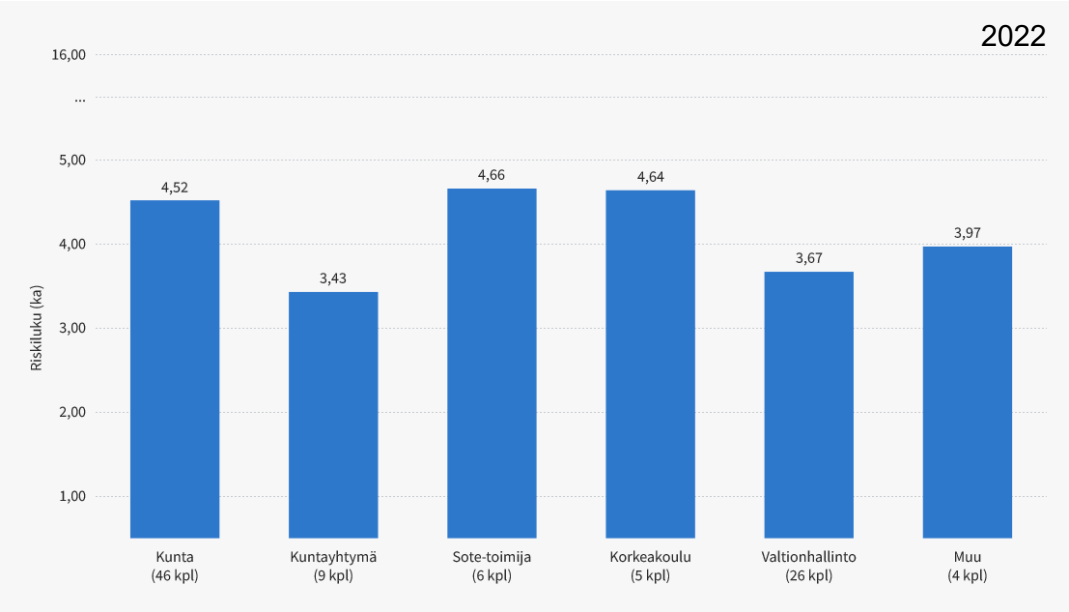
2 Yleisnäkemykset riskien kehityksestä

Koko kyselyn osalta kaikkien erilaisten riskien todennäköisyyden ja vaikutusten keskiarvot eivät ole erityisen hyvä indikaattori riskitasosta sinänsä, mutta sen muutoksen voidaan katsoa heijastelevan yleistä tilannetta. Muutoksia tulisi pitää vain suuntaa antavina, johtuen muuttuneesta kyselyn toteutustavasta ja sisällöstä.

Todennäköisyyden keskiarvo oli 1,94, nousten hieman aiemmasta (2021: 1,88), minkä voidaan nähdä sisältyvän tarkastelun epätarkkuuteen. Tämä olemattoman muutoksen merkitys korostuu, kun sitä verrataan vaikutuksen keskiarvoon 2,10, joka kuitenkin nousi yli kymmenyksen (2021: 1,98). Vaikutusten merkityksen nähdään siis nousevan suhteessa enemmän.

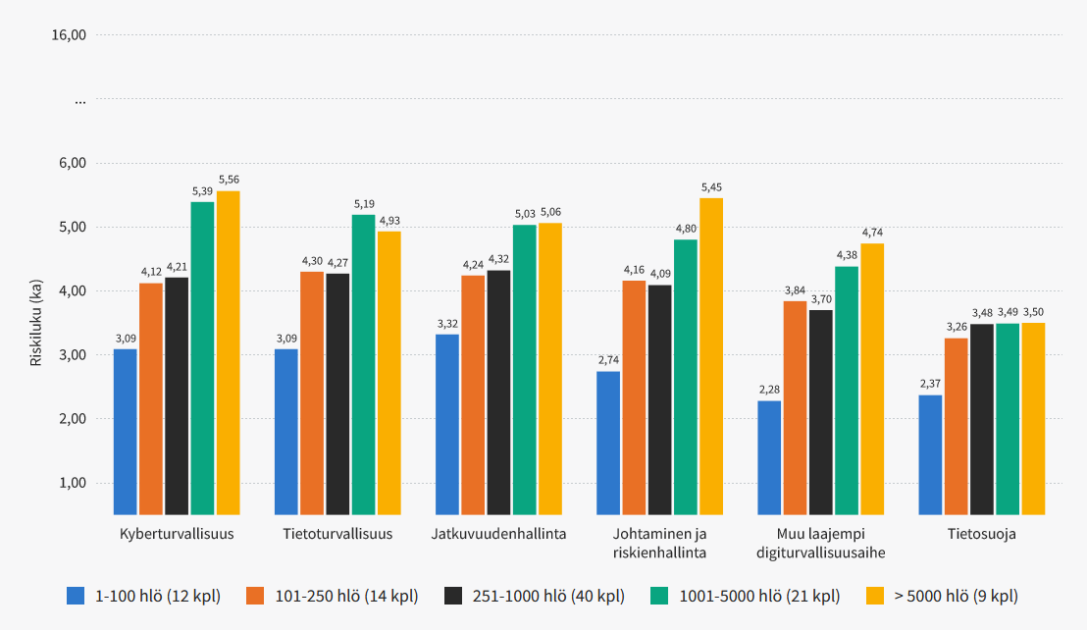
2.1 Eri vastaajatyyppien ero ovat korostuneet

Eri organisaatiotyyppien mukaisessa ryhmittelyssä on nähtävissä eri kehityssuuntia. Kuntien ja SOTE-toimijoiden riskit nähdään kasvavan, mahdollisesti osin johtuen sekä hyvinvointialueiden tuomista muutoksista, mutta se ei kuitenkaan sinänsä korostunut kyselyssä nimenomaisena riskinä. SOTE-toimijoiden digiturvan kokonaiskuva-kyselyssä saama pistekeskiarvo oli selvästi kuntien ryhmää parempi, mikä erottaa näitä kahta. Valtionhallinnon pisteytys digiturvallisuuden kokonaiskuvassa oli vielä parempi, mikä näyttäisi heijastuvan luonnollisemmin riskinäkymään.



Kuva 2b: Vuoden 2022 riskilukujen keskiarvot organisaatiotyyppien mukaan.

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. Tässä on nähtävissä kyselyajankohtien välillä kasvua edellä kuvatussa eriytymisessä. Suurten toimijoiden riskien suuruuteen voi ilmiönä liittyä merkittävä uhkien, suojattavien asioiden sekä suojautumisjärjestelyiden hallinnan kompleksisuuden kasvu skaalautuessa.



Kuva 3: Digiturvan eri osa-alueiden riskilukujen keskiarvot vastaajaorganisaatioiden koon mukaan.

2.2 Digiturvan taloudelliset riskivaikutukset nähdään selvästi kasvavina

Riskien vaikutusta tarkasteltiin jakamalla se kolmeen osaan: vaikutus talouteen, vaikutus maineeseen sekä vaikutus palveluiden tuottamiseen [eli toimintakykyyn]. Näistä merkityksellinen muutos on taloudellisten vaikutusten korostuminen edellisvuodesta, 1,76 (2021) nousi 1,88:aan (2022). Maineen osalta muutos oli vain hieman vähäisempi, 2,10 nousi 2,18:aan. Palveluiden tuottamisen osalta muutos oli minimaalinen, 2,17 nousi 2,19:aan.

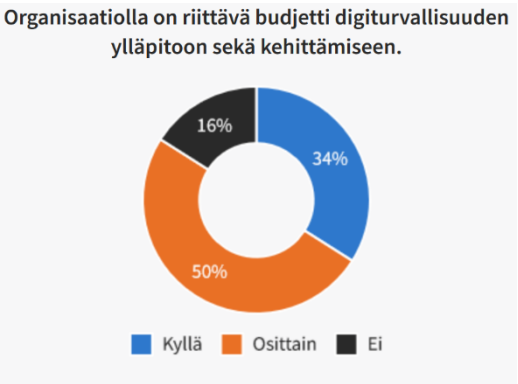
Koska kyselyn tarkastelussa katsottiin tulevaan, noin 1-3 vuoden päähän, on tästä pääteltävä, että digitaalisen turvallisuuden yhteys julkisen hallinnon organisaatioiden talouteen nähdään saavan enemmän merkitystä tulevaisuudessa. Tämä heijastelee yleisen taloustilanteen näkymiä ja ymmärryksen kasvua digitaalisten riskien toteutuessa rahallisten kustannusten kasvusta. Riskien todennäköisyyden taso keskiarvoisesti on kuitenkin pysymässä melko vakaana. Tämän voi nähdä luottamuksena suomalaisen yhteiskunnan osaamiseen, varautumiseen ja kykyyn kohdata digitaalisen turvallisuuden haasteita, eikä näkemys ole merkittävästi muuttunut turvallisuusympäristön uhkakuvien nopeiden muutosten mukana. On kuitenkin huomattava, että tämä ei indikoi yksittäisten riskien tai riskialueiden mahdollisia muutoksia, jotka vaihtelevat.

Yleisten talousennusteiden[1] mukaan kustannukset tulevat kasvamaan eri tavoin[2] ja indikaattorien mukaan tämä tulee kestämään seuraavat kaksi tai kolme vuotta. 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

[1] https://vm.fi/talouden-ennusteet
[2] https://www.enisa.europa.eu/news/cybersecurity-investments-in-the-eu-is-the-money-enough-to-meet-the-new-cybersecurity-standards

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. Vakuutusten merkitys on julkishallinnossa vähäinen, mutta ne voivat tulla esiin välillisesti digiturvallisuuteenkin liittyen, esimerkiksi palveluntuottajien kautta. Tämä voi aiheuttaa ylimääräistä rasitusta, mutta laajemmassa kuvassa lisävaatimuksia voidaan pitää myös positiivisena sivuvaikutuksena digiturvallisuuden kehittämisessä.

Digitaalisen turvallisuuden kokonaiskuvan kyselyssä on nähtävissä viitteitä puutteisiin taloudellisessa resursoinnissa tällä hetkellä julkisessa hallinnossa. Puolet vastanneista piti budjetointia vaillinaisena joiltain osin ja enemmän kuin joka kymmenes selvästi riittämättömänä. Tämä on huolestuttavaa, sillä ennakkoon toteutetut toimet 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. Myös eri tavat tehostaa resurssien käyttöä, esimerkiksi yhteiskäytöllä tai -hankinnoissa, tulisi harkita.



Kuva 6: Digiturvallisuuden tilanne julkisessa hallinnossa budjetoinnin osalta.

2.3 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.

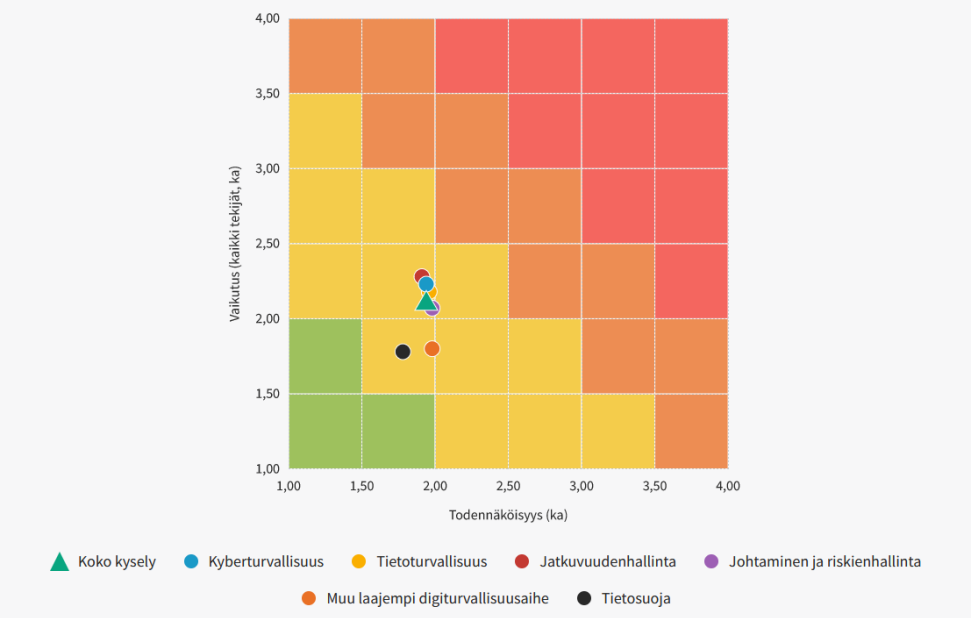
Käytetyt luokittelut ja niiden ryhmittelevät otsikoinnit olivat:

- 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*)

- Digitaalisen turvallisuuden hallintamalli (*Johtaminen ja riskienhallinta, Jatkuvuudenhallinta, Kyberturvallisuus, Tietosuoja, Tietoturvallisuus, Muu laajempi digiturvallisuusaihe*)

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 luokkiin lisättiin uusia riskiaiheita.

Digiturvallisuuden osa-alueiden luokittelulla tarkasteltuna huomattavaa on, että tietosuojaa sivuavien riskien nähdään olevan selvästi vähäisempiä yhdessä laajempien digiturvallisuusaiheiden kanssa. Näiden kahden kohdalla on tarkemmassa tarkastelussa nähtävissä, että niissä käytetyt indikaattorit kuvaavat useita toissijaisia uhkia, joiden vaikutukset eivät ole välittömiä, mikä voi vaikuttaa näkemyksiin niistä. Useissa muissa riskeissä on myös tunnistettavissa, että niiden toteutuessa seuraukset johtaisivat usein tietosuojan vaarantumiseen. Toisaalta, tarkasti säädeltynä osa-alueena, tietosuojan vaatimusten noudattaminen tarkoittaa, että riskit ovat hallinnassa, jolloin niiden ei nähdä myöskään kehittyvän negatiivisesti. Tätä tukee organisaatioiden digiturvan tilaa kartoittaneet vastaukset, jossa tietosuojan osa-alue sai korkeimmat keskiarvopisteet.



Kuva 7: Riskinäkemysten sijoittuminen digiturvallisuuden luokkien mukaan ryhmiteltynä.