Resultat från enkäten om risker inom den digitala säkerheten – hösten 2021

MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

Sammanfattning

- Aktörerna inom den offentliga förvaltningen tillfrågades om sina synpunkter på 36 riskpåståenden i början av september 2021 och vi fick N = 126, inklusive statsförvaltningen 39 procent, kommunala aktörer (inkl. Social- och hälsovården) 46 procent, högskolor 9 procent och övriga 6 procent. I utvärderingarna begärdes synpunkter i 3 års tidsfönster.
- **De mest centrala riskerna gäller attacker mot myndigheternas tjänster och infrastrukturen bakom dem.** Därefter kan man se en oro för hur komplexiteten ska hanteras och hur resurserna ska allokeras. Man strävar efter att svara på de två första riskerna genom att informera om hot och på de senare genom att bland annat förbättra hanteringen av information om digital säkerhet (inkl. sökbarhet) i olika former, eftersom effektiveringen i detta område också underlättar användningen av befintliga resurser.
- Medeltalen för risktalen är måttliga och inga stora skillnader mellan olika förvaltningshelheter förekommer, men i noggrannare klassificeringar kan man se olika betoningar bl.a. inom olika verksamhetsområden och inom statens förvaltningsområden. Dessa kan beaktas genom en bättre inriktning av de digitala säkerhetsåtgärderna.
- Resultaten bekräftar skillnaden mellan statens och kommunaktörernas riskprofiler. Kommunernas åsikt fokuserar på att närma sig riskerna på ett mer praktiskt sätt och på att beakta den digitala tryggheten i planeringen av verksamheten. **Det fanns inga betydande skillnader i åsikterna hos respondentklasserna i olika storlekar, vilket stärker uppfattningen att man med olika resurser är tvungen att svara på samma risker** – endast de största har en något högre syn på riskerna.
- De risker som ses som mindre centrala, bl.a. artificiell intelligens och påverkan, bör följas upp, eftersom de kan aktiveras i framtiden.

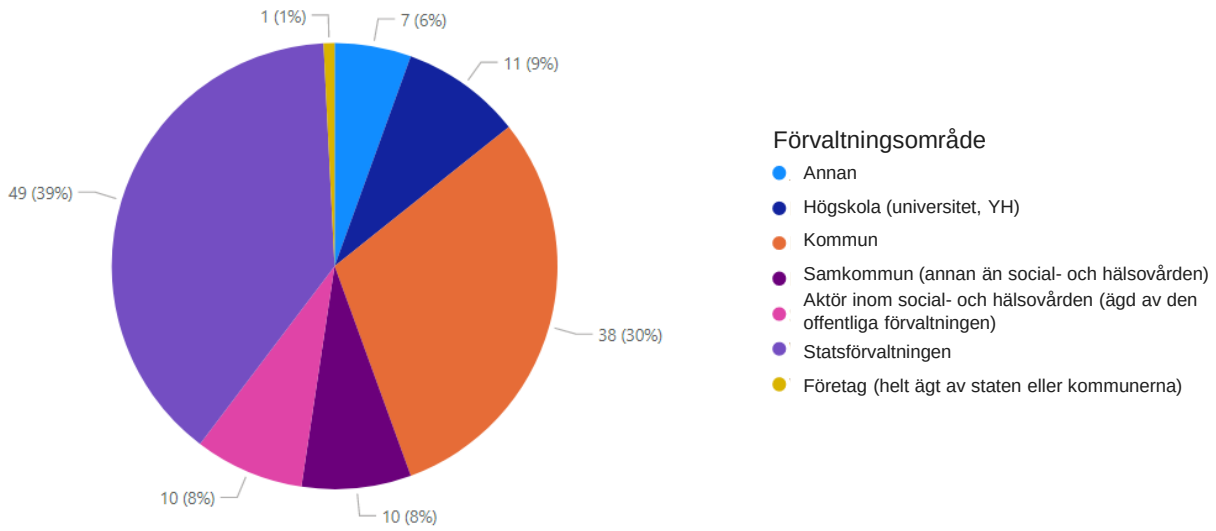
Genomförande av enkäten

- MDB och finansministeriet utredde i samarbete under hösten 2021 de mest betydande riskerna för den digitala säkerheten inom den offentliga förvaltningen som en del av pilotförsöket med en strategisk riskbedömningsmodell för digital säkerhet inom den offentliga förvaltningen.
  - Utgångspunkten var påståendena i den tidigare riskenkäten som genomfördes för kommunerna 2020 och som kompletterades och formulerades utifrån responsen på enkäten.
- Enkäten omfattade 36 riskpåståenden och möjlighet att presentera kompletterande riskområden i öppna frågor
  - Påståendena hade rubricerats enligt OECD:s perspektiv på digital säkerhet:
    - Nationell och internationell säkerhet
    - Laglighetsövervakning
    - Ekonomisk och social välfärd
    - Teknik
  - Riskpåståendena finns i bilaga 1
- Respondenterna ombads bedöma riskpåståendena ur fyra perspektiv:
  - Inverkan på ekonomin
  - Inverkan på ryktet
  - Inverkan på produktionen av tjänster
  - Sannolikhet för att risken realiseras
- I svaren användes en skala med fyra nivåer (1 = osannolik/liten effekt, 4 = nästan säker/kritisk). Det var inte obligatoriskt att svara på perspektiven.
- I första hand har de samlats in för handledning om digitala risker inom den offentliga förvaltningen. Resultaten presenterades för den strategiska ledningsgruppen för digital säkerhet och VAHTI för arbetsgruppen för utveckling av riskhanteringen 1.12.2021.

Enkätens nyckeltal

- Svarstid 25.8–21.9.2021
- 617 tog emot enkäten
- Antalet svarande var 139, av vilka N = 126 olika organisationer räknades ut genom utjämning
  - Respondenter från samma organisation
  - Samma FO-nummer för respondenterna
- Fördelningen av respondenterna enligt förvaltningshelhet:
  - Kommuner och samkommuner 58 st. (46 procent)
  - Statsförvaltningen 49 st. (39 procent)
  - Högskolor 11 st. (9 procent)
  - Övriga 8 st. (6 procent)

Respondenter enligt förvaltningsområde



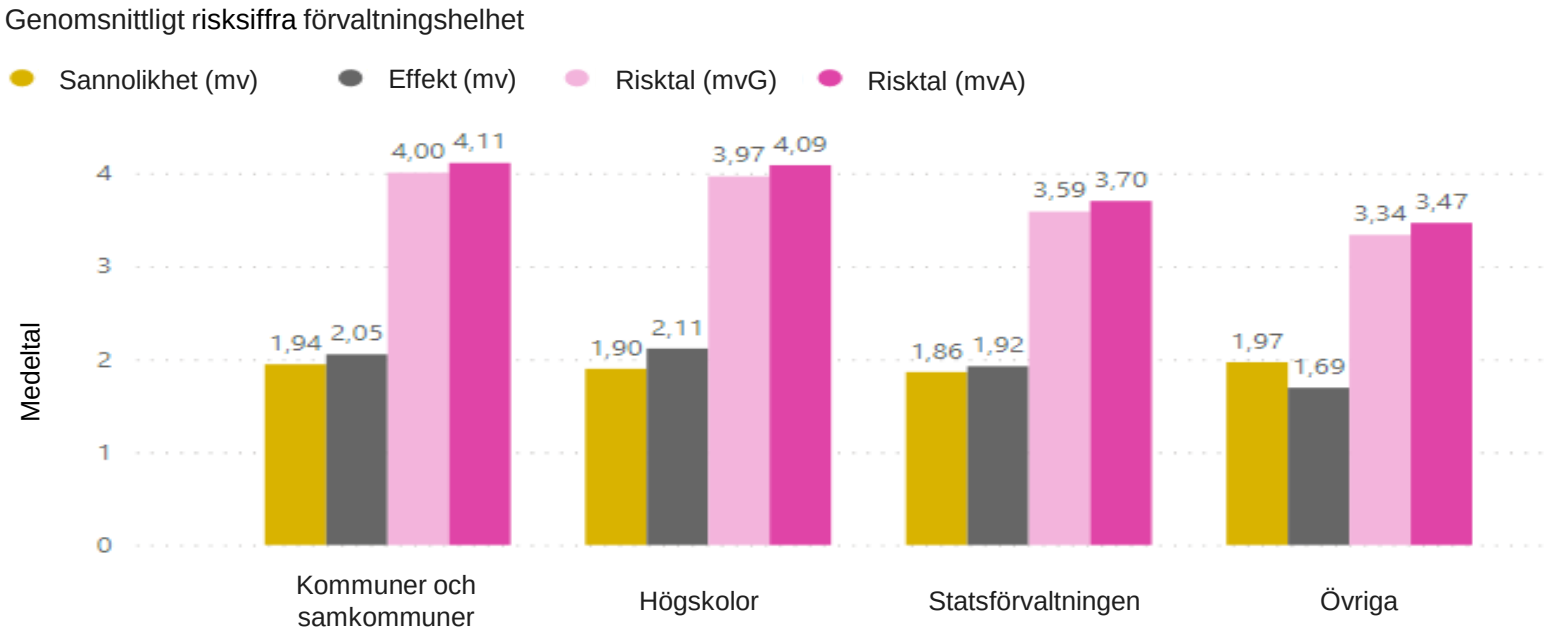
Hantering av enkätens material

- Eftersom enkäten inte innehöll korrekthetskontroller av uppgifterna, gjordes manuella korrigeringar i svarsmaterialet med anknytning till FO-nummer (saknade lades till, presentationsformen förenhetligades, felaktiga korrigerades) och kompletteringar av organisationernas personaluppgifter som saknades.
- I analysens datamodell infördes utöver svaren även riskpåståenden klassificerade enligt tre olika kategorier (OECD, World Economic Forum, delområden som använts i genomförandet av den digitala säkerheten), beskrivningar av statsförvaltningens struktur samt nyckeltal för kommunernas ekonomi.
- För varje enskilt riskpåstående i varje svar har man beräknat det aritmetiska medelvärdet av tre olika effektfaktorer samt det risktal som erhållits genom att multiplicera den genomsnittliga effekten med sannolikheten. På grund av beräkningssättet och avrundningarna ger värdena för de stapelbilder som visualiserar föreställningen inte exakt risktalet. Detta påverkar inte klassernas jämförbarhet.
- På basis av antalet svar kunde man göra djupare jämförelser endast för statsförvaltningens och kommunernas del, men även dessa var endast riktgivande.

Nyckeltal

Risksiffra i medeltal (aritm.) indelat enligt förvaltningshelhet:

- Kommuner och samkommuner 4,1
  - Kommuner 4,2
  - Samkommuner 4,1
  - Social- och hälsovården (SOTE) 3,7
- Högskolor 4,1
- Statsförvaltningen 3,7
- Övriga 3,5

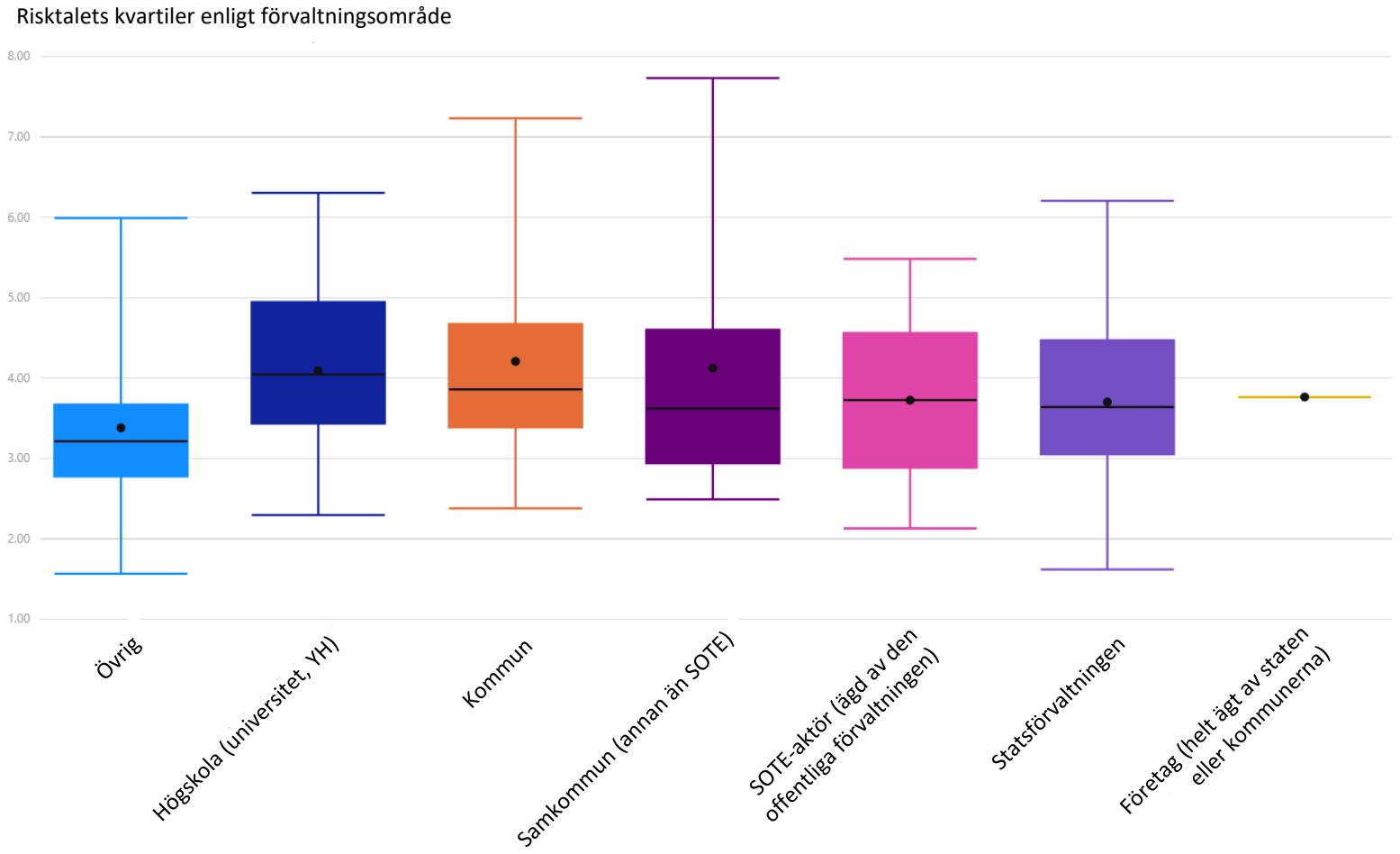


- Kommuner och samkommuner samt högskolor är ganska på samma nivå
- Statsförvaltningens och social- och hälsovårdsområdets uppskattningar är lägre

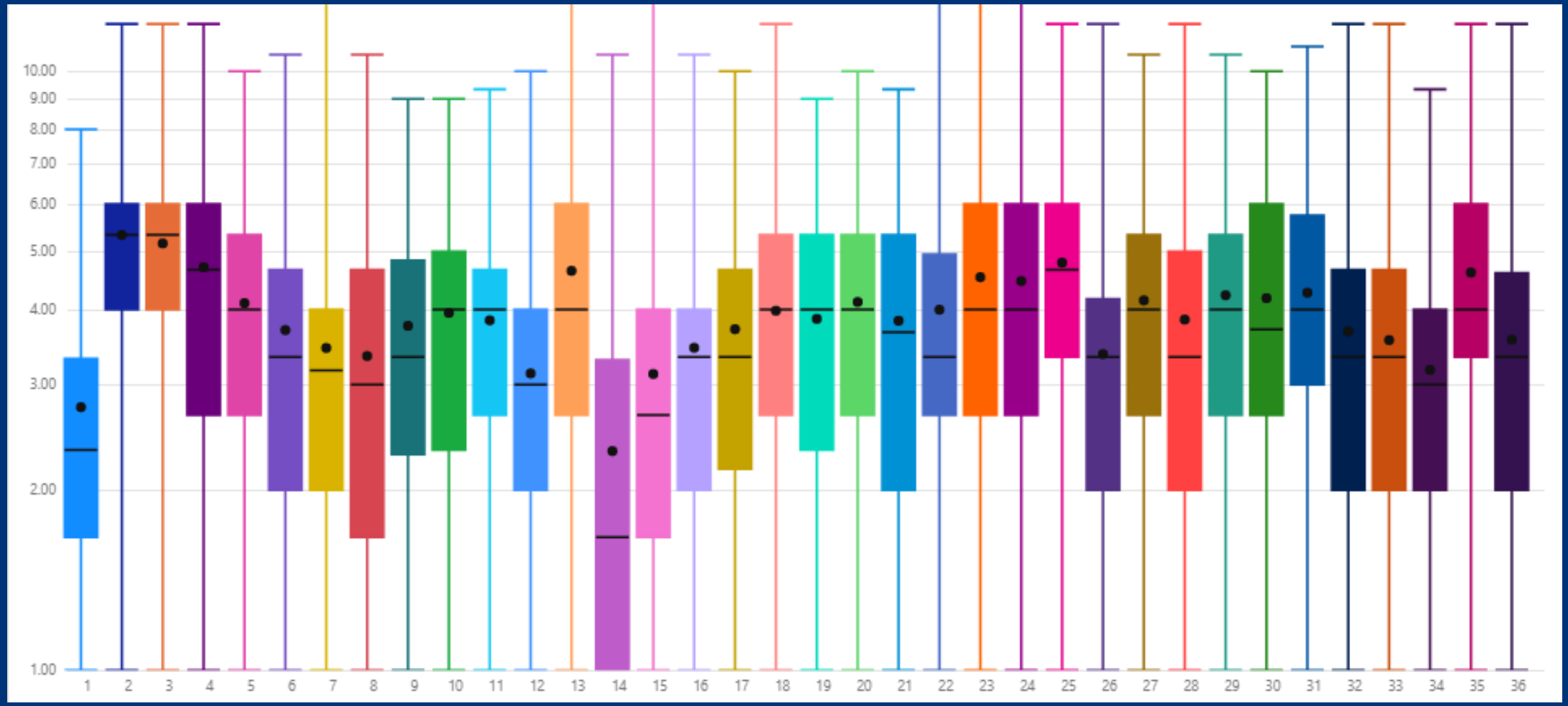
Bakom nyckeltalen

I bedömningarna kan man se olika uppfattningar om riskerna bland aktörer i olika områden, vilket inte helt förklaras av att riskerna är olika. Detta stöds av skillnaderna i fördelningen av svaren i helheterna, dvs. ytterligheterna i grafen samt storleken och placeringen i mitten av kvartalet.

- Inom statsförvaltningen kan de förklarande faktorerna vara en bättre delad risksyn och en mer enhetlig kompetens.
- Social- och hälsovårdsaktörerna kan ha en noggrannare avgränsning och mer enhetliga risker överlag.



Spridning av svaren, viktningskvartilerna samt medelvärden och medianerna i riskpåståenden

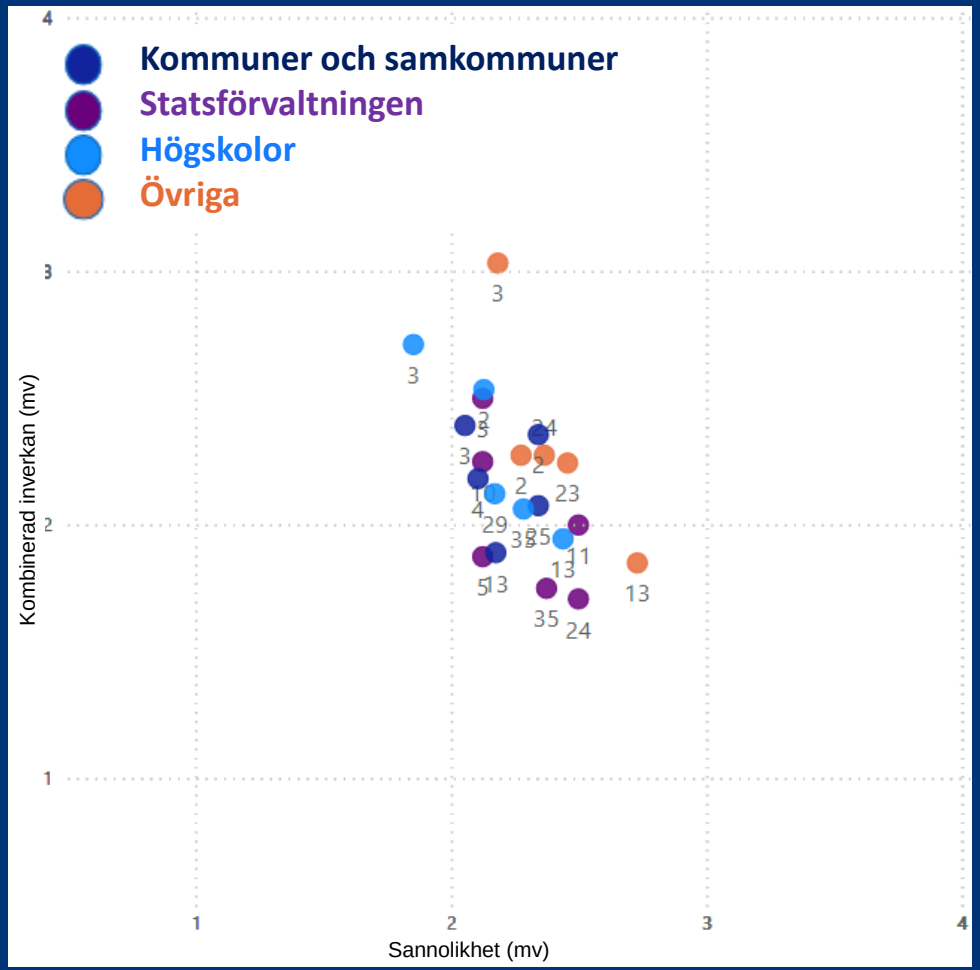


Risker som betraktas som centrala: Alla svarande, top-10

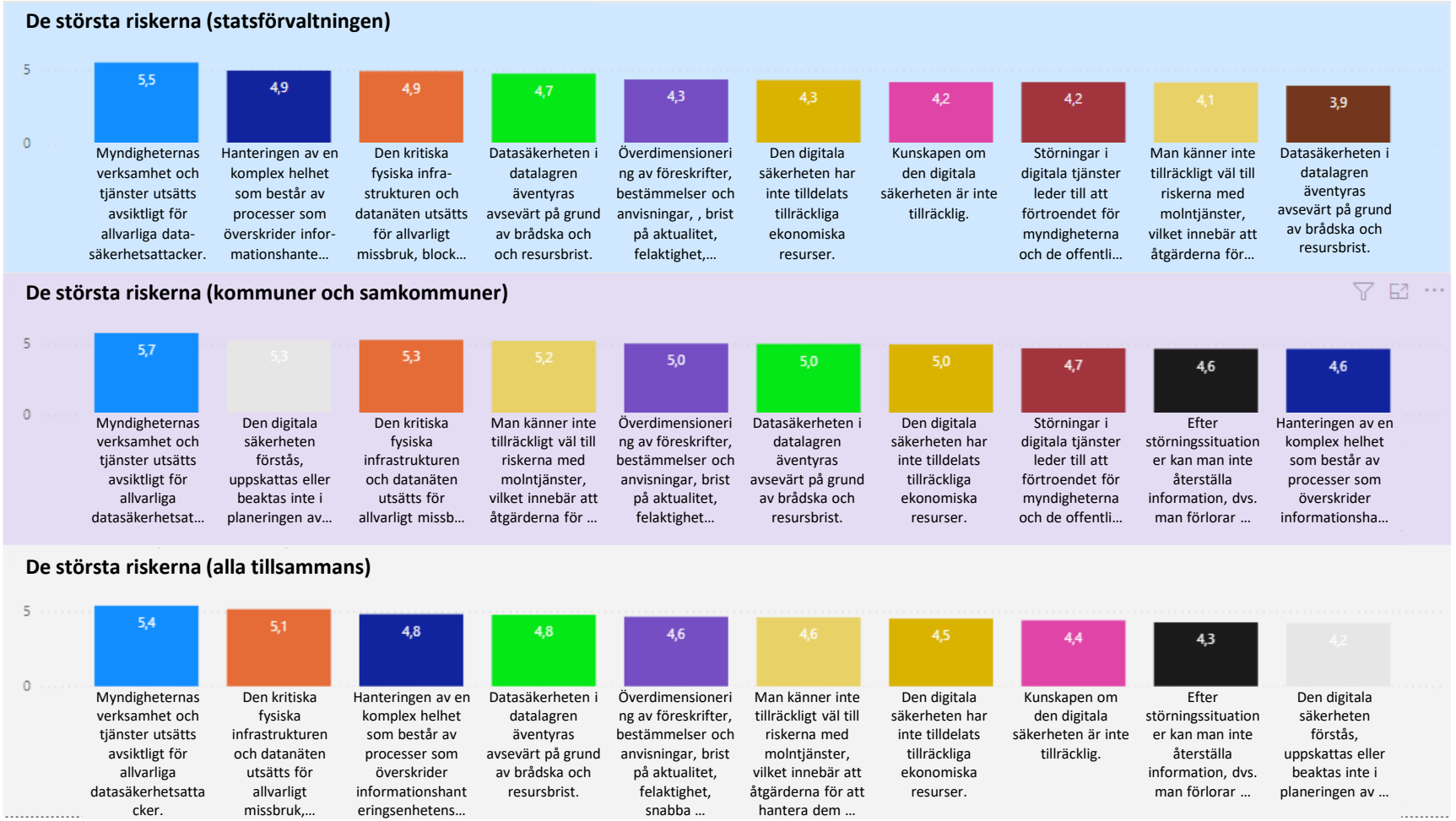
Riskpåståendets nummer	Riskpåstående	Risktal (medelvärde)	Sannolikhet (medelvärde)
2	Myndigheternas verksamhet och tjänster utsätts avsiktligt för allvarliga datasäkerhetsattacker.	**5,3**	2,2
3	Den kritiska fysiska infrastrukturen och datanäten utsätts för allvarligt missbruk, blockering, sabotage eller datasäkerhetsattacker.	**5,2**	2,0
25	Hanteringen av en komplex helhet som består av processer som överskrider informationshanteringsenhetens verksamhetsområden, ICT-leverantörer, underleverantörer och produktionsmiljöer misslyckas, vilket orsakar störningar och serviceavbrott.	**4,8**	2,2
4	Datasäkerheten i datalagren äventyras avsevärt på grund av *brådska och resursbrist*.	**4,7**	2,0
13	Överdimensionering av föreskrifter, bestämmelser och anvisningar, brist på aktualitet, felaktighet, snabba förändringar eller andra omständigheter förknippade med regleringens kvalitet resulterar i oskäliga skyldigheter.	**4,6**	2,3
35	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.	**4,6**	2,1
23	Den digitala säkerheten har inte tilldelats tillräckliga ekonomiska resurser.	**4,5**	2,2
24	Kunskapen om den digitala säkerheten är inte tillräcklig.	**4,5**	2,2
31	Efter störningssituationer kan man inte *återställa information*, dvs. man förlorar information, immateriella rättigheter eller programvara.	**4,3**	1,7
29	Den digitala säkerheten förstås, uppskattas eller beaktas inte i planeringen av verksamheten.	**4,2**	2,0

Granskning av risklistan

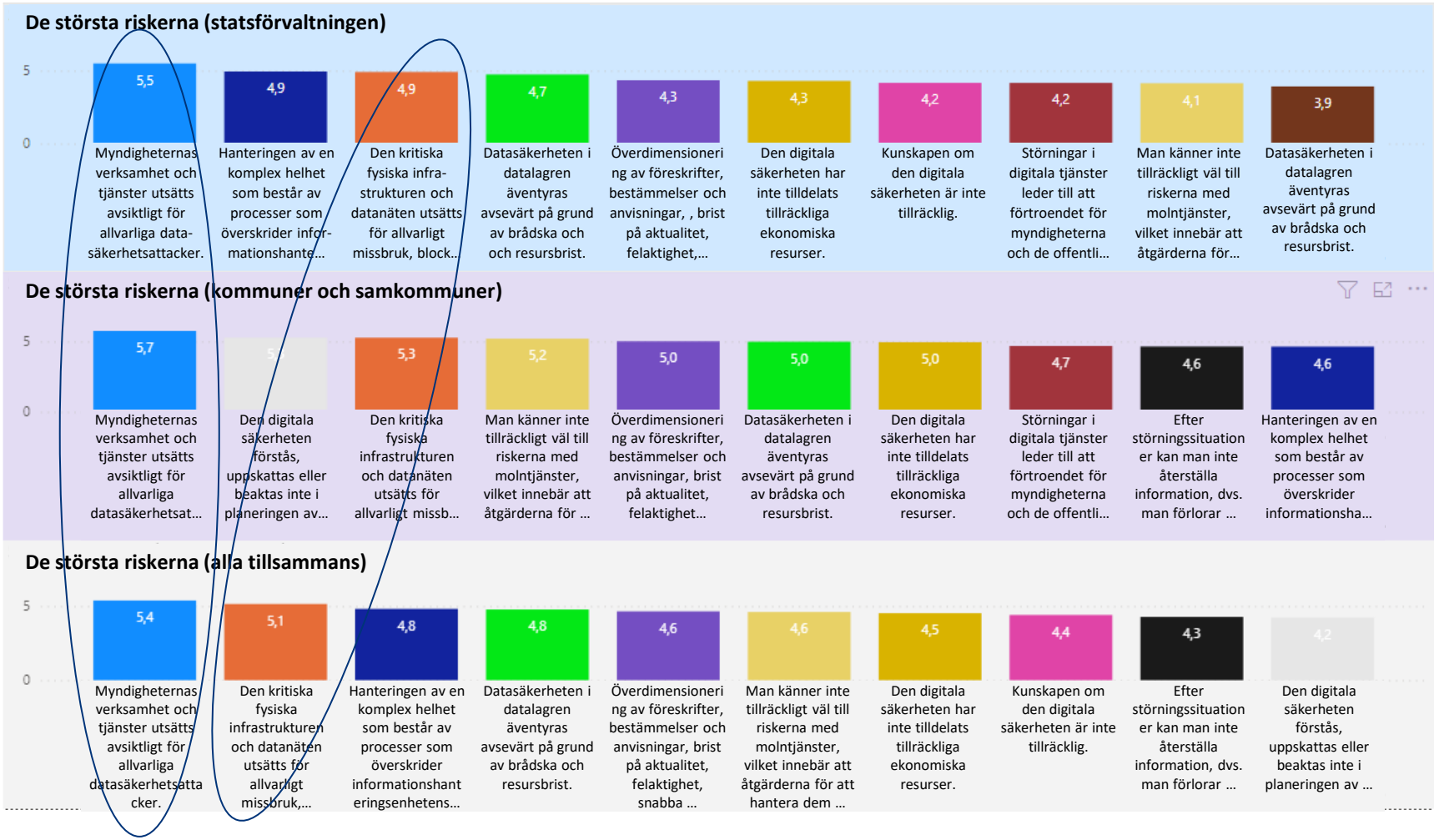
- Riskpåståendena 2 och 3 ses som de viktigaste
  - *2: Myndigheternas verksamhet och tjänster utsätts avsiktligt för allvarliga datasäkerhetsattacker.*
  - *3: Den kritiska fysiska infrastrukturen och datanäten utsätts för allvarligt missbruk, blockering, sabotage eller datasäkerhetsattacker.*
  - *Betoning alltså på yttre hot*
- Följande risker framhäver å ena sidan utmaningarna i fråga om hantering, bristen på tydlighet, tillgången till information och kvaliteten på informationen samt å andra sidan resursutmaningarna
  - Genom att förbättra kontrollerbarheten underlättas resursanvändningen till det väsentliga
- Som helhet bedöms riskerna ligga rätt nära varandra i olika förvaltningshelheter och inga separata kluster bildas. I diagrammet visas top-5 riskerna
  - Skillnaderna syns först i en djupare granskning



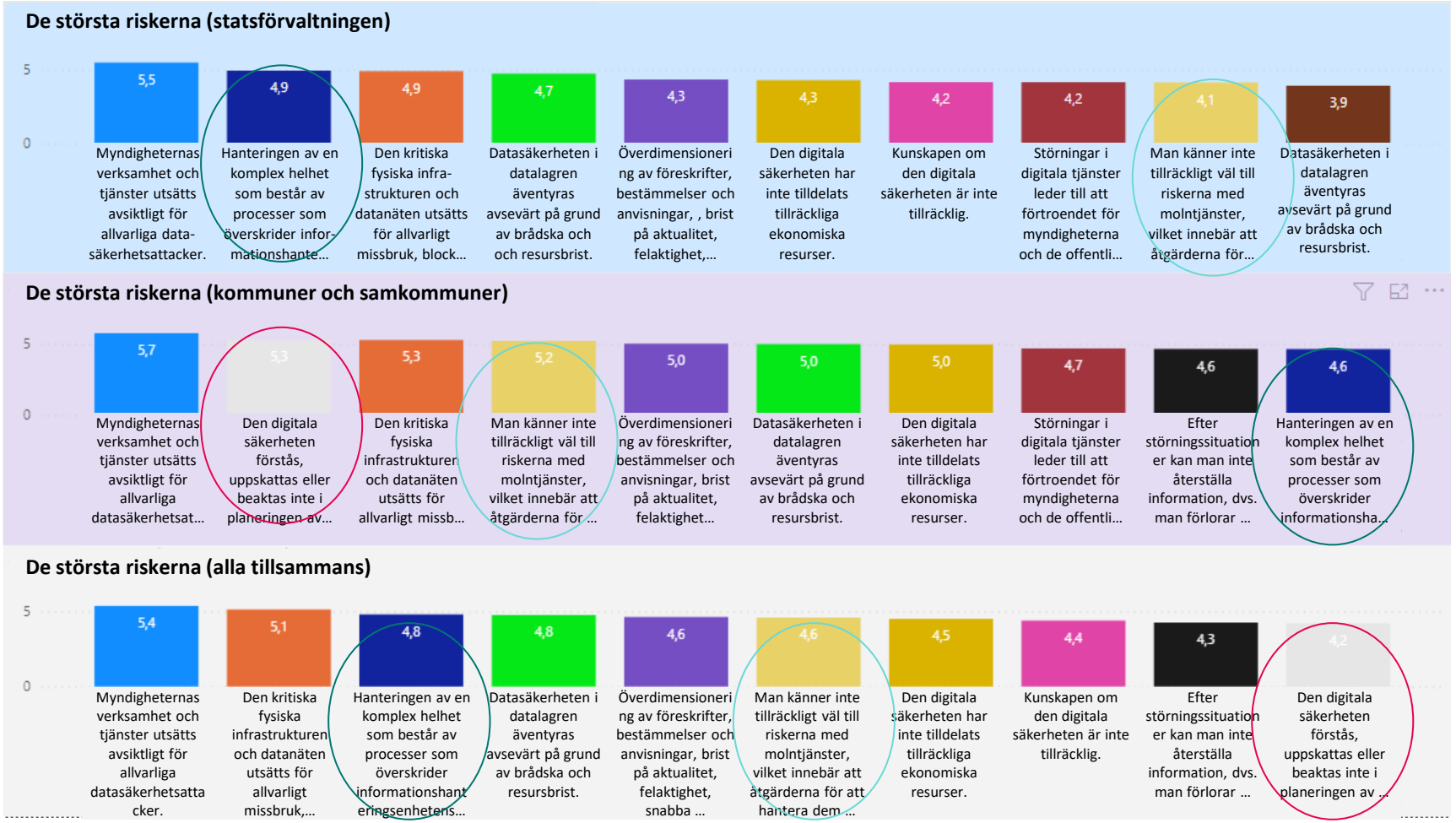
Risker som betraktas som centrala: jämförelse mellan riskprofiler



Risker som betraktas som centrala: jämförelse mellan riskprofiler (de två översta)



Risker som betraktas som centrala: jämförelse mellan riskprofiler (olika viktningar)

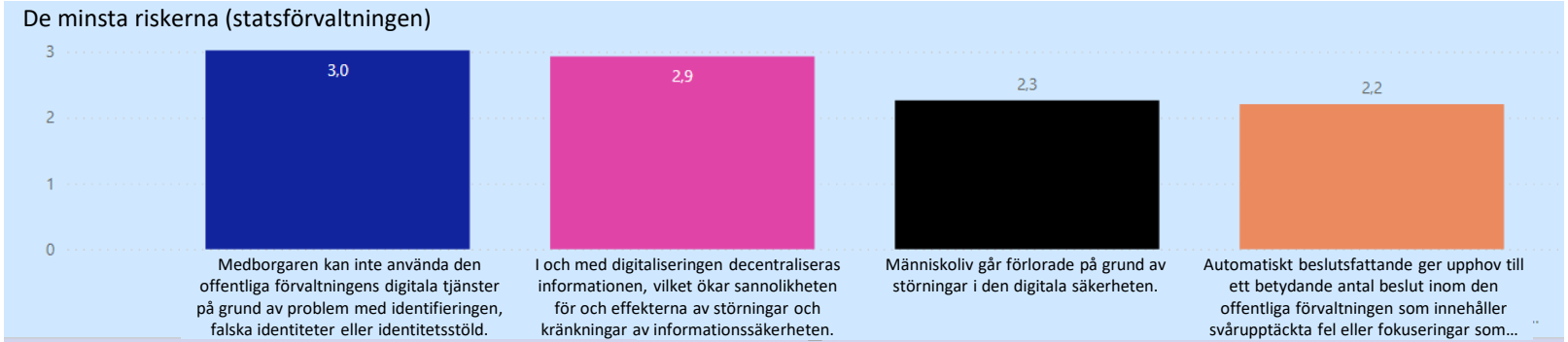


Risker som betraktas som mindre centrala: Alla svarande, bottom-10

Riskpåståendets nummer	Riskpåstående	Risktal (medelvärde)	Sannolikhet (medelvärde)
14	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.	**2,3**	1,3
1	Människoliv går förlorade på grund av störningar i den digitala säkerheten.	**2,7**	1,3
12	Informationshanteringsenheten varken bedömer eller följer upp den digitala säkerhetens mognadsnivå.	**3,1**	1,8
15	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.	**3,1**	1,9
34	I och med digitaliseringen *decentraliseras informationen*, vilket ökar sannolikheten för och effekterna av störningar och kränkningar av informationssäkerheten.	**3,2**	1,8
8	Statliga eller kriminella aktörer försöker med olagliga medel utnyttja den offentliga förvaltningens datalager för att främja sina egna politiska, militära eller ekonomiska ändamål.	**3,3**	1,7
26	Medborgaren kan inte använda den offentliga förvaltningens digitala tjänster på grund av problem med identifieringen, falska identiteter eller identitetsstöld.	**3,4**	1,9
7	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.	**3,5**	2,0
16	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.	**3,5**	1,9
33	I och med digitaliseringen *centraliseras informationen*, vilket ökar sannolikheten för och effekterna av störningar och kränkningar av informationssäkerheten.	**3,6**	1,8

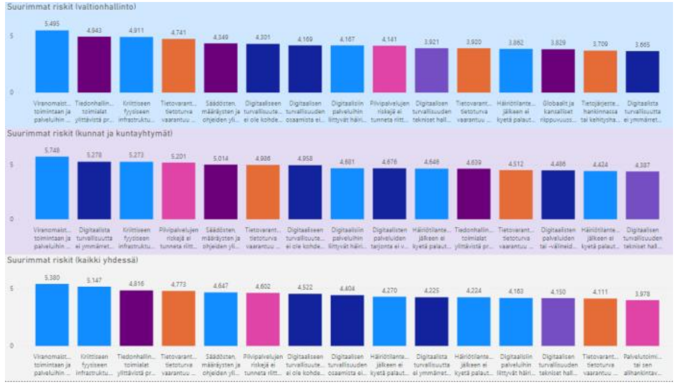
Risker som betraktas som mindre centrala: jämförelse mellan riskprofiler

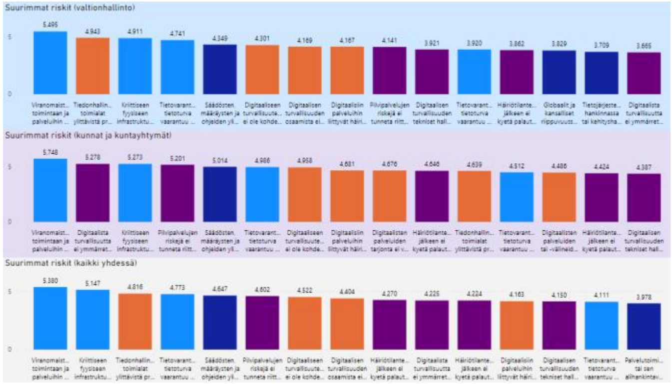
- Skillnaderna mellan profilerna syns också i slutet
- Kommunerna har betydligt större splittring av risktalen, ”svansen” är lägre
- Ingen skillnad mellan centralisering och decentralisering
- Kommunerna upplever inte påverkan eller känner inte igen den?
- Riskerna med automatiskt beslutsfattande är kanske inte ännu relevanta (jämfört med andra)?

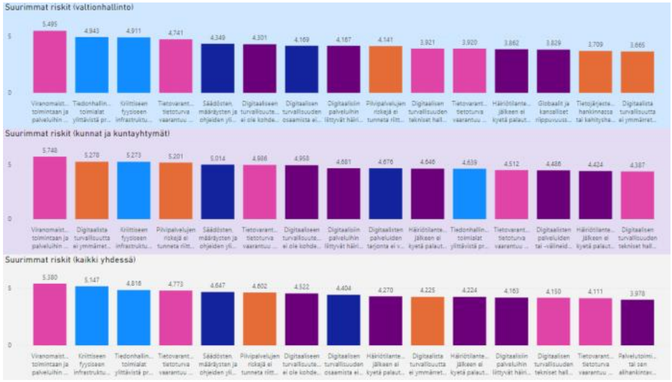


Klassificeringsjämförelse – olika profiler

- En analys som gjorts enligt olika klassificeringar av top-15 riskerna visar också olika betoningar i riskprofilerna, men inte tydliga fenomen som enkelt kan uttryckas. Utvecklingen och dess betydelse ska granskas med flera års tidsspann.
  - I jämförelsen av deskriptorerna statsförvaltningen är högst upp, kommunsektorn i mitten och alla andra längst ner.
  - Samma risker i färg enligt olika klasser. Till vänster sex kategorier i World Economic Forum; i mitten OECD:s fyra klasser; till höger fem områden för genomförande av digital säkerhet och till höger ett sjätte bredare perspektiv på riskpåståenden.

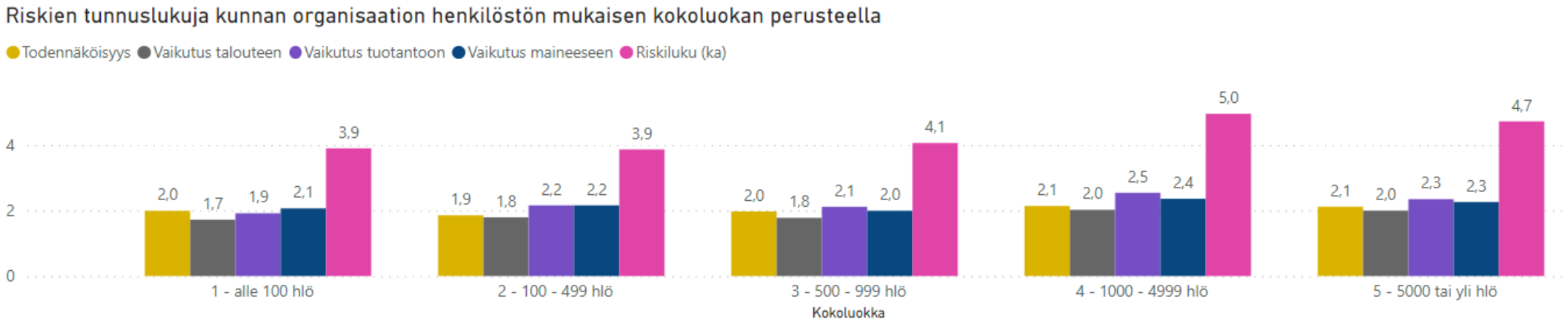






Kommunsektor

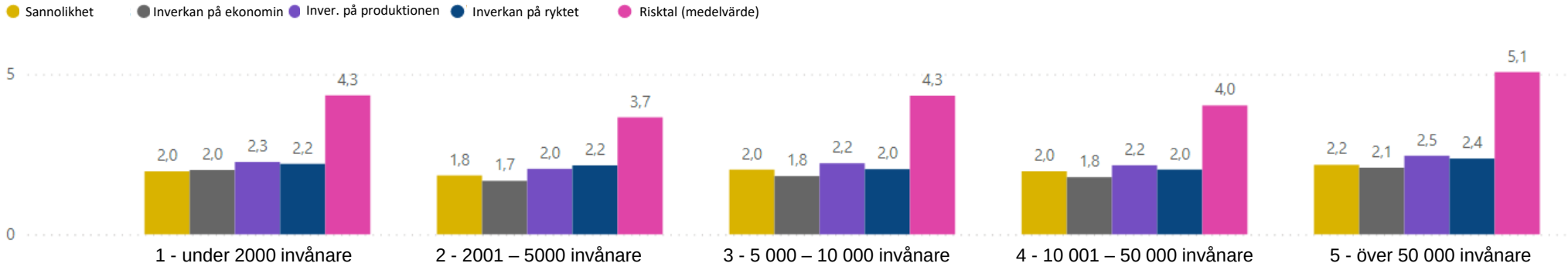
- Svar, risktal och sannolikhet
- Risksiffror för kommunerna är ganska lika oberoende av deras storlek enligt invånarantalet eller antalet anställda i organisationen.
  - Endast för de största kommunerna kan man urskilja högre risksiffror. Förklaringen kan vara delaktighet i mer omfattande funktioner (inklusive bland annat mer omfattande kontakter utanför närområdet och mer komplexa påverkningsnätverk) och riskerna som dessa medför.
- Detta stärker tanken "samma risker för alla, men olika resurser att svara på dem”
  - Se Enkäten för organisationens digitala säkerhet



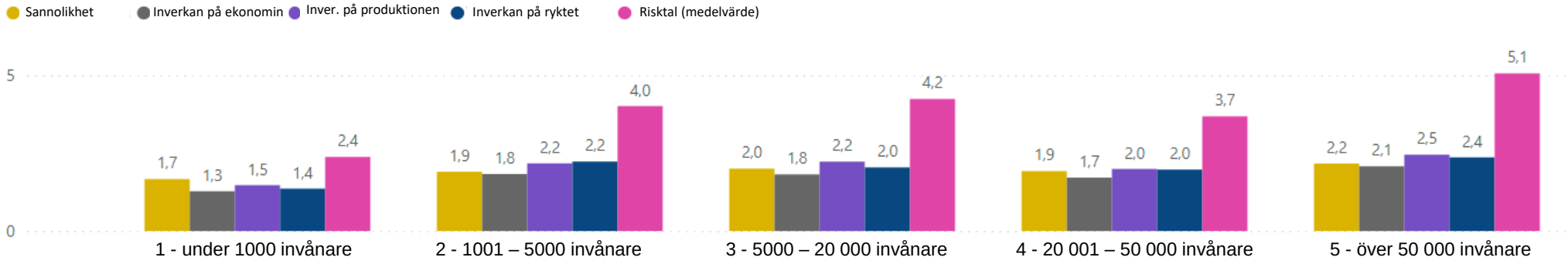
Respondenter i klasserna (st.): 36 12 12 5

Risksiffor för kommunsektorn i storleksklasser enligt invånarantal (olika gränsvärden)

Riskernas nyckeltal enligt storleksklass enligt kommunernas invånarantal, klassificering A



Riskernas nyckeltal enligt storleksklass enligt kommunernas invånarantal, klassificering B



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

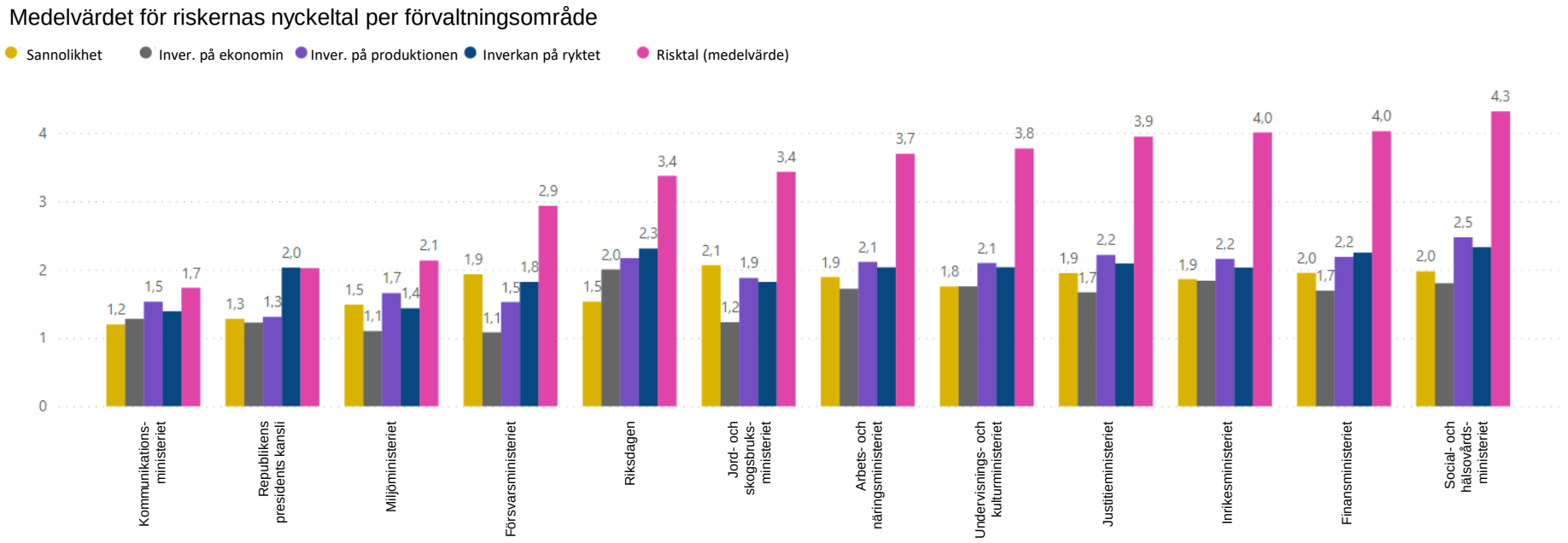
Nyckeltal för riskvyerna inom statsförvaltningen

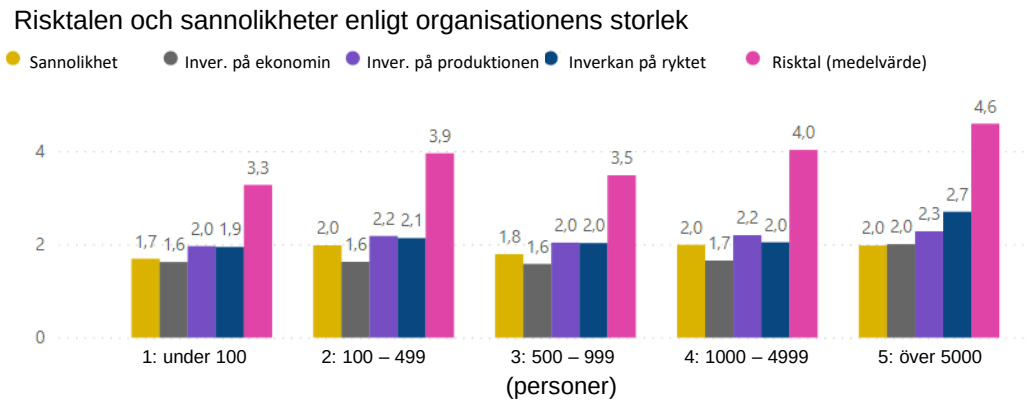
- Svar från 49 enheter
- Medelvärde för risksiffan 3,7
- Medelvärde för sannolikheten 1,9
- Skillnaderna som upplevts i de digitala riskerna syns i risksiffan enligt förvaltningsområde som betydande i förhållande till varandra
  - Förklarande faktorer är bl.a. egna förmågor, resurser och strukturer jämfört med både de objekt som ska skyddas och deras värde och de hot som upplevts

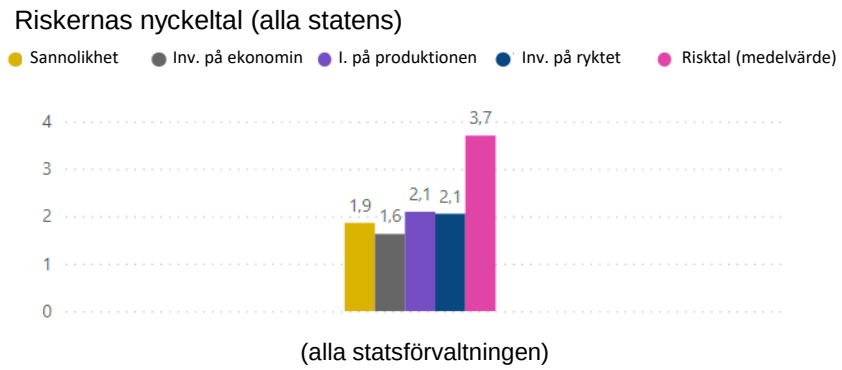
Storleksklass (personer)	**Sannolikhet** (medelvärde)	**Risktal** (medelvärde)	**Respondenter** (st.)
Under 100	1,7	**3,3**	16
100–499	2,0	**3,9**	19
500–999	1,8	**3,5**	6
1000–4999	2,0	**4,0**	7
5 000 eller fler	2,0	**4,6**	1

Förvaltningsområden som svarat	**Sannolikhet** (medelvärde)	**Risktal** (medelvärde)	**Respondenter** (st.)
Kommunikationsministeriet	1,2	**1,7**	1
Republikens presidents kansli	1,3	**2,0**	1
Miljöministeriet	1,5	**2,1**	2
Försvarsministeriet	1,9	**2,9**	2
Riksdagen	1,5	**3,4**	1
Jord- och skogsbruksministeriet	2,1	**3,4**	2
Arbets- och näringsministeriet	1,9	**3,7**	5
Undervisnings- och kulturministeriet	1,8	**3,8**	5
Justitieministeriet	1,9	**3,9**	13
Inrikesministeriet	1,9	**4,0**	5
Finansministeriet	2,0	**4,0**	9
Social- och hälsovårdsministeriet	2,0	**4,3**	3

Statsförvaltningens riskvyer som grafer







Övriga observationer om resultaten

- Av riskmatrisens poängkluster som finns bifogade ser man att en allvarlig störningssituation i den digitala infrastrukturen i WEF-kategorierna är betydligt mer effektiv än den teknologiska skadliga utvecklingen som är har ett lägre medelvärde än genomsnittet. Det sistnämnda innehåller risker som till sin karaktär är långsammare och svaren på dem är mer tidskrävande och omfattande, dvs. betoningen ligger på "omedelbara" risker.
- De utvecklade systemen (artificiell intelligens, algoritmer, maskininlärning, automatisering osv.) fick lite uppmärksamhet, men ämnesområdet kan bli viktigare i framtiden
  - Det finns skäl att i förväg bekanta sig med riskerna eftersom de börjar förekomma i produkterna
- Påverkan på beslutsfattandet har visat sig vara ett mindre hot
  - Antagligen har tyngdpunkten legat på COVID-19 hos andra lokala och statliga aktörer och man är åtminstone något känsligare för påverkan idag
  - Man bör undvika blinda punkter ifall det upptäcks nya metoder att påverka.
- Betydelsen av de risker och nya fenomen som respondenterna uppgav kunde inte jämföras, men framkom flera gånger (formulerade på olika sätt) bl.a.
  - En intern aktörs uppsåtliga verksamhet
  - Välfärdsområdena, social- och hälsovårdsreformen och förändringar
  - Belastning och personrisk i små organisationer
  - Svårighet att skapa en läges-, ansvars- och riskbild och att dela information, särskilt när det gäller gemensamma och externa tjänster
  - Att man glömmer en bredare bild av digital säkerhet, inkl. kunder och processer
  - Klimatkonsekvenser, omfattande och extrema förhållanden
  - Långtidseffekter, bl.a. i fråga om förvaring och kryptering av information
  - Brist på gemensamma krav och lösningar, men också ojämn tillämpning och spridning av information

Annat om ämnet

- **Organisationens Digitalsäkerhetsenkät** (MDB, augusti 2021)
  - Organisering av den digitala säkerheten, inkl. riskhantering
    - Bör utvecklas tydligt i riskhanteringen, har hamnat på efterkälken från andra delområden
    - 18 utvecklingsförslag för att svara på bl.a. riskpåståenden
- **Barometern för digital säkerhet** (MDB, oktober 2021)
  - Förtroendet för tjänsterna minskar, de flesta har upplevt bl.a. avbrott i uppgifterna
  - Förtroende för arbetsgivare och myndigheter ca 80 procent, båda något sjunkande
- **Lägesbild av digitaliseringen** (FM juni, oktober, december 2021)
  - Granskar motsvarande strategiska frågor och risker mer omfattande, men på mycket samma sätt och liknande risker
  - Lyft: Splittring på olika sätt samt omfattande utnyttjande av information utmaningar
- **Cybersäkerhet och riskhantering vid tillämpning av artificiell intelligens** (Traficom, november 2021)
  - En syn på ett område som håller på att utvecklas, med en mycket specifik del av riskerna med mer strategiska betydelser
- Även blickar utanför enkäten: bl.a. Program för veckan för digital säkerhet (inspelningar: https://www.mediaserver.fi/live/digiturvaviikko2021), där man på fredagsförmiddagen diskuterade framtidens risker och t.ex. beaktade bl.a. följderna av solstormen:
  - En större solaktivitet förväntas under de kommande decennierna och dessutom kan det uppstå en extra stor utbrott.
    - Varningen är högst 17 timmar från observationen.
  - Inducerade strömmar till eldistributionen kan bryta de globala förbindelserna. Finlands elöverföring är dock förhållandevis mer störningstålig.
    - Den digitala betydelsen har ännu inte utretts exakt här eller ute i världen. Lokala störningar i nätet är möjliga även här, men sannolikt är det problem med länkade tjänster (särskilt olika världsdelar) → omfattande långvariga nätstörningar
      - Förmågan till lokal verksamhet och självförsörjning betonas, precis som vid andra störningar i internationella kontakter
- EU-lagstiftningen utvecklas snabbt inom digiområdet 2021–2022 och även därefter
  - Datahantering, artificiell intelligens, digitala tjänster, digitala marknader, chip, dataöverföring...

Utnyttjande i organisationer: öppnad egen riskbild genom jämförelse

- Hur jämförs organisationens egen syn på riskerna med top-10-listan?
  - Täcker den egna riskhanteringen riskerna i fråga?
    - Om riskpåståendena inte exakt stämmer överens med den egna situationen, med vilka förändringar blir de relevanta?
      - Förändring i den egna situationen och verksamheten (inkl. externa krav, reglering, nya funktioner...)
      - Förändring i riskutformningen (t.ex. noggrannare eller mer omfattande inriktning, anpassning till det praktiska genomförandet)
  - Det här är inte alla risker: hur påverkar och relaterar de övriga (digi)riskerna i organisationen till de som presenteras i enkäten – kumulativa effekter och dominoeffekter
    - Exempelvis kan kraven i regleringen belasta juridiska tjänster, men denna belastning kan också komma från andra håll än digital: ärresursfördelningen tillräcklig och tillräckligt djup?
- Hur har man förberett sig på dessa risker, vilka kontrollåtgärder borde vidtas?
  - Var borde man vara om 2–3 år och hur kommer man dit?
  - Hanteringsåtgärderna är inte symmetriska med omfattande risker (se nästa dia)

De åtta viktigaste rekommendationerna i organisationernas enkät om digital säkerhet och deras effekter

En fullständig lista med rekommendationer finns som bilaga till rapporten från Organisationsenkäten på MDB:s webbplats.

Allmän rekommendation: riskhanteringsprocessen tas i aktivt bruk, utveckling av den samt utvidgning till olika aktörer

→Förbättrar allmänt situationen i fråga om olika risker (särskilt: 2, 3, 12, 16, 17, 19, 30, 31, 35)

1. Utveckling av personalens kompetens
   →Förbättrar allmänt situationen i fråga om olika risker (särskilt: 2, 3, 6, 29)
2. Utveckling av och deltagandet i övningsverksamhet
   →Förbättrar allmänt situationen i fråga om olika risker (särskilt: 2, 3, 9, 11, 30, 31)
3. Rapportering till organisationens ledning och ledningen informerar aktivt om läget
   →Förbättrar allmänt situationen i fråga om olika risker (särskilt: 16, 17, 23, 29)
4. Bedömning av riskerna i anslutning till distansanvändning samt omfattande ibruktagande av VPN och MFA
   →Minskar möjliga sannolikheter och effekter (särskilt 2, 3)
5. Säkerhetskopiering, testning av den och övning i återställning
   → Minskar eventuella effekter (särskilt 2, 3)
6. Säkerställande av insamlingen av logguppgifter och ett effektivt utnyttjande av dem
   →Minskar möjliga sannolikheter och effekter (särskilt 2, 3)
7. Uppföljning av hotfulla situationer och verksamhetsmiljön samt riskhantering, inkl. tillsammans med serviceproducenter och samarbetspartner
   → Minskar eventuell sannolikheterna (särskilt 2, 3, 5, 9, 11, 27, 28, 29)
8. Förbättring av tjänsternas feltolerans
   → Minskar eventuella effekter (särskilt 3, 9, 18, 20, 25, 30, 31)

Sammanfattning för mer omfattande utveckling

- **De viktigaste utvecklingsuppgifterna utifrån enkäten och förteckningen över risker**
  - **Riskerna 2 och 3:** Utvecklingen av en enhetlig och delad riskbild som är mer omfattande än de omedelbara hoten bör främjas. Under VAHTI-evenemangen informerar MDB om det externa cyberhotets verklighet och styrmedel under 2022.
  - **Riskerna 25 och 13 (m.fl.):** Det är viktigt att utveckla stödet för en enhetlig kontroll och förståelse på olika nivåer och sätt. MDB utvecklar hur anvisningarna för digital säkerhet kan hittas under 2022.
  - **Insikten i kommunernas riskprofil har fördjupats:** Rätt inriktning och utformning av åtgärder och stöd för att effektivera effekterna. Man strävar efter att bättre beakta och utnyttja JUDO-projektet, i synnerhet i Kommunernas samprojekt under 2022.

Lista över riskpåståenden

Bilaga 1
Resultat från enkäten om risker inom den digitala säkerheten, hösten 2021

MYNDIGHETEN FÖR DIGITALISERING
OCH BEFOLKNINGSDATA

Riskpåståenden som använts i enkäten, 1/3

Risk nr	Riskiväite	Riskpåstående	OECD	WEF	Digital säkerhet
1	Digitaalisen turvallisuuden häiriötilanteiden takia menetetään ihmishenkiä.	Människoliv går förlorade på grund av störningar i den digitala säkerheten.	Nationell och internationell säkerhet	Allvarlig störning i den digitala infrastrukturen	Cybersäkerhet
2	Viranomaisten toimintaan ja palveluihin kohdistuu tahallisia vakavia tietoturvahyökkäyksiä.	Myndigheternas verksamhet och tjänster utsätts avsiktligt för allvarliga datasäkerhetsattacker.	Nationell och internationell säkerhet	Allvarlig störning i den digitala infrastrukturen	Informationssäkerhet
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.	Nationell och internationell säkerhet	Allvarlig störning i den digitala infrastrukturen	Cybersäkerhet
4	Tietovarantojen tietoturva vaarantuu merkittävästi, johtuen keskeisesti kiireestä ja resursointivajeesta.	Datasäkerheten i datalagren äventyras avsevärt på grund av brådska och resursbrist.	Nationell och internationell säkerhet	Försummelse av digital säkerhet	Informationssäkerhet
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.	Nationell och internationell säkerhet	Försummelse av digital säkerhet	Informationssäkerhet
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.	Nationell och internationell säkerhet	Försummelse av digital säkerhet	Informationssäkerhet
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.	Nationell och internationell säkerhet	Koncentration av digitala resurser	Cybersäkerhet
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.	Nationell och internationell säkerhet	Skadlig teknologisk utveckling	Cybersäkerhet
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.	Laglighetsöverv akning	Misslyckad styrning av digital säkerhet	Verksamhetens kontinuitet och beredskap
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.	Laglighetsöverv akning	Försummelse av digital säkerhet	Riskhantering
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.	Laglighetsöverv akning	Försummelse av digital säkerhet	Riskhantering
12	Tiedonhallintayksikkö ei arvioi eikä seuraa digitaalisen turvallisuuden kypsyystasoa.	Informationshanteringsenheten varken bedömer eller följer upp den digitala säkerhetens mognadsnivå.	Laglighetsöverv akning	Misslyckad styrning av digital säkerhet	Riskhantering
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.	Laglighetsöverv akning	Misslyckad styrning av digital säkerhet	Annat mer omfattande tema för digital säkerhet

Riskpåståenden som använts i enkäten, 2/3

Risk nr	Riskiväite	Riskpåstående	OECD	WEF	Digital säkerhet
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.	Laglighetsöverv akning	Skadlig teknologisk utveckling	Dataskydd
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.	Laglighetsöverv akning	Misslyckad styrning av digital säkerhet	Dataskydd
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.	Laglighetsöverv akning	Misslyckad styrning av digital säkerhet	Riskhantering
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.	Laglighetsöverv akning	Misslyckad styrning av digital säkerhet	Riskhantering
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.	Laglighetsöverv akning	Koncentration av digitala resurser	Verksamhetens kontinuitet och beredskap
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.	Ekonomisk och social välfärd	Misslyckad styrning av digital säkerhet	Riskhantering
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.	Ekonomisk och social välfärd	Allvarlig störning i den digitala infrastrukturen	Verksamhetens kontinuitet och beredskap
21	Digitaalisten palveluiden tarjonta ei vastaa kansalaisten tarpeita.	Utbudet av digitala tjänster motsvarar inte medborgarnas behov.	Ekonomisk och social välfärd	Ojämlikhet i den digitala verksamhetsmiljön	Annat bredare tema för digital säkerhet
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.	Ekonomisk och social välfärd	Ojämlikhet i den digitala verksamhetsmiljön	Verksamhetens kontinuitet och beredskap
23	Digitaaliseen turvallisuuteen ei ole kohdennettu riittävästi taloudellisia resursseja.	Den digitala säkerheten har inte tilldelats tillräckliga ekonomiska resurser.	Ekonomisk och social välfärd	Ojämlikhet i den digitala verksamhetsmiljön	Verksamhetens kontinuitet och beredskap
24	Digitaalisen turvallisuuden osaamista ei ole käytettävissä riittävästi.	Kunskapen om den digitala säkerheten är inte tillräcklig.	Ekonomisk och social välfärd	Ojämlikhet i den digitala verksamhetsmiljön	Annat bredare tema för digital säkerhet
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.	Ekonomisk och social välfärd	Misslyckad styrning av digital säkerhet	Cybersäkerhet

Riskpåståenden som använts i enkäten, 3/3

Risk nr	Riskiväite	Riskpåstående	OECD	WEF	Digital säkerhet
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.	Ekonomisk och social välfärd	Skadlig teknologisk utveckling	Dataskydd
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.	Teknik	Skadlig teknologisk utveckling	Informationssäkerhet
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.	Teknik	Misslyckad styrning av digital säkerhet	Verksamhetens kontinuitet och beredskap
29	Digitaalista turvallisuutta ei ymmärretä, arvosteta tai huomioida toiminnan suunnittelussa.	Den digitala säkerheten förstås, uppskattas eller beaktas inte i planeringen av verksamheten.	Teknik	Ojämlikhet i den digitala verksamhetsmiljön	Riskhantering
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.	Teknik	Allvarlig störning i den digitala infrastrukturen	Verksamhetens kontinuitet och beredskap
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.	Teknik	Allvarlig störning i den digitala infrastrukturen	Verksamhetens kontinuitet och beredskap
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.	Teknik	Försummelse av digital säkerhet	Cybersäkerhet
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.	Teknik	Koncentration av digitala resurser	Informationssäkerhet
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.	Teknik	Koncentration av digitala resurser	Informationssäkerhet
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.	Teknik	Koncentration av digitala resurser	Riskhantering
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.	Teknik	Skadlig teknologisk utveckling	Riskhantering

Enligt World Economic Forums kategorier, alla respondenter

Bilaga 2
Resultat från enkäten om risker inom den digitala säkerheten, hösten 2021

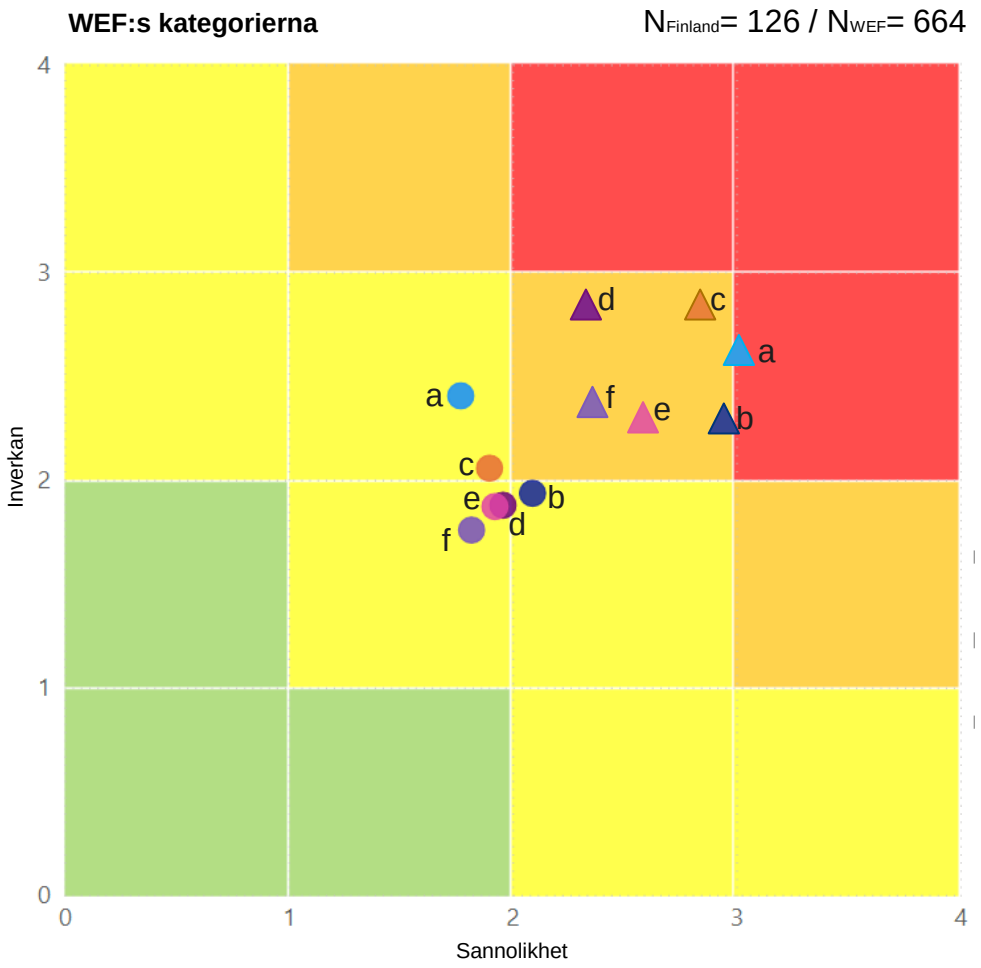
MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

WEF:s riskkategorier

	Riskkategori	Beskrivning
a	Koncentration av digitala resurser	Om digitala resurser och egendom koncentreras till ett fåtal stater eller individer leder det till exempel till en behovsprövad prissättning på marknaden, brist på tillsyn samt en ojämlik ställning i utnyttjandet av data.
b	Ojämlikhet i den digitala verksamhetsmiljön	Individernas användning av teknik samt tillgång till datanät varierar mellan de olika länderna och inom enskilda länder. Detta beror på att investeringarna sker vid olika tidpunkter, på bristen på kompetens och förståelse hos personer i arbetsför ålder samt på marknadens mognad och politiska begränsningar.
c	Försummelse av cybersäkerheten	Föråldrade eller ouppdaterade element inom hushållens, företagens och samfundens digitala säkerhet samt inom den offentliga förvaltningen hindrar inte attacker. Detta leder till betydande kostnader och förluster och skapar politiska spänningar och instabilitet i samhället.
d	Allvarlig störning i den digitala infrastrukturen	Avbrott eller försämring av den kritiska infrastruktur som krävs för digitala tjänster och tjänster i anslutning till upprätthållandet av den på grund av tekniskt beroende av nätverk eller teknik: system som kräver artificiell intelligens, Internet, tjänster i allmänhetens intresse, satelliter osv.
e	Misslyckad styrning av digital säkerhet	På grund av bristen på globala standarder och referensramar tar staterna i bruk teknik som inte är kompatibel med andra länder.
f	Skadlig teknologisk utveckling	Avsiktliga eller oavsiktliga negativa konsekvenser av den tekniska utvecklingen för individer, företag, ekosystem och/eller ekonomi: artificiell intelligens, gränssnitt mellan hjärna och dator, bioteknik, geoteknik, kvantberäkning osv.

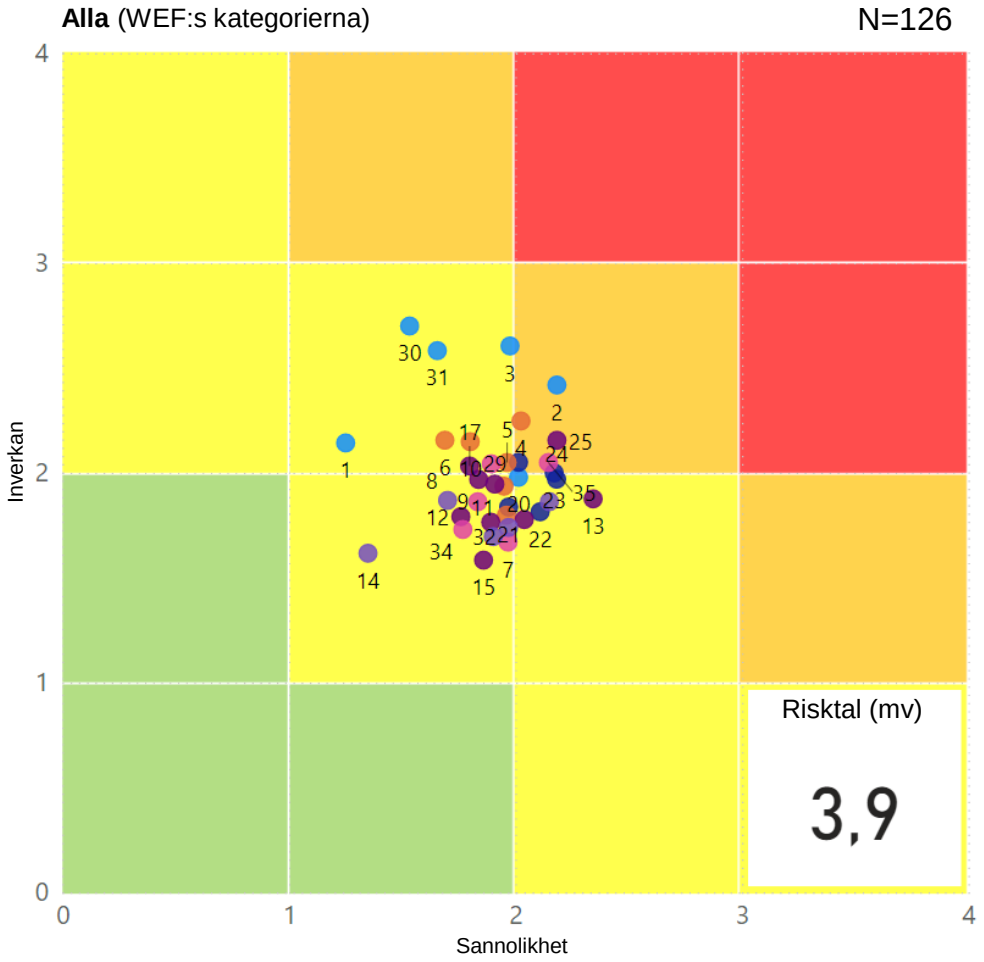
Källa: https://www.weforum.org/reports/the-global-risks-report-2021 (bland annat s.89, 11-12, 47, 29-37)

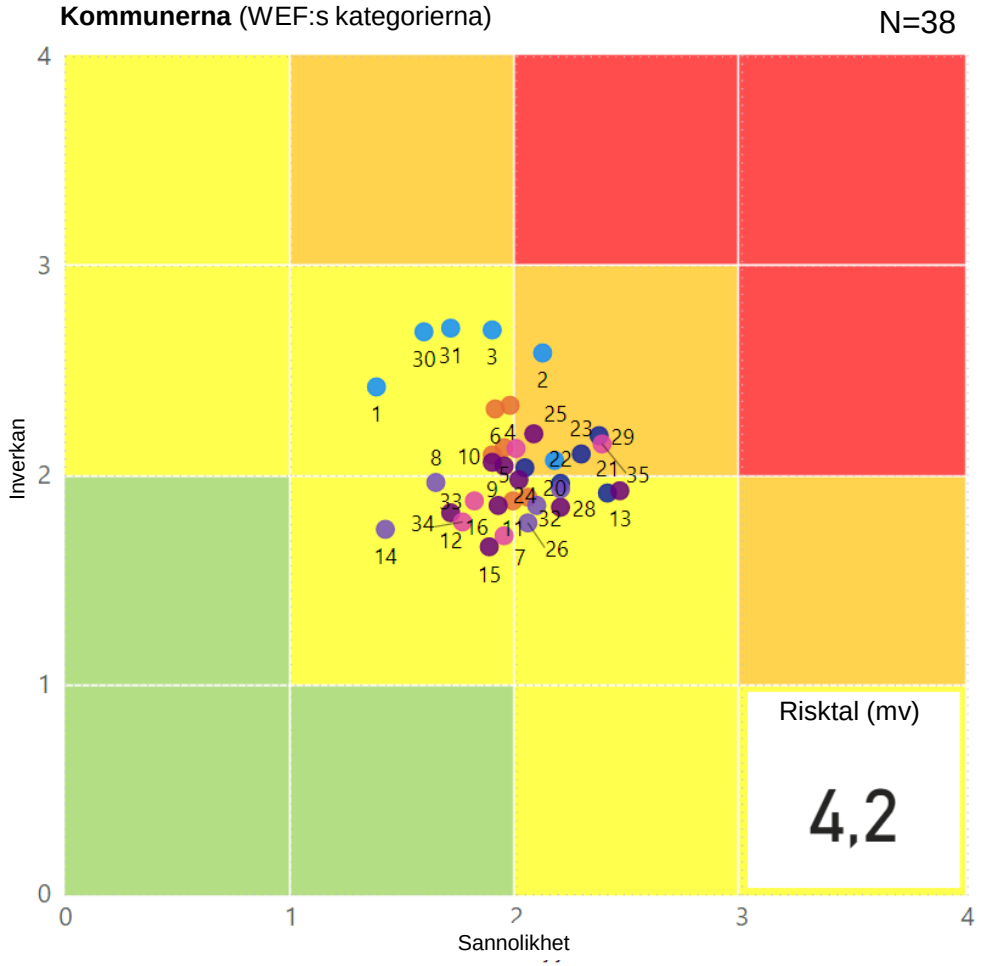
Riskenkätens resultat – jämförelse med den globala visionen mellan WEF-kategorierna



- Jämförelse mellan åsikterna i riskenkäten och motsvarande riskmatris för World Economic Forum, där man bedömer den globala utvecklingen med ett tidsperspektiv på 10 år (tre år i riskenkäten)
- Riskenkätens värden markerade med cirklar, WEF-undersökningens värden med triangel:
  a. Koncentration av digitala resurser
  b. Ojämlikhet i den digitala verksamhetsmiljön
  c. Försummelse av cybersäkerheten
  d. Allvarlig störning i den digitala infrastrukturen
  e. Misslyckad styrning av digital säkerhet
  f. Skadlig teknologisk utveckling
- WEF:s kluster har klart högre värden och betydande skillnader i kategorierna a och c jämfört med vyerna från Finland
- Värdena är endast riktgivande på grund av de metodologiska skillnaderna, såsom tidsperspektivet
  - WEF-undersökning från 2020, publicerad i rapport 2021 (s. 12)

Riskenkätens resultat – klassificering enligt WEF-rubrikerna, alla och jämförelse av kommunerna





Alla svarande
Enligt OECD:s klassificering av delområden inom digital säkerhet

Bilaga 3
Resultat från enkäten om risker inom den digitala säkerheten, hösten 2021

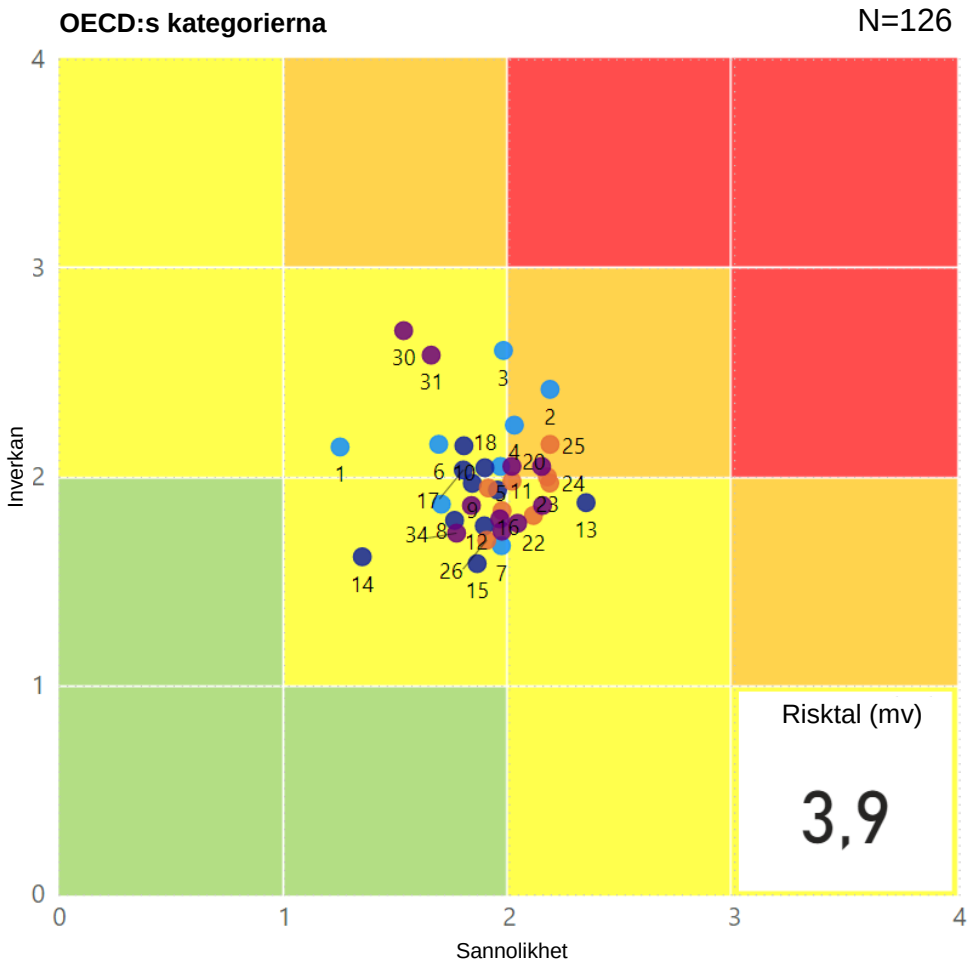
MYNDIGHETEN FÖR DIGITALISERING
OCH BEFOLKNINGSDATA

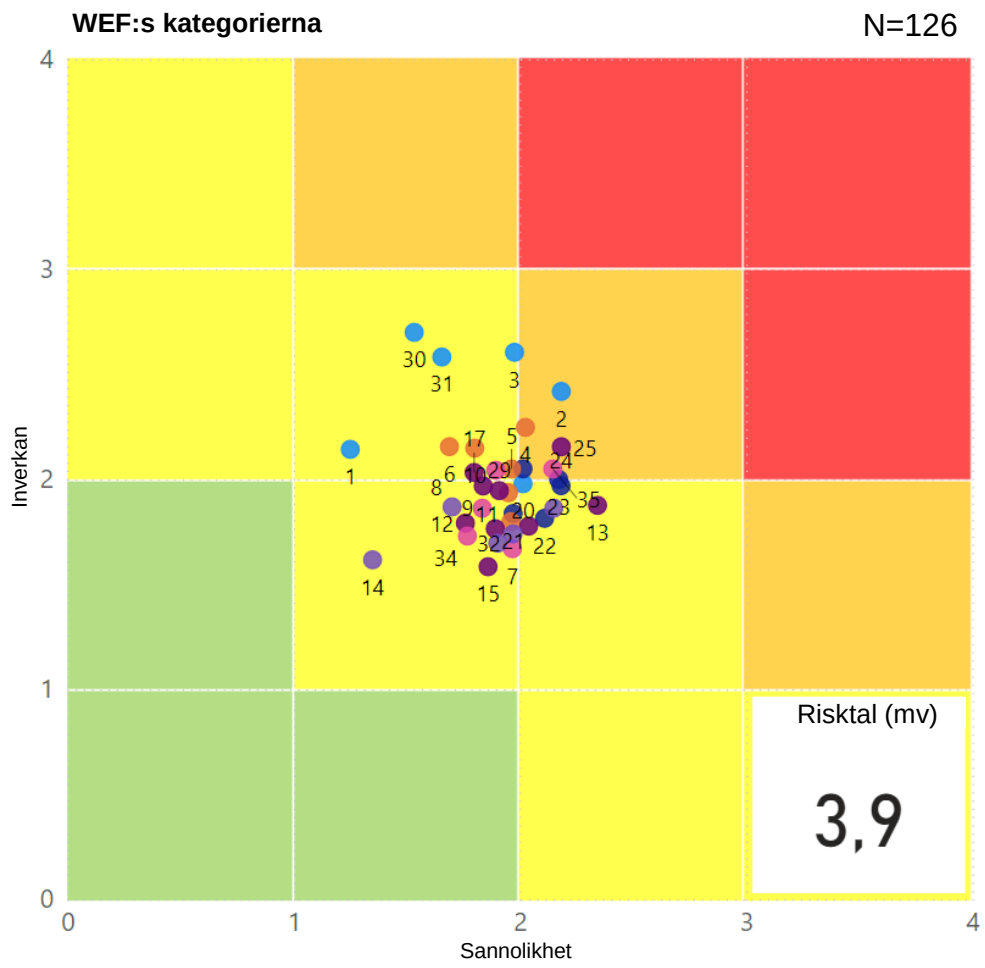
OECD:s klassificering av den digitala säkerhetens delområden

Enligt OECD: *Man kan närma sig digital säkerhet ur åtminstone fyra olika synvinklar, av vilka var och en har sin egen kultur och bakgrund, sin etablerade praxis och mål:*

- ***teknik*** *dvs. fokus på den digitala miljöns funktion (experterna använder ofta orden "informationssäkerhet" eller "nätverkssäkerhet")*
- ***laglighetsövervakning*** *och de juridiska aspekterna i vidare bemärkelse (t.ex. it-brottslighet)*
- ***nationell och internationell säkerhet*** *som omfattar bl.a. informations- och kommunikationsteknikernas roll i underrättelseverksamhet, konfliktbekämpning, krig osv.*
- ***ekonomisk och social välfärd*** *som omfattar skapande av välstånd, innovationsverksamhet, tillväxt, konkurrenskraft och sysselsättning inom alla ekonomiska delområden, samt olika aspekter såsom individuella friheter, hälsa, utbildning, kultur, demokratiskt deltagande, vetenskap, fritid och andra välfärdsdimensioner där den digitala miljön fungerar som drivkraft för utvecklingen.*

Riskenkätens resultat – jämförelse av OECD och WEF, alla svarande





Alla svarande
Enligt den digitala säkerhetens genomförandestruktur samt kategorin "övriga”

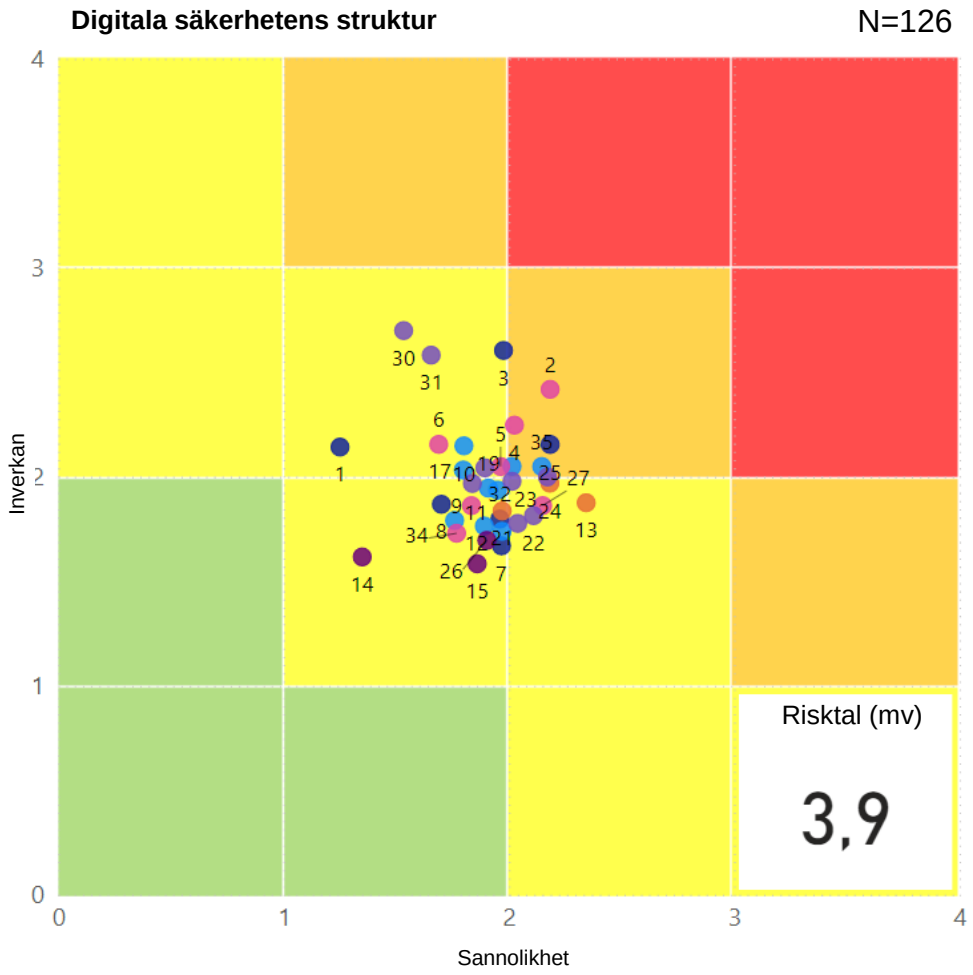
Bilaga 4
Resultat från enkäten om risker inom den digitala säkerheten, hösten 2021

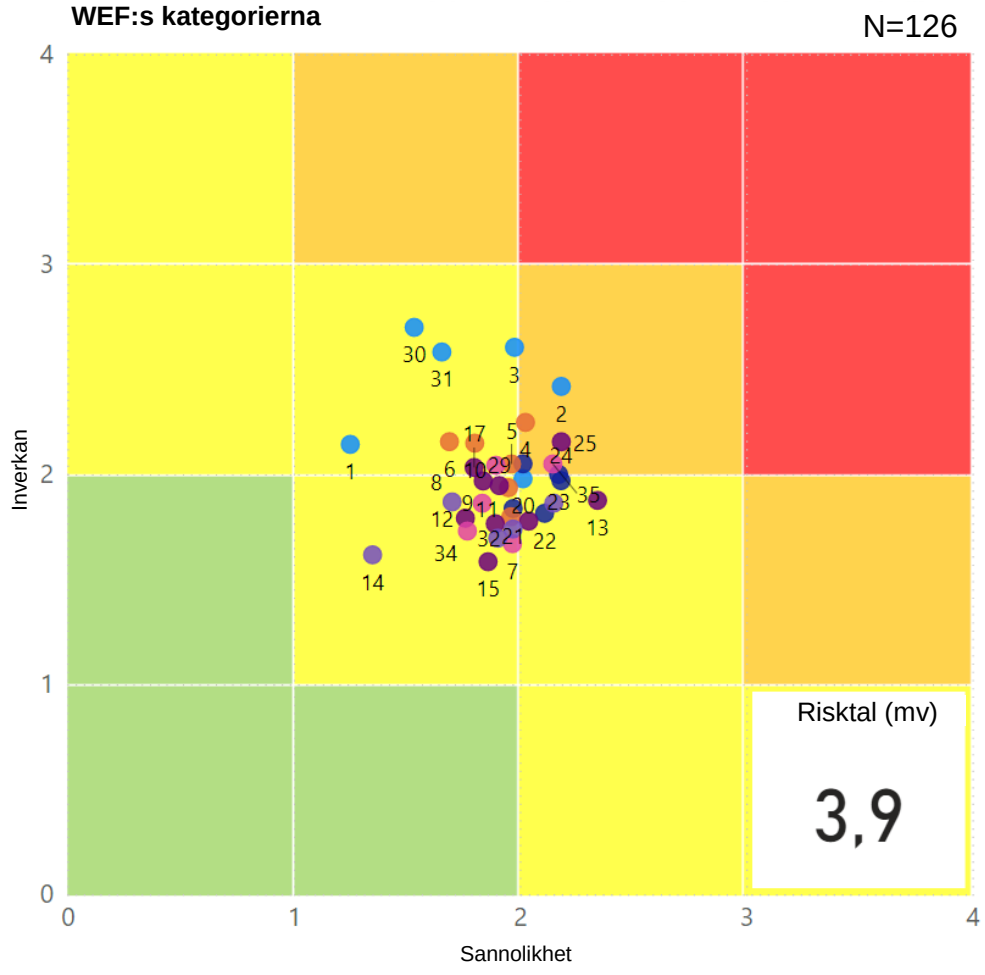
MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

Delområdena i den digitala säkerhetens genomförandestruktur som klassificering

1. **Ledning och riskhantering**
2. **Dataskydd**
3. **Informationssäkerhet**
4. **Kontinuitetshantering**
5. **Cybersäkerhet**
6. **Andra mer omfattande teman för digital säkerhet** inklusive frågor som påverkar den digitala säkerheten och som inte ingår i ovan nämnda områden för digital säkerhet

Riskenkätens resultat – jämförelse av den digitala säkerhetens struktur och WEF, alla svarande





MYNDIGHETEN FÖR DIGITALISERING
OCH BEFOLKNINGSDATA

dvv.fi