LIITE 4

STRATEGIA 22

Digi- ja kyberturvallisuuden huomioiminen yrityksen eri strategioissa 2021

KYSELYTUTKIMUKSEN TULOKSET

Vaihe 2
23.10.2021

Huopalahdentie 24 I 00350 HELSINKI I FINLAND I www.cyberwatchfinland.fi

Sisällys

Tutkimuksen toteutus

Kysymyspatteri:	9 taustakysymystä ja 56 varsinaista kysymystä 4 osa-alueeseen jaettuna
Kyselyalusta:	LimeSurvey
Vastausmäärä:	69 kappaletta
Vastausaika:	9.9.- 15.10.2021

Yrityksen ja sen strategisen toiminnan suhde strategiaprosessiin, summamuuttujat

	Toimenpiteiden nykytilanne	Strategiatyön lähtökohdat	Strategiatyö	Toimeenpano ja mittaaminen
Strategiset tavoitteet Kyberturvallisuus		**1,2,3,4,5,12**	**4,5,6**	
Strategioiden toteutumisen turvaaminen 1. Strategiatyöskentely 2. Kyberriskianalyysi 3. Valvonta, viestintä, koulutus 4. Operatiivisen toiminnan johtaminen	1,2,3,12,13,14	6,7,8	1,2,3,7,9	2,3,8,10
Ympäristöanalyysit Tilannekuva: makrotaso, toimiala, asiakas, toimitusketju, kilpailu	4,5,6,7	11,13,14	8	4
Sisäisen tehokkuuden analyysi 1. Organisaatio 2. Toiminnot ja prosessit 3. Talous	8,9,10,11,16,17	9,10		1,5,6,7,9,11,12

Painopiste

Johtopäätökset 1

Johtopäätökset 2

Tukevat

Johtopäätökset 3

Johtopäätökset 4

Yrityksen strategiset tavoitteet

Positiivista olemassa olevaa:

Yrityksen kokonaistoiminnan näkökulmasta tuotanto- ja palvelutoiminnalle on asetettu tehokkuustavoitteet sekä tuotteille ja palveluille digiturvallisuustavoitteita.

Yrityksen strategiassa (tai vastaavassa) on asetettu keskeiset tavoitteet turvallisuuden osatekijöille pl. kyberturvallisuus.

Kehitettävää jatkossa:

- Yrityksen digitalisaatioon liittyvät mahdollisuudet ja menestystekijät.
- Digiturvallisuudelle asetetut taloudelliset tavoitteet.
- Kyberturvallisuuden tehokkuusvaatimukset (kustannus - vaikuttavuus).

Yrityksen strategioiden toteutumisen turvaaminen

Positiivista olemassa olevaa:

Yrityksillä on säännöllinen ja toimiva strategiaprosessi tai toimintamalli yrityksen strategian (tai vastaavan tason ohjauksen) laatimiseen. Yrityksillä on johdon hyväksymät, toimintaan sovitetut riskienhallinnan linjaukset, vastuut ja prosessi. Yrityksen strategian (tai vastaavan) laatimisesta vastaa yleisimmin toimitusjohtaja / johtoryhmä.

Yleisesti voidaan todeta, että yrityksillä tehtävät ja vastuut ovat selkeät myös poikkeustilanteissa ja poikkeusoloissa. Yrityksillä on toteuttamiskelpoinen varautumisen ja jatkuvuuden hallinnan suunnitelma, sekä näihin liittyvä häiriö- ja kriisitilanteiden viestintäsuunnitelma.

Yrityksen johto on sitoutunut digitaalisen turvallisuuden kehittämiseen. Toimeenpanoon käytetään johdon hyväksymää tietoturvapolitiikkaa tai vastaava tietoturvallisuuden toteuttamista ohjaavaa asiakirjaa. Yrityksellä on olemassa käyttövaltuuspolitiikka ja prosessi käyttövaltuuksien hallintaan.

Strategiatyössä on määritelty viestinnän linjaukset ja avoimuusperiaatteet mahdollisen kriisitilanteen varalta. Yrityksissä viestitään digiturvallisuuden riskitilanteesta ja uusista riskeistä koko yrityksen laajuisesti.

Kehitettävää jatkossa:

- strategiatyön laadinnassa tulisi käyttää standardoitua tai muuta vastaavaa menettelyä.
- yksittäisillä yrityksellä ei ole kykyä arvioida riittävä resurssointi ja budjetti digi- ja kyberturvallisuuteen.
- tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja ei tehdä säännöllisesti.

Yrityksen ympäristöanalyysit

Positiivista olemassa olevaa:

Kyselyn perusteella voidaan todeta, että yritykset tekevät digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt (kyberturvallisuus), toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen.

Yritykset kartoittavat digitaalista turvallisuutta ohjaavaa lainsäädäntöä ja tunnistavat siitä aiheutuvat velvoitteet. Samoin kartoitetaan keskeiset sidos- ja asiakasryhmät sekä niiltä tulevat digiturvavaatimukset.

Yrityksessä on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten yritysten tai yhteiskunnan toimintaan. Yrityksellä on menettely, jolla se seuraa toimintaympäristössä tapahtuvia ilmiöitä ja arvioi niiden vaikutusta yrityksen toimintaan.

Kehitettävää PK-yritysten ja pienempien osalta

- menettely, jolla voidaan tunnistaa yrityksen digitalisaatioon liittyvät uhkatekijät.
- kyberturvallisuuskatsauksien (tilannekuva) hyödyntäminen strategisessa suunnittelussa.

Yrityksen sisäisen tehokkuuden analyysi

Positiivista olemassa olevaa:

Vastausten mukaan yrityksillä on riittävästi osaavaa henkilöstöä kyberturvallisuuden eri osa-alueilla. Heillä on riittävät resurssit ja osaaminen digitaalisen turvallisuuden ylläpitoon ja kehittämiseen osana yrityksen prosesseja, toimintamalleja ja järjestelmiä.

Yrityksen digitaalisen turvallisuuden osa-alueita kehitetään järjestelmällisesti hyödyntäen yhtä tai useampaa selkeää prosessia tai hallintamallia. Yrityksissä kehitetään riskienhallintaprosessia riskienhallinnan tavoitteiden tai saatujen kokemusten perusteella. Yrityksillä on kyky valita toiminnan edellyttämät kyberturvalliset teknologiat. Yrityksessä tietoturvasta ja tietosuojasta huolehtiminen on muuttunut toiminnaksi, kulttuuriksi ja asenteeksi.

Tietoturva- ja tietosuojavaatimukset ovat osa hankintavaatimuksia ja sopimuksia. Kriittisten toimittajien ja alihankkijoiden kanssa käsitellään digiturvallisuutta säännöllisesti toimittaja/palvelunhallintakokouksissa, (toimitusketjun hallinta). Yrityksellä on prosessi ja valmiudet nopeaan ja tehokkaaseen digiturvallisuuden häiriöiden, uhkien ja poikkeamien käsittelyyn. Digitaalisen turvallisuuden kokonaistilanteesta raportoidaan säännöllisesti yrityksen johdolle.

Kehitettävää PK-yritysten ja pienempien osalta

- digitaaliseen turvallisuuteen liittyvien mittareiden määrittäminen
- auditointien säännöllistäminen tietoturvallisuuteen ja tietojärjestelmiin.
- harjoitustoiminta säännölliseksi toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista varten.

Kyselytutkimuksen johtopäätökset

Toimintasuosituksien kehittämisessä huomioitava erityisesti

- Strategiatyön vakiointi suuryrityksistä pienempiin, standardit ja/tai vastaavat menettelyt.
- Toimintaympäristön seuranta, PK-yritysten ja pienempien kybertilannekuvan sisältö ja laatu.
- Digiturvallisuustavoitteet ja menestystekijät osaksi tuotteita ja palveluita
- Digiturvallisuudelle taloudelliset/tehokkuus tavoitteet/vaatimukset
- Riskien hallinnan ja jatkuvuuden kehittämiseen, resilienssin kasvattamiseen, digitaalisen turvallisuuden mittarit.
- Digitaalisen turvallisuuden yhteistoiminnan kehittäminen, toimitusketjut
- Viestinnän ja harjoittelun kehittäminen poikkeustilanteisiin liittyen

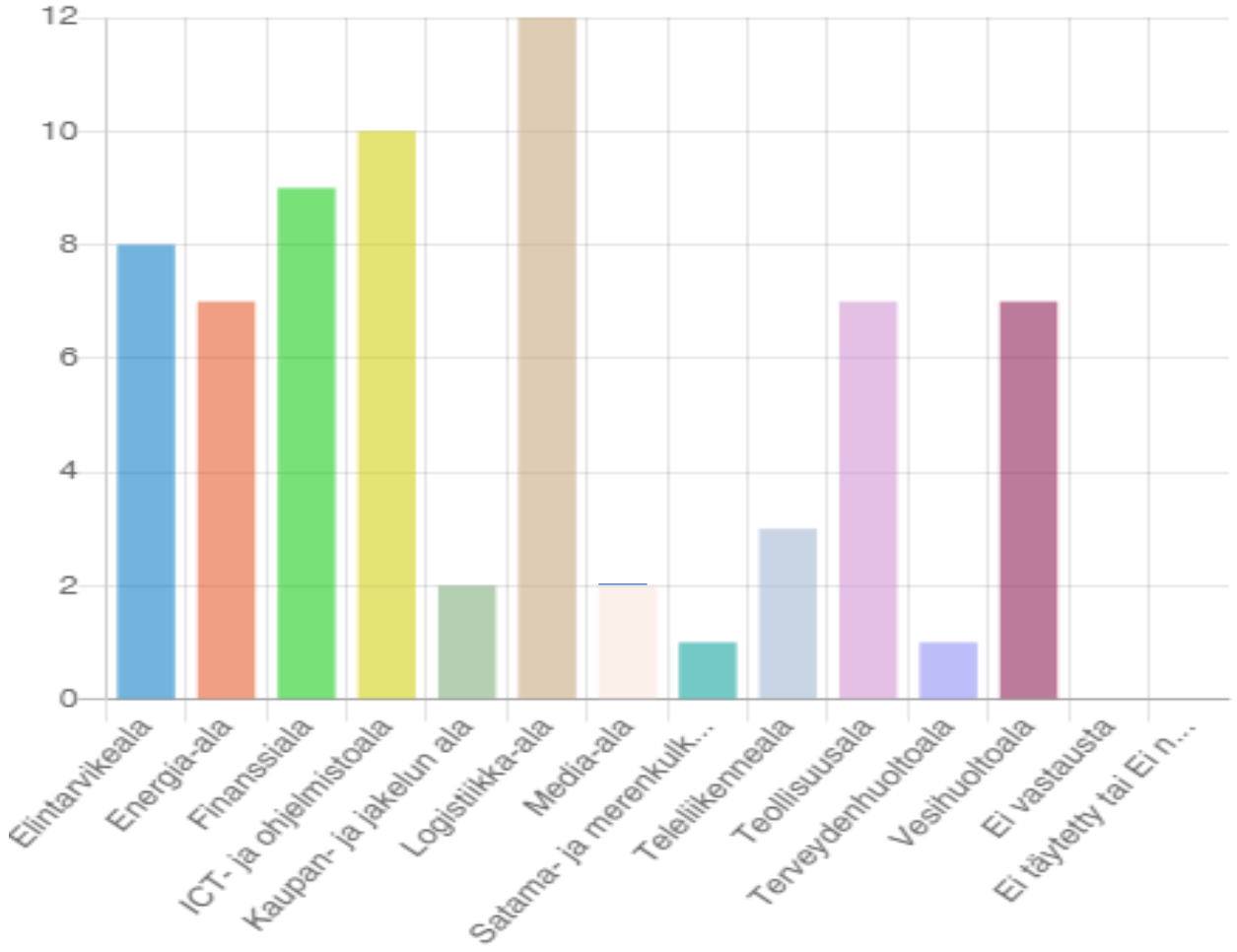
Kyselyn vastaukset kysymyksittäin

N = 69

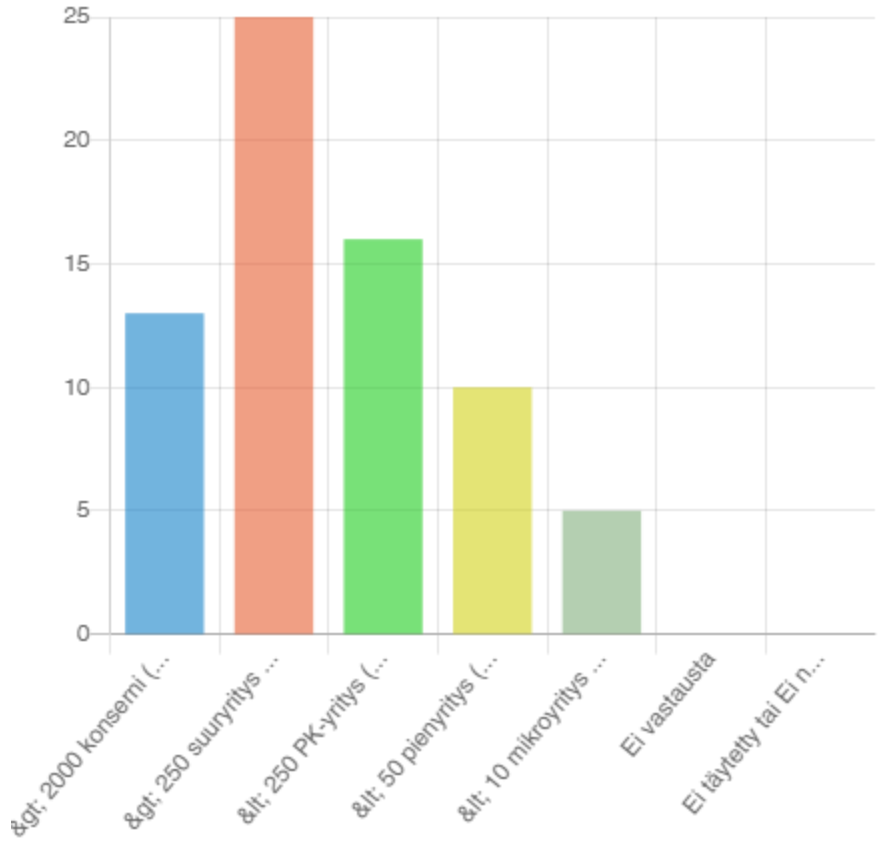
Koottu 17.10.2021

HUOM! Dioissa graafien asteikot vaihtelevat.

4. Yrityksen toimiala

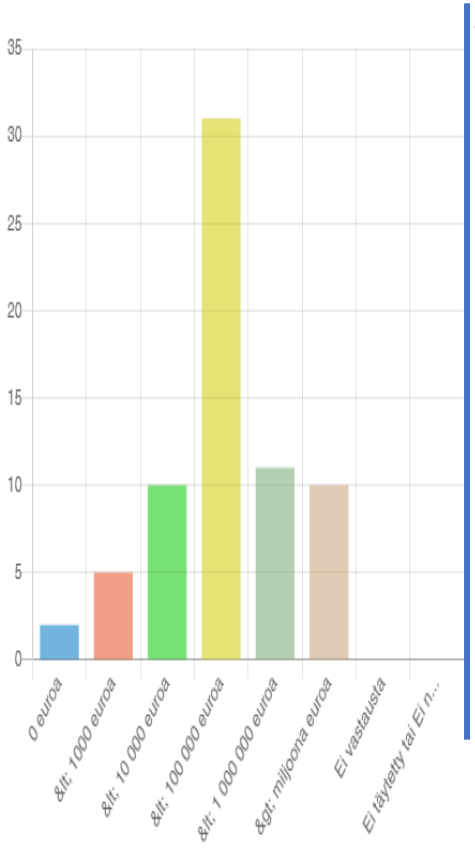


5. Mikä on yrityksen koko henkilöstön ja/tai liikevaihdon määrän mukaisesti?

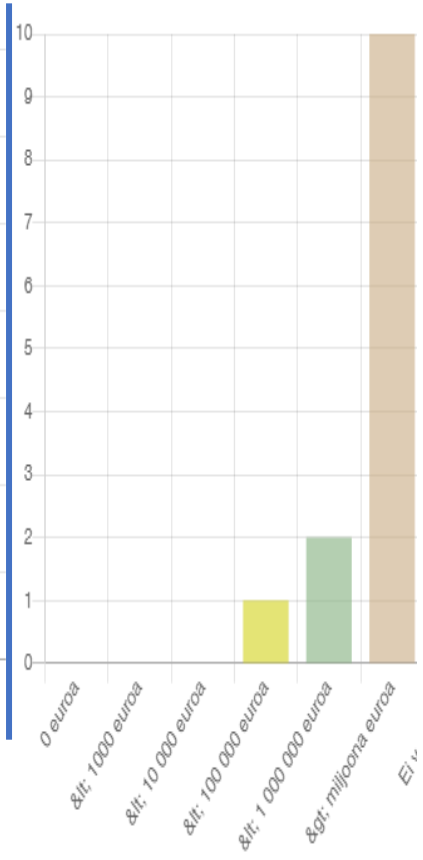


6. Kuinka paljon ovat olleet digitaalisen turvallisuuden kehittämis- ja ylläpitokustannukset vuonna 2020, arviotarkkuus riittää?

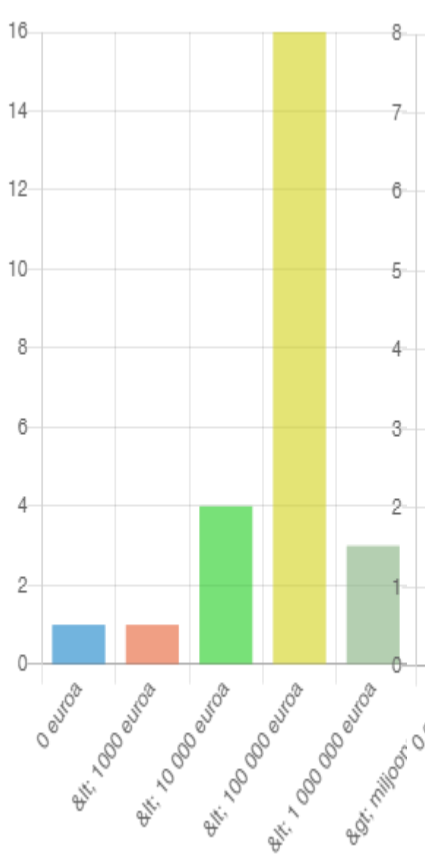
Kaikki



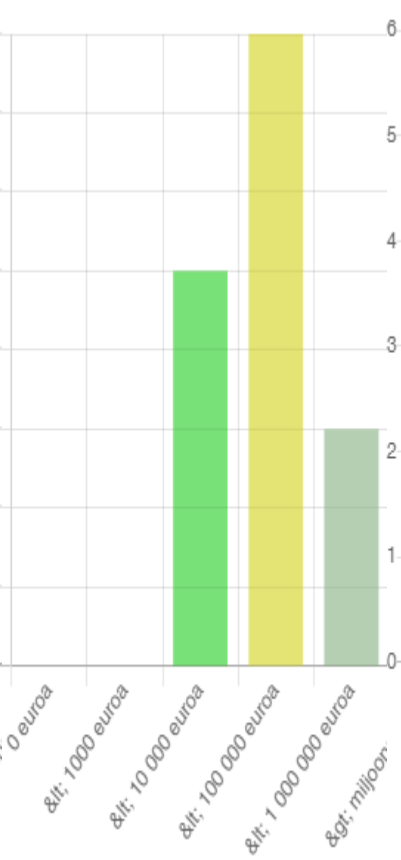
Konserni



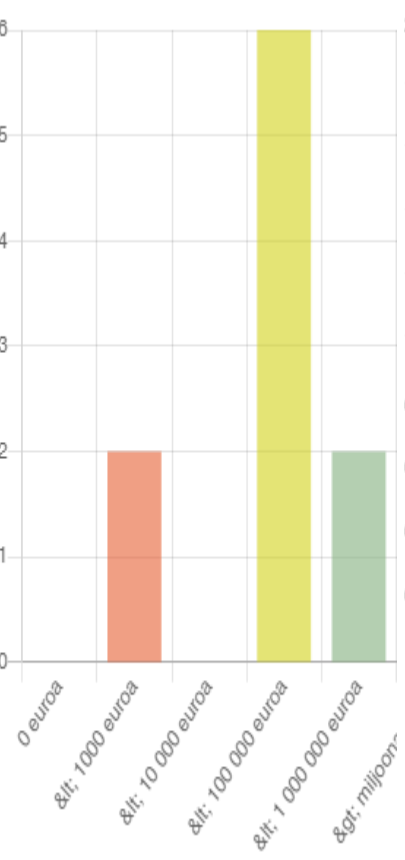
Suuryritys



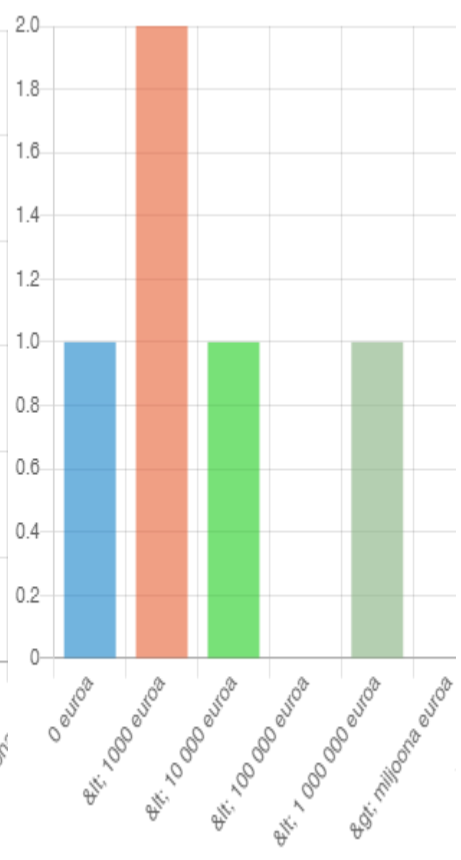
PK-yritys



Pienyritys

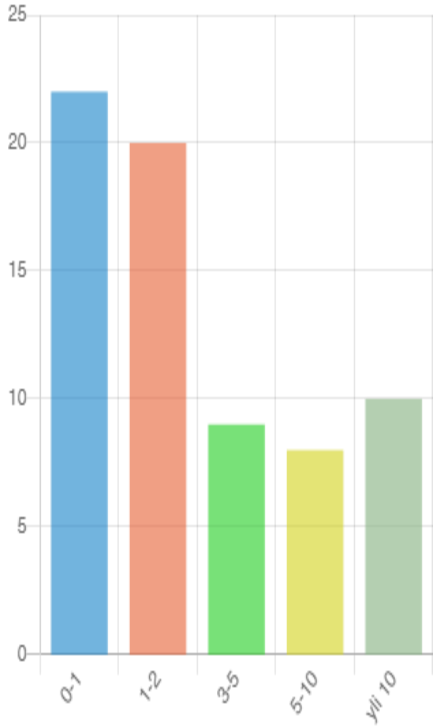


Mikroyritys

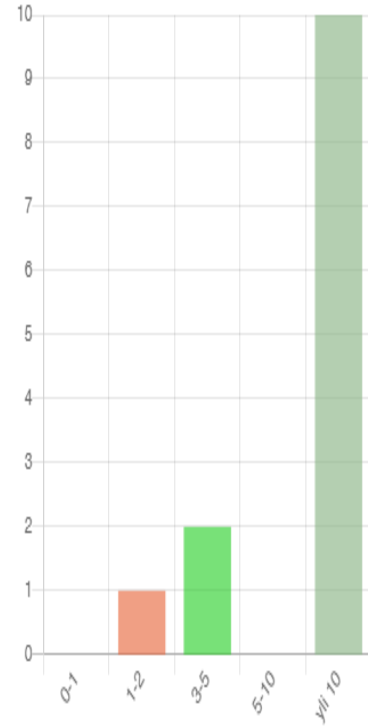


7. Mikä on yrityksen käyttämä henkilötyövuosimäärä (htv) omien ja ulkoisten henkilöiden digiturvatehtäviin vuonna 2020 (riskienhallinta, jatkuvuus ja valmius, tietoturva, kyberturva, tietosuoja), arviotarkkuus riittää?

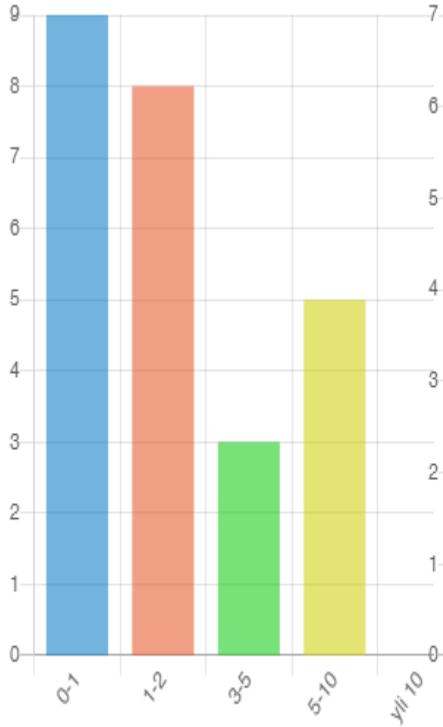
Kaikki



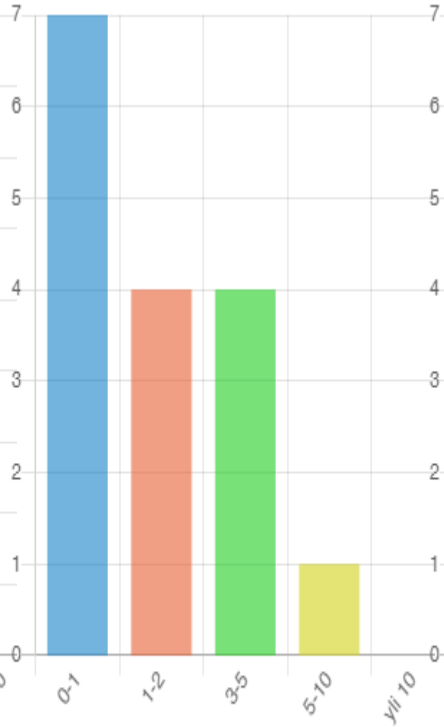
Konserni



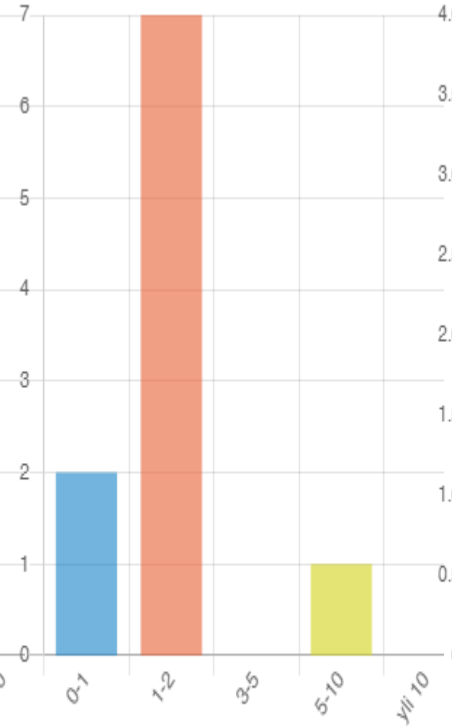
Suuryritys



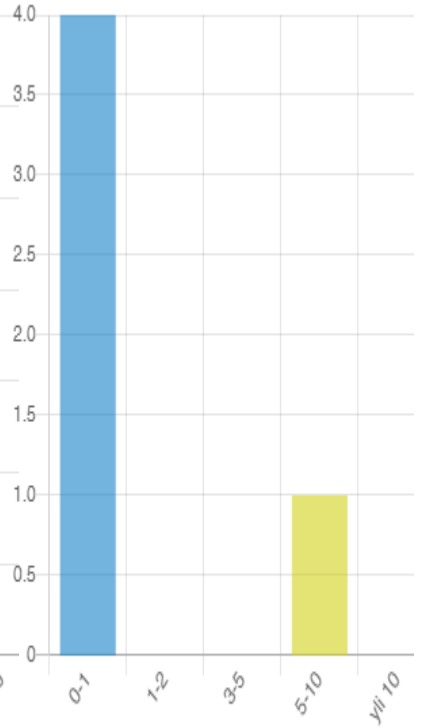
PK-yritys



Pienyritys



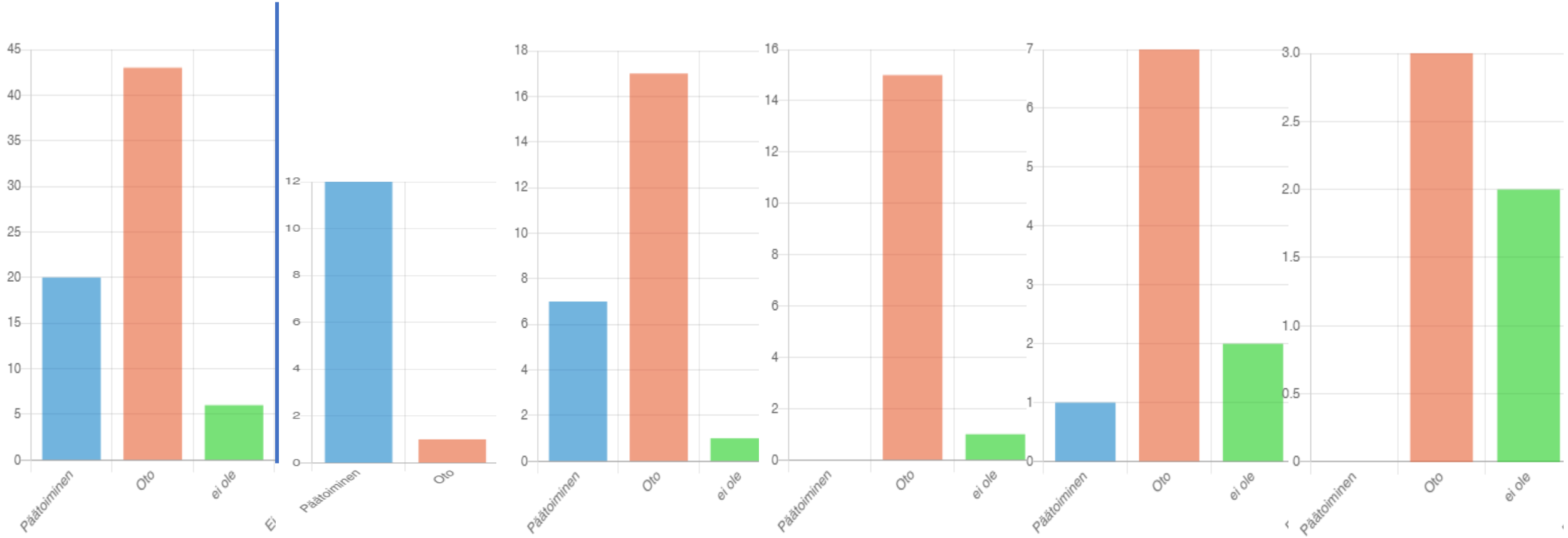
Mikroyritys



8. Onko yrityksessä vähintään yksi päätoiminen/oto henkilö seuraavilla digiturvallisuuden osa-alueilla?

Riskienhallinta

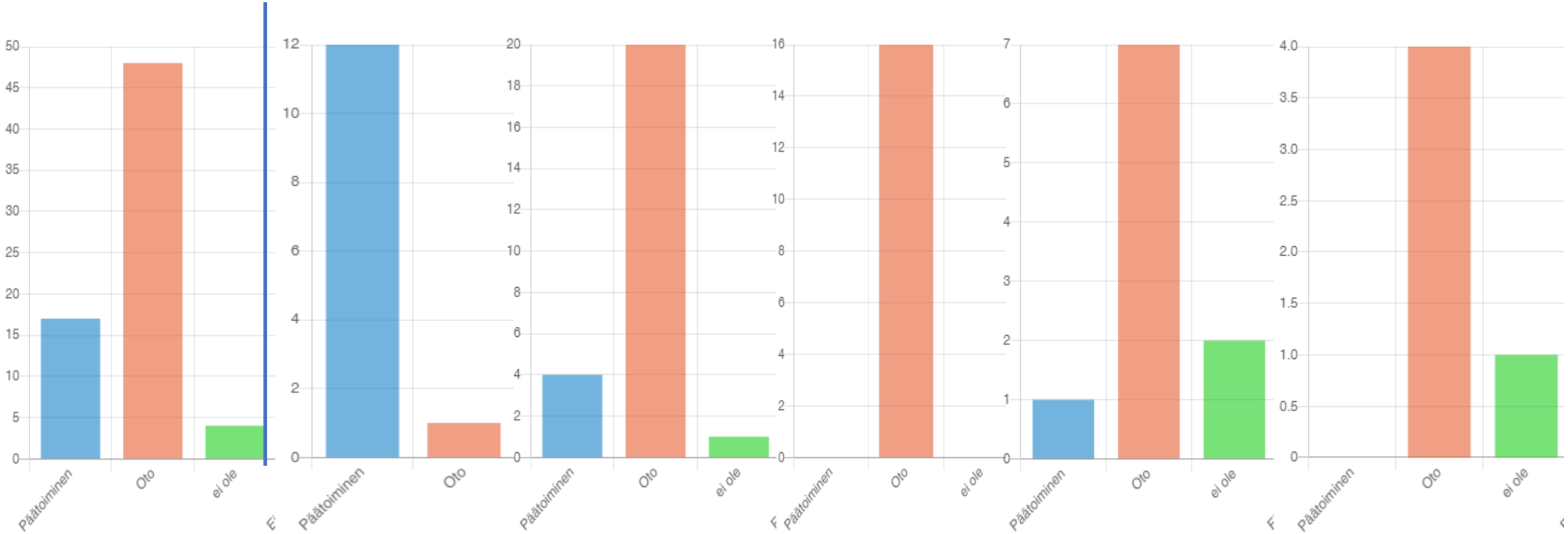
Kaikki | Konserni | Suuryritys | PK-yritys | Pienyritys | Mikroyritys



8. Onko yrityksessä vähintään yksi päätoiminen/oto henkilö seuraavilla digiturvallisuuden osa-alueilla?

Jatkuvuus ja varautuminen

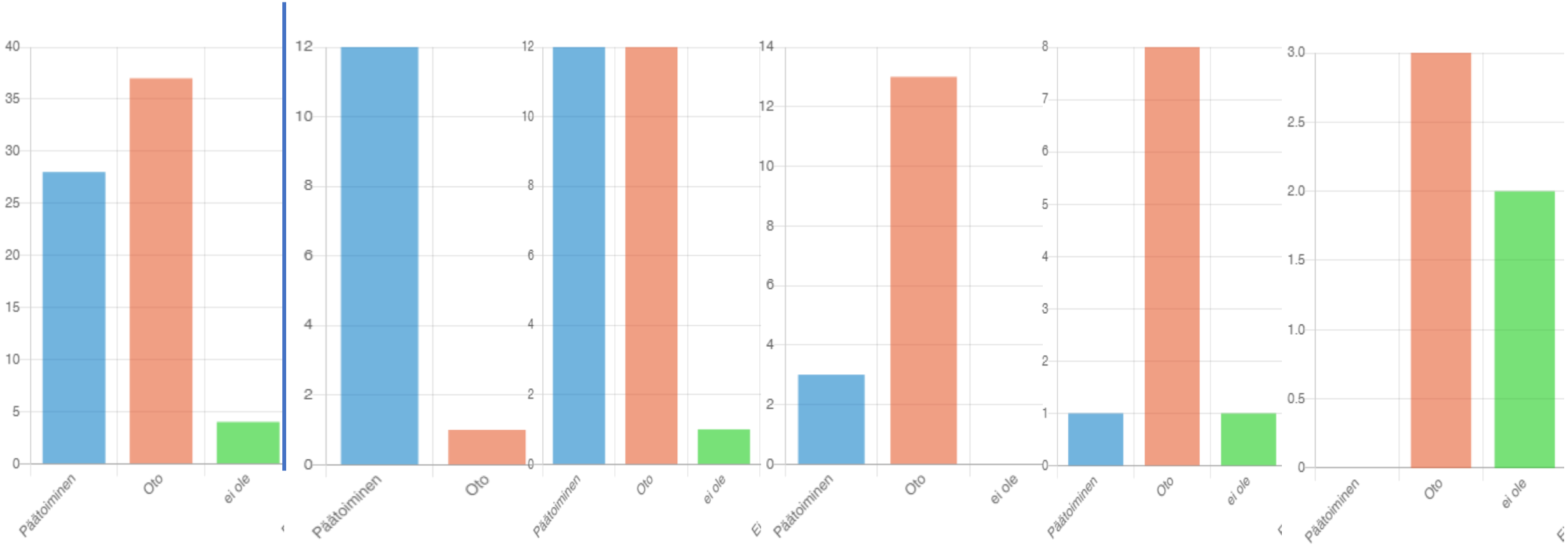
Kaikki | Konserni | Suuryritys | PK-yritys | Pienyritys | Mikroyritys



8. Onko yrityksessä vähintään yksi päätoiminen/oto henkilö seuraavilla digiturvallisuuden osa-alueilla?

Tietoturvallisuus

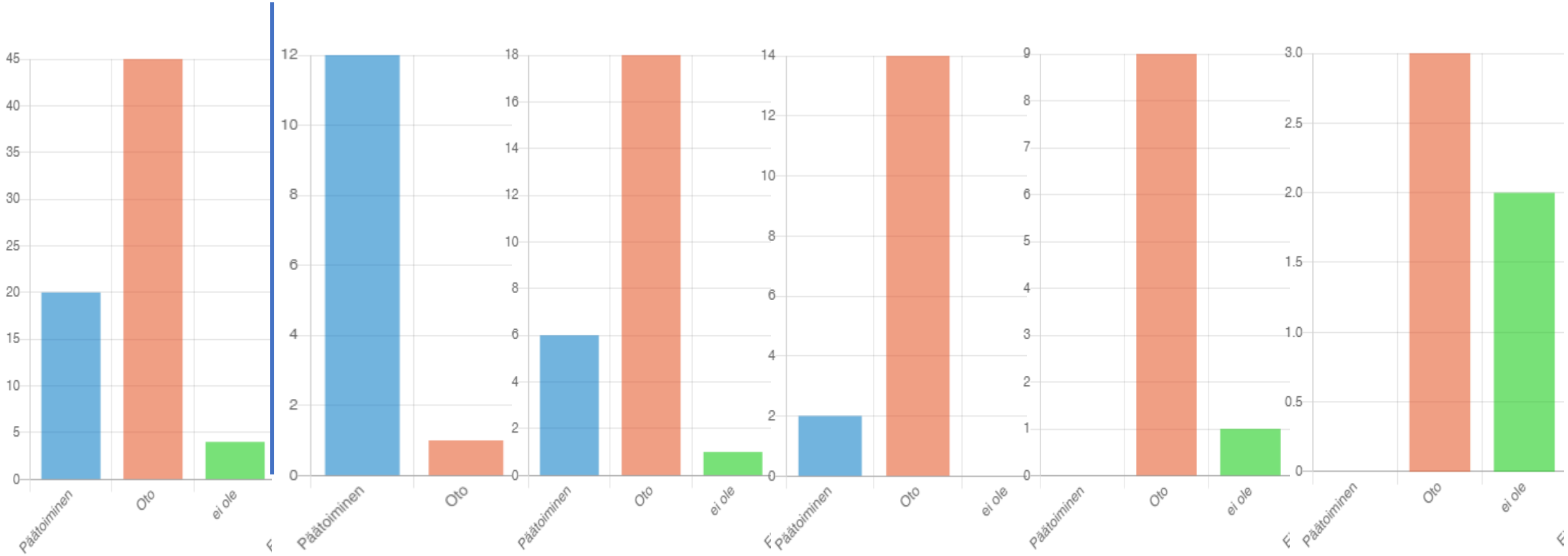
Kaikki | Konserni | Suuryritys | PK-yritys | Pienyritys | Mikroyritys



8. Onko yrityksessä vähintään yksi päätoiminen/oto henkilö seuraavilla digiturvallisuuden osa-alueilla?

Tietosuoja

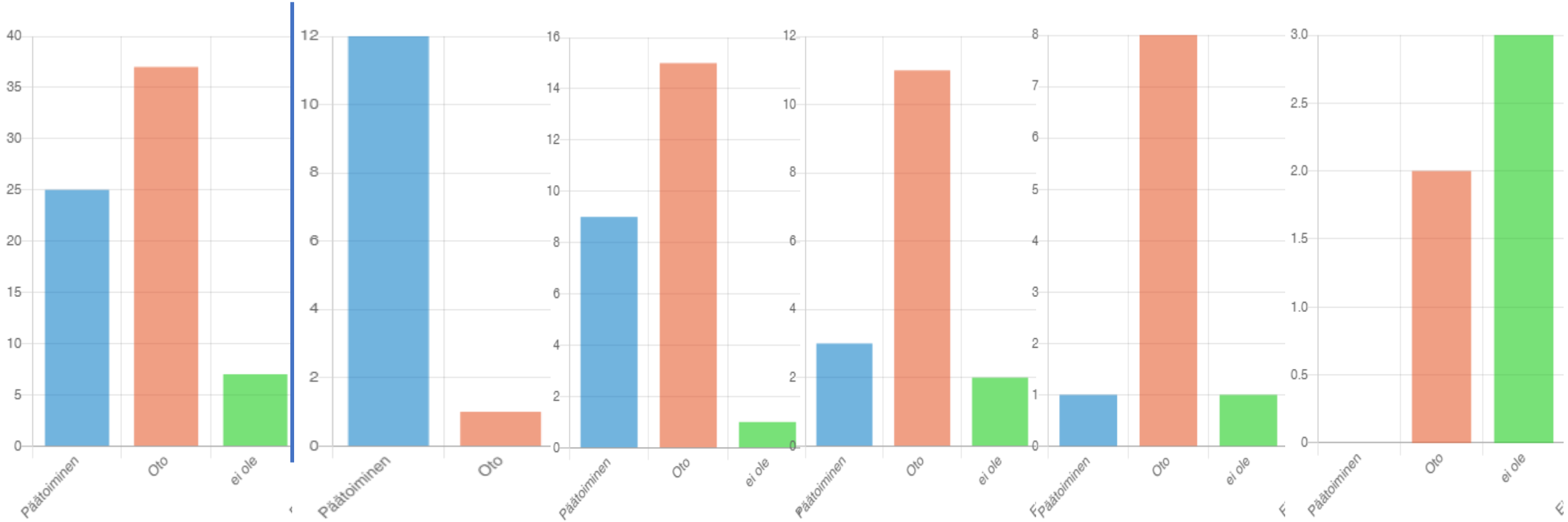
Kaikki | Konserni | Suuryritys | PK-yritys | Pienyritys | Mikroyritys



8. Onko yrityksessä vähintään yksi päätoiminen/oto henkilö seuraavilla digiturvallisuuden osa-alueilla?

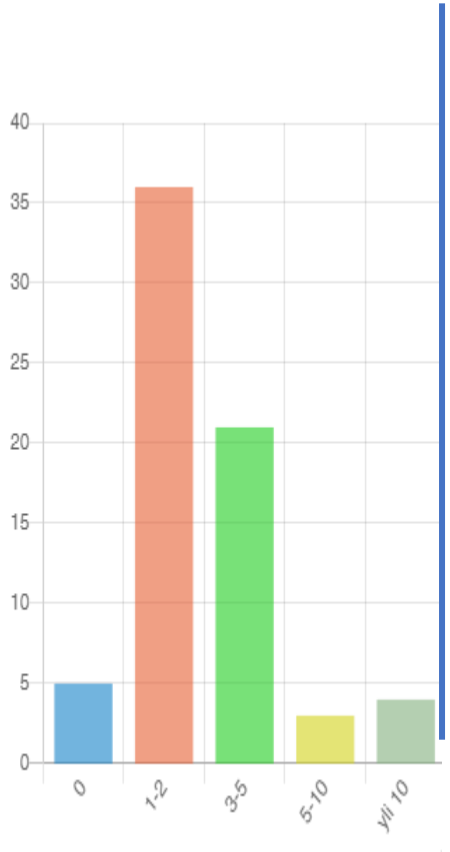
Kyberturvallisuus

Kaikki | Konserni | Suuryritys | PK-yritys | Pienyritys | Mikroyritys

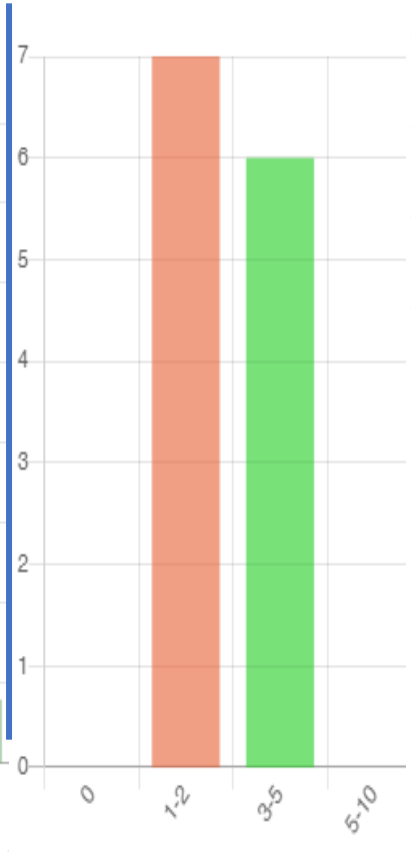


9. Kuinka monta tuntia digitaalisen turvallisuuden koulutusta yrityksen henkilöstö on keskimäärin saanut vuonna 2020 (tuntia/henkilö), arviotarkkuus riittää?

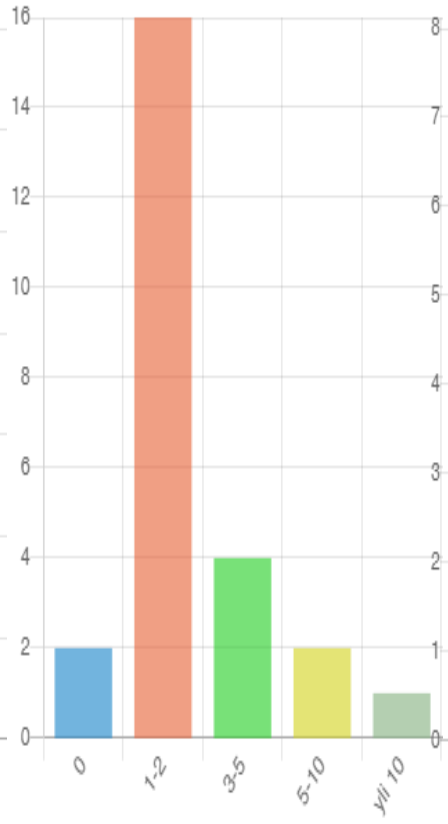
Kaikki



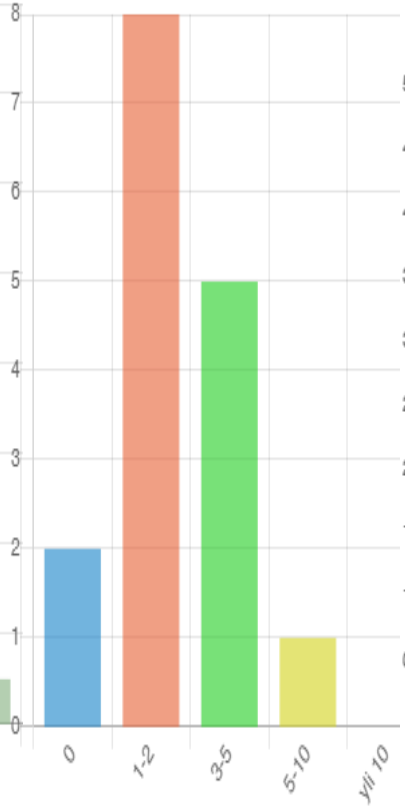
Konserni



Suuryritys

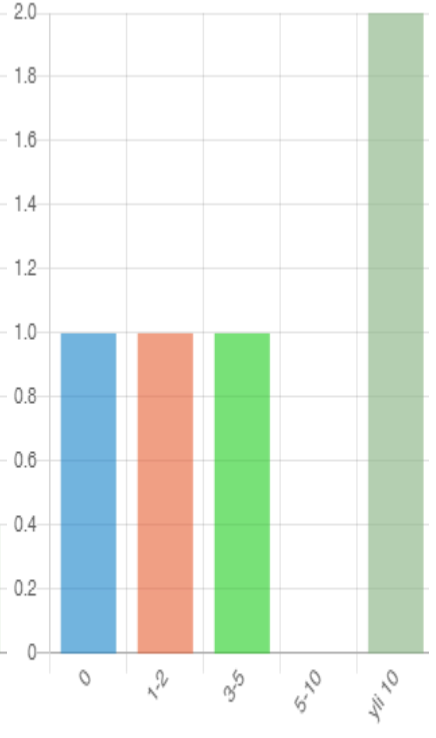


PK-yritys

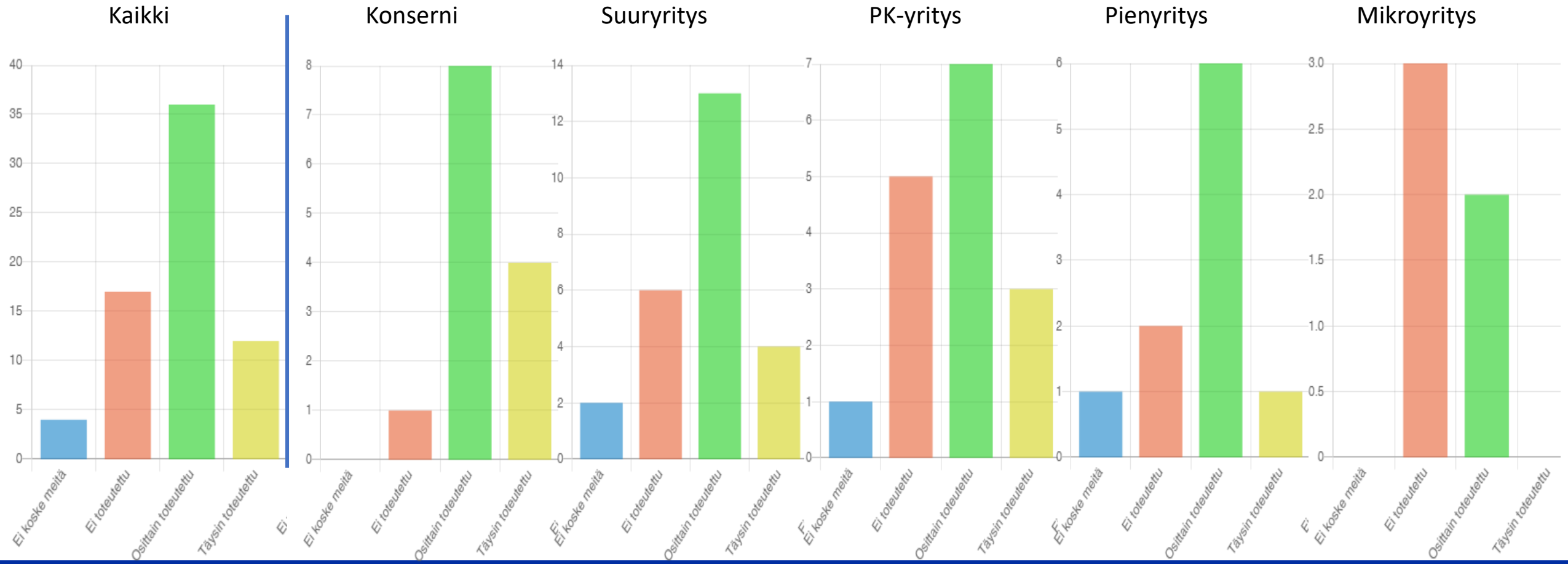


Pienyritys

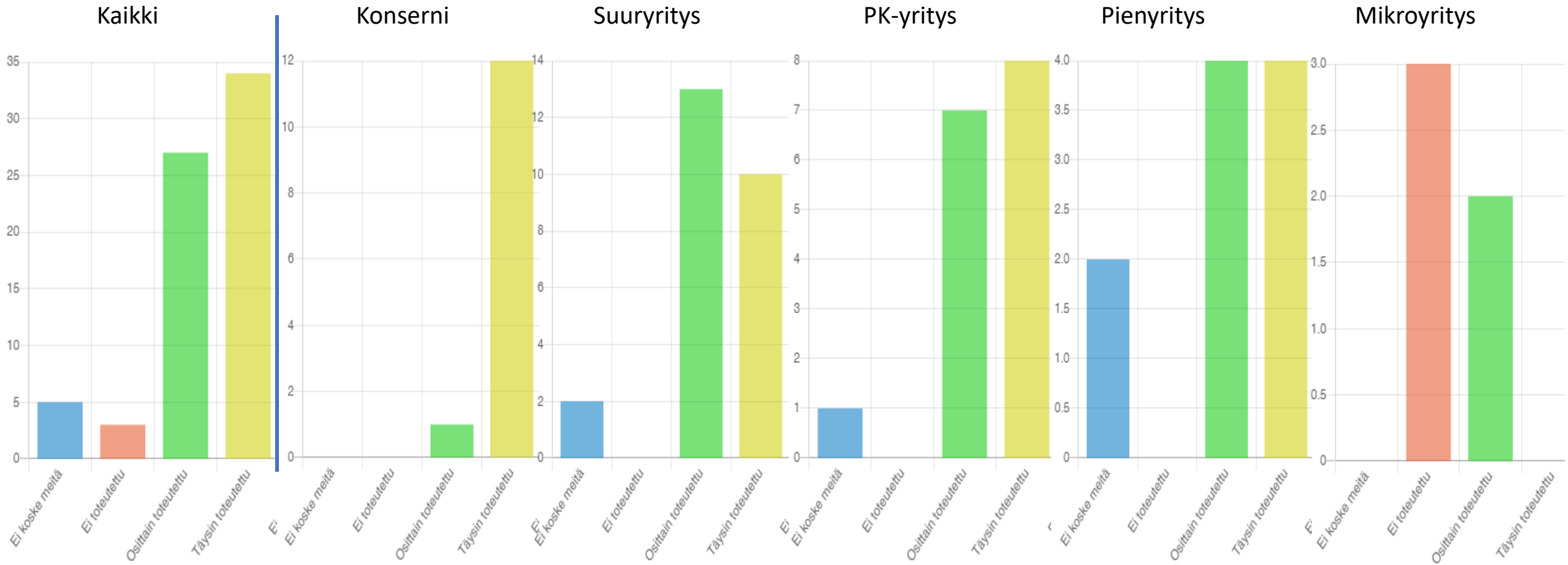
Mikroyritys



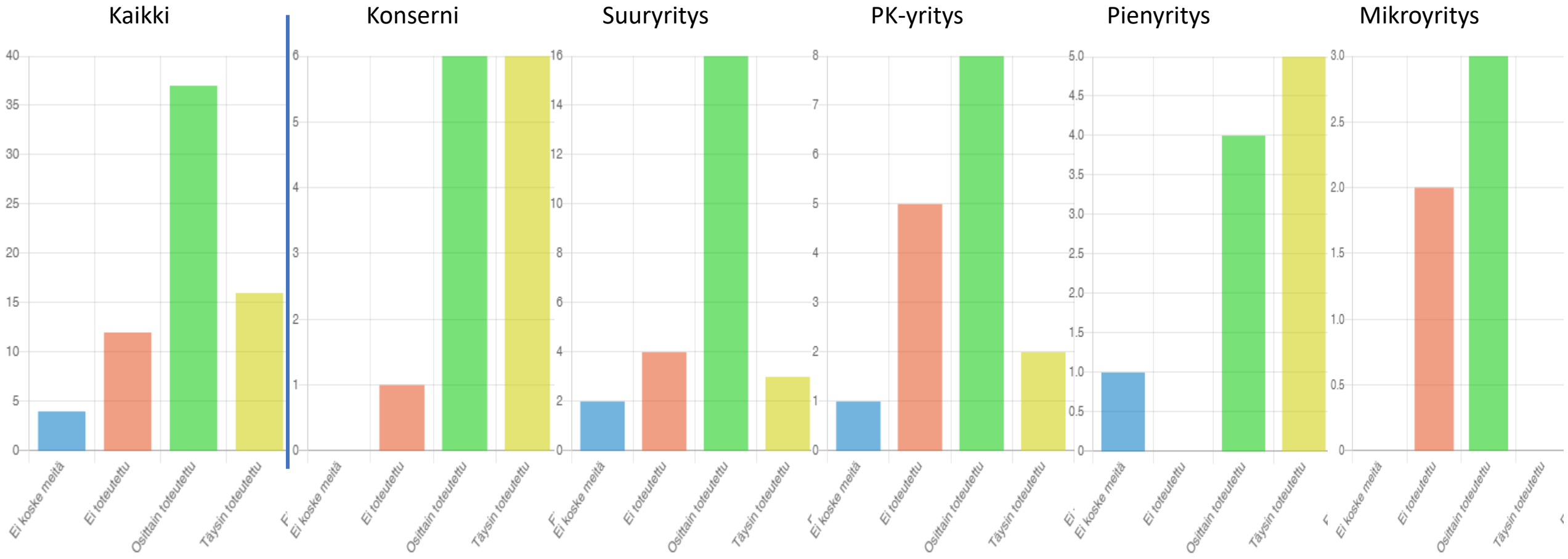
1. Yrityksen arvot sisältävät digitaalisen turvallisuuden tekijät (Digitaalinen turvallisuus käsittää viisi osa-aluetta: riskienhallinnan, toiminnan jatkuvuuden ja varautumisen, tietoturvallisuuden, kyberturvallisuuden sekä tietosuojan.).



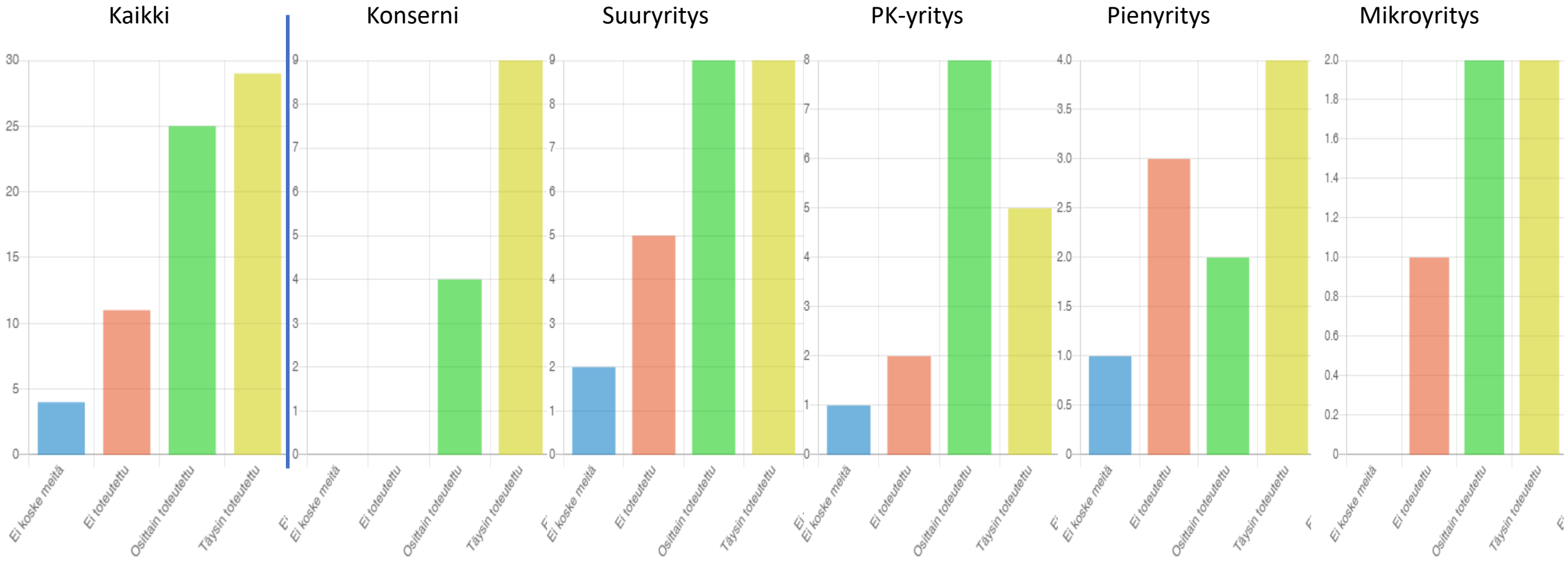
2. Yrityksen tuotanto- ja palvelutoiminnalle on asetettu tehokkuustavoitteet.



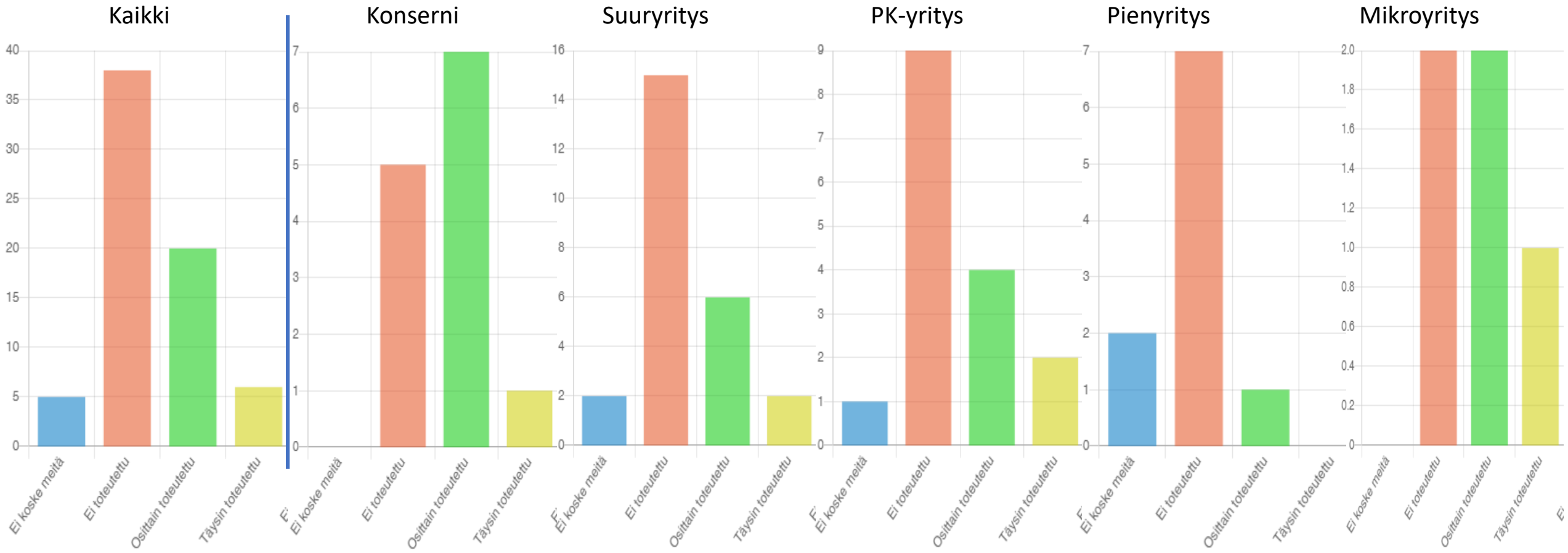
3. Yrityksen tuottamille tuotteille ja palveluille on asetettu digiturvallisuustavoitteet. (Digitaalisen turvallisuuden tavoitteena on suojata yrityksen toiminta niiltä riskeiltä ja uhkilta, jotka voivat kohdistua yrityksen henkilötietoihin ja tuotteisiin sekä prosesseihin, palveluihin ja tietoaineistoihin digitalisoituneessa toimintaympäristössä.)



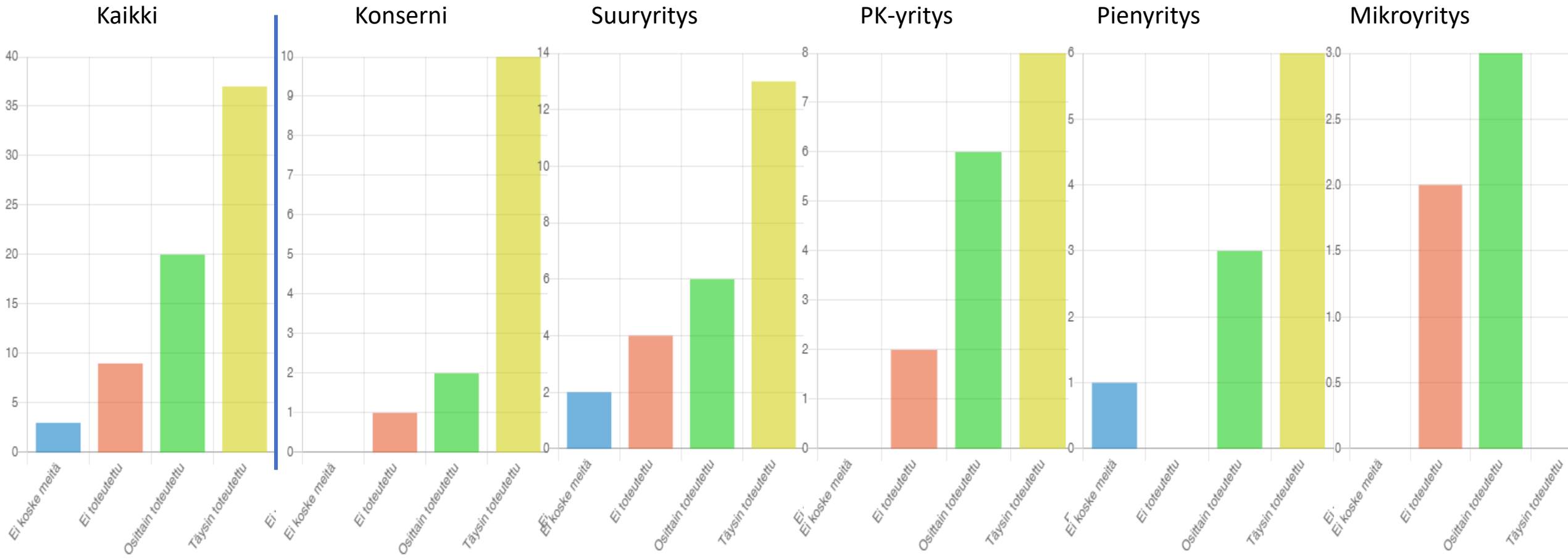
4. Strategiatyössä on menettely, jolla voidaan tunnistaa yrityksen digitalisaatioon liittyvät mahdollisuudet.



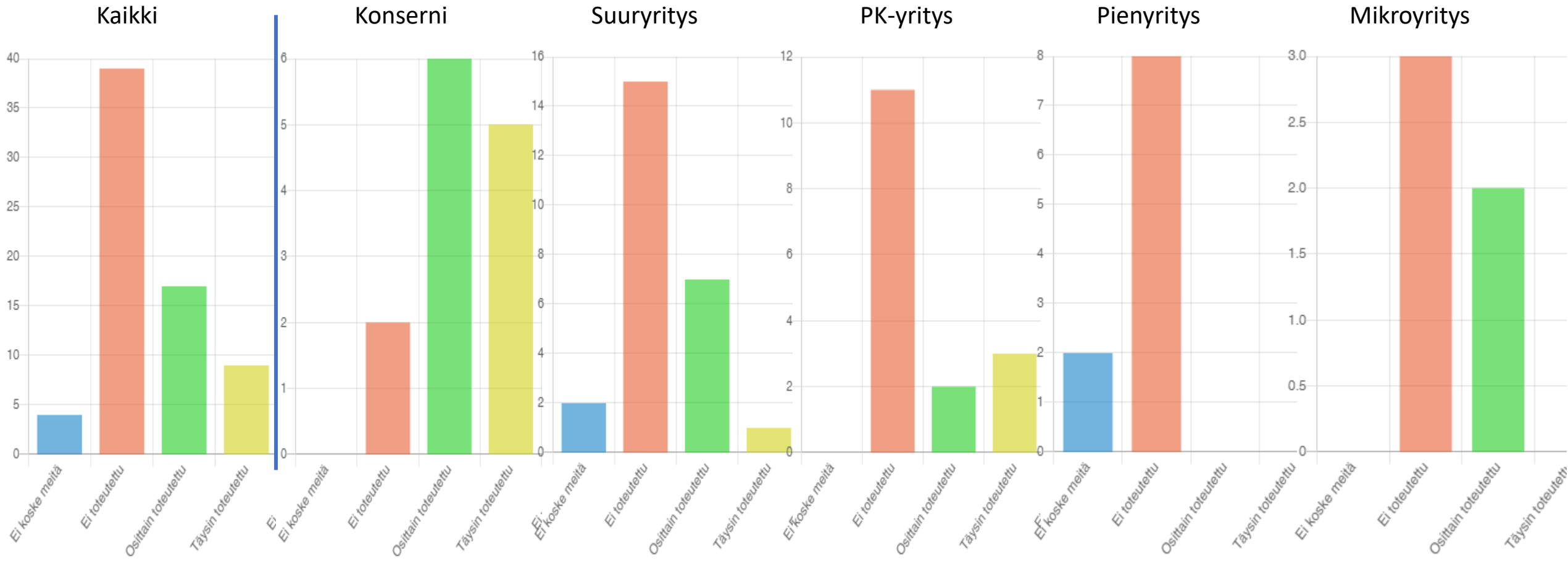
5. Digiturvallisuudelle on asetettu taloudelliset tavoitteet.



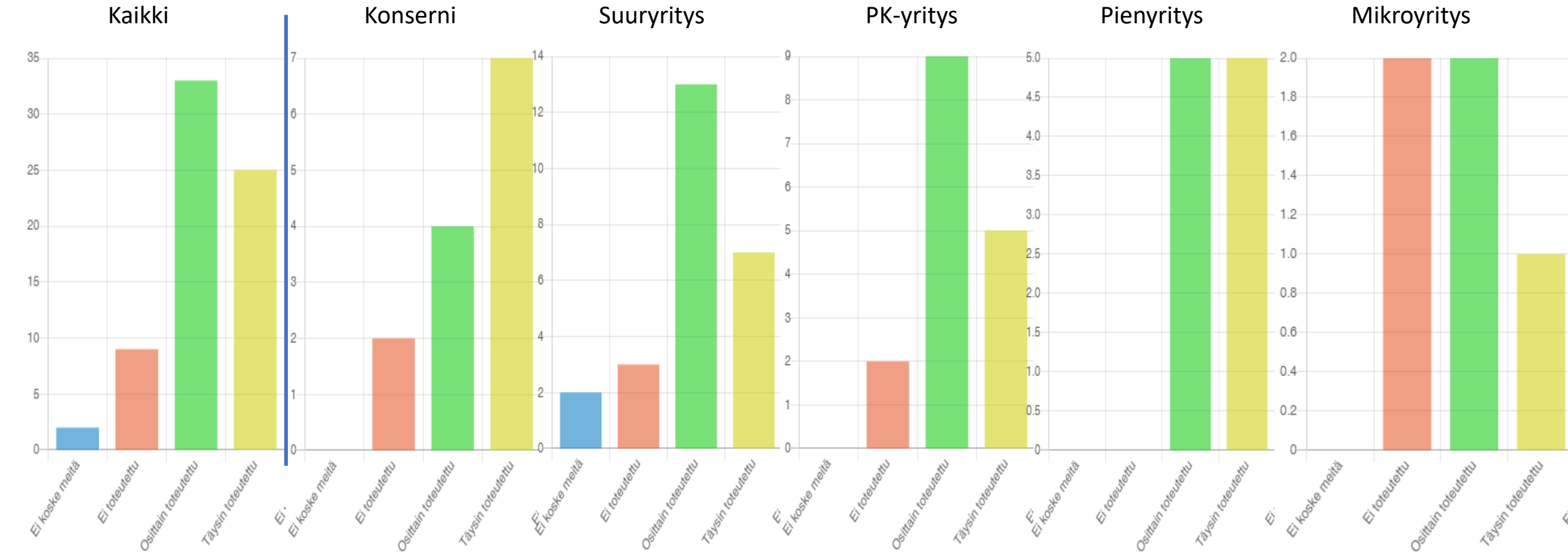
6. Yrityksellä on johdon hyväksymät, toimintaan sovitetut riskienhallinnan linjaukset, vastuut ja prosessi.



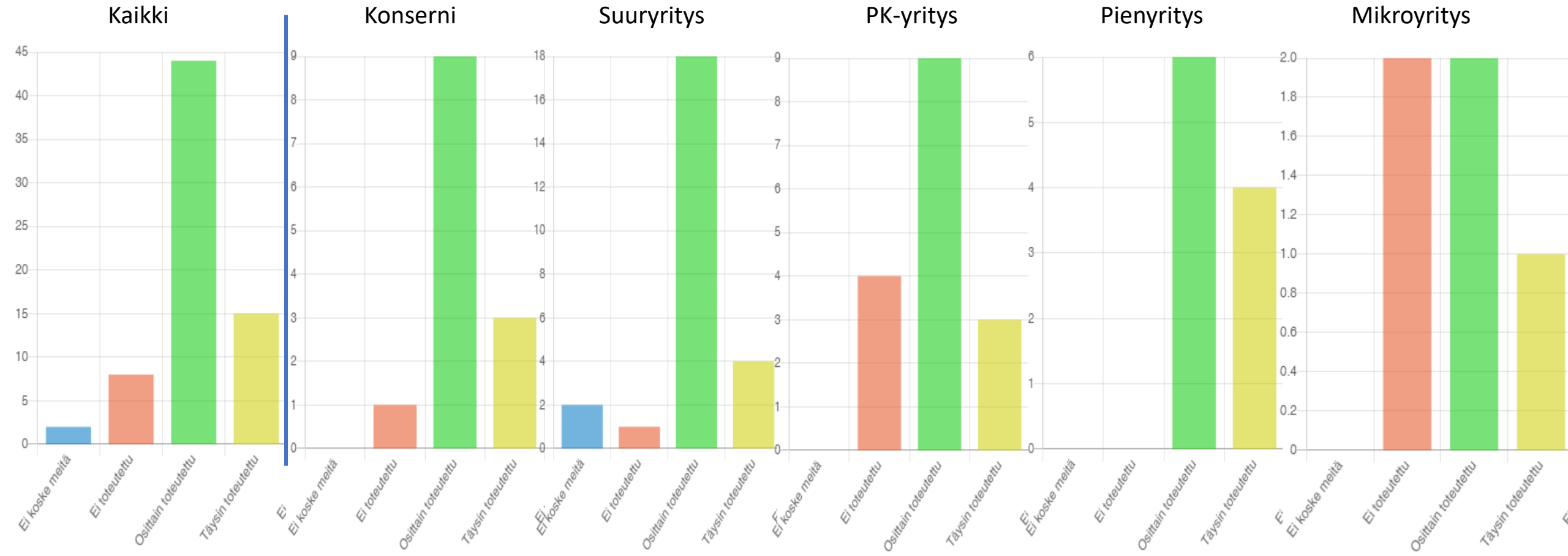
7. Yritys käyttää standardoitua tai muuta vastaavaa menettelyä strategiatyön lähtökohtana.



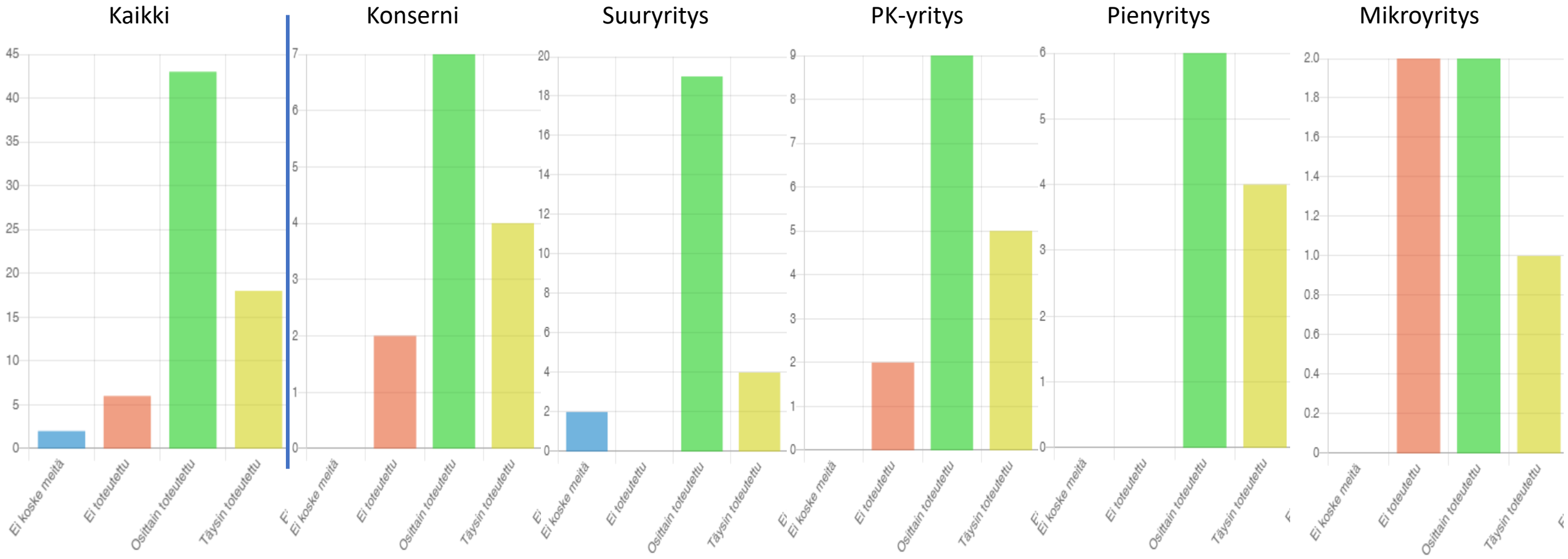
8. Yrityksellä on kyky arvioida riittävä resurssointi ja budjetti digi- ja kyberturvallisuuteen.



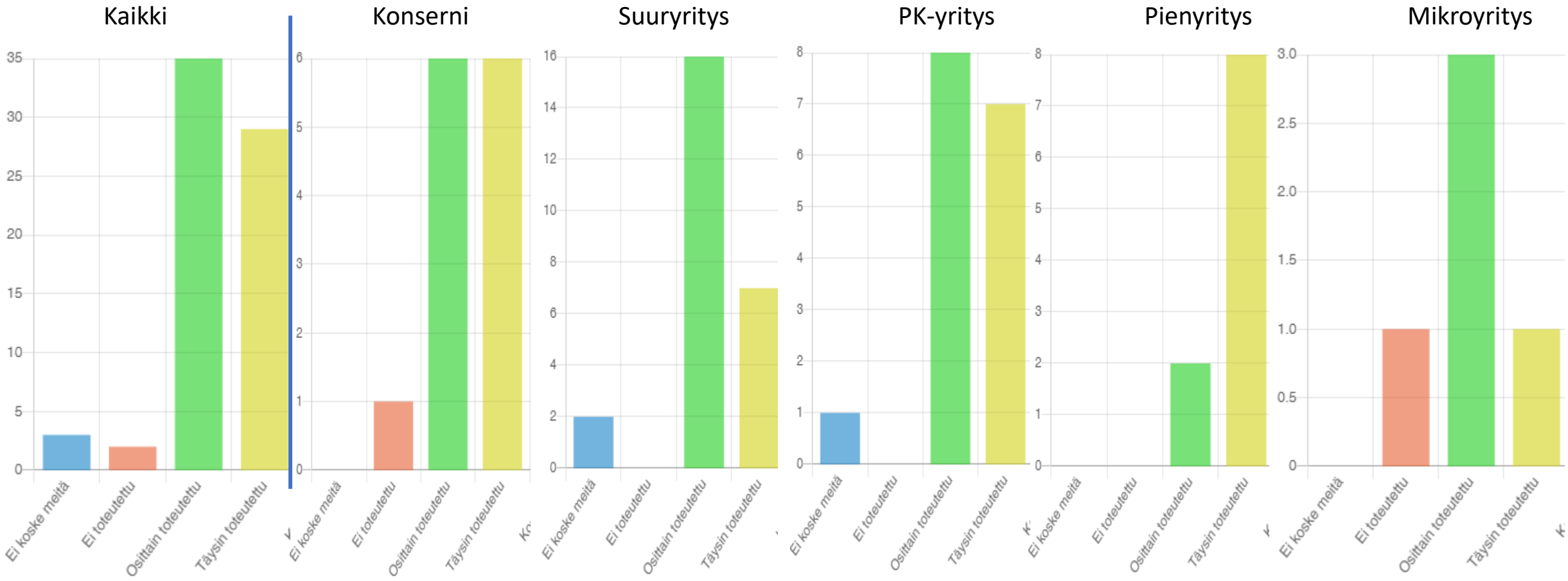
9. Yrityksellä on riittävästi osaavaa henkilöstöä kyberturvallisuuden eri osa-alueilla.



10. Yrityksellä on riittävät resurssit ja osaaminen digitaalisen turvallisuuden ylläpitoon ja kehittämiseen osana yrityksen prosesseja, toimintamalleja ja järjestelmiä (kokonaisarkkitehtuuria).



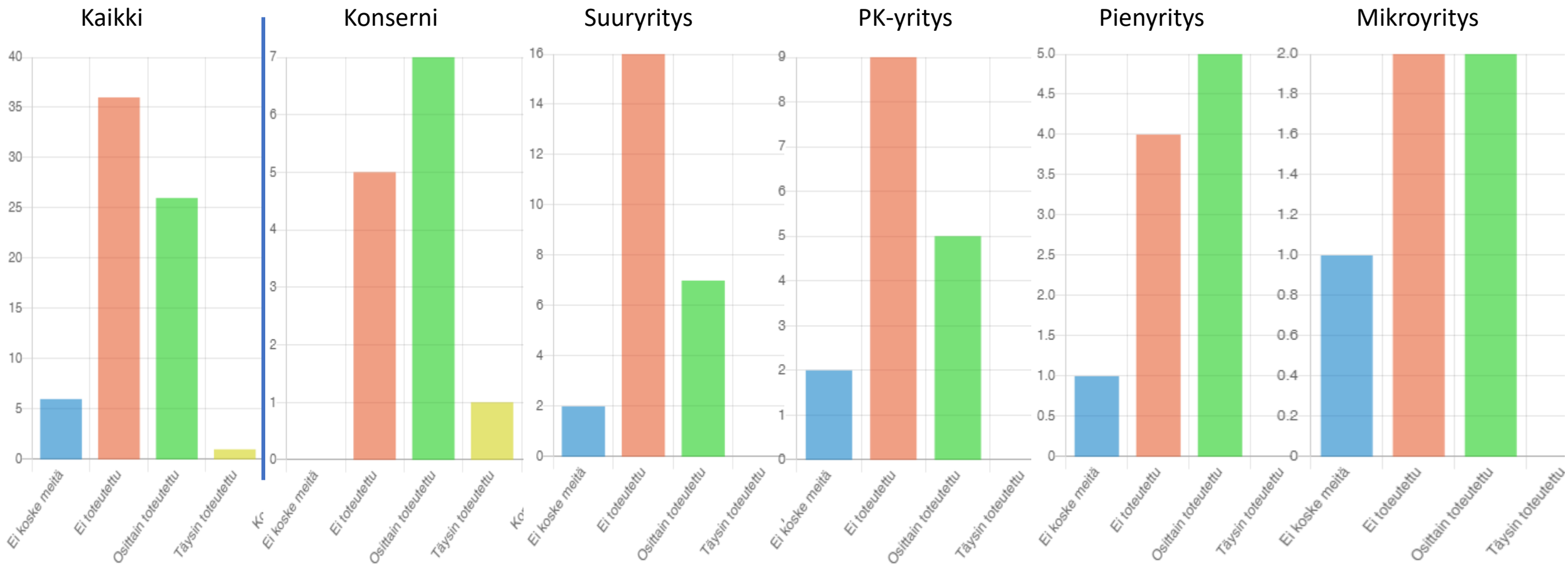
11. Yrityksen on tunnistanut sen liiketoiminnan kannalta kriittiset toiminnot, palvelut, tiedot, tietovarannot ja tietojärjestelmät.



11. Jos kyllä, niin miten ne ovat vaikuttaneet esimerkiksi alihankintaketjuihin?

1. On arvioitu, ei dokumentoitu
2. Kaksi keskeisintä palveluamme perustuu tähän.
3. Laadittu Disaster Recovery Plan ja se osana tunnistettu
4. Kompleksisessa ympäristössä nykypäivänä jopa mahdoton vaatimus
5. listaus tietoturvariskeistä, henkilöstö suurin riski, mietitty korvaavia tapoja toimia lyhyellä aikavälillä, jos esim. tietoverkko- tai sähköverkko putoaa pois käytöstä, hlöstön tietoturva-koulutus säännöllistä
6. Osana liiketoimintojen jatkuvuussuunnittelua
7. Kyberturvallisuus on tunnistettu/tunnustettu olemassa olevana ilmiönä ja siihen suhtaudutaan vakavasti. Konkreettiset toimenpiteet vielä epäselvät. Tietojärjestelmiä kartoitetaan ja kybermittari on päätetty toteuttaa 2021/22 aikana. Koulutus- ja tiedotustarpeet sekä puutteet niissä on havaittu ja niitä ollaan korjaamassa.
8. Monialaisessa liiketoiminnassa keskeiset toiminnot on tunnistettu, marginaali voi jäädä alle
9. Työturvallisuudessa ja tuotannon jatkuvuus asioissa ollut painopiste. Ei niinkään digitaalisen turvallisuuden puolella.
10. Osa digiturvallisuuteen liittyvistä asioista hoidetaan globaalin organisaation kautta, ei maatasolla.
11. Tietojärjestelmien käytettävyys ja varautuminen/ toipuminen kriisitilanteista.
12. Tänä vuonna siirretty kaikki omat serverit pilvipalveluja tarjoavan yrityksen hoidettavaksi. Logistiikassa on toiminnallinen jatkuvuus a ja o. Jos IT katkeaa, loppuu tavaran liikkuminen miltei välittömästi.
13. Kriittisten tietojärjestelmien ja ICT-palveluiden läpikäynti on työn alla. Tässä tarkastellaan palvelutasosopimukset toimittajien kanssa ja kuvataan prosesseja mm. häiriöviestinnän osalta.
14. ISO/IEC 27001 sertifikaatti ohjaa meitä tämän osalta
15. Työtä on aloitettu ja riippuvuuksia tunnistettu.
16. Tuotamme ko suorituskykyjä, joita myös käytämme omassa toiminnassa ml kriittiset asiakkaat.
17. Valtaosa toiminnan kannalta kriittisistä alueista tunnistettu. Aukkoja kuitenkin on, erityisesti tuotannon osalta.
18. Kriittiset toiminnot ja tietojärjestelmät ovat pääsääntöisesti hyvin tunnistettu, mutta niiden suojaaminen ja jatkuvuuden varmistaminen ei aina eroa normaalin kriittisyyden järjestelmistä. Sama tietovarantojen suojauksen osalta.
19. Niin paljon on tunnistettu kuin oma osaaminen sen mahdollistaa

12. Kyberturvallisuudelle on määritetty tehokkuusvaatimukset (kustannus-vaikuttavuus).

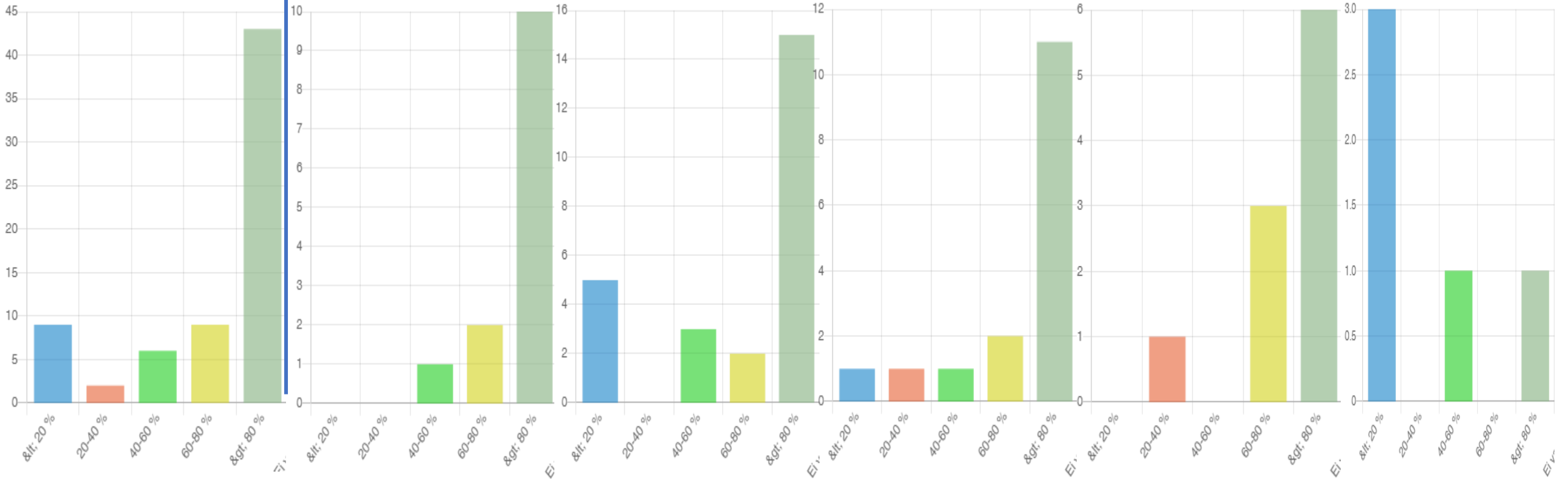


12. Jos kyllä, niin anna toteutuksesta lyhyt digi- ja kyberturvallisuusesimerkki.

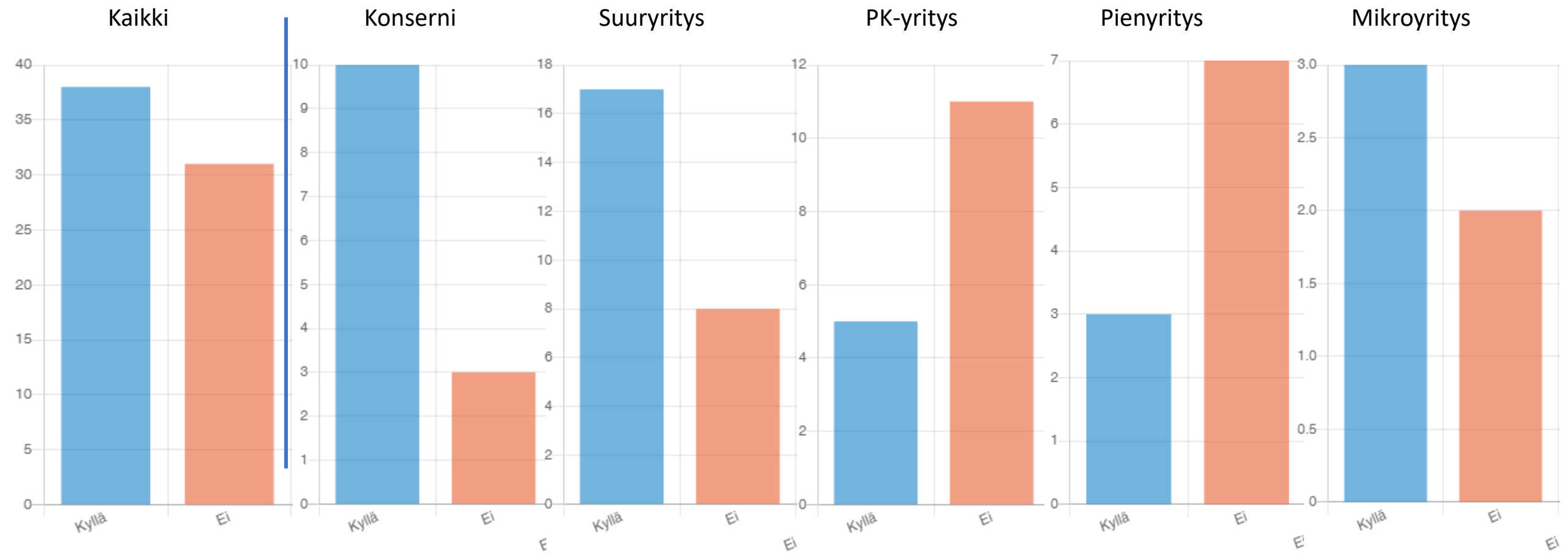
1. Prosessi on osittain olemassa, suullinen, ei dokumentoitu
2. Ajatuksellisesti on, mutta sitä ei ole kirjoitettu suoraan kustannusvaikuttavuutta arvioiden.
3. Ei ole määritetty maaorganisaatiossa.
4. Kyberturvallisuus huomioidaan kyllä tärkeänä osana mm. tietojärjestelmien kehitystä ja uusien järjestelmien hankintaa, muttei erikseen siten, että nimenomaisesti sille asetettaisi jokin tietty budjetti.
5. Joitain mittareita on mutta vähemmän liittyen kustannus/tehokkuus/vaikuttavuus puolelle.
6. Tuotamme ko suorituskykyjä, joita myös käytämme omassa toiminnassa ml kriittiset asiakkaat.
7. Suoranaisia tehokkuusvaatimuksia ei ole, mutta tiekartan edistymistä ja riskien mitigoimista seurataan hyvinkin tarkasti

13. Kuinka suuri osa yrityksen liiketoiminnasta on riippuvainen järjestelmien ja datan toimivuudesta ja digitaalisen tiedon eheydestä?

Kaikki | Konserni | Suuryritys | PK-yritys | Pienyritys | Mikroyritys



14. Yritys hyödyntää kyberturvallisuuskatsauksia (tilannekuva) strategisessa suunnittelussa.



15. Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa?

1. Alihankkijoiden ja kumppaneiden merkitys kyberturvallisuuden hallintaan.
2. Ei näin pk-yrityksen edustajana kyllä osaa edes sanoa!
3. Yritysrakenne: globaali konserni hoitaa joitain asioita yhteisesti globaalilla tasolla, ja osan maatasolla. Kysymyksiin vastaaminen ei anna ihan koko kuvaa tilanteesta.
4. Menestystekijä: erittäin hyvä osaaminen kyberturvallisuusuhista ja niiden kiertämistekniikoista.

Johtopäätökset

Yrityksen arvoihin sisältyy digiturvallisuus suurelta osin. Siitä huolimatta parannettavaa on erityisesti PK-yritysten ja niitä pienempien osalta. Yritysten tuotanto- ja palvelutoiminnalle on asetettu tehokkuusvaatimuksia, erityisesti konserneilla. Edelliseen liittyen digiturvallisuustavoitteissa on parannettavaa kaikilla.

Pienyritysten digitalisaation mahdollisuuksia ylipäätään olisi parannettava.

Kaikissa kokoluokissa digiturvallisuuden taloudellisille tavoitteiden asettamisessa on kehittämisen varaa. Riskienhallintaan kiinnitetään hyvin huomiota.

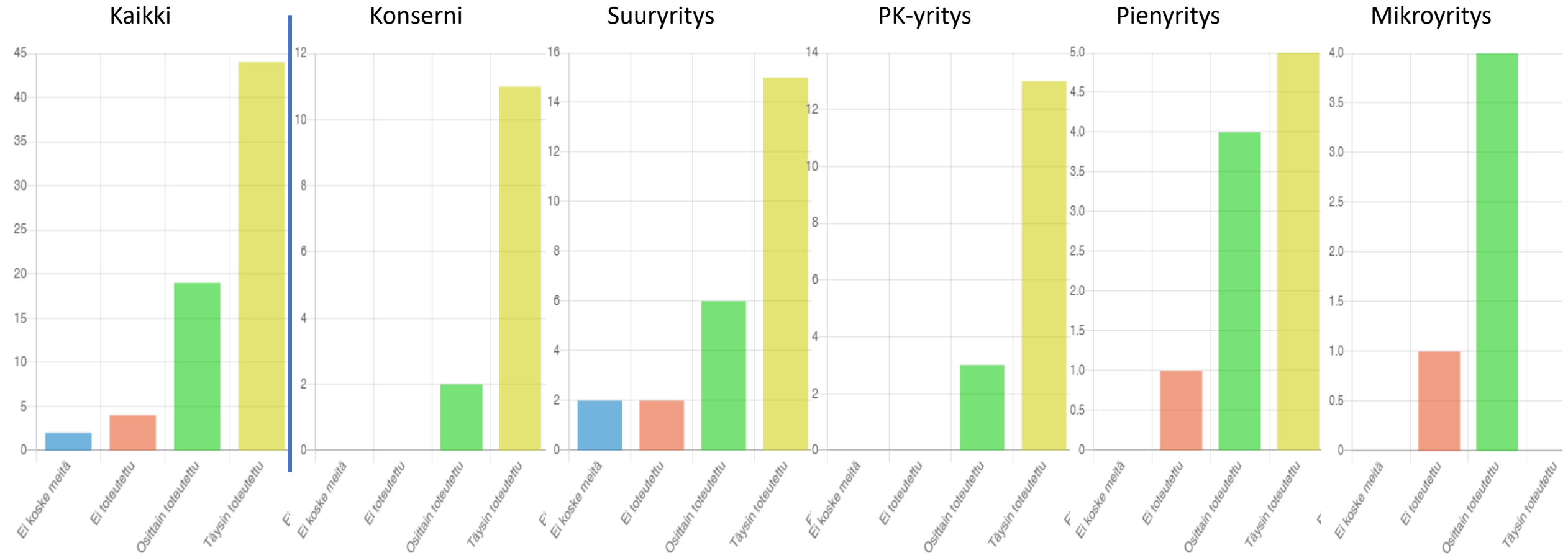
Strategiatyön vakiointiin tulisi kiinnittää enemmän huomiota suuryrityksistä pienempiin, standardit ja vastaavat menettelyt ovat selkeästi vierailta. Digi- ja kyberturvallisuuteen tarvittavien resurssien arviointi on hyvällä tasolla. Kyberturvallisuuteen tarvittavien resurssien ja henkilöstön osaamisen katsotaan pääsääntöisesti riittäväksi. Liiketoiminnan kriittiset tekijät on pääsääntöisesti tunnistettu.

Selkeä tarkistuskohde on kyberturvallisuuden tehokkuusvaatimukset (kustannukset – vaikuttavuus)

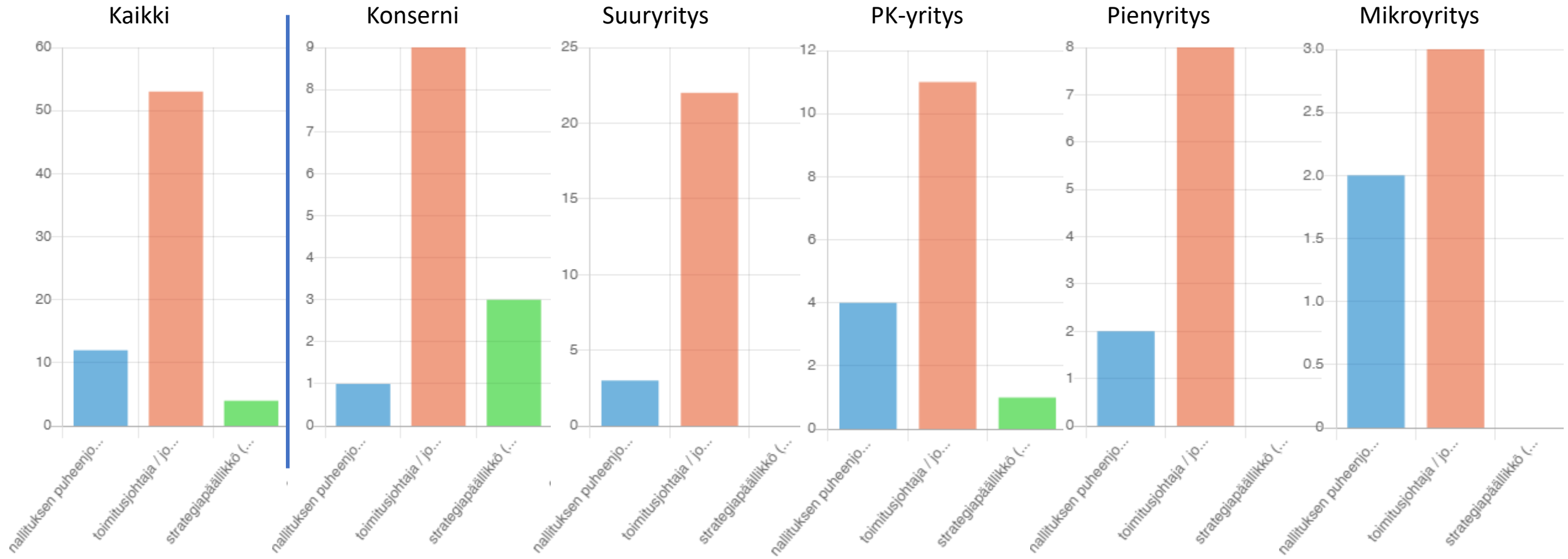
PK-yritysten ja pienempien kybertilannekuvan sisältöä ja laatua tulisi kehittää, mahdollisesti tälle luokalle omansa.

Yrityksen strategiatyö

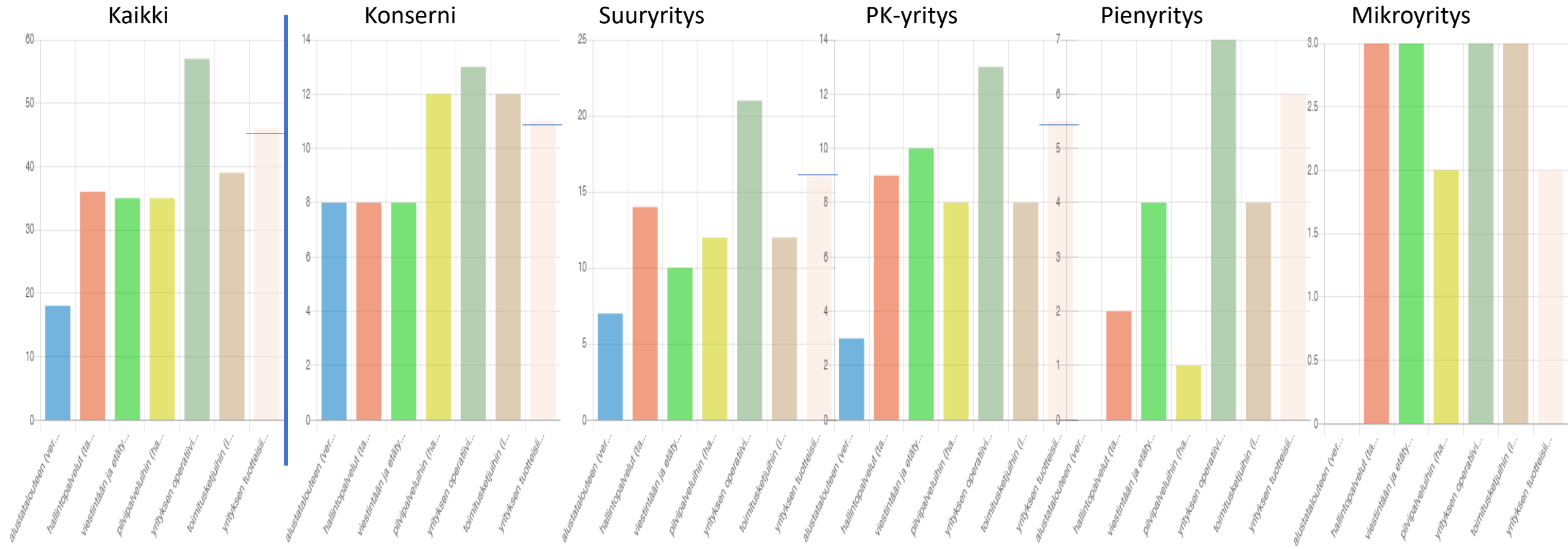
1. Yrityksellä on säännöllinen ja toimiva strategiaprosessi tai toimintamalli yrityksen strategian (tai vastaavan tason ohjauksen) laatimiseen



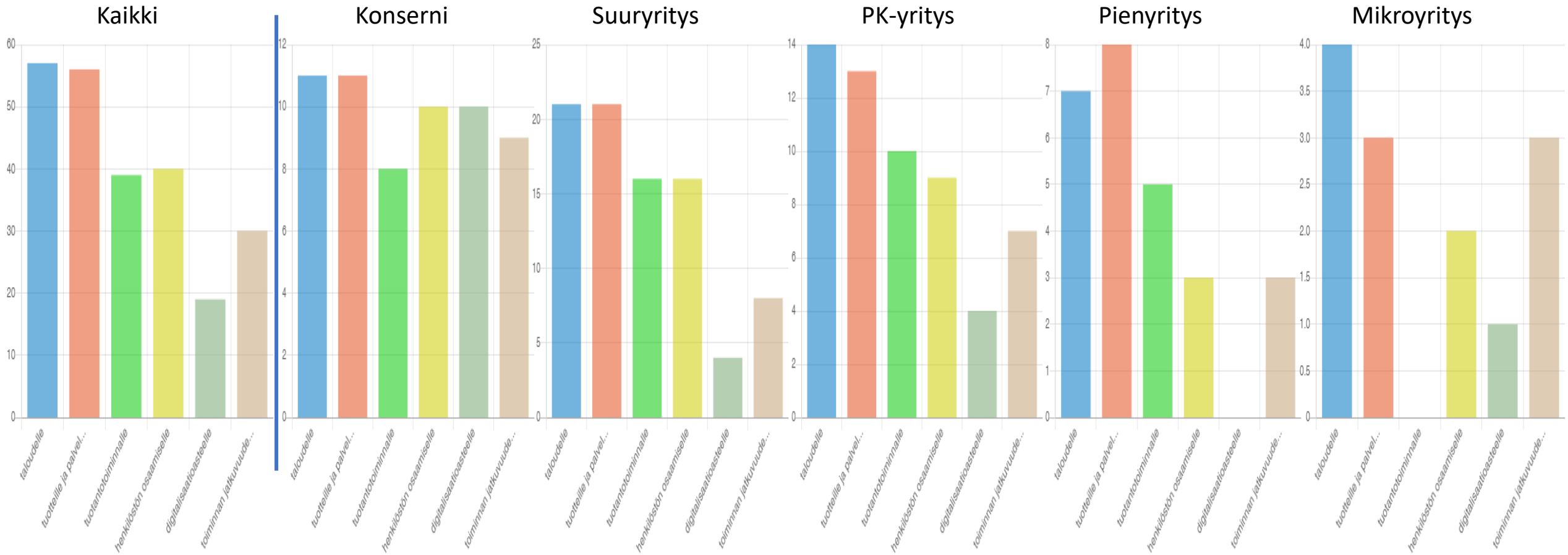
2. Yrityksen strategian (tai vastaavan) laatimisesta vastaa



3. Strategian (tai mission) perusteella yrityksen digitalisaatio liittyy (valitse tarvittaessa useampi)



4. Strategiatyössä on asetettu tavoitteet yrityksen



4. Jos johonkin em kyllä, niin millaisia tavoitteita on asetettu? (1/2)

TALOUDELLE

1. numeeriset tavoitteet
2. liikevaihdon kasvu
3. tuotto ja omavaraisuus tavoite
4. euromääräisiä katteen ja liikevaihdon osalta
5. Raamitukset taloudelle
6. tulos
7. Yrityksen on tultava toimeen asiakasmaksuilla toimintasuunnitelman mukaisesti
8. normaalit liiketoiminnan taloustavoitteet, Revenue, EBITDA, Profit, EPS, Capex, Opex...
9. omavaraisuus ja tuotot omistajalle
10. Liikevaihto
11. Liikevaihto, tulos
12. liikevaihto ja ebit
13. Haluamme kasvaa kannattavasti
14. liikevaihto ja kannattavuus
15. budjetointi
16. liikevaihto
17. Määrällinen
18. kannattava

TUOTTEILLE JA PALVELUILLE

1. määrälliset tavoitteet
2. Läpimenoaika ja virheettömyys
3. toimintavarmuus ja häiriöttömyys, energiatehokkuus
4. Läpimenoaika ja virheettömyys
5. asiakastyytyväisyys, toimintavarmuus
6. Kasvupotentiaali uusien tuotteiden ja palveluiden kautta
7. tuotantomäärät
8. markkina-asemaan, volyymeihin ja kannattavuuteen
9. laadukkaat ja kohtuuhintaiset tuotteet
10. Palveluportfolion tarkistusta
11. Tuotekehitys, markkinaosuudet
12. Turvalliset ja kilpailukykyiset ICT-infra- ja perustietotekniikan palvelut
13. toimitusvarmuus
14. laatuvaatimukset
15. Laadullinen
16. kestävästi ympäristövastuulliset, eettiset ja ekologiset tuotteet

TUOTANTOTOIMINNALLE

1. Läpimenoaika ja virheettömyys
2. toimintavarmuus ja häiriöttömyys, päästötavoitteet
3. Läpimenoaika ja virheettömyys
4. erilaiset toiminnan tehokkuuden mittarit
5. laatu, kustannukset, investoinnit
6. toimitusvarmuus
7. Tehokkuus
8. Tehokkuus, prosessit
9. tehokkuus
10. tuotteisto
11. Laadullinen

4. Jos johonkin em kyllä, niin millaisia tavoitteita on asetettu? (2/2)

HENKILÖSTÖN OSAAMISELLE

1. koulutussuunnitelma
2. Kulttuurimme tukee ihmisten hyvinvointia ja kehittymistä
3. asiakastyytyväisyys, työtyytyväisyys
4. osaamisen kehittyminen
5. osaava ja motivoitunut henkilökunta
6. Koulutustarjonta sekä konsernilta että maayhtiössä: lakisääteinen pakollinen koulutus, sekä yrityksen määrittelemät muut pakolliset kurssit sekä vapaaehtoisten valikoima
7. Osaava henkilöstö
8. Tietoturvan- ja tietosuojan hallinta on keskeinen osa palveluitamme ja niiden kehittämistä
9. Henkilöstön osaamista kehitetään vastaamaan muuttuvia vaatimuksia
10. osaamisen johtaminen

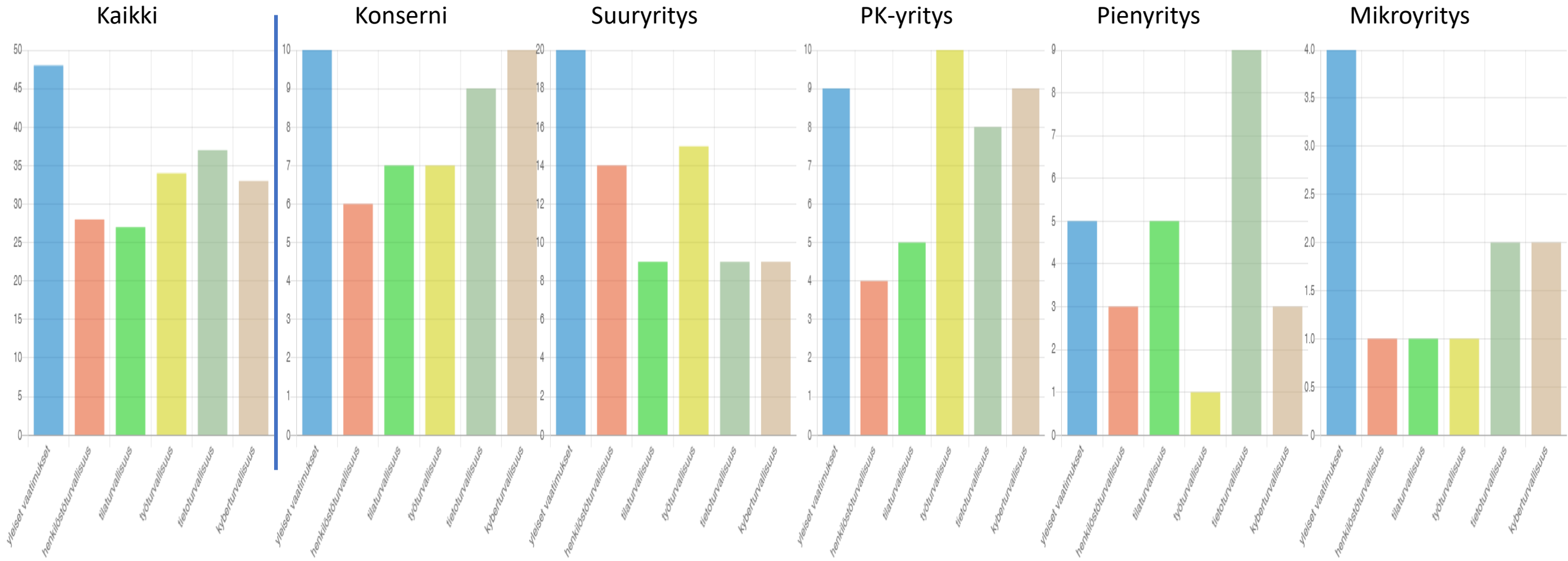
DIGITALISAATIOASTEELLE

1. erillisen digistrategian luonti
2. osana tuotannollisia tavoittetia
3. Seurataan mm. sähköisten tilausten osuutta, sekä automatisoitujen prosessien osuutta -> lukuisia projekteja
4. Liiketoimintaa tukeva ja mahdollistava
5. Ymmärrämme asiakkaidemme prosesseja, olemme mukana suunnittelemassa heidän palveluidensa kokonaisarkkitehtuuria,sekä tuomme osaamisellamme ja verkostoillamme asiakkaidemme tarpeisiin sopivat ratkaisut
6. Näemme digitalisaation yhtenä merkittävimmistä kilpailueduista tulevaisuudessa
7. Suunnitteilla

TOIMINNAN JATKUVUUDELLE (RESILIENSSI)

1. toimintavarmuus ja häiriöttömyys, toiminnan varmistaminen kaikissa tilanteissa jatkuvuuden hallinnan avulla
2. Toimialan jatkuvuuden vaatimukset
3. laatutavoitteet
4. toimintaa pystyttävä suorittamaan kaikkina aikoina
5. IT:ssä jatkuvuussuunnitelmat, palautumissunnitelmat, varayhteydet, varavoimavirtaratkaisuja, jne. Tuotannon puolella laajemmat jatkuvuussuunnitelmat.puolella
6. tavoitteita 3 ja 5 vuoden sykleille
7. Laadullinen

5. Yrityksen strategiassa (tai vastaavassa) on asetettu tavoitteet turvallisuuden osatekijöille



5. Jos johonkin em. kyllä, niin millaisia tavoitteita on asetettu? (1/2)

YLEISET VAATIMUKSET

1. Ei ole tavoitteita mutta tarkoin kuvattu ja määritetty
2. yritysturvallisuusohjeisto
3. Ei määritetty tavoitteita, mutta ovat hyvin tarkoin kuvattuja
4. Ei selkeitä turvallisuuteen liittyviä viittauksia ellei yhdenvertaisuus ja tasa-arvo periaatteita lasketa niiksi.
5. wsp
6. Vastuullisuus on yksi yrityksen pääarvoista.
7. AEO(F) sertifioituna yhtiönä perusedellytys
8. infra, liikenne, raaka-aineiden saatavuus, energian saatavuus, ympäristön tuomat riskit jne riskienhallinnan kautta
9. ERM riskienarviointi
10. ympäristöturvallisuus

HENKILÖSTÖTURVALLISUUS

1. AEO(F) sertifioituna yhtiönä perusedellytys
2. lain edellyttämät
3. infra, liikenne, raaka-aineiden saatavuus, energian saatavuus, ympäristön tuomat riskit jne riskienhallinnan kautta

TILATURVALLISUUS

1. Ei ole tavoitteita mutta tarkoin kuvattu ja määritetty
2. Ei määritetty tavoitteita, mutta ovat hyvin tarkoin kuvattuja
3. ISO 14001 kautta
4. Tapa, Tullin AEO. Auditoinnit. Pääsy yrityksen eri tiloihin on rajattu tarkasti + seuranta. Yrityksen työntekijöillä on oltava henkilökortti, ja vierailijoilla vierailijakortti. Kiinteistöjen piha-alueet on aidattu. Kattava kameravalvonta.
5. AEO(F) sertifioituna yhtiönä perusedellytys
6. pelastusturvallisuuden edellyttämät

5. Jos johonkin em. kyllä, niin millaisia tavoitteita on asetettu? (2/2)

TYÖTURVALLISUUS

1. nolla tapaturmaa -tavoite
2. turvallinen työ kaiken lähtökohtana
3. 0-tapaturmaa
4. nolla tapaturmaa
5. Tapaturmien huomattava vähentäminen, mitataan sairauslomapäivien määrällä.
6. Työtapaturmien seuranta ja mittarointi
7. AEO(F) sertifioituna yhtiönä perusedellytys
8. lain edellyttämät
9. nolla työtapaturmaa, vaaditaan työturvallisuuskortti
10. työtapaturmien määrä

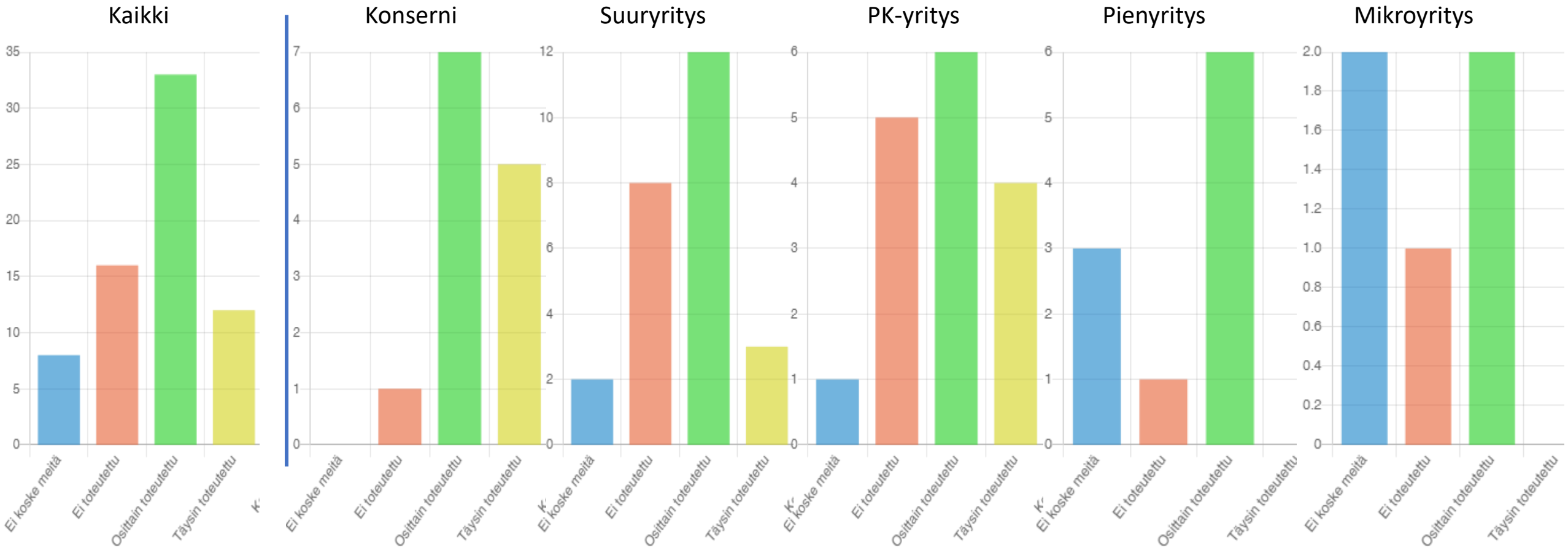
TIETOTURVALLISUUS

1. Ei ole tavoitteita mutta tarkoin kuvattu ja määritetty
2. Ei tavoitteita mutta tarkoin kuvattu ja määritetty.
3. omistajan tietoturvallisuusohjeistus
4. Ei määritetty tavoitteita, mutta ovat hyvin tarkoin kuvattuja
5. tietoturvariskien minimointi ja liiketoiminnan jatkuvuuden turvaaminen
6. salasanat
7. Jatkuvuuden varmistaminen
8. Toimiminen siten, että tietoturva on koko ajan ajan tasalla, jatkuva seuranta ja havaittujen poikkeamien välitön korjaaminen.
9. GDPR mukainen toiminta, liiketoimintatiedon suojaus
10. AEO(F) sertifioituna yhtiönä perusedellytys
11. Tietoturvan- ja tietosuojan hallinta on keskeinen osa palveluitamme ja niiden kehittämistä
12. tietoturvapolitiikan mukaiset
13. lainsäädännön mukainen toiminta

KYBERTURVALLISUUS

1. Oli pakko vastata, että pääsi eteenpäin - ei asetettu
2. toimintavarmuuden kehittäminen kyberturvallisen toimintatavan kautta
3. Ei yhtään tietomurtoa. Tietoturvan toteuttaminen kaikilla IT:n osa-alueilla (verkot, palvelimet, sovellukset, sopimukset....)
4. Hyökkäysten eston hallinta, pääsyn hallinta
5. AEO(F) sertifioituna yhtiönä perusedellytys
6. täytyy olla
7. Osaamisemme kehittäminen on toiminnan jatkuvuuteen, vastuunkantoon ja muutoskyvykkyyteen tähtäävää
8. tietoturvapolitiikan mukaiset
9. seurataan tiedotusta aiheesta, nojataan ulkopuoliseen palveluntarjoajaan.

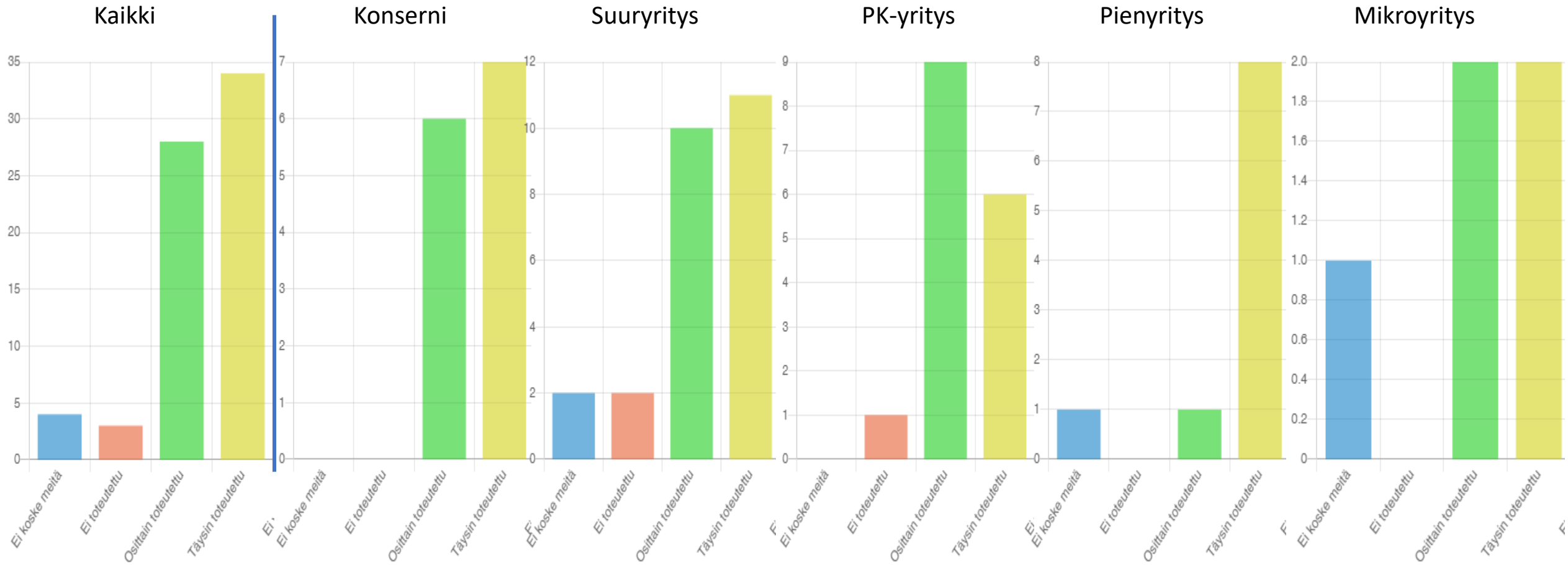
6. Yrityksen liiketoimintastrategiassa on määritetty digitaaliset menestystekijät.



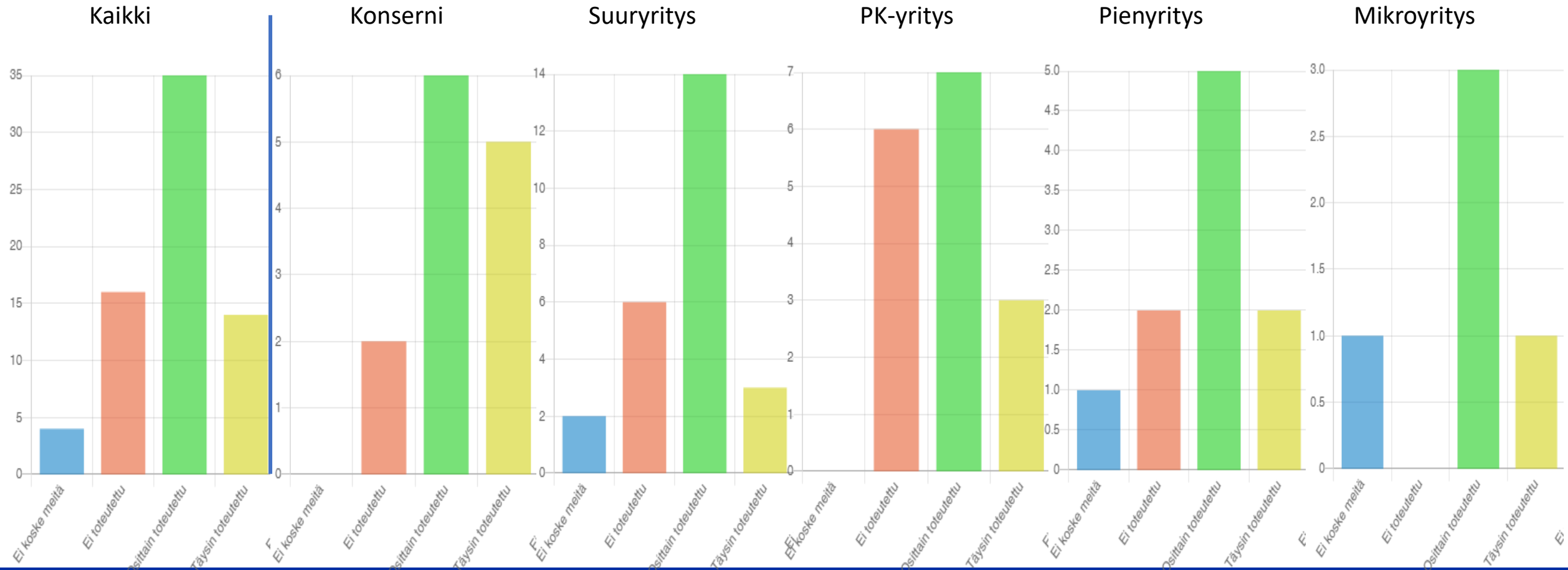
6. Jos kyllä, niin millaisia menestystekijöitä on määritetty?

1. Ketteryyttä ja kokeilullista toimintatapaa. Digitalisaation mahdollisuuksien hyödyntäminen.
2. digitalisaatioasteen nostaminen ja asiakaskokemuksen parantaminen (helppokäyttöisyyden lisääminen)
3. ICT strategia omana kokonaisuutena yrityksen strategiassa

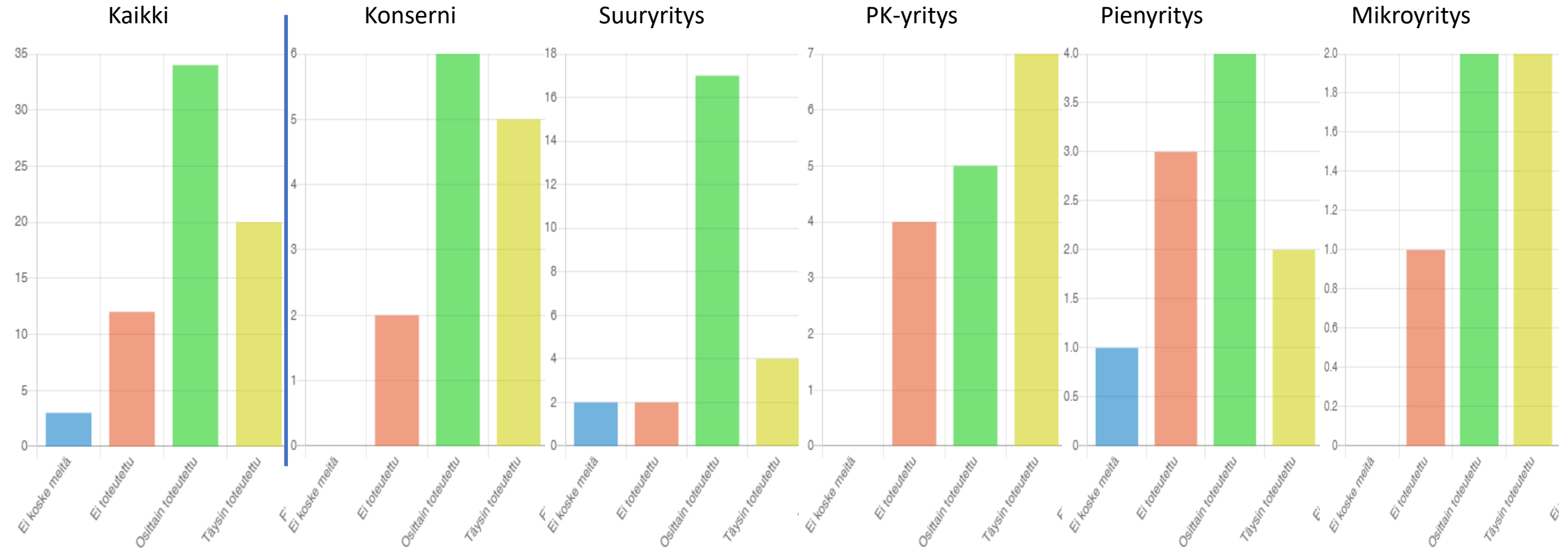
7. Yrityksen johto on sitoutunut digitaalisen turvallisuuden kehittämiseen.



8. Strategiatyössä on menettely, jolla voidaan tunnistaa yrityksen digitalisaatioon liittyvät uhkatekijät.



9. Strategiatyössä on määritelty viestinnän linjaukset ja avoimuusperiaatteet mahdollisen kriisitilanteen varalta.



10. Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa?

1. Yrityksen strategiassa ei välttämättä juurikaan puhuta tietoturvasta, mutta yrityksen turvallisuus-/tietoturvatoiminta perustuu yrityksen strategian toteuttamiseen.
2. Mitä tässä kyselyssä strategiatyöllä tarkoitetaan? itselleni se on johtoryhmätasoista työtä ja vastasin siltä kantilta.
3. Tässä osuudessa kysytään asioita, joita käsitellään, mutta ei osana strategiaprosessia. Esim. kriisiviestintä ei kuulu strategisiin teemoihin, vaikka on olennaisen tärkeä. Samoin turvallisuuden tavoitteet ovat pääosin muualla. Listasta puuttui keskeinen osa-alue - tietosuoja, jonka toteuttamiseen turvallisuus tuo merkittävän osan.
4. Moni asia on mietitty ja toteutettu muuten, mutta EI strategiatyössä. Esim. viestinnän linjaukset.
5. Kysymykset liiaksi sidottuja strategiatyöhön. Strategiatyöllä on omat tavoitteet jotka jalkautuvat operatiivisessa toiminnassa.

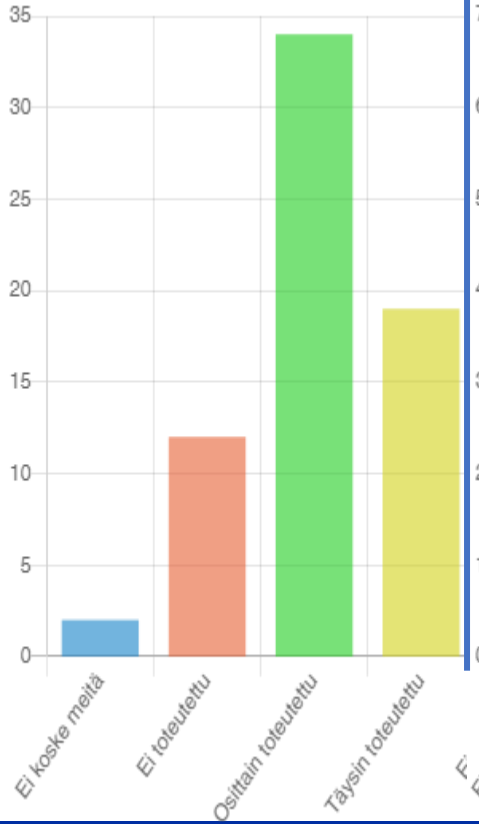
Johtopäätökset

Kaikilla on strategiatoimintamalli. Vastuu pääsääntöisesti on toimitusjohtajalla, poikkeuksen tekee konsernitaso, joilla voi olla myös erillinen strategiapäällikkö. Pienemmissä yrityksissä myös hallituksenpuheenjohtajalla on rooli strategiatyössä. Yrityksen johto koetaan sitoutuneeksi digiturvallisuuden kehittämiseen.

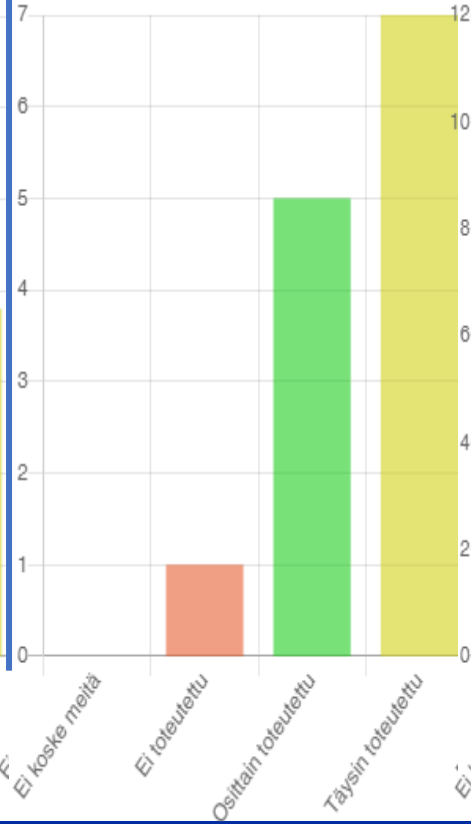
Digitalisaatio liittyy käytännössä kaikkeen yritystoimintaan. Strategiatyössä yleensä asetetaan yrityksen liiketoiminnalle tavoitteet, mutta selkeitä puutteita on digitalisaatioasteen ja jatkuvuuden vaatimuksissa. Digitaaliset menestystekijät on vain osittain määritetty yrityksissä.

1. Yrityksen digitaalisen turvallisuuden osa-alueita kehitetään järjestelmällisesti hyödyntäen yhtä tai useampaa selkeää prosessia tai hallintamallia.

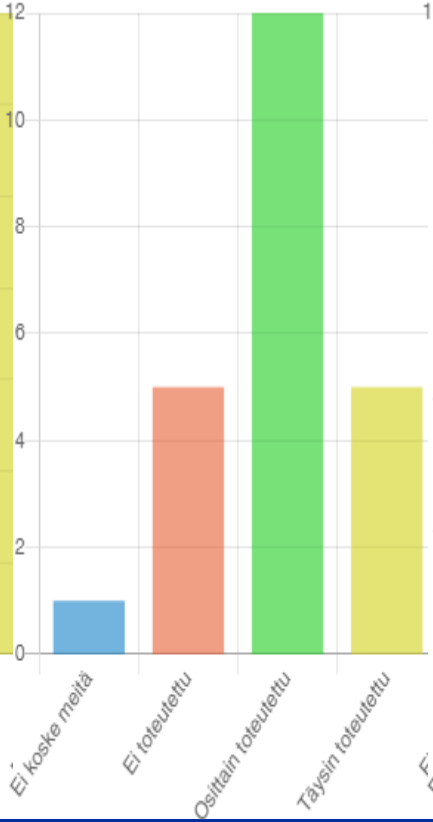
Kaikki



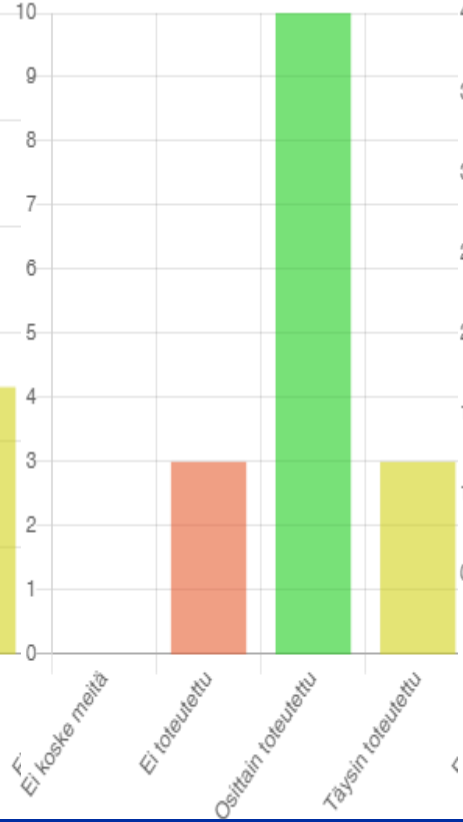
Konserni



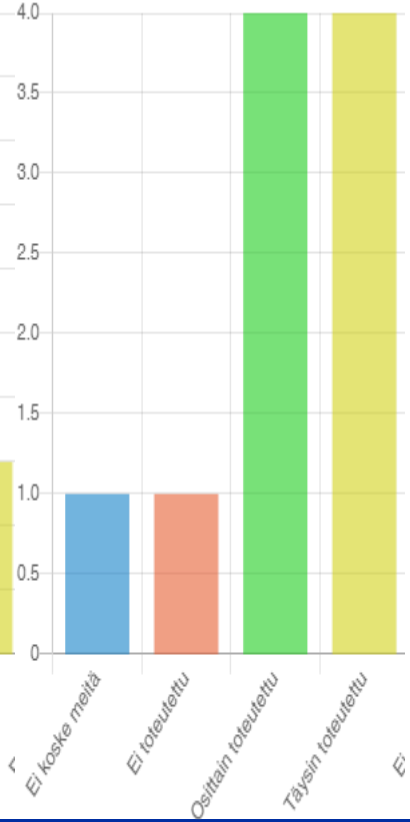
Suuryritys



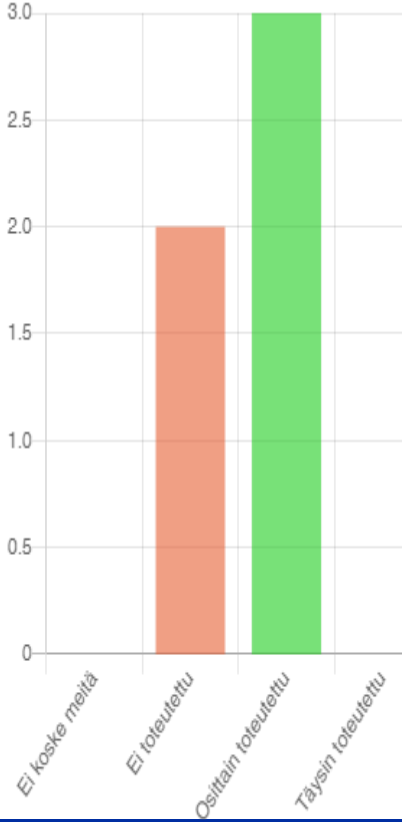
PK-yritys



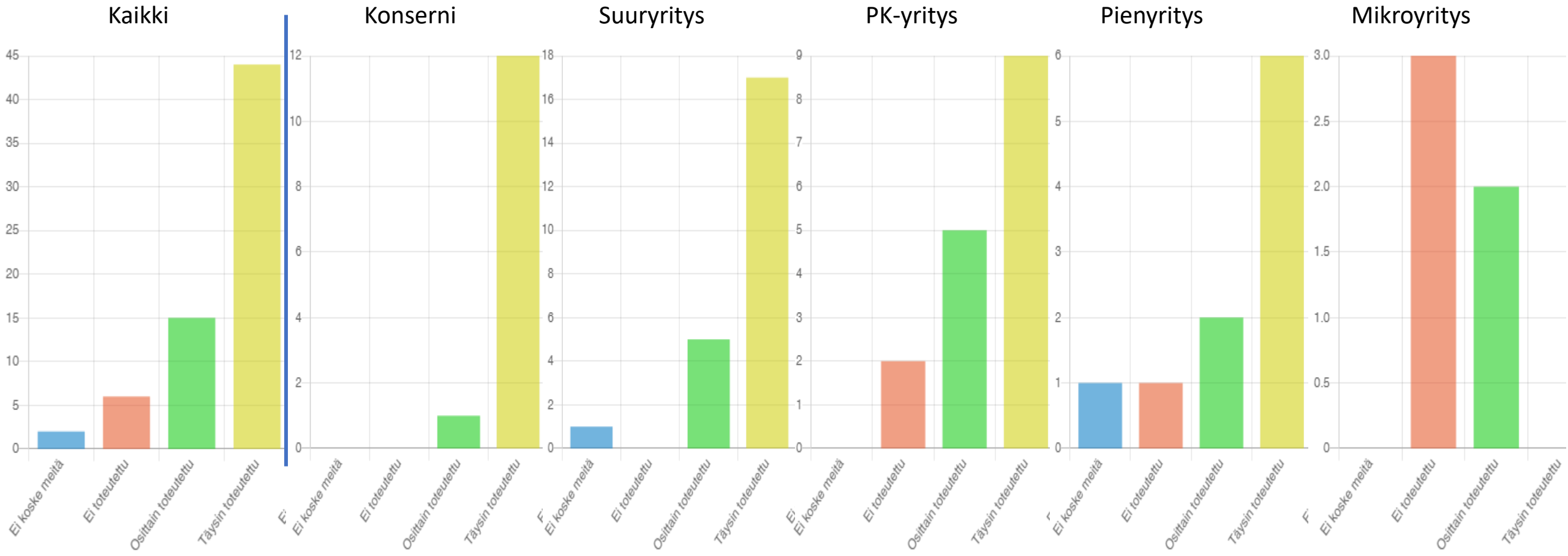
Pienyritys



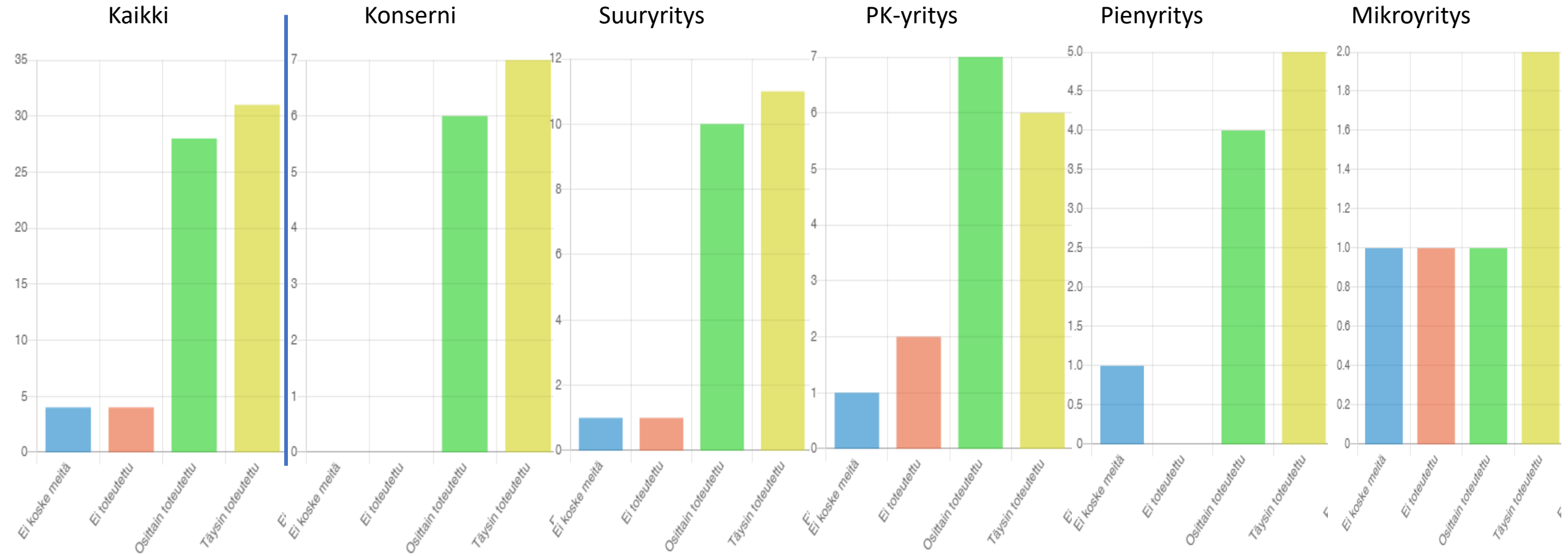
Mikroyritys



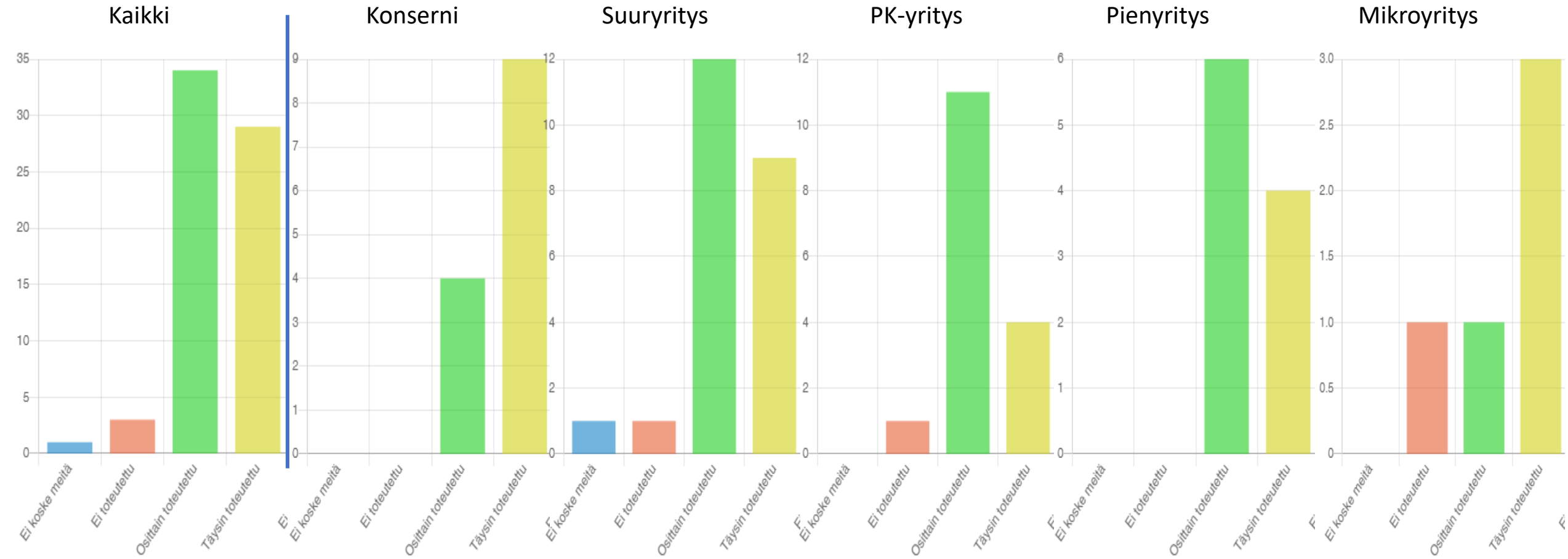
2. Yrityksellä on johdon hyväksymä tietoturvapolitiikka tai vastaava tietoturvallisuuden toteuttamista ohjaava asiakirja.



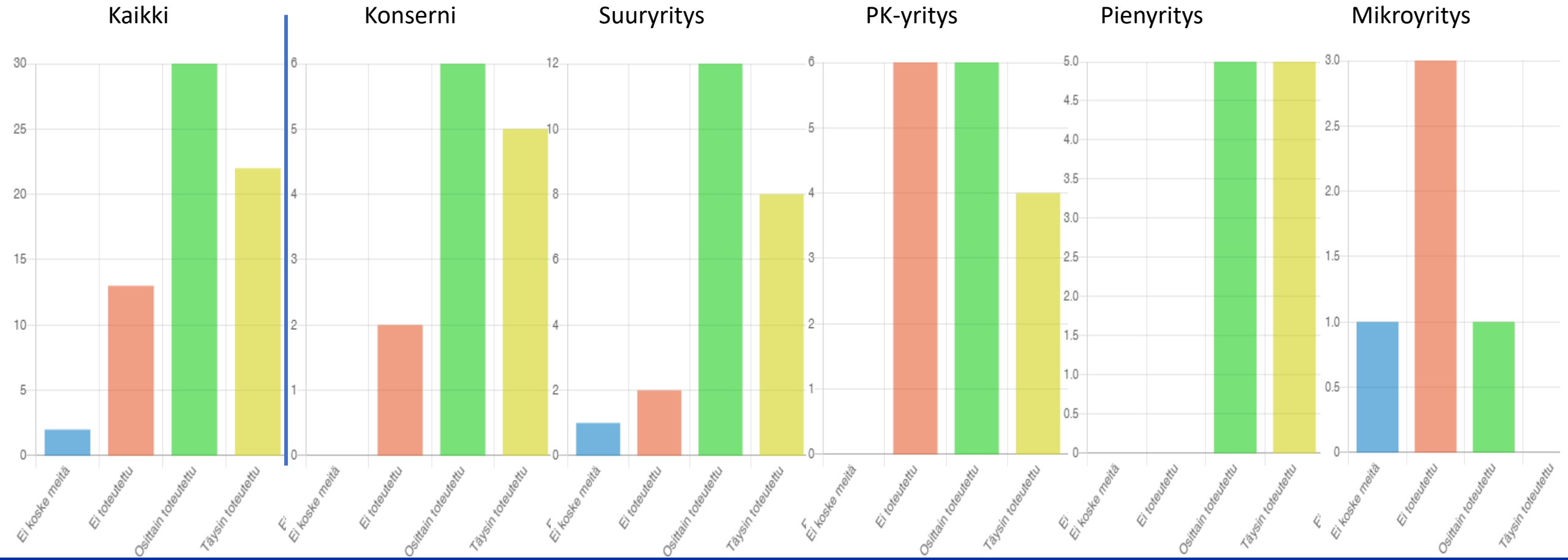
3. Yrityksellä on olemassa käyttövaltuuspolitiikka ja prosessi käyttövaltuuksien hallintaan.



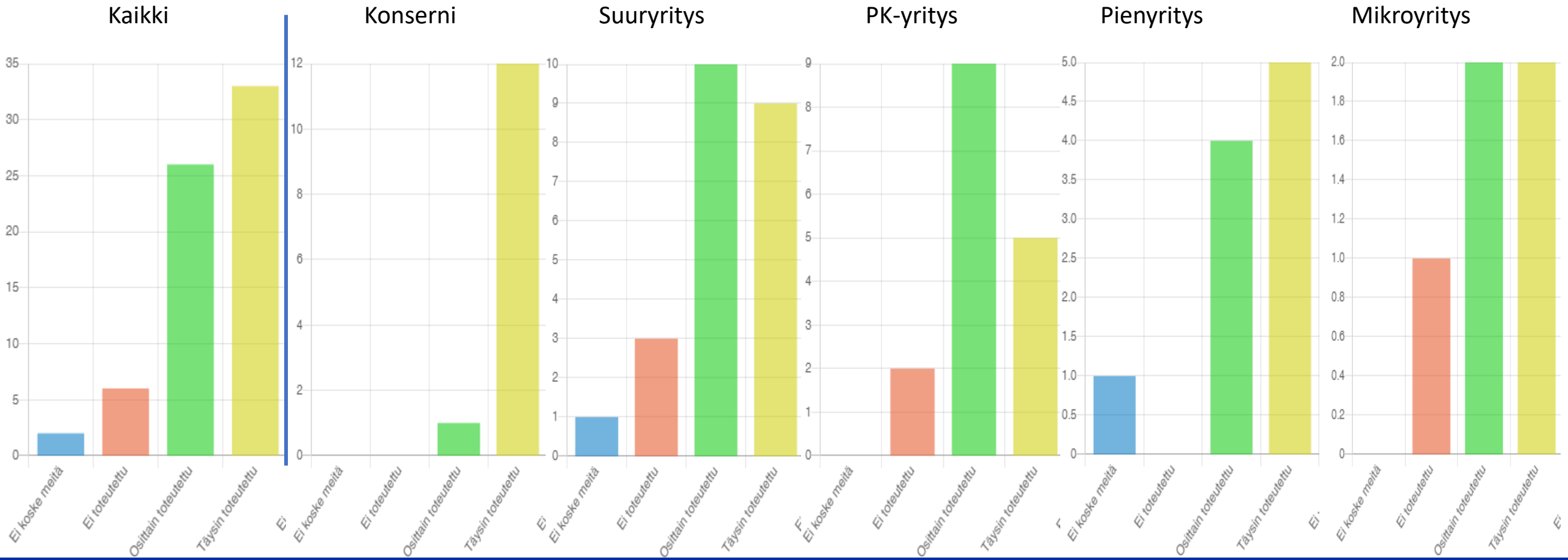
4. Yrityksellä on menettely, jolla se seuraa toimintaympäristössä tapahtuvia ilmiöitä ja arvioi niiden vaikutusta yrityksen toimintaan.



5. Kriittisten toimittajien ja alihankkijoiden kanssa käsitellään digiturvallisuutta säännöllisesti toimittaja/palvelunhallintakokouksissa, (toimitusketjun hallinta).

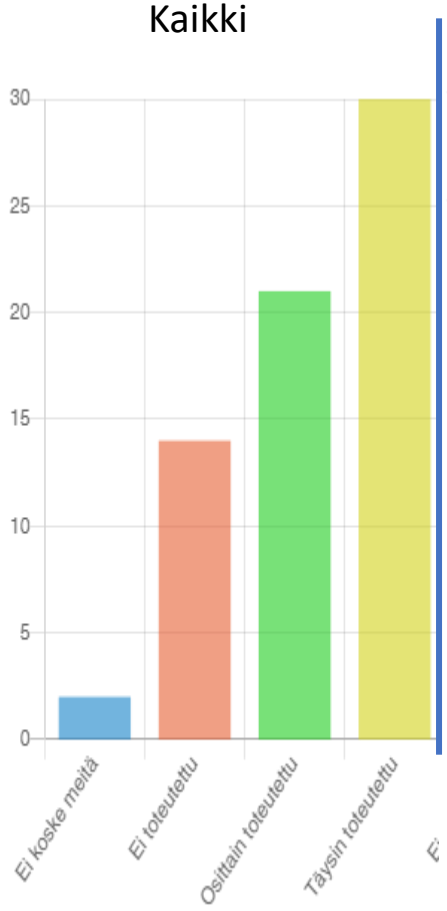


6. Yrityksellä on prosessi ja valmiudet nopeaan ja tehokkaaseen digiturvallisuuden häiriöiden, uhkien ja poikkeamien käsittelyyn.

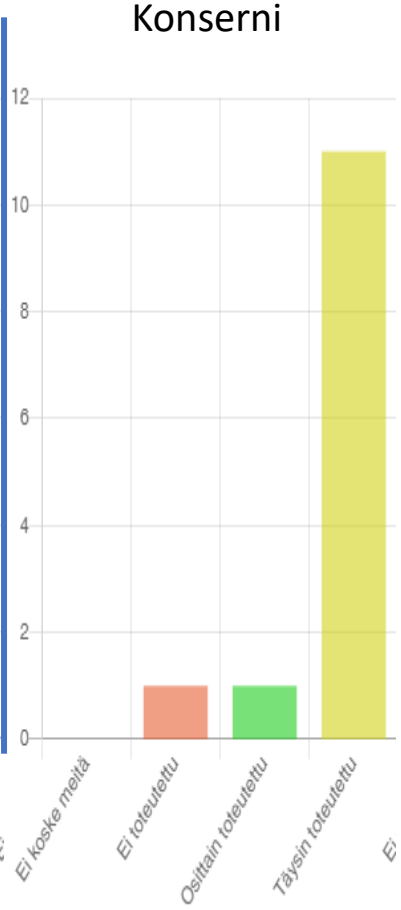


7. Digitaalisen turvallisuuden kokonaistilanteesta raportoidaan säännöllisesti yrityksen johdolle.

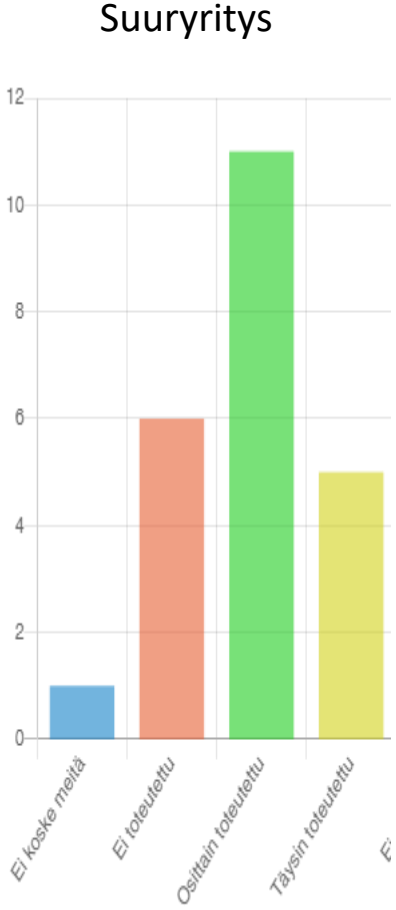
Kaikki



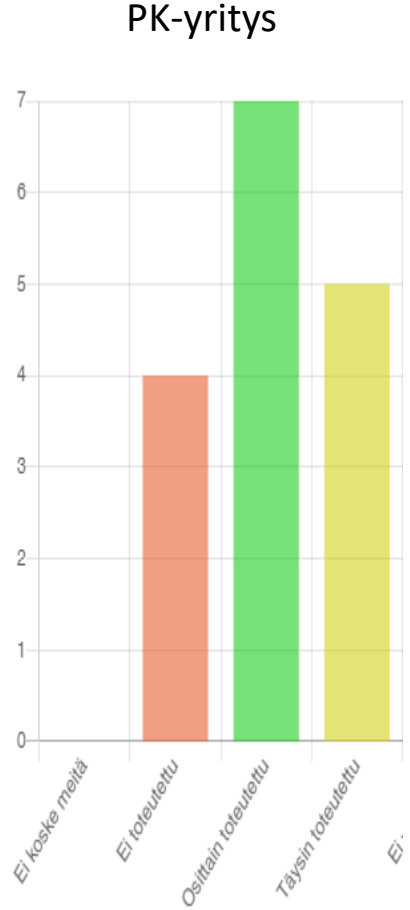
Konserni



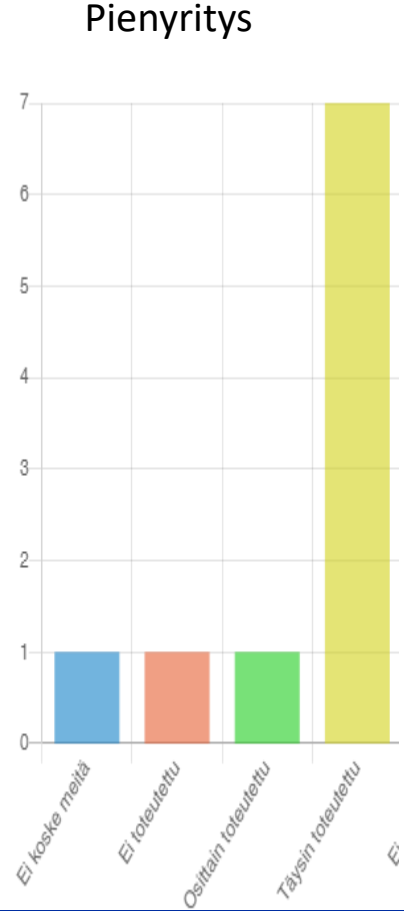
Suuryritys



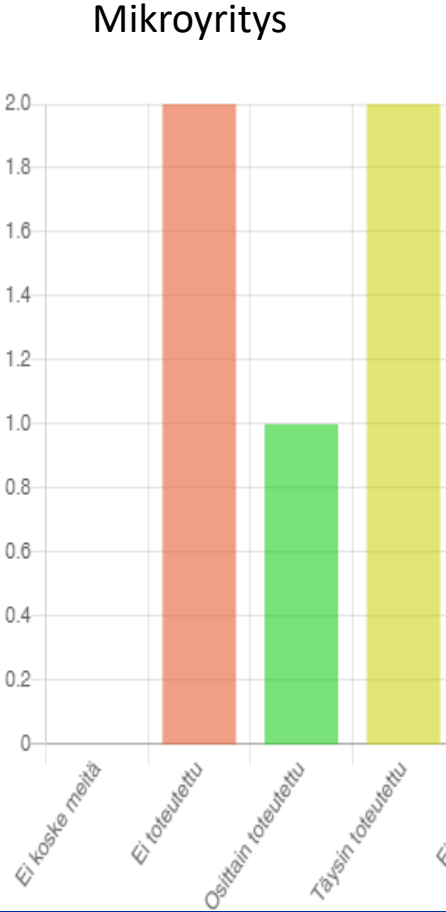
PK-yritys



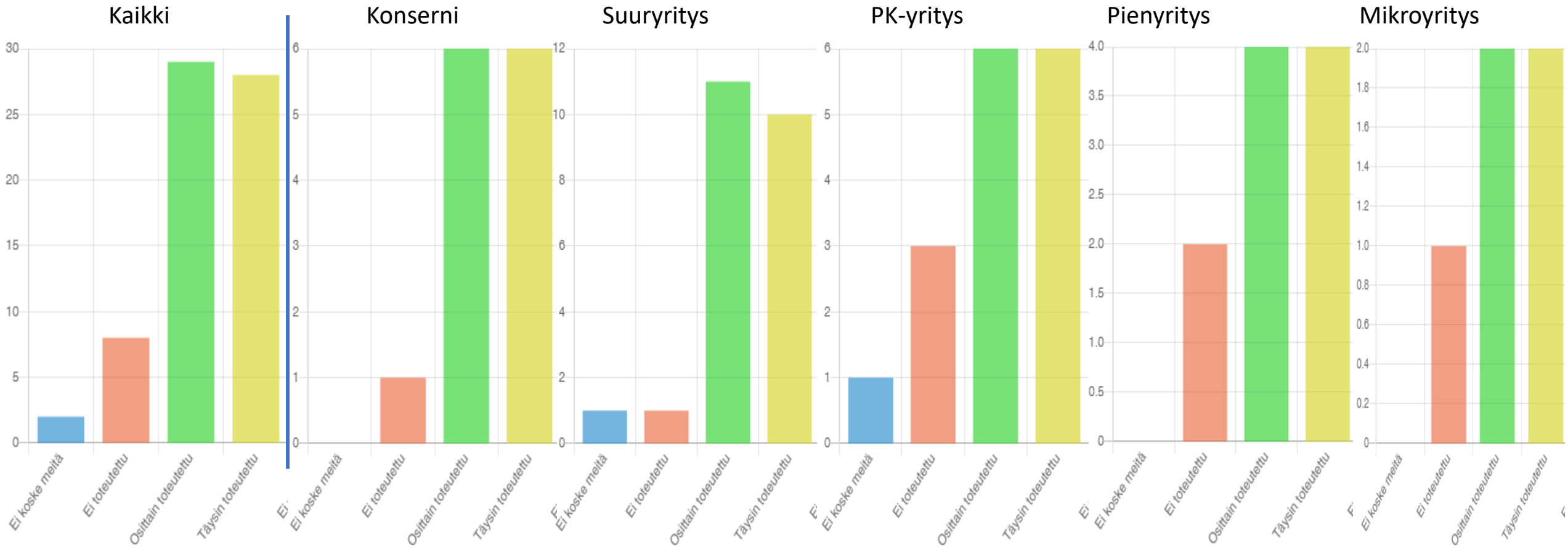
Pienyritys



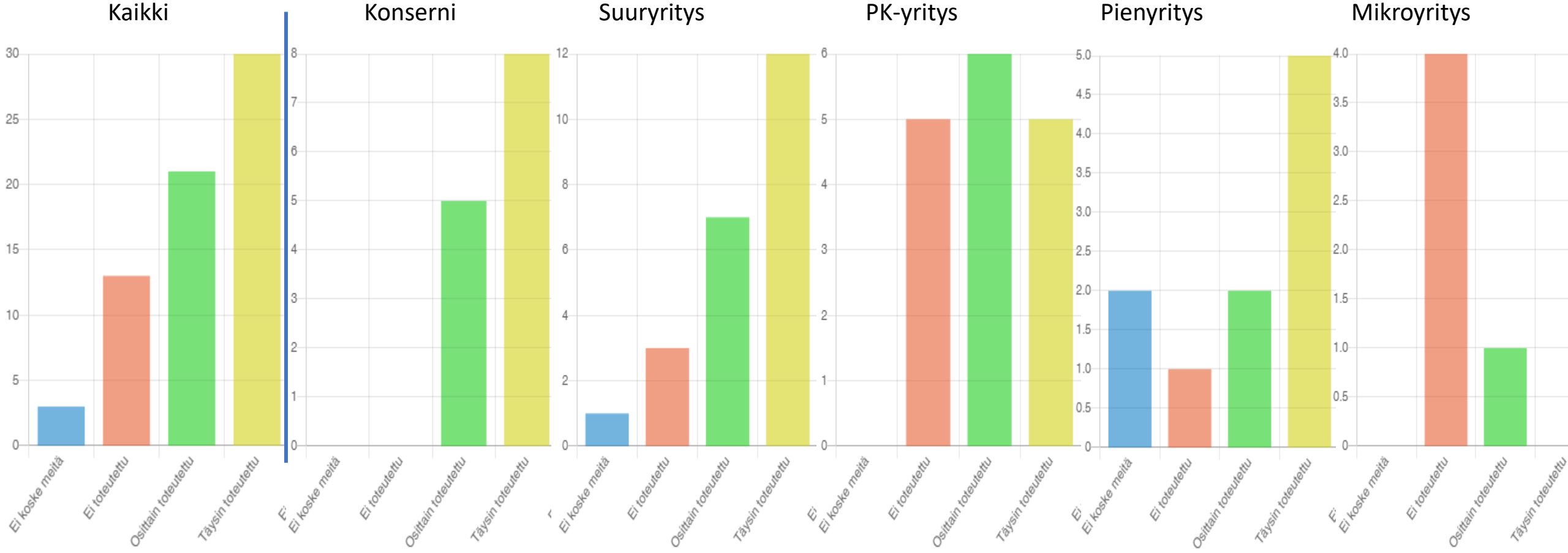
Mikroyritys



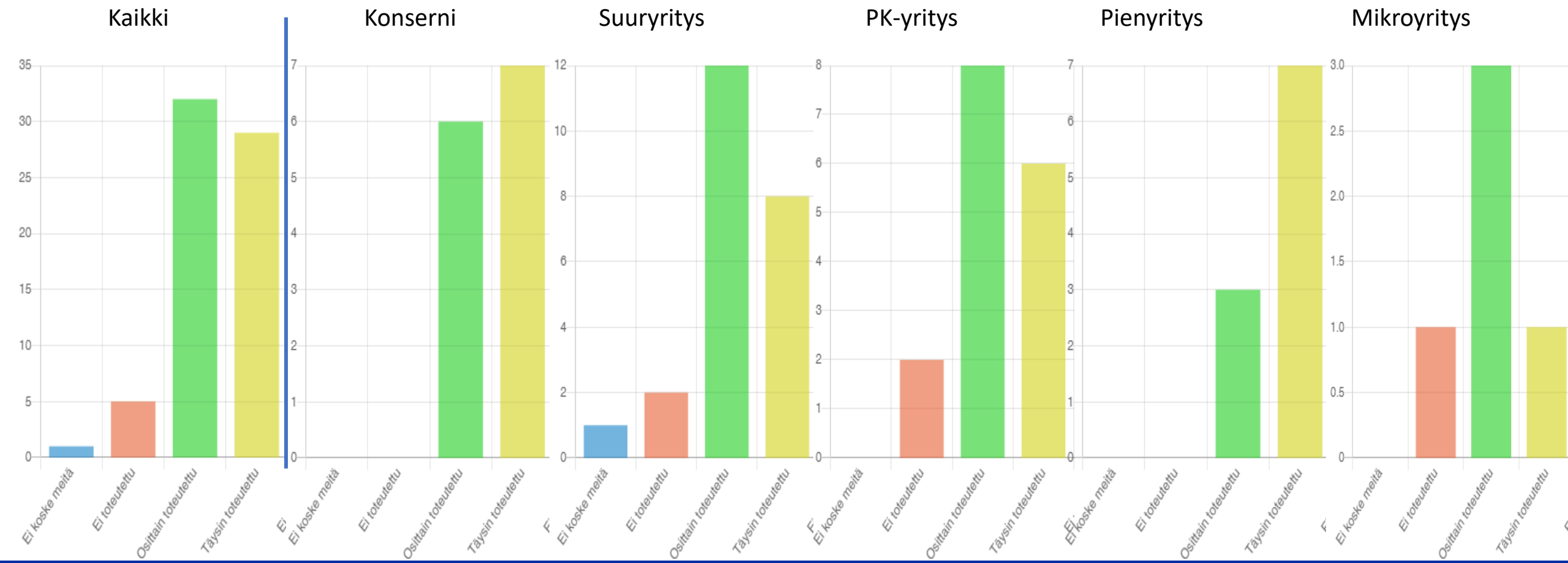
8. Yrityksessä viestitään digiturvallisuuden riskitilanteesta ja uusista riskeistä koko yrityksen laajuisesti.



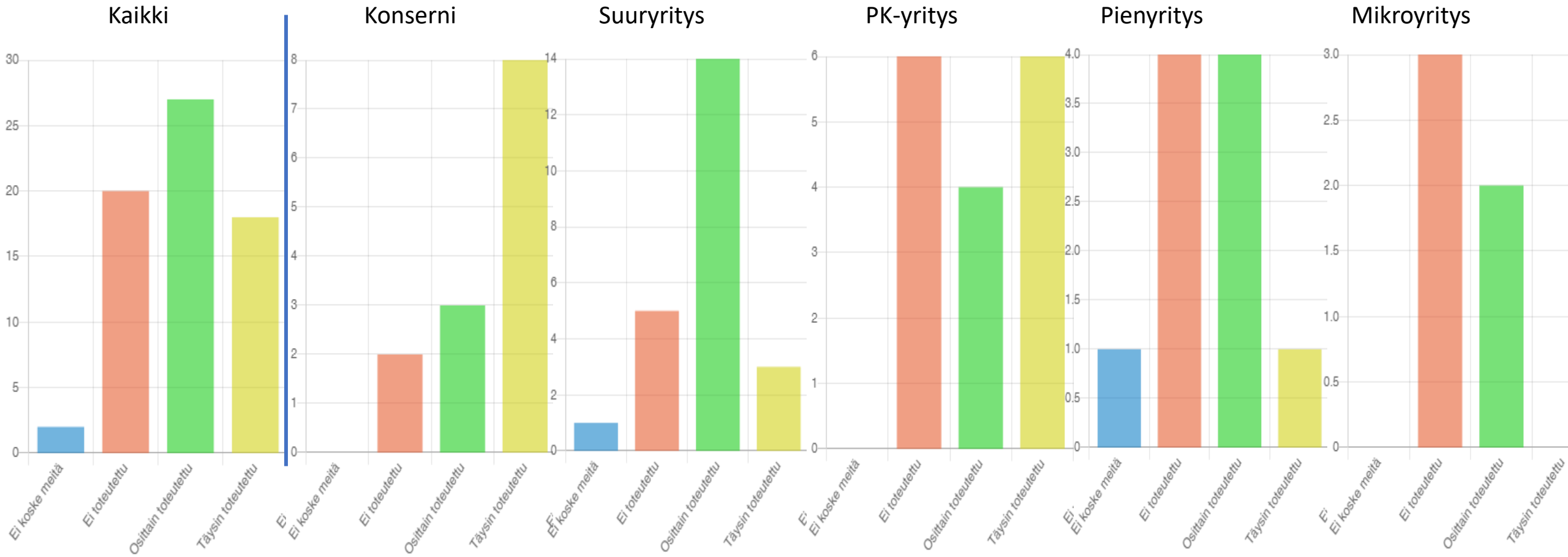
9. Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti.



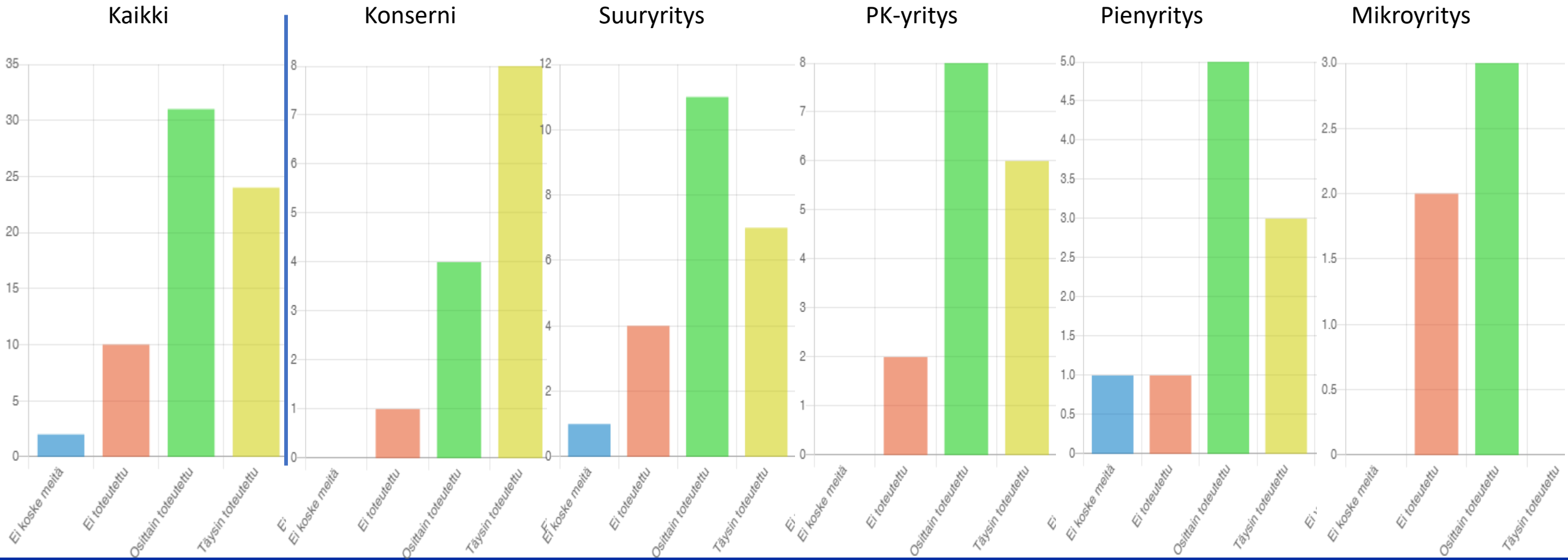
10. Henkilöstölle on olemassa riittävä ohjeistus digitaalisesta turvallisuudesta ja henkilöstölle annetaan säännöllisesti koulutusta digitaalisesta turvallisuudesta.



11. Yritys harjoittelee säännöllisesti sen toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista.



12. Jatkuvuus-, toipumis- ja viestintäsuunnitelmia päivitetään harjoitusten tai toteutuneiden häiriötilanteiden perusteella.



13. Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa?

1. Laaja-alaisessa liiketoiminnassa absoluuttiset vastaukset ovat hankalasti konkretisoitavissa.

Johtopäätökset

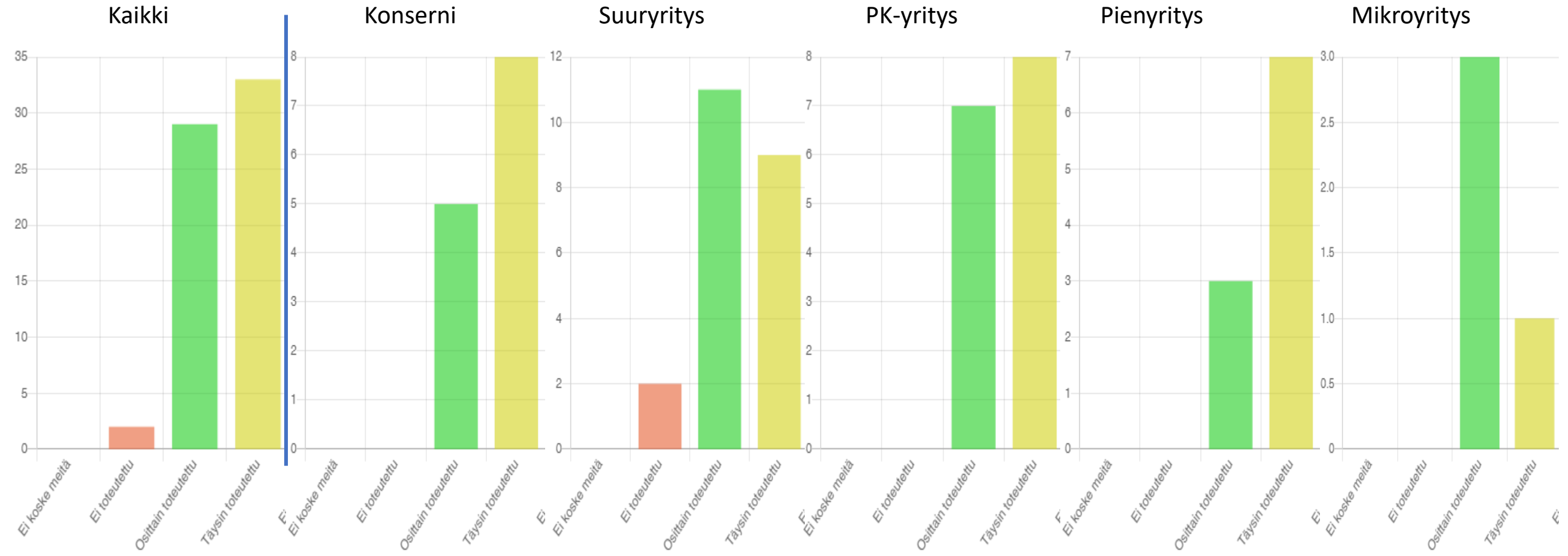
Pääsääntöisesti yrityksillä on hallintamalli digiturvallisuuden kehittämiseen, vaikka yksittäisiä yrityksiä, joilla ei ole, löytyy kaikista kokoluokista. Tietoturva- ja käyttövaltuuspolitiikat ovat useimmilla yrityksillä toimeenpanoa ohjaavia dokumentteja.

Toimintaympäristön seurantaan PK-yrityksillä on eniten parannettavaa ml. digiturvallisuus toimitusketjuissa.

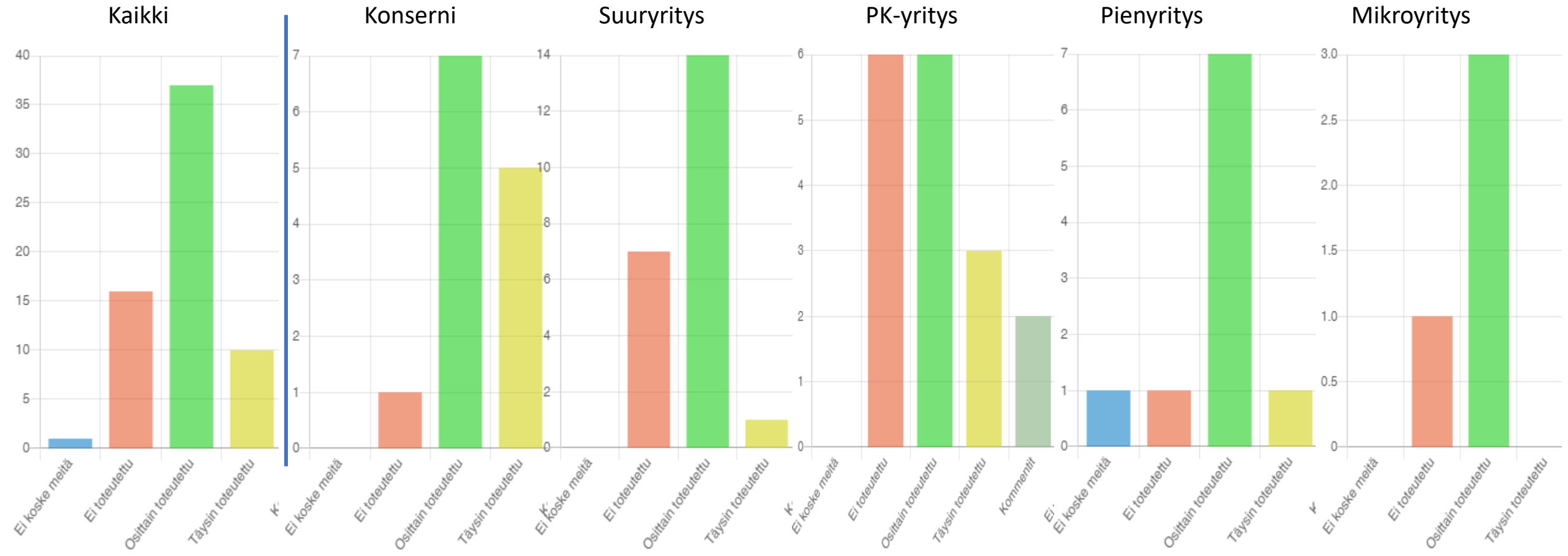
Yritysjohdon raportointiin ja riskeistä viestimiseen tulee kiinnittää huomiota myös pienissä yritysluokissa.

PK-yritysten auditoinneissa on kehitettävää. Ohjeistukset jatkuvuuden, toipumisen ja viestinnän osalta näyttävät olevan kohdallaan, mutta säännöllinen harjoittelu on harvaa tai puuttuu kokonaan.

1. Yrityksen tehtävät ja vastuut on tunnistettu ja kuvattu selkeästi.



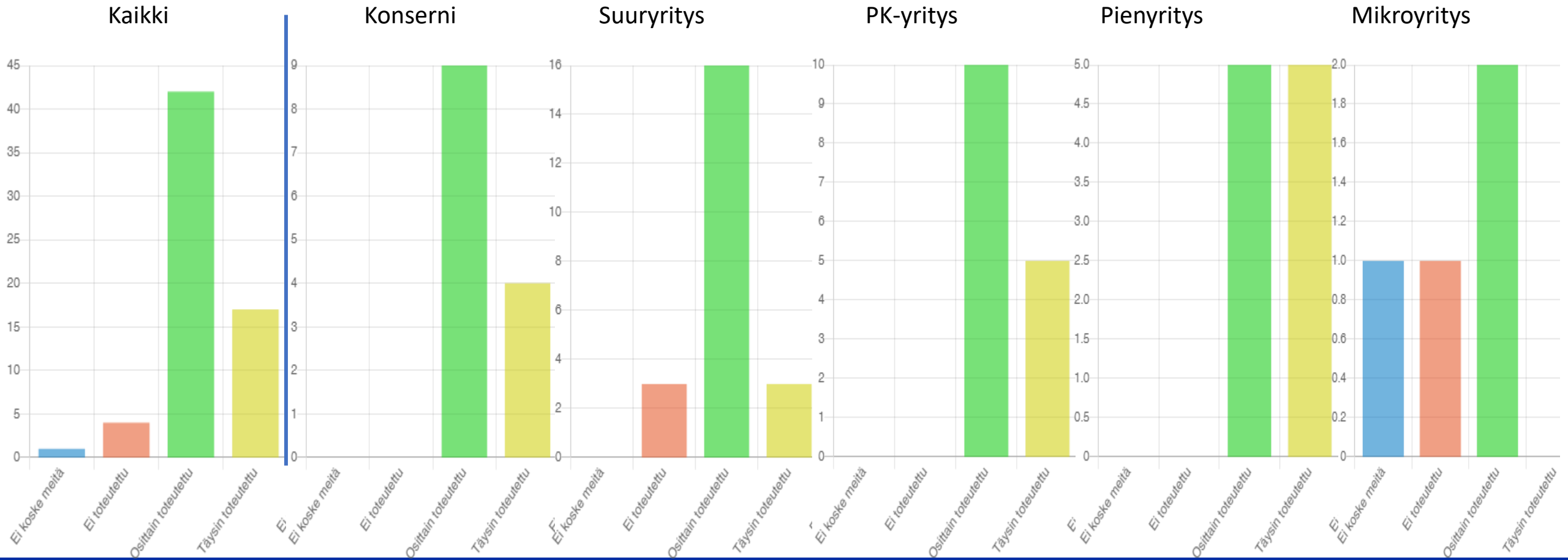
2. Yrityksellä on strategiaprosessi, joka huomioi kyberympäristön vaikutukset omaan liiketoimintastrategiaan.



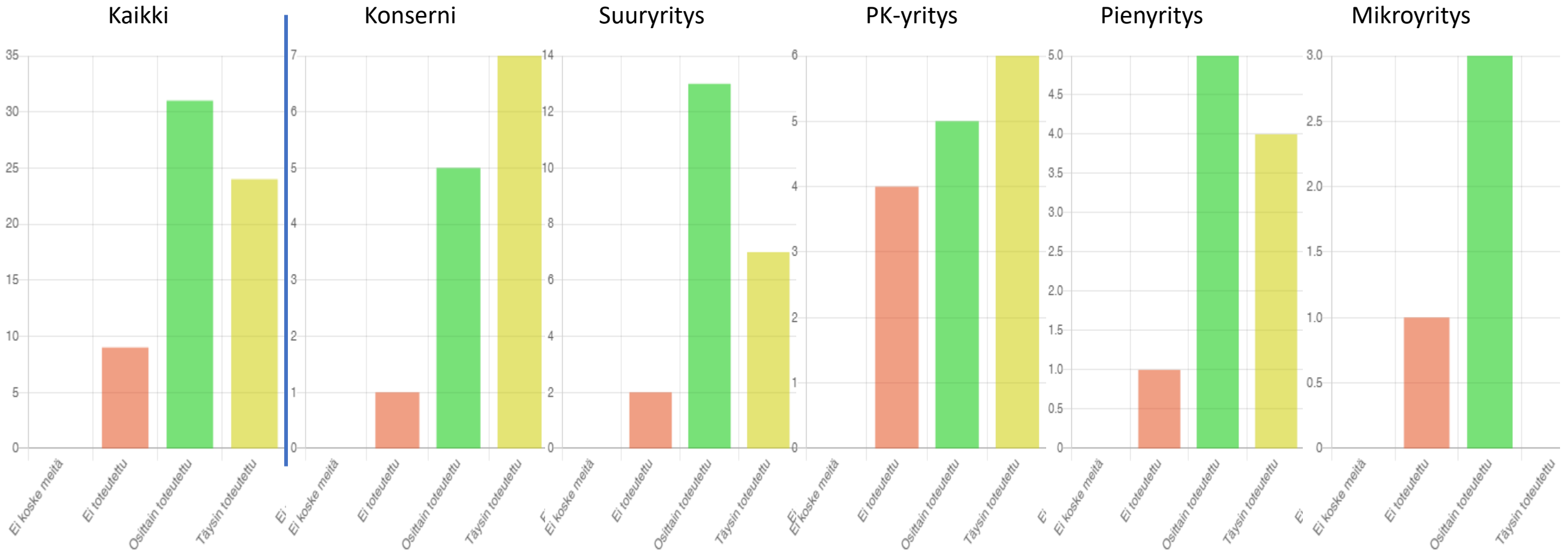
2. Anna toteutuksesta esimerkki.

1. Kaikki toimintaympäristön vaikutukset otetaan strategiatyössä huomioon
2. Osana yleistä ympäristöseurantaa
3. Osana ICT strategiaa

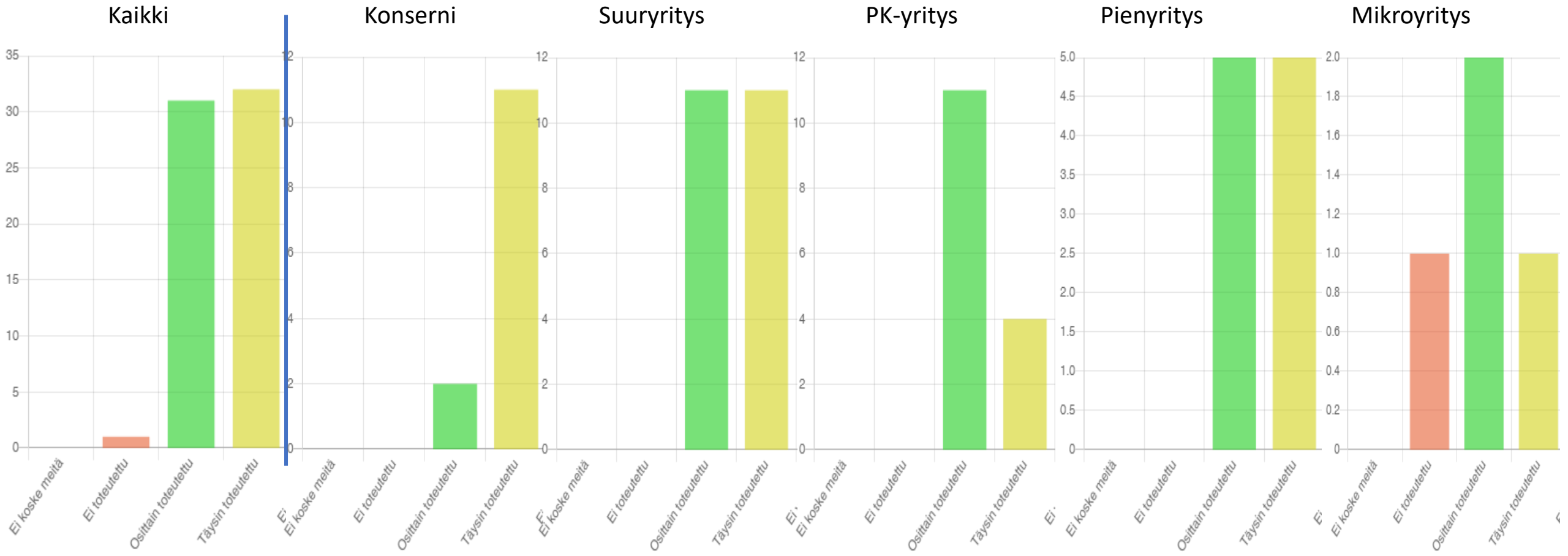
3. Yritys on huomioinut digitaalisen turvallisuuden osana yrityksen prosesseja, toimintamalleja ja järjestelmiä (kokonaisarkkitehtuuria).



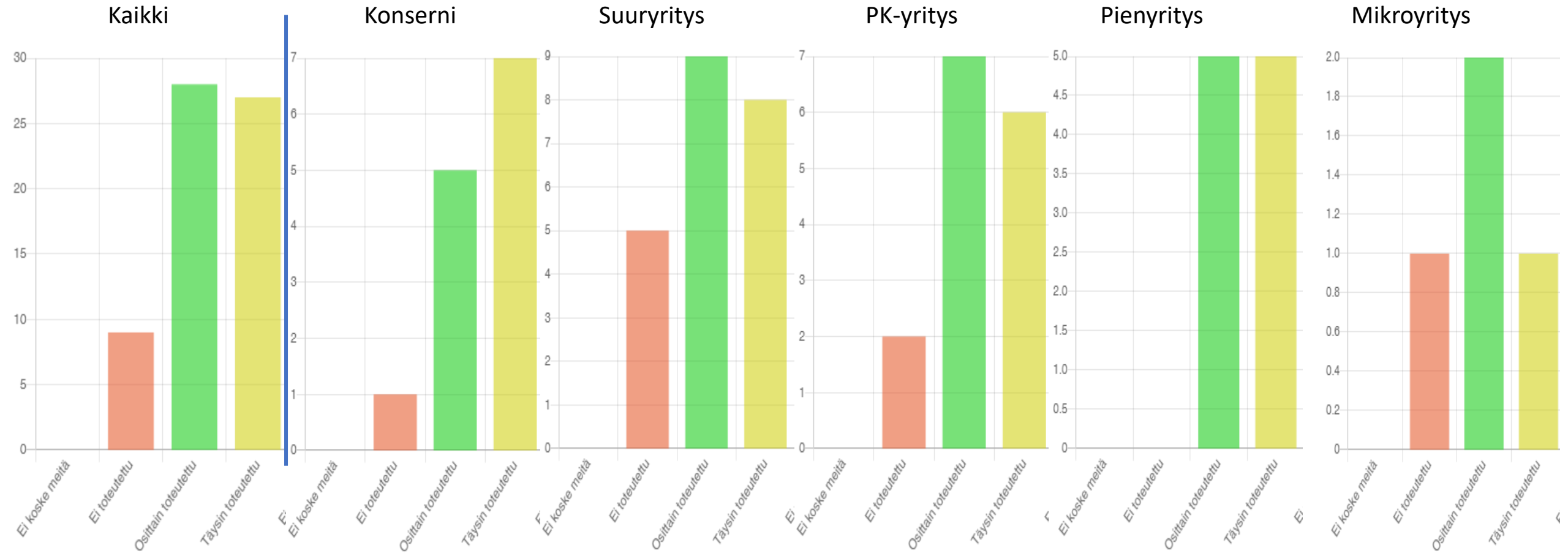
4. Yritys tekee digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt (kyberturvallisuus), toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen.



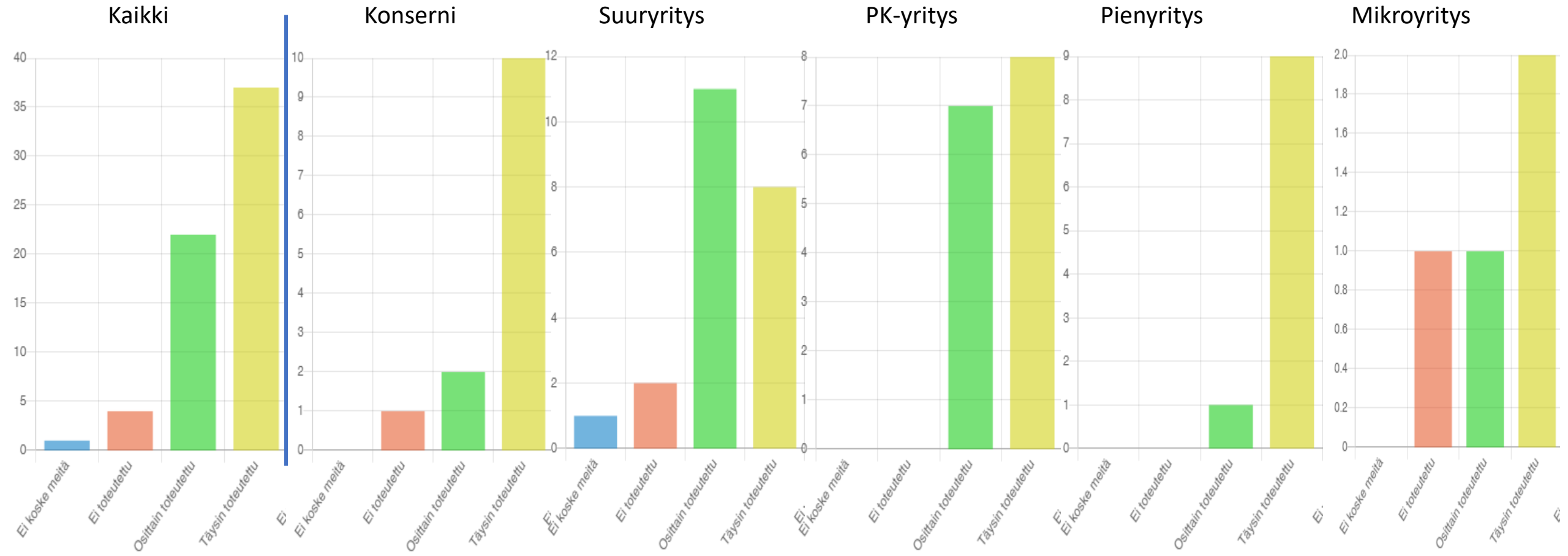
5. Yritys on kartoittanut sen digitaalista turvallisuutta ohjaavan lainsäädännön ja tunnistanut siitä aiheutuvat velvoitteet.



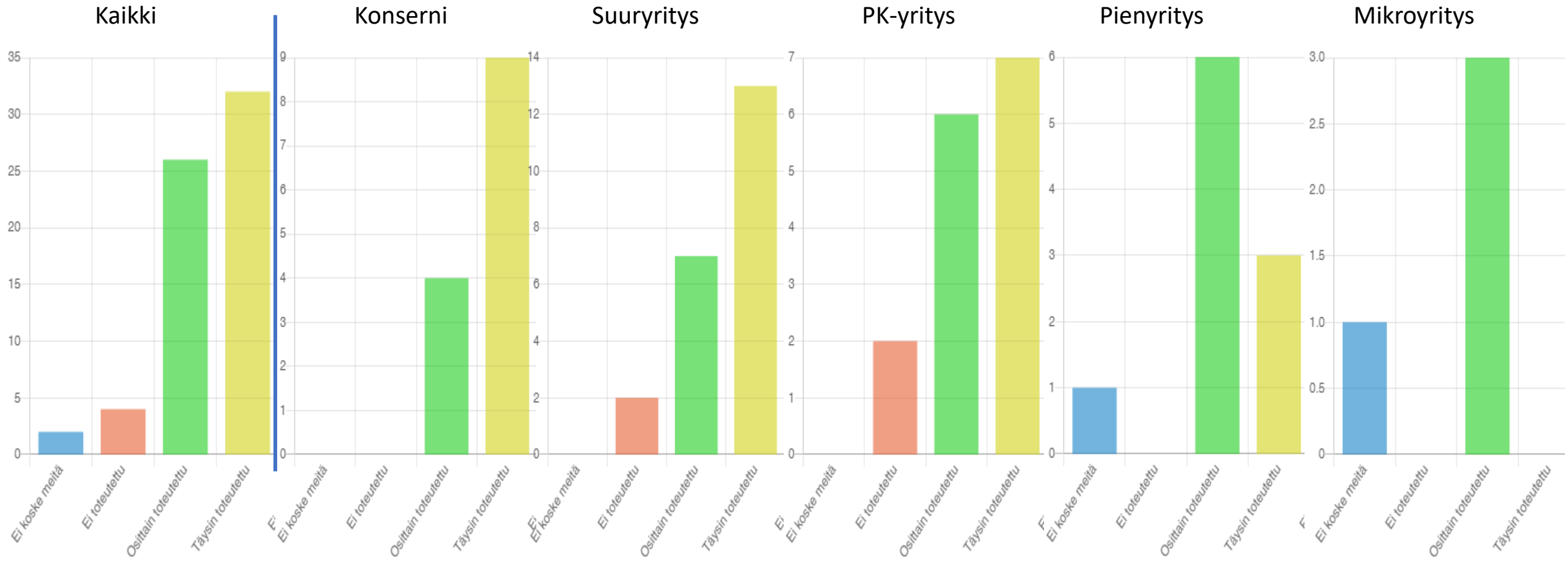
6. Yritys on kartoittanut keskeiset sidos- ja asiakasryhmät sekä niiltä tulevat digiturvavaatimukset.



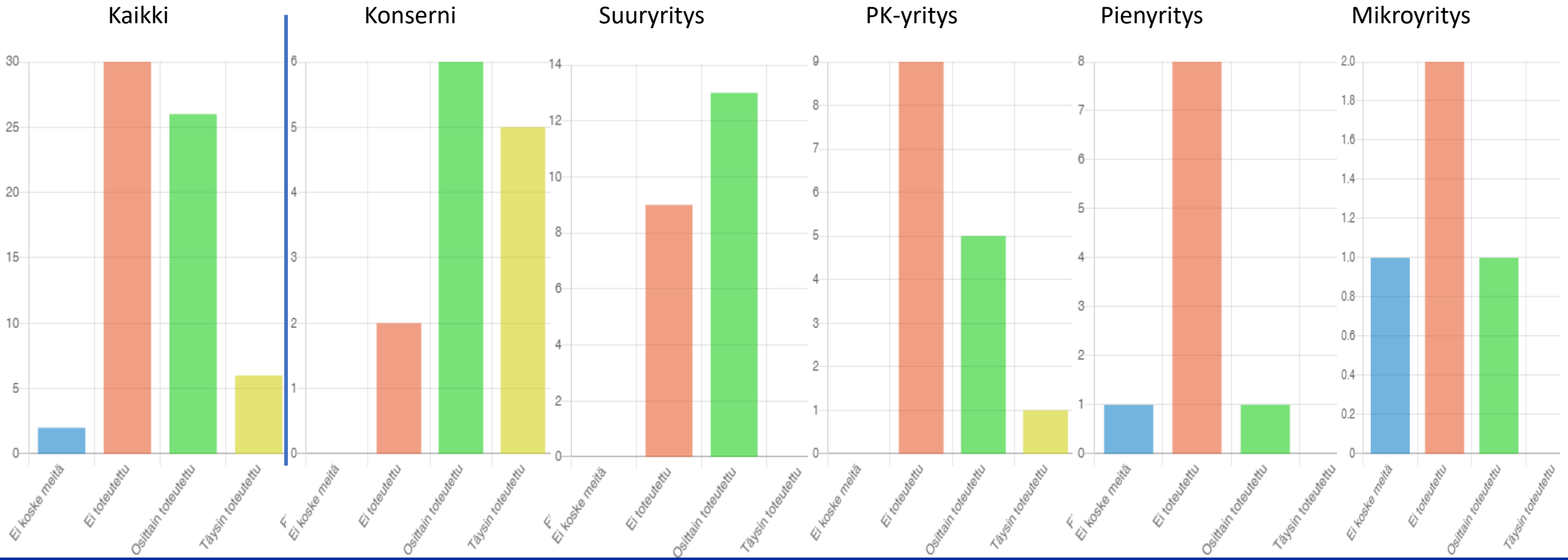
7. Yrityksessä on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten yritysten tai yhteiskunnan toimintaan.



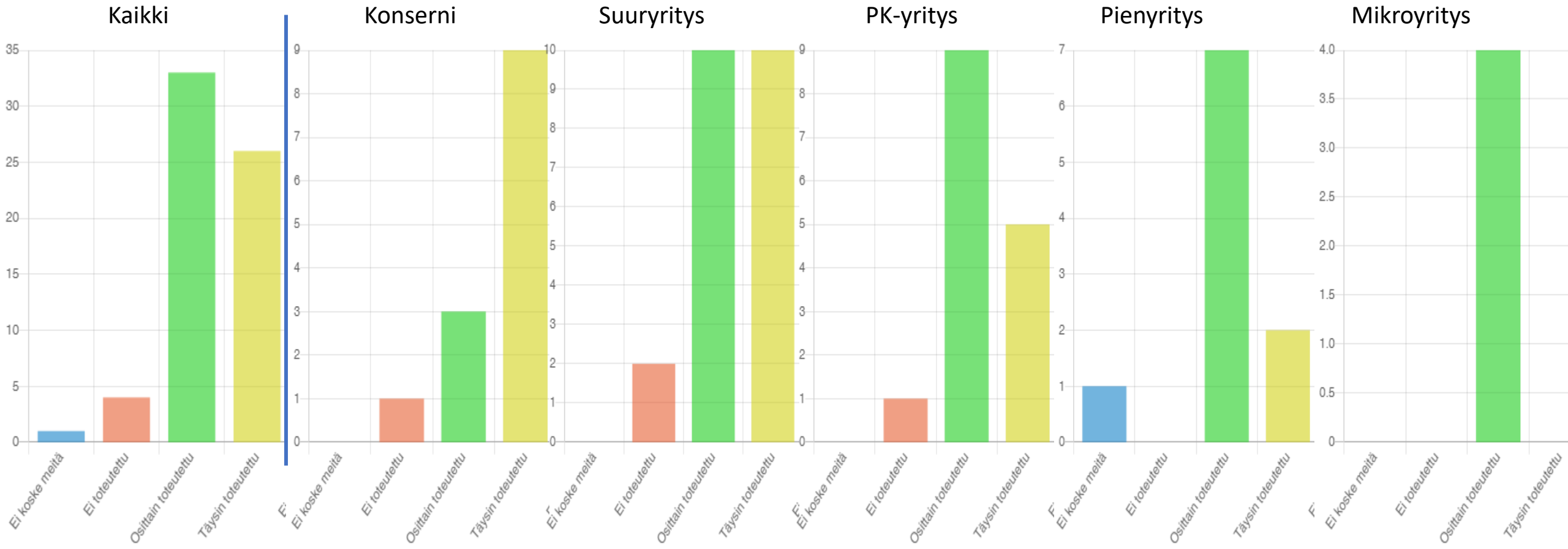
8. Tietoturva- ja tietosuojavaatimukset ovat osa hankintavaatimuksia ja sopimuksia.



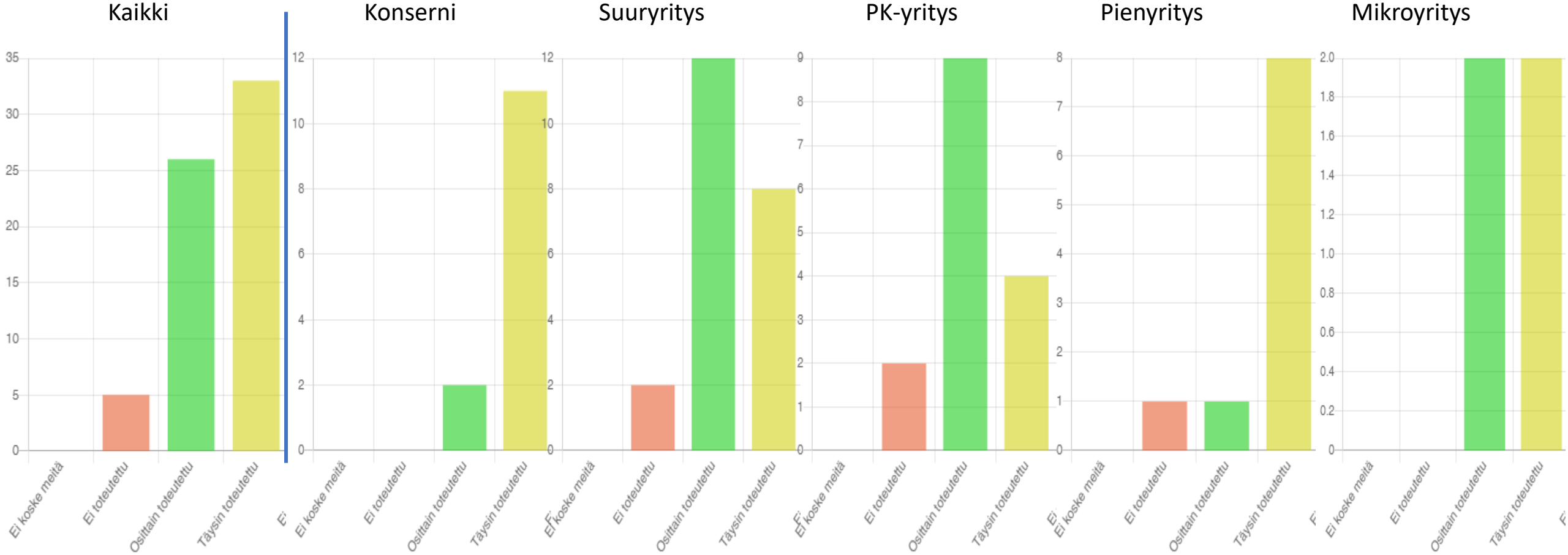
9. Yrityksessä on määritelty digitaaliseen turvallisuuteen liittyvät mittarit, joiden avulla yritys voi seurata osa-alueiden kehittymistä.



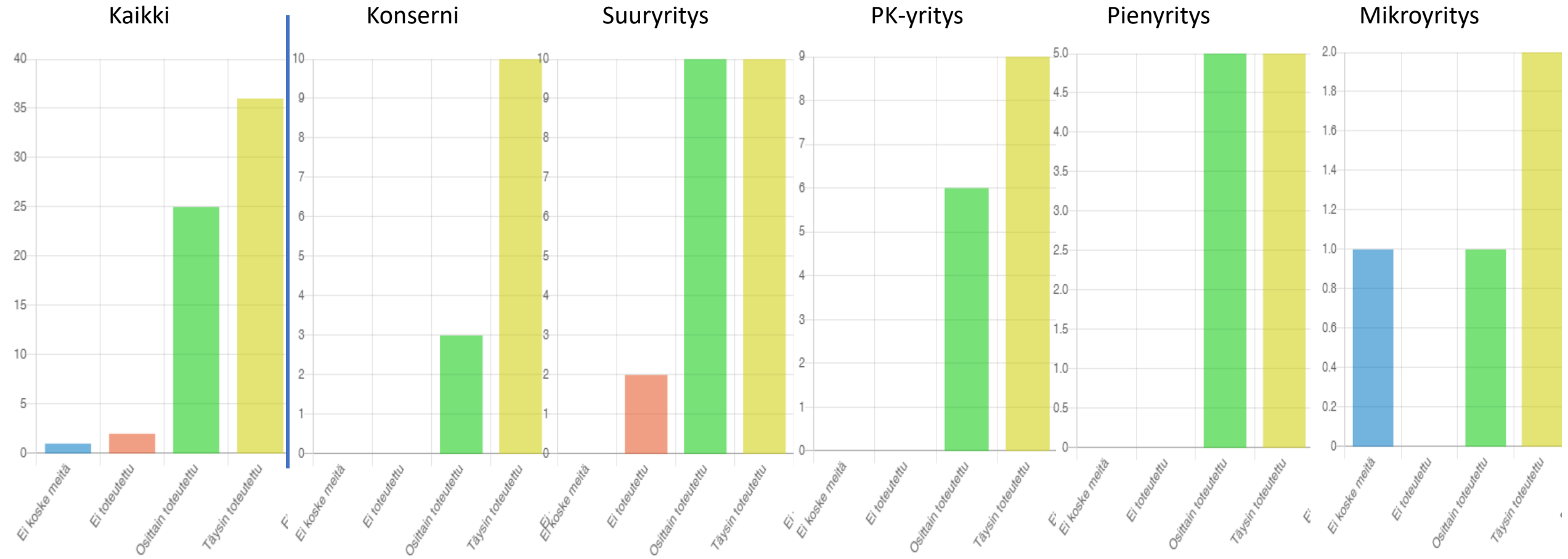
10. Yrityksessä kehitetään riskienhallintaprosessia riskienhallinnan tavoitteiden tai saatujen kokemusten perusteella.



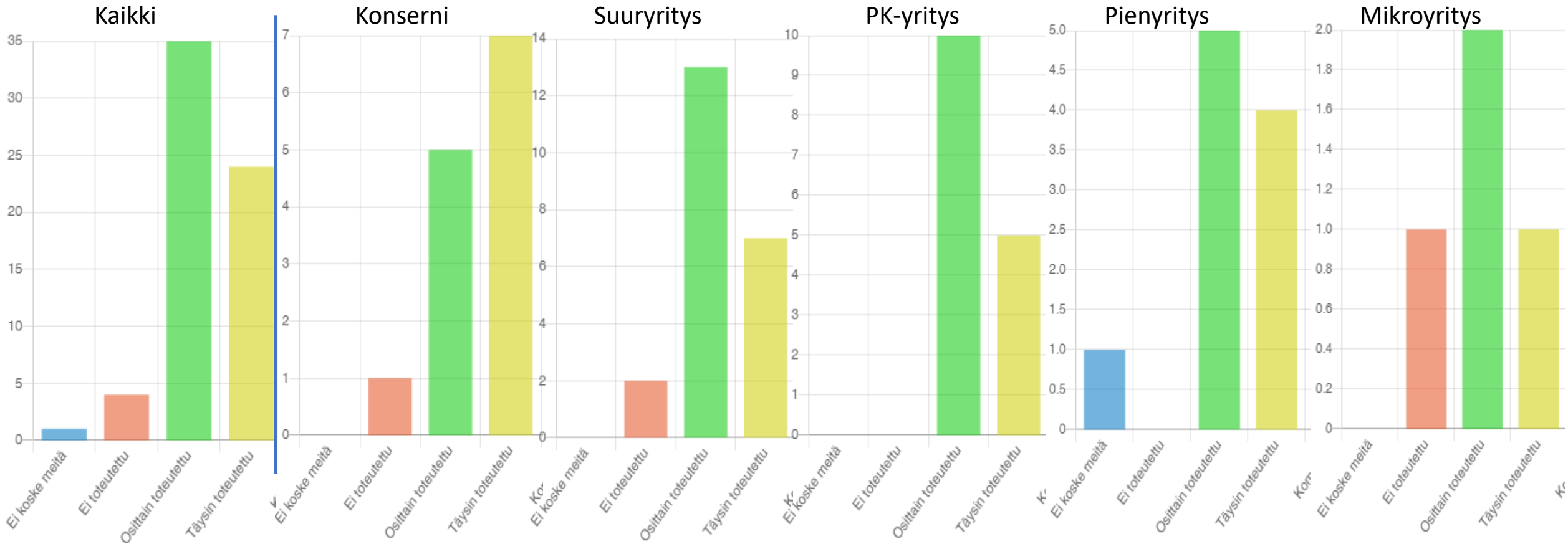
11. Yrityksellä on kyky valita toiminnan edellyttämät kyberturvalliset teknologiat.



12. Yrityksen tehtävät ja vastuut ovat selkeät myös poikkeustilanteissa ja poikkeusoloissa.



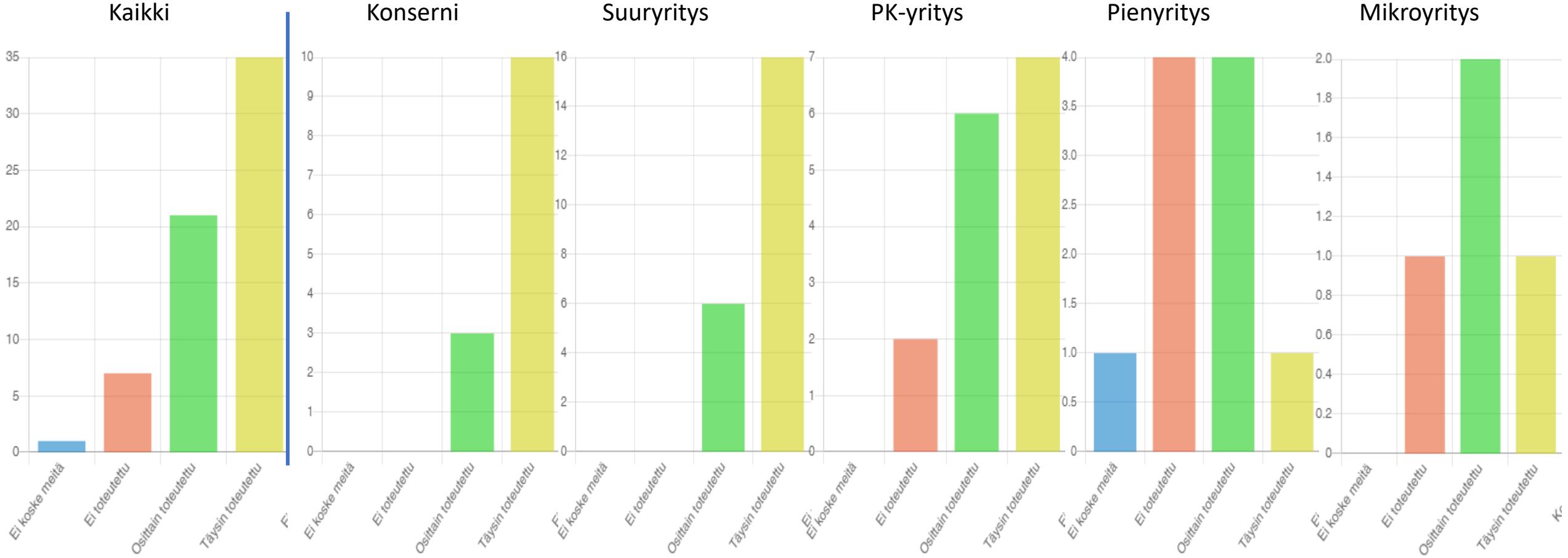
13. Yrityksellä on toteuttamiskelpoinen varautumisen ja jatkuvuuden hallinnan suunnitelma.



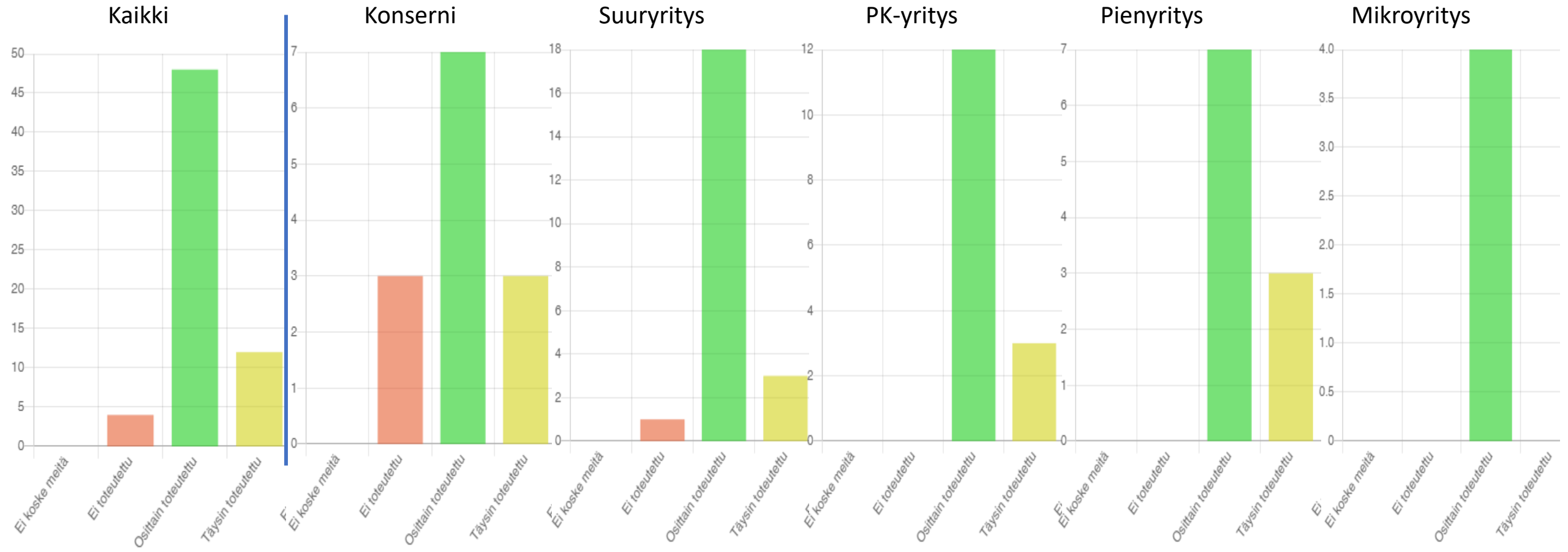
13. Jos kyllä, niin anna toteutuksesta lyhyt digi- ja kyberturvallisuusesimerkki

1. vuosittainen päivittäminen
2. Suunniteltu poikkeuksien varalle
3. Työn alla
4. Monoliittista suunnitelmaa ei ole. Kokemuksemme mukaan se vanhenee ennen valmistumistaan. Toimitamalli perustuu toiminnan skaalaamiseen ja johtamisen muutoksiin sekä alemman tason toipumissuunnitelmiin.
5. Työn alla ja tarkentumassa. Jatkuvaa työtä.
6. ICT:n osalta on laadittu toipumissuunnitelmat
7. Ajantasaisuutta voisi varmasti tarkastella
8. Tuotamme ko suorituskykyjä, joita myös käytämme omassa toiminnassa ml kriittiset asiakkaat.
9. Liiketoiminnoittain olemassa.
10. Ja sitä harjoitellaan säännöllisesti niin sisäisesti kuin ulkoisesti kumppanien kanssa.

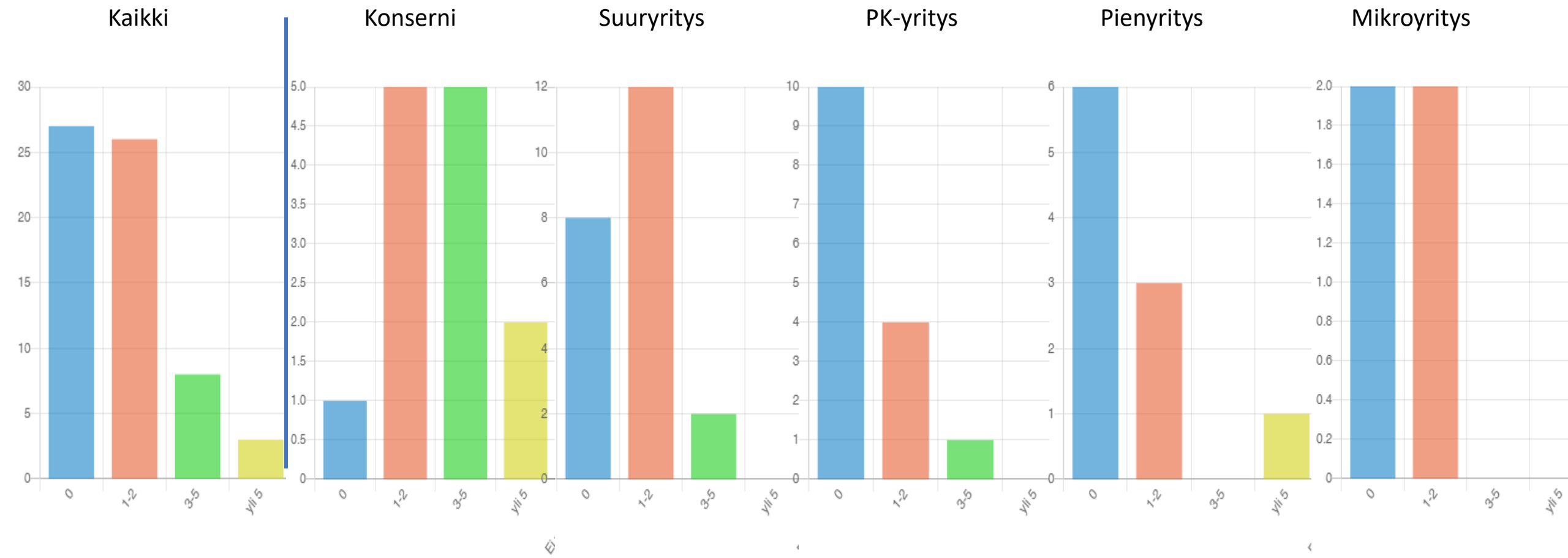
14. Yrityksellä on häiriö- ja kriisitilanteiden viestintäsuunnitelma.



15. Yrityksessä tietoturvasta ja tietosuojasta huolehtiminen on muuttunut toiminnaksi, kulttuuriksi ja asenteeksi.

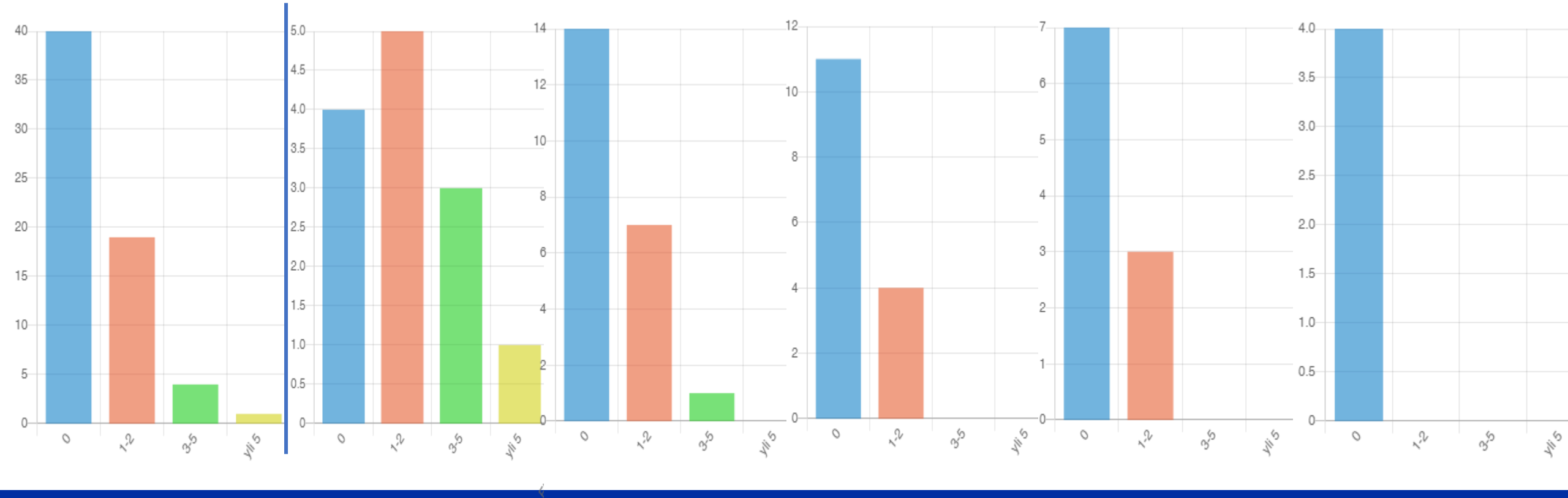


16. Kuinka moneen digitaaliseen turvallisuuteen liittyvään harjoitukseen yritys on osallistunut vuoden 2020 aikana?



17. Kuinka monta digitaaliseen turvallisuuteen liittyvää harjoitusta **yritys on itse järjestänyt** vuoden 2020 aikana?

Kaikki | Konserni | Suuryritys | PK-yritys | Pienyritys | Mikroyritys



18. Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa?

Mikäli kysely olisi ollut englanniksi, olisin löytänyt vastaajaksi strategiatyötämme paremmin tuntevan henkilön.

Johtopäätökset

Yrityksen johtaminen ja toimintamallit ovat selkeästi kuvattuja. Myös liiketoimintaympäristöä havainnoidaan säännöllisesti. Digitaalinen turvallisuus on huomioitu yrityksen prosesseissa, toimintamalleissa ja järjestelmissä. Riskien arviointi kaikilta osin on osa toimintaa, pois lukien PK-yritykset.

Digitaalisuuteen liittyvät velvoitteet on kartoitettu, myös sidos- ja asiakasryhmien osalta kriittiset palvelut. Tietoturva- ja suojavaatimukset ovat osa toimintaa, vaatimuksia ja sopimuksia. Riskien hallintaan on käytössä menettelyt. Teknologioiden valintaa ei nähdä ongelmana.

Hyvästä nykytilasta huolimatta yrityksissä nähdään puutteita:

1. digitaalisen turvallisuuden mittareissa
2. pienyritysten häiriö- ja viestintäsuunnitelmissa
3. harjoittelussa erityisesti PK- ja pienyritysten osalta

Cyberwatch Finland

Huopalahdentie 24 I 00350 HELSINKI I FINLAND I www.cyberwatchfinland.fi