Selvitys kyberturvallisuusdirektiivin (NIS2-direktiivi) riskienhallintavelvoitteiden taloudellisista vaikutuksista elintarvike- ja valmistussektoreille

Loppuraportti

Tilaaja: Liikenne- ja viestintäministeriö

Sisällysluettelo

1 Johdanto

1.1 Selvityksen tausta ja tarkoitus

Selvityksessä arvioidaan liikenne- ja viestintäministeriöltä (”LVM”) maaliskuussa 2023 saadun toimeksiannon mukaisesti kyberturvallisuusdirektiivin[1] (jäljempänä ”NIS2-direktiivi”) taloudellisia vaikutuksia niihin elintarvike- ja valmistussektoreiden toimijoihin, joiden on arvioitu kuuluvan direktiivin soveltamisalaan. Selvitys on osa liikenne- ja viestintäministeriössä asetettua säädöshanketta, jonka tavoitteena on laatia hallituksen esitys NIS2-direktiivin velvoitteiden saattamiseksi osaksi kansallista lainsäädäntöä.

Selvityksessä NIS2-direktiivin taloudellisia vaikutuksia arvioidaan kartoittamalla vastauksia seuraaviin kysymyksiin:

1) Mitkä ovat NIS2-direktiivin elintarvike- ja valmistussektoriin kuuluvien, Suomeen sijoittautuneiden yritysten keskimääräiset kyberturvallisuuskustannukset;

2) Millaisia taloudellisia vaikutuksia NIS2-direktiivin riskienhallintavelvoitteista (artikla 21) aiheutuu elintarvike- ja valmistussektoriin kuuluville yrityksille sekä lyhyellä että pitkällä aikavälillä, ottaen huomioon direktiivin riskienhallintavelvoitteiden mukaisten palvelujen hankintakustannukset;

3) Mitä velvoitteiden noudattamisesta syntyviä kustannushyötyjä voidaan tunnistaa yritysten kybermaturiteetin parantuessa.

Selvityksen kohteena ovat NIS2-direktiivin liitteen II kohtien 4 ja 5 mukaiset elintarvike- ja valmistussektorit. Kyseiset sektorit eivät ole kuuluneet aiemman niin sanotun NIS1-direktiivin[2] soveltamisalaan.

Selvityksen on laatinut Insta Advance Oy (”Insta”). Selvityksen lopullinen versio on luovutettu LVM:lle 23.5.2023.

1.2 Selvityksen rajaus

Selvityksessä arvioidaan yritysten nykyisten kyberturvallisuuskustannusten ja NIS2-direktiivin noudattamisesta syntyvien kustannushyötyjen lisäksi erityisesti sitä, millaisia taloudellisia vaikutuksia NIS2-direktiivin 21 artiklassa säädetyistä riskienhallintavelvoitteista aiheutuu Suomeen sijoittautuneille elintarvike- ja valmistussektoriin kuuluville yrityksille.

Riskienhallintavelvoitteiden lisäksi NIS2-direktiivistä on tunnistettu aiheutuvan mahdollisia kustannuksia ainakin 20 artiklan hallinnointitoimenpiteistä, 23 artiklan raportointivelvoitteista sekä 32–33 artiklan valvonta- ja täytäntöönpanotoimenpiteistä. Muut kuin 21 artiklasta

---

[1] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta.

[2] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.

johtuvat taloudelliset vaikutukset on rajattu saadun toimeksiannon mukaisesti tämän selvityksen ulkopuolelle.

1.3 Toteutustapa ja kattavuus

Instan suorittama selvitys on toteutettu haastattelemalla elintarvike- ja valmistussektorin yrityksiä sekä kuulemalla yrityksiä sähköisen kyselylomakkeen avulla (yhdessä ”kyselytutkimus”). Haastatteluissa Instan tietoturva-asiantuntijat täyttivät kyselylomakkeen saatujen vastausten perusteella ja keskustelivat arviointikysymyksistä yritysten edustajien kanssa.

Haastattelun kysymykset ovat olleet ennalta määriteltyjä ja niissä on arvioitu yritysten

a) tämänhetkistä tilannetta liittyen NIS2-direktiivin 21 artiklan mukaisten riskienhallintavelvoitteiden täyttämiseen,

b) velvoitteiden täyttämiseen tarvittavia lisäresursseja,

c) velvoitteiden täyttämisestä saatavia kustannushyötyjä sekä

d) kyberturvallisuuden ylläpidon vuotuisia kustannuksia.

Haastatteluissa ja kyselylomakkeella on käytetty samoja kysymyksiä.

Kyselytutkimuksen tulokset on esitetty tämän selvityksen lisäksi liitteenä olevassa työ- ja elinkeinoministeriön (TEM) sääntelytaakkalaskurissa (LIITE 1 & 2).

Kyselytutkimukseen osallistui 20 yritystä, joista 15 oli suuria yrityksiä ja 5 keskisuuria yrityksiä. Yrityksen koon arvioinnissa on käytetty suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaisia keskisuuria yrityksiä koskevia kynnysarvoja. Kyselytutkimukseen osallistui elintarvikesektorilta 10 yritystä, joista 6 osallistui haastatteluun ja 4 täytti kyselylomakkeen. Valmistussektorilta kyselytutkimukseen osallistui 10 yritystä, joista 7 osallistui haastatteluun ja 3 täytti kyselylomakkeen.

TAULUKKO 1. Vastaajat sektoreittain

Sektori	Suuria yrityksiä	Keskisuuria yrityksiä	Haastatellut yritykset	Kyselylomakkeen täyttäneet yritykset	Osallistuneet yhteensä
Elintarvike	7	3	6	4	10
Valmistus	8	2	7	3	10

2 Selvityksen tulokset

2.1 Nykyiset kyberturvallisuuskustannukset elintarvike- ja valmistussektoreilla

Osana kyselytutkimusta yritykset arvioivat nykyisiä kyberturvallisuuskustannuksiaan. Kyselytutkimuksessa yrityksiä pyydettiin ilmoittamaan vuosittaiset kyberturvallisuuskustannukset prosentteina liikevaihdosta.

Kyberturvallisuuskustannuksilla tarkoitetaan yritysten kyberturvallisuuteen liittyviä kuluja, jotka lukeutuvat useimmiten laajemmin toimijoiden ICT-kokonaiskustannuksiin. Kyberturvallisuuskustannuksiin on katsottu kuuluvan laajasti erilaisia menolajeja, kuten laitteistot, ohjelmistot ja tietoliikenneyhteydet. Kyselytutkimuksessa muina esimerkkeinä kyberturvallisuutta edistävistä kustannuksista annettiin erilaiset hallinnolliset kulut, henkilöstökulut sekä auditoinnit ja koulutukset. Lisäksi taloudellisia vaikutuksia katsottiin voivan aiheutua verkko- ja tietojärjestelmien fyysisen turvallisuuden ylläpitämisestä, kuten esimerkiksi laitteistojen ja kaapeleiden asennus- ja ylläpitotoimista.

2.1.1 Tulokset

Elintarvikesektorin yritykset arvioivat nykyisiksi kyberturvallisuuskustannuksiksi keskimäärin 0,28 % vuotuisesta liikevaihdosta. Elintarvikesektorilla vastaukset vaihtelivat välillä 0,02–1 %.

Valmistussektorilla yritykset arvioivat nykyisiksi kyberturvallisuuskustannuksiksi keskimäärin 0,69 % vuotuisesta liikevaihdosta. Valmistussektorilla vastaukset vaihtelivat välillä 0,1–1,8 %. Kolme valmistussektorin yritystä ei osannut arvioida nykyisiä kyberturvallisuuskustannuksia.

TAULUKKO 2. Nykyiset kyberturvallisuuskustannukset

Sektori	**Kyberturvallisuuskustannukset liikevaihdosta (%)**		**Arviointia ei tehty (kpl)**
	Vaihteluväli	Keskiarvo	
Elintarvike	0,02–1	0,28	0
Valmistus	0,1–1,8	0,69	3

2.1.2 Keskeiset havainnot ja päätelmät

Haastattelujen perusteella kyberturvallisuuteen käytettyjen varojen arviointi koettiin monen yrityksen kohdalla haastavaksi, koska näiden kulujen erottaminen laajemmasta ICT-kustannusten ryhmästä on tulkinnanvaraista. Lisäksi haasteita nykykustannusten arvioinnille loi suurten yritysten ja konsernien kohdalla niiden monikansallisuus sekä rakenteellinen kompleksisuus.

Elintarviketoimialan liikevoittomarginaalit ovat TEM:n toimialaraportin (2022:6) mukaan keskimäärin pienempiä kuin muissa teollisuusyrityksissä. Tämä saattaa osaltaan vaikuttaa siihen, että myös kyberturvallisuuskustannusten prosenttiosuus liikevaihdosta on elintarviketoimialan yrityksillä keskimäärin pienempi kuin valmistustoimialalla.

Näin ollen voidaan todeta, etteivät yrityksiltä saadut arviot vuotuisista kyberturvallisuuskustannuksista ole sellaisenaan verrannollisia keskenään samaan sektoriin kuuluvien yritysten välillä taikka elintarvike- ja valmistussektorin yritysten välillä.

Siitä huolimatta, että yritykset kokivat nykyisten kyberturvallisuuskustannusten arvioimisen haastavaksi, voidaan huomata, että tulokset ovat kutakuinkin linjassa EU-komission NIS2-direktiiviehdotuksen taustalla olevan vaikutustenarvioinnin[3] kanssa. EU-komission selvityksen

[3] Ks. komission vaikutustenarviointi ehdotukseen NIS2-direktiiviksi (SWD 2020/345 final).

mukaan yritysten kyberturvallisuuskustannusten (*ICT security spending*) on arvioitu olevan 0,52 % vuotuisesta liikevaihdosta.

Instan kyselytutkimuksen perusteella elintarvikesektorin yritysten vuotuiset keskiarvoiset kyberturvallisuuskustannukset (0,28 %) jäävät hieman alle komission esittämän arvion, kun taas valmistussektorin yritysten osalta tulos (0,69 %) ylittää hieman komission arvion. On kuitenkin huomattava, että myös komission vaikutustenarvioinnissa on tunnistettu lukuisia muuttujia, jotka voivat vaikuttaa siihen, miltä vuotuiset kyberturvaan käytetyt kustannukset näyttäytyvät suhteessa liikevaihtoon.

2.2 NIS2-direktiivin 21 artiklan riskienhallintavelvoitteista aiheutuvat kustannukset

NIS2-direktiivin 21 artiklassa säädetään kyberturvallisuusriskien hallintatoimenpiteistä. Artiklassa tarkoitettujen toimenpiteiden on perustuttava kaikki vaaratekijät huomioivaan toimintamalliin, jolla pyritään suojaamaan verkko- ja tietojärjestelmät ja näiden järjestelmien fyysinen ympäristö poikkeamilta, ja niihin on sisällyttävä vähintään seuraavat:

a. riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat;

b. poikkeamien käsittely;

c. toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta;

d. toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat;

e. verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen;

f. toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta;

g. perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus;

h. toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä;

i. henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta;

j. tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.

Kyberturvallisuusriskien hallintatoimenpiteiden oikeasuhteisuutta arvioitaessa on 21 artiklan 1 kohdan mukaan otettava huomioon, missä määrin toimija altistuu riskeille, toimijan koko ja poikkeamien esiintymisen todennäköisyys sekä niiden vakavuus ottaen huomioon niiden yhteiskunnalliset ja taloudelliset vaikutukset. Riskienhallintavelvoitteet eivät täten edellytä kaikilta toimijoilta samanlaisia toimenpiteitä, vaan niitä on arvioitava riskiperusteisesti.

Selvityksessä on arvioitu kunkin 21 artiklan riskienhallintavelvoitteiden täyttämisen nykytilaa sekä velvoitteeseen sopeutumisesta ja sen noudattamisesta aiheutuvia työpäiviä sekä muita kustannuksia.

2.2.1 Kyselytutkimuksen toteutustapa

Selvityksessä yritykset ovat ensinnäkin antaneet **arvion kunkin 21 artiklan riskienhallintavelvoitteiden täyttämisen nykytilasta asteikolla 1–5**, jossa 1 on ”merkittäviä puutteita” ja 5 on ”ei puutteita”. Arvioinnin tueksi yrityksille tarjottiin esimerkkejä siitä, mitä niiden tulisi ottaa huomioon kunkin velvoitteen täyttämisessä. Esimerkit perustuivat NIS2-direktiivin johdanto-osan kappaleisiin sekä Instan asiantuntijoiden arvioihin.

Toisekseen yrityksiltä pyydettiin arviota velvoitteen täyttämiseen **vaadituista henkilötyöpäivistä**[4] ja kolmanneksi arvio velvoitteen täyttämiseen vaadittavista **muista kustannuksista.** Työpäiviä sekä muita kustannuksia arvioidessa yritysten tuli antaa arviot niistä työpäivistä ja kustannuksista, joita yritykselle aiheutuu NIS2-direktiivin velvoitteista nykyisin käytettävän työajan ja muiden kustannusten lisäksi.

Sekä työpäivät että muut kustannukset jaettiin **kertaluonteisiin** ja **jatkuvaluonteisiin**. Kertaluonteisilla tarkoitetaan sellaisia työpäiviä ja muita kustannuksia, jotka yritykset käyttävät ensimmäisenä vuonna sopeutuakseen uusiin velvoitteisiin. Jatkuvaluonteisilla tarkoitetaan sellaisia työpäiviä ja muita kustannuksia, joita yritykselle aiheutuu NIS2-direktiivin velvoitteista vuosittain sopeutumisen jälkeen.

Työpäivillä kyselyssä tarkoitettiin sellaisia työpäiviä, joita yritys käyttää sisäisesti sopeutumiseen ja velvoitteen noudattamiseen. Muilla kustannuksilla tarkoitettiin velvoitteeseen sopeutumisesta sekä sen noudattamisesta aiheutuvia muita kustannuksia, kuten koneiden ja laitteiden hankinnoista, ohjelmistolisensseistä, tietoturvakonsultoinnista sekä muista tuotteista ja palveluista aiheutuneita kustannuksia.

Kyselylomakkeella annettiin vaihtoehdot käytettävistä työpäivistä ja muista kustannuksista. Lisätyöpäivät jaettiin kuuteen suuruusluokkaan:

- Velvoitteeseen sopeutuminen / velvoitteen täyttäminen ei aiheuta henkilötyöpäiviä,
- alle 10 HTP,
- 10–20 HTP,
- 21–50 HTP,
- 51–100 HTP sekä
- yli 100 HTP.

Muut kustannukset jaettiin seitsemään suuruusluokkaan:

- Ei kertaluonteisia/jatkuvaluonteisia kustannuksia,

[4] Henkilötyöpäivä tarkoittaa tässä yhteydessä 7,5 h työpäivää

- alle 5 000 euroa,
- 5 000–15 000 euroa,
- 15 001–30 000 euroa,
- 30 001–50 000 euroa,
- 50 001–100 000 euroa sekä
- yli 100 000 euroa.

Lisäksi yrityksille annettiin mahdollisuus olla arvioimatta nykytilaa sekä työpäiviä ja muita kustannuksia.

Kyselytutkimuksen tulosten pohjalta on lisäksi täytetty selvityksen liitteenä 1 ja 2 olevat TEM:n sääntelytaakkalaskurit. Sääntelytaakkalaskuri laskee yhteen työpäivistä ja muista kustannuksista yrityksille aiheutuneen taakan kullekin riskienhallintavelvoitteelle. Henkilötyöpäivistä aiheutunutta taakkaa laskiessa työntekijän kuukausipalkaksi on oletettu sääntelytaakkalaskurissa annettu ylemmän tason asiantuntijan palkka 4 700 euroa.

Yritysten antamat vastaukset ”yli 100 HTP" on sääntelytaakkalaskurin täytössä oletettu 100 henkilötyöpäiväksi ja ”yli 100 000 euroa” osalta 100 000 euroksi. Muiden suuruusluokkien kohdalla on määräksi otettu alimman ja ylimmän luvun keskiarvo.

Kuten tässä selvityksessä myös jäljempänä ilmenee, suurten yritysten kohdalla yli 100 000 euroa tai yli 100 henkilötyöpäivää voi tietyn velvoitteen tai kustannushyödyn kohdalla tarkoittaa huomattavan suuria euromääriä tai tarvittavia henkilötyöpäiviä. Tämä on syytä huomioida tarkasteltaessa vastausten keskiarvoja erityisesti niiden velvoitteiden kohdalla, joiden täyttämisestä useampi yritys on arvioinut aiheutuvan yli 100 000 euron kustannus tai yli 100 lisätyöpäivää.

2.2.2 Tulokset

2.2.2.1 Riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat

NIS2-direktiivin 21 artiklan 2 kohdan a alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä riskianalyyseja sekä tietojärjestelmien turvallisuutta koskevat politiikat.

Kyselytutkimuksessa yritysten kybermaturiteetin tasoa tämän vaatimuksen osalta arvioitiin muun muassa kysymyksillä siitä, onko yrityksellä olemassa säännöksessä tarkoitetut politiikat, kuinka kattavia nämä politiikat ovat, päivitetäänkö politiikkoja säännöllisesti ja valvotaanko niiden noudattamista. Lisäksi arvioitiin, kuinka kattavasti ja säännöllisesti yritys käytännössä toteuttaa riskianalyysejä määriteltyjen politiikkojen mukaisesti, vaikka 21 artiklan 2 kohdan a alakohta ei yksiselitteisesti edellytä varsinaisia riskianalyysien toteuttamistoimenpiteitä.

Tietojärjestelmien turvallisuutta koskevien politiikkojen osalta on syytä huomioida, että direktiivissä ei määritellä yksityiskohtaisesti, mitä politiikkoja yritysten on vähintään laadittava. Yritysten vastaukset perustuvat näin ollen niiden omaan arvioon tarvittavan dokumentaation laajuudesta. Toimialasta, liiketoimintaympäristöstä ja dokumentoinnin nykytilasta riippuen tarvittavan työmäärän ja kustannusten arvioissa voi olla merkittäviä eroja.

2.2.2.1.1 Elintarvikesektori

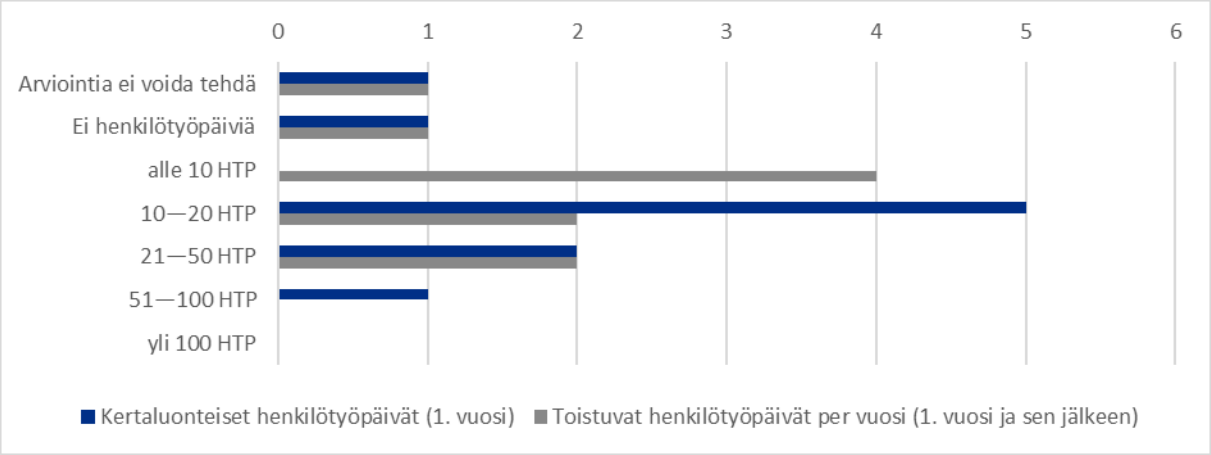
Asteikolla 1–5 elintarvikesektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 3. Yrityksistä 40 % antoi vastauksiksi 2 tai 4, jotka olivat yleisimmät arviot nykytilanteesta.

TAULUKKO 3. Velvoite 1: elintarvikesektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	4	40
3	2	20
4	4	40
5	0	0

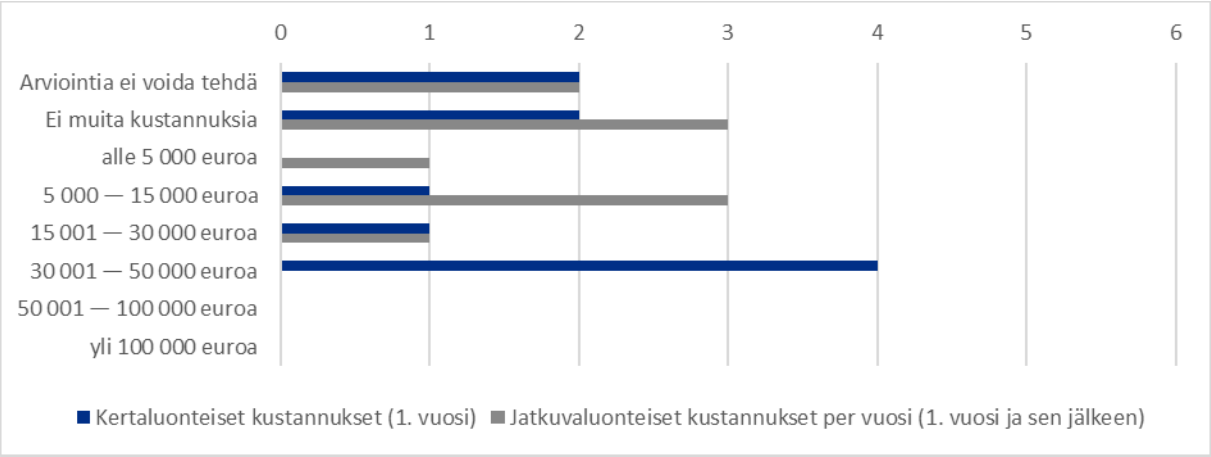
Elintarvikesektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10–20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli alle 10 henkilötyöpäivää.

KUVIO 1. Velvoite 1: elintarvikesektorille aiheutuvat henkilötyöpäivät



Elintarvikesektoriin kuuluvien yritysten yleisin arvio niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista oli 30 001–50 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia muita kustannuksia arvioidessa yleisimmät arviot olivat ”Ei muita kustannuksia” sekä 5 000–15 000 euroa.

KUVIO 2. Velvoite 1: elintarvikesektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 32 300 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 11 400 euroa vuosittain tämän jälkeen.

2.2.2.1.2 Valmistussektori

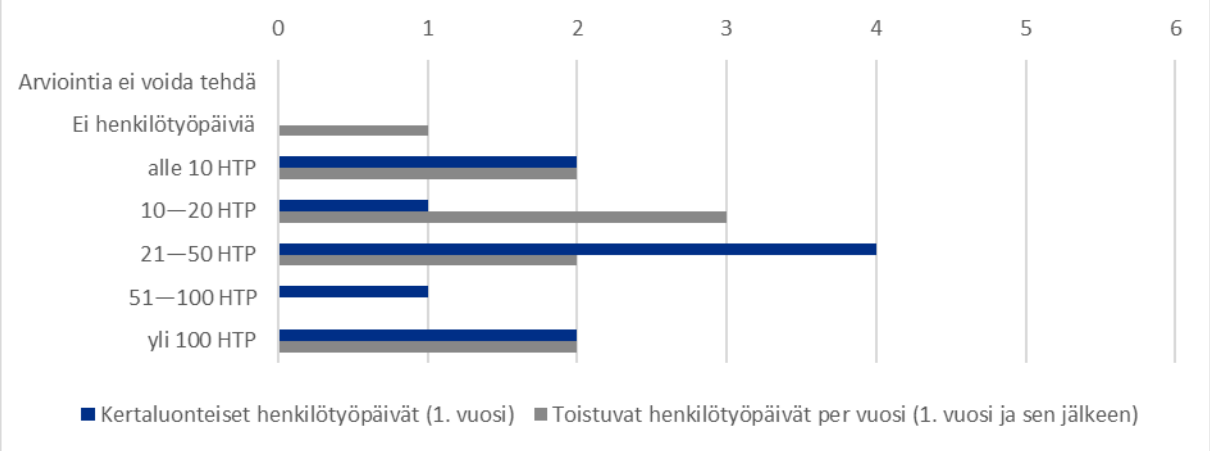
Asteikolla 1–5 valmistussektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 3,2. Yrityksistä 40 % antoi vastaukseksi 3 tai 4, jotka olivat yleisimmät arviot nykytilanteesta.

TAULUKKO 4. Velvoite 1: valmistussektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	2	20
3	4	40
4	4	40
5	0	0

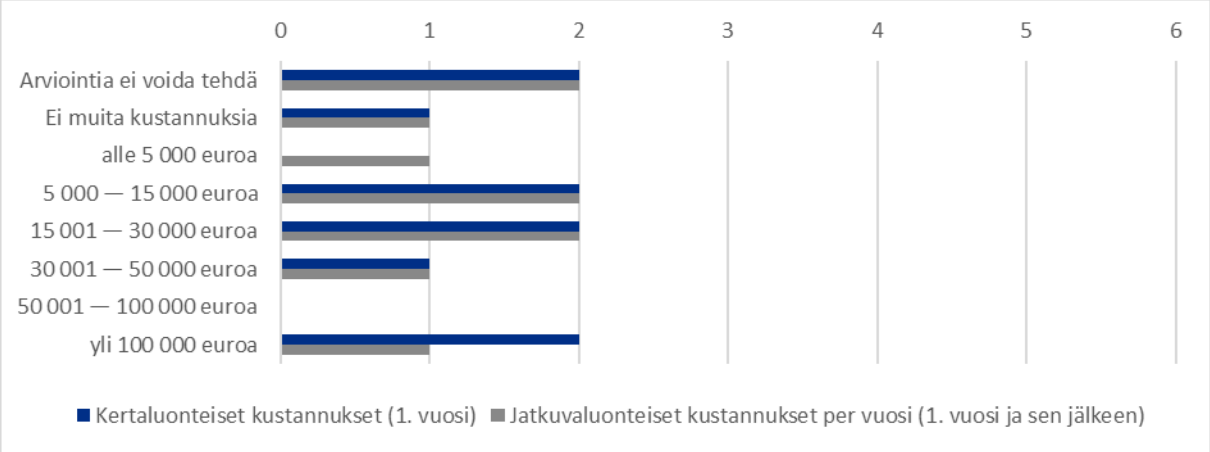
Valmistussektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 21–50 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli 10–20 henkilötyöpäivää.

KUVIO 3. Velvoite 1: valmistussektorille aiheutuvat henkilötyöpäivät



Valmistussektoriin kuuluvien yritysten yleisimmät arviot niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista olivat 5 000–15 000 euroa, 15 001–30 000 euroa sekä yli 100 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia muita kustannuksia arvioidessa yleisimmät arviot olivat 5 000–15 000 euroa sekä 15 001–30 000 euroa.

KUVIO 4. Velvoite 1: valmistussektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 52 900 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 36 900 euroa vuosittain tämän jälkeen.

2.2.2.2 Poikkeamien käsittely

NIS2-direktiivin 21 artiklan 2 kohdan b alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä poikkeamien käsittely.

NIS2-direktiivin johdanto-osan 78 kohdan mukaan hallintatoimenpiteisiin ”olisi sisällyttävä toimenpiteitä, joilla tunnistetaan poikkeamariskit, ehkäistään, havaitaan ja hallitaan poikkeamia, palaudutaan niistä ja lievennetään niiden vaikutuksia”. NIS2-direktiivin 6 artiklan 6 alakohdan määritelmän mukaan poikkeamalla tarkoitetaan ”tapahtumaa, joka vaarantaa verkko- ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen,

siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden".

Instan asiantuntijoiden arvion mukaan tavoitteen täyttämisessä voidaan yrityksen riskianalyysin mukaisesti ottaa huomioon erilaisia teknisiä ratkaisuja havainnointikyvykkyyden parantamiseksi, kuten keskitetty lokienhallinta, poikkeamien tunnistamiseen käytettävät SIEM-järjestelmät (*Security Information and Event Management*) ja päätelaitteiden suojausratkaisut, kuten EDR (*Endpoint Detection and Response*). Lisäksi yrityksen tulisi tunnistaa käytössään olevat verkot, niihin liitetyt ICT-palvelut, -tuotteet ja -laitteet sekä niiden kautta kulkeva liikenne. Yrityksellä tulisi olla käytössä poikkeama- ja häiriötilanteisiin prosessit, jotka kattavat näiden tilanteiden tunnistamisen ja niiden aikana toimimisen sekä toimintatavat poikkeamista viestimiseen sisäisesti, asiakkaille ja viranomaisille.

2.2.2.2.1 Elintarvikesektori

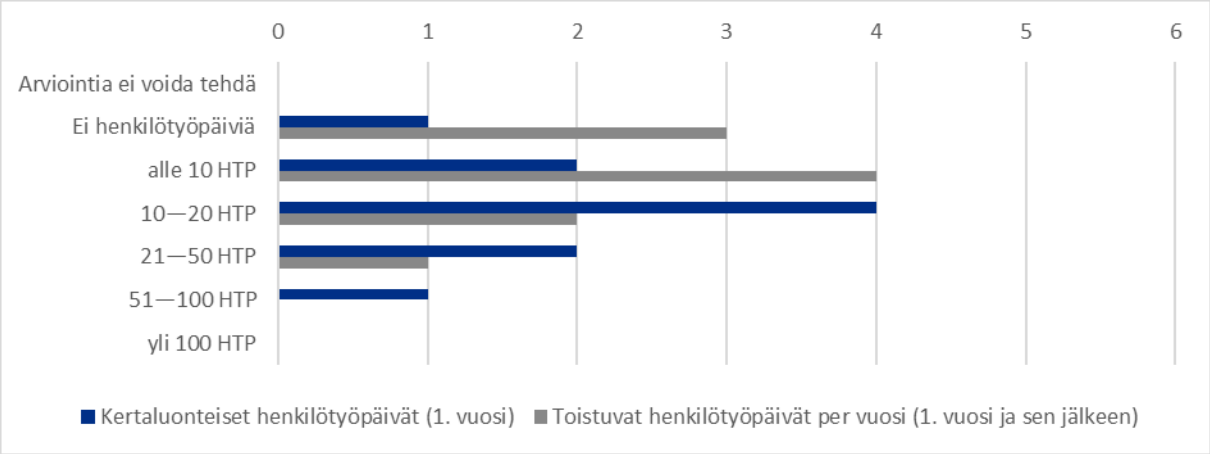
Asteikolla 1–5 elintarvikesektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 3,1. Yleisin arvio nykytilanteesta oli 4, jonka vastasi 40 % yrityksistä.

TAULUKKO 5. Velvoite 2: elintarvikesektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	1	10
2	2	20
3	2	20
4	5	50
5	0	0

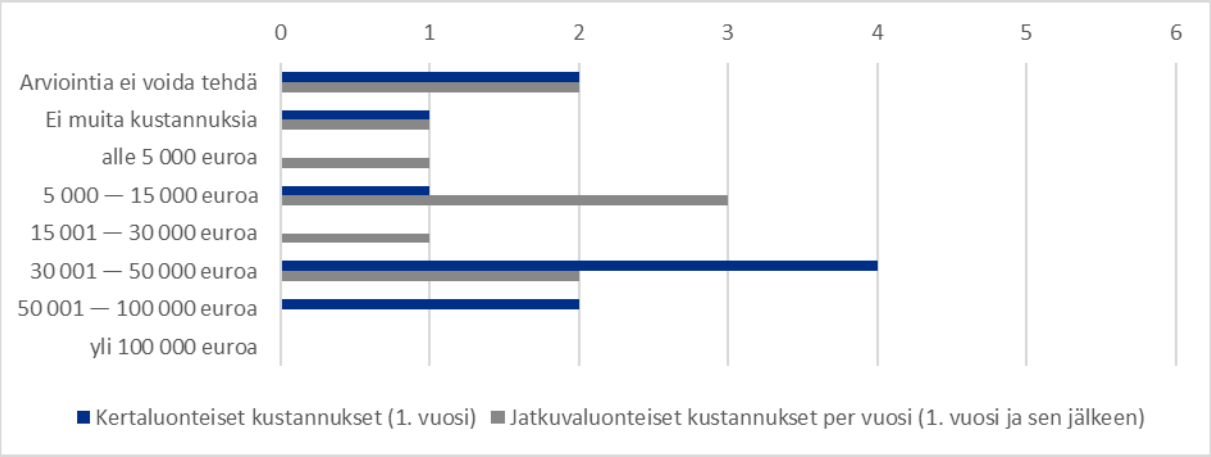
Elintarvikesektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10–20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli alle 10 henkilötyöpäivää.

KUVIO 5. Velvoite 2: elintarvikesektorille aiheutuvat henkilötyöpäivät



Elintarvikesektoriin kuuluvien yritysten yleisin arvio niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista oli 30 001–50 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia muita kustannuksia arvioidessa yleisin arvio oli 5 000–15 000 euroa.

KUVIO 6. Velvoite 2: elintarvikesektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 47 200 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 19 700 euroa vuosittain tämän jälkeen.

2.2.2.2.2 Valmistussektori

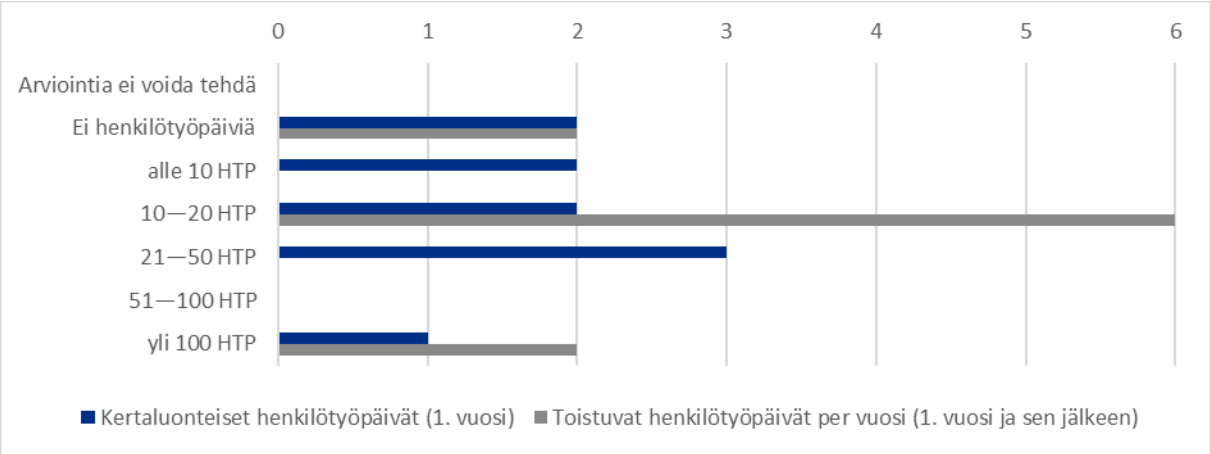
Asteikolla 1–5 valmistussektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 3,3. Yleisin arvio nykytilanteesta oli 4, jonka vastasi 40 % yrityksistä.

TAULUKKO 6. Velvoite 2: valmistussektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	3	30
3	2	20
4	4	40
5	1	10

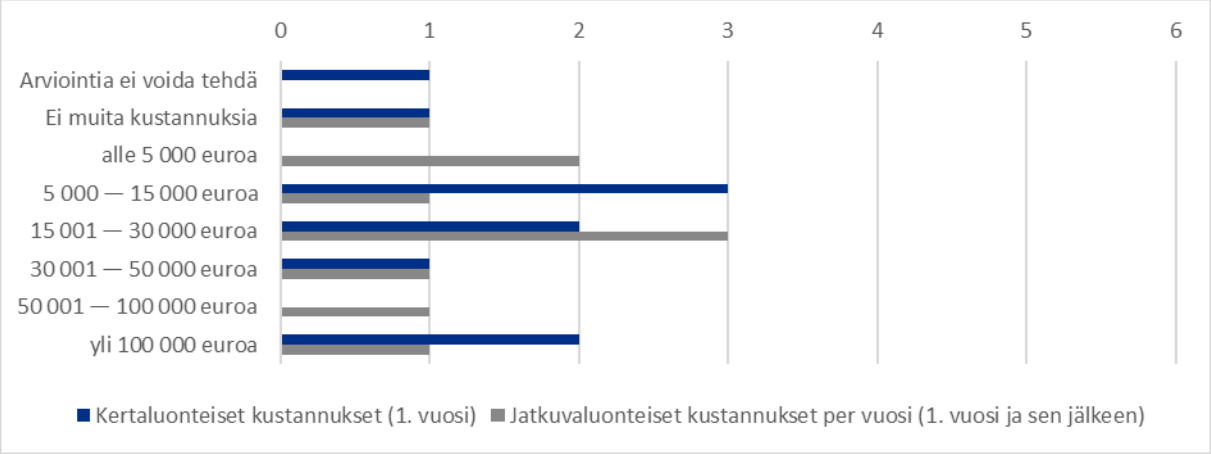
Valmistussektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 21–50 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli 10–20 henkilötyöpäivää.

KUVIO 7. Velvoite 2: valmistussektorille aiheutuvat henkilötyöpäivät



Valmistussektoriin kuuluvien yritysten yleisin arvio niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista oli 5 000–15 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia kustannuksia arvioidessa yleisin arvio oli 15 001–30 000 euroa.

KUVIO 8. Velvoite 2: valmistussektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 43 200 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 39 500 euroa vuosittain tämän jälkeen.

2.2.2.3 Toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta

NIS2-direktiivin 21 artiklan 2 kohdan c alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta.

Instan asiantuntijoiden arvion mukaan toiminnan jatkuvuuden hallinnan sekä kriisinhallinnan hallintatoimenpiteisiin voi sisältyä muun muassa ICT-tuotteet ja -palvelut kattavat jatkuvuus- ja toipumissuunnitelmat, ICT-tuotteiden ja -palveluiden palautumisen testauksen määrittäminen osaksi edellisiä suunnitelmia sekä ICT-tuotteiden ja -palveluiden palautumisen ja kyberturvallisuuspoikkeamien aikaisen toiminnan säännöllinen harjoitteleminen.

2.2.2.3.1 Elintarvikesektori

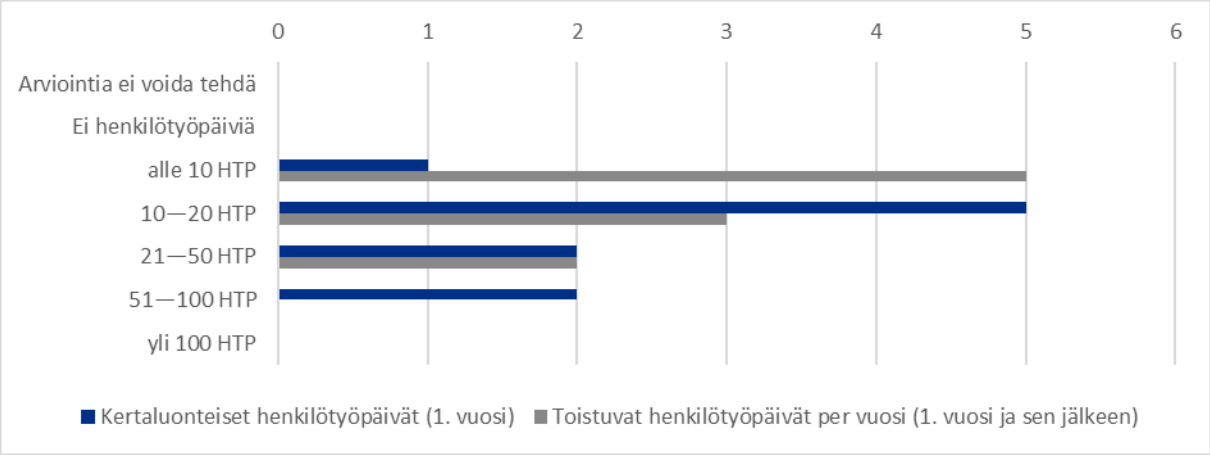
Asteikolla 1–5 elintarvikesektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 2,5. Yleisin arvio nykytilanteesta oli 3, jonka vastasi 60 % vastanneista.

TAULUKKO 7. Velvoite 3: elintarvikesektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	1	10
2	3	30
3	6	60
4	0	0
5	0	0

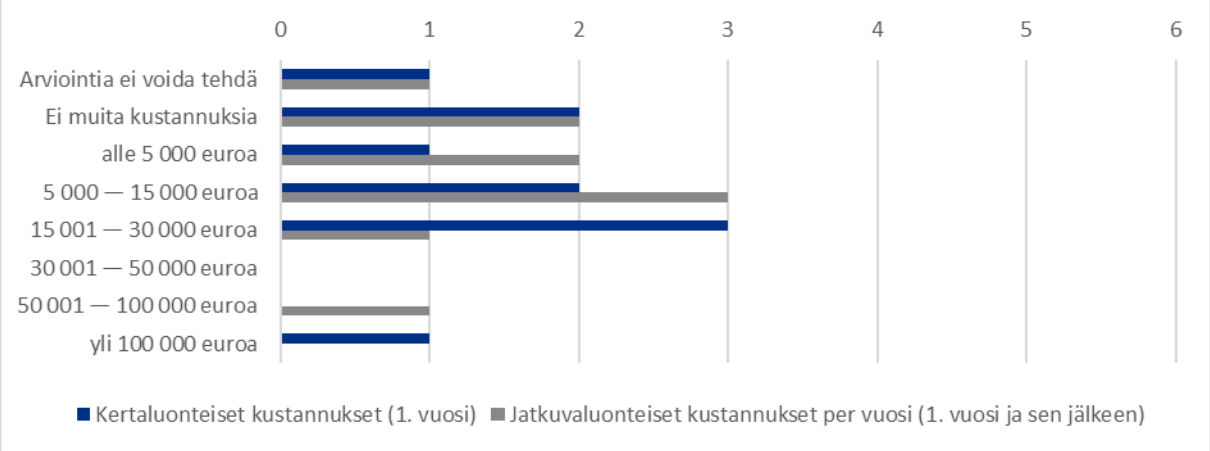
Elintarvikesektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10–20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli alle 10 henkilötyöpäivää.

KUVIO 9. Velvoite 3: elintarvikesektorille aiheutuvat henkilötyöpäivät



Elintarvikesektoriin kuuluvien yritysten yleisin arvio niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista oli 15 001–30 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia muita kustannuksia arvioidessa yleisin arvio oli 5 000–15 000 euroa.

KUVIO 10. Velvoite 3: elintarvikesektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 31 200 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 19 400 euroa vuosittain tämän jälkeen.

2.2.2.3.2 Valmistussektori

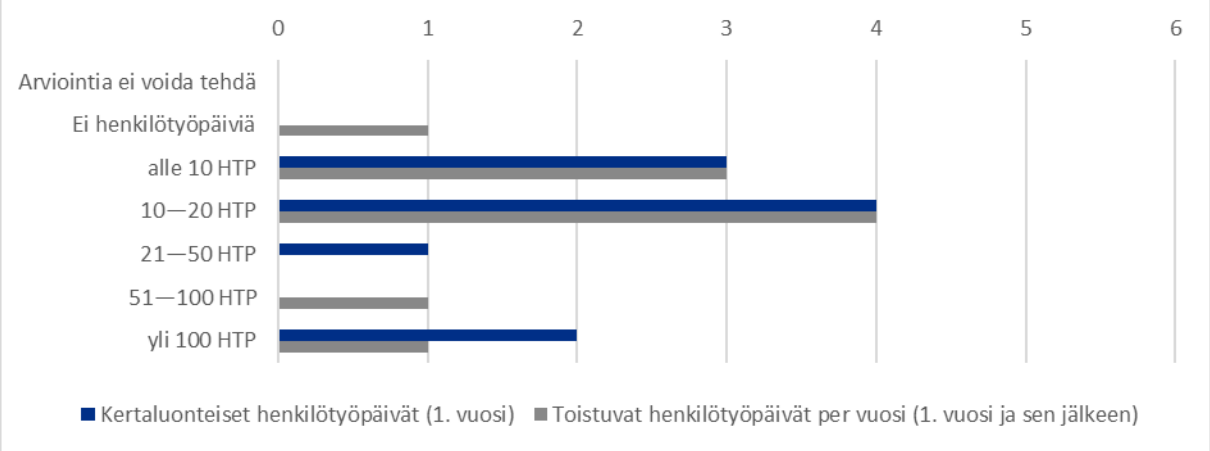
Asteikolla 1–5 valmistussektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 2,8. Yleisin arvio nykytilanteesta oli 4, jonka vastasi 40 % yrityksistä.

TAULUKKO 8. Velvoite 3: valmistussektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	2	20
2	2	20
3	2	20
4	4	40
5	0	0

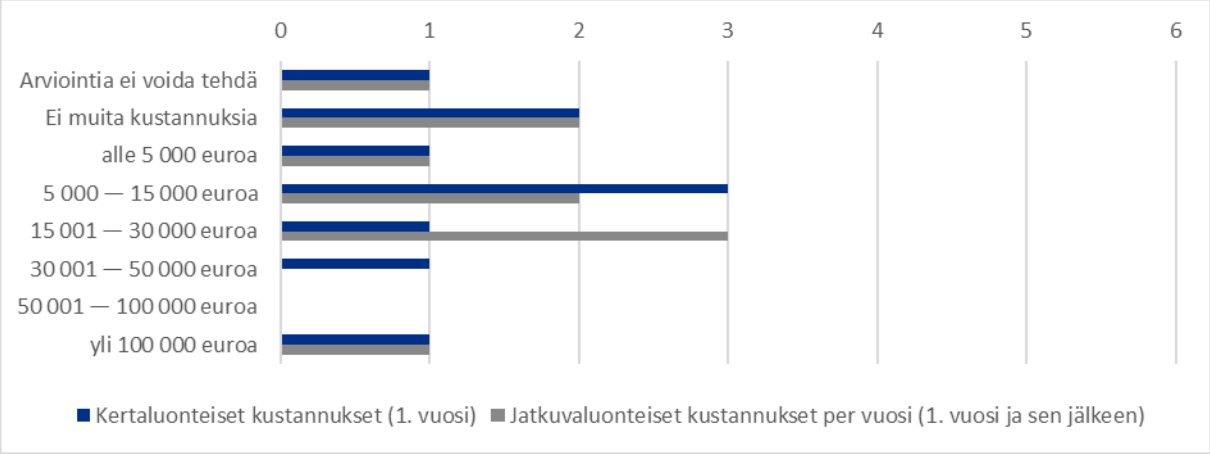
Valmistussektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10–20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli 10–20 henkilötyöpäivää.

KUVIO 11. Velvoite 3: valmistussektorille aiheutuvat henkilötyöpäivät



Valmistussektoriin kuuluvien yritysten yleisin arvio niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista oli 5 000–15 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia kustannuksia arvioidessa yleisin arvio oli 15 001–30 000 euroa.

KUVIO 12. Velvoite 3: valmistussektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 32 100 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 29 500 euroa vuosittain tämän jälkeen.

2.2.2.4 Toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat

NIS2-direktiivin 21 artiklan 2 kohdan d alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteissä on otettava huomioon toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat.

NIS2-direktiivin johdanto-osan 85 kohdan mukaan yritysten olisi ”arvioitava ja otettava huomioon toimittajiensa tuotteiden ja palveluntarjoajiensa palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet ja toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt, mukaan lukien tuotekehityksen suojausmenettelyt. Keskeisiä ja tärkeitä toimijoita olisi erityisesti

kannustettava sisällyttämään kyberturvallisuusriskien hallintatoimenpiteitä sopimusjärjestelyihin, joita ne tekevät välittömien toimittajiensa ja palveluntarjoajiensa kanssa. Kyseiset toimijat voisivat käsitellä myös alemman tason toimittajistaan ja palveluntarjoajistaan johtuvia riskejä."

Täyttääkseen toimitusketjujen turvallisuutta koskevan velvoitteen yritysten tulisi Instan asiantuntijoiden arvion mukaan yrityksen toimintaympäristö huomioiden määritellä roolit, vastuut ja valtuudet kyberturvallisuudelle sekä yrityksen sisällä että koko toimitusketjussa. Lisäksi yritysten tulisi ylläpitää toimitusketjusta kuvausta, joka sisältää riippuvuudet, haavoittuvuudet, uhat ja riskien vaikutukset. Kuvauksen tulisi kattaa myös palveluntarjoajien ja toimittajien keskeiset alihankkijat. Yritysten tulisi myös valvoa ICT-tuotteiden ja -palveluiden kyberturvallisuutta koko niiden elinkaaren ajan sekä tehdä yhteistyötä sisäisten ja ulkoisten sidosryhmien kanssa jakamalla tietoa sekä parhaita käytänteitä.

2.2.2.4.1 Elintarvikesektori

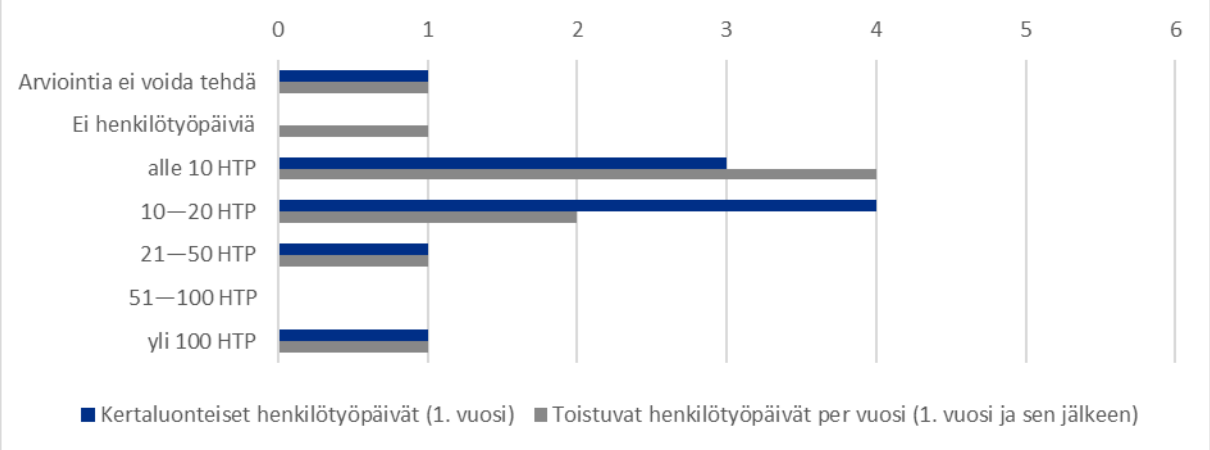
Asteikolla 1–5 elintarvikesektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 2,6. Yleisin arvio nykytilanteesta oli 2, jonka vastasi 40 % vastanneista.

TAULUKKO 9. Velvoite 4: elintarvikesektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	1	10
2	4	40
3	3	30
4	2	20
5	0	0

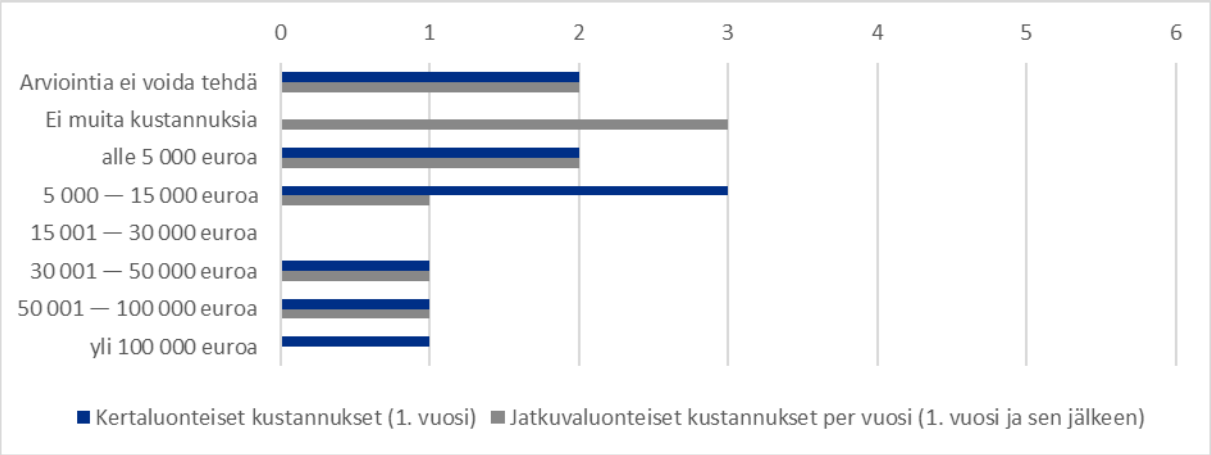
Elintarvikesektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10–20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli alle 10 henkilötyöpäivää.

KUVIO 13. Velvoite 4: elintarvikesektorille aiheutuvat henkilötyöpäivät



Elintarvikesektoriin kuuluvien yritysten yleisin arvio niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista oli 5 000–15 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia muita kustannuksia arvioidessa yleisin arvio oli, ettei tämän velvoitteen noudattamisesta aiheudu muita kustannuksia.

KUVIO 14. Velvoite 4: elintarvikesektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 39 100 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 23 200 euroa vuosittain tämän jälkeen.

2.2.2.4.2 Valmistussektori

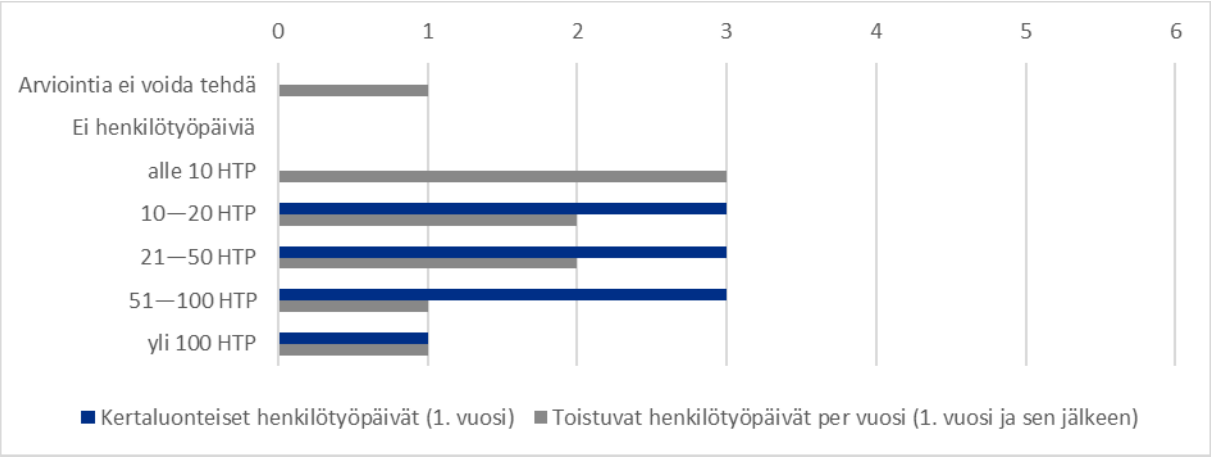
Asteikolla 1–5 valmistussektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 2,8. Yrityksistä 40 % antoi vastaukseksi 2 tai 3, jotka olivat yleisimmät arviot nykytilanteesta.

TAULUKKO 10. Velvoite 4: valmistussektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	4	40
3	4	40
4	2	20
5	0	0

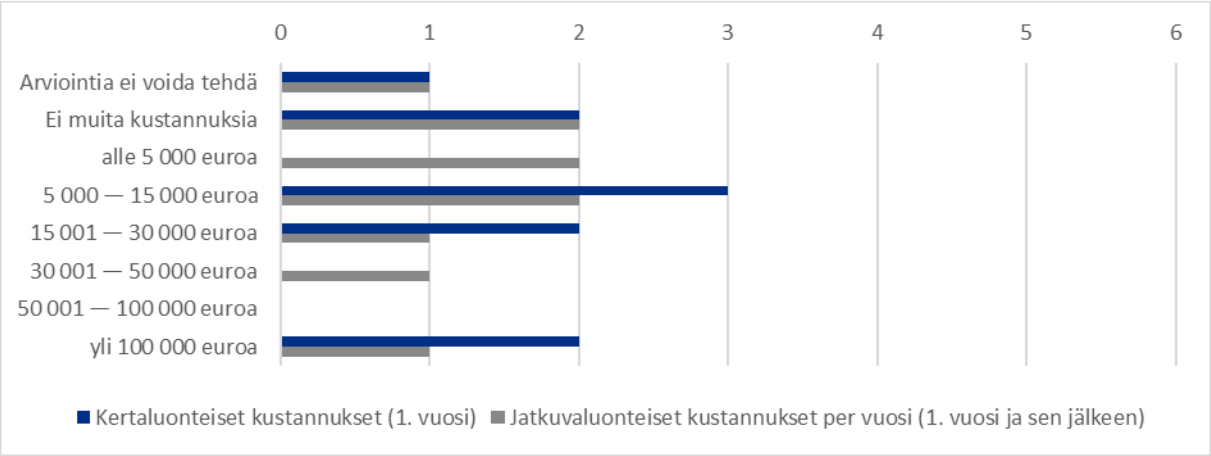
Valmistussektoriin kuuluvien yritysten yleisimmät arviot niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä olivat 10–20 henkilötyöpäivää, 21–50 henkilötyöpäivää sekä 51–100 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli alle 10 henkilötyöpäivää.

KUVIO 15. Velvoite 4: valmistussektorille aiheutuvat henkilötyöpäivät



Valmistussektoriin kuuluvien yritysten yleisin arvio niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista oli 5 000–15 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia muita kustannuksia arvioidessa yleisimmät arviot olivat ”Ei muita kustannuksia”, alle 5 000 euroa sekä 5 000–15 000 euroa.

KUVIO 16. Velvoite 4: valmistussektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 46 500 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 31 700 euroa vuosittain tämän jälkeen.

2.2.2.5 Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen

NIS2-direktiivin 21 artiklan 2 kohdan e alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen.

NIS2-direktiivin johdanto-osan 80 kohdan mukaan jäsenvaltioiden olisi ”edistettävä asiaa koskevien eurooppalaisten ja kansainvälisten standardien käyttöä keskeisten ja tärkeiden toimijoiden keskuudessa tai ne voivat vaatia toimijoita käyttämään sertifioituja TVT-tuotteita, TVT-palveluja ja TVT-prosesseja”. Lisäksi johdanto-osan 78 kohdan mukaan ”Verkko- ja tietojärjestelmien turvallisuuden olisi katettava säilytettävien, siirrettävien ja käsiteltävien

tietojen turvallisuus. Kyberturvallisuusriskien hallintatoimenpiteisiin olisi kuuluttava järjestelmäanalyysi, jossa otetaan huomioon inhimilliset tekijät, jotta saadaan täydellinen kuva verkko- ja tietojärjestelmän turvallisuudesta".

Instan asiantuntijoiden arvion mukaan yritysten tulisi ottaa huomioon, onko niillä käytössä hankintojen vaatimusmäärittely ja seurataanko toimittajien vaatimustenmukaisuutta säännöllisesti. Yritysten tulisi lisäksi ottaa huomioon toimittajien sertifikaatit sekä ICT-tuotteiden ja -palveluiden kohdalla tietoturvaan liittyvät viitekehykset, kun ne arvioivat toimittajia sekä ICT-tuotteita ja -palveluita.

Verkko- ja tietojärjestelmien turvallisuutta arvioitaessa tulisi Instan asiantuntijoiden arvion mukaan huomioida myös inhimilliset uhkatekijät esimerkiksi käytettävyystestauksen, käyttötapauskuvausten ja tehtävien eriyttämisen kautta. Lisäksi velvoitteen täyttämiseen vaikuttaa se, saadaanko ja seurataanko toimittajilta sekä ICT-tuotteista ja -palveluista saatuja tietoturvapoikkeamatiedotteita. Verkko- ja tietojärjestelmien kehittämisen kannalta yrityksellä tulisi olla käytössä turvallisen ohjelmistokehityksen prosessi ja sitä tulisi valvoa.

2.2.2.5.1 Elintarvikesektori

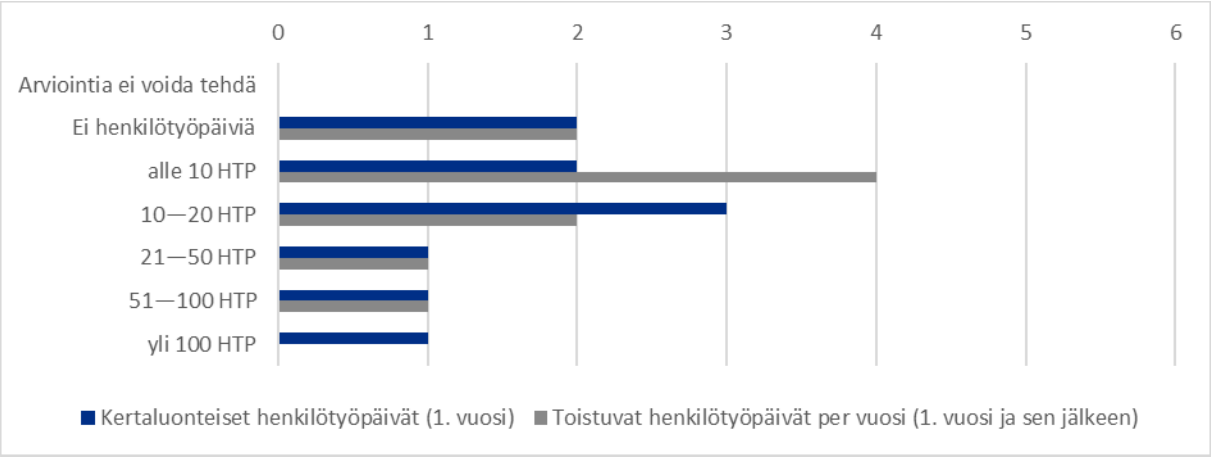
Asteikolla 1–5 elintarvikesektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 2,5. Yrityksistä 30 % antoi vastaukseksi 1 tai 3, jotka olivat yleisimmät arviot nykytilanteesta.

TAULUKKO 11. Velvoite 5: elintarvikesektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	3	30
2	2	20
3	3	30
4	1	10
5	1	10

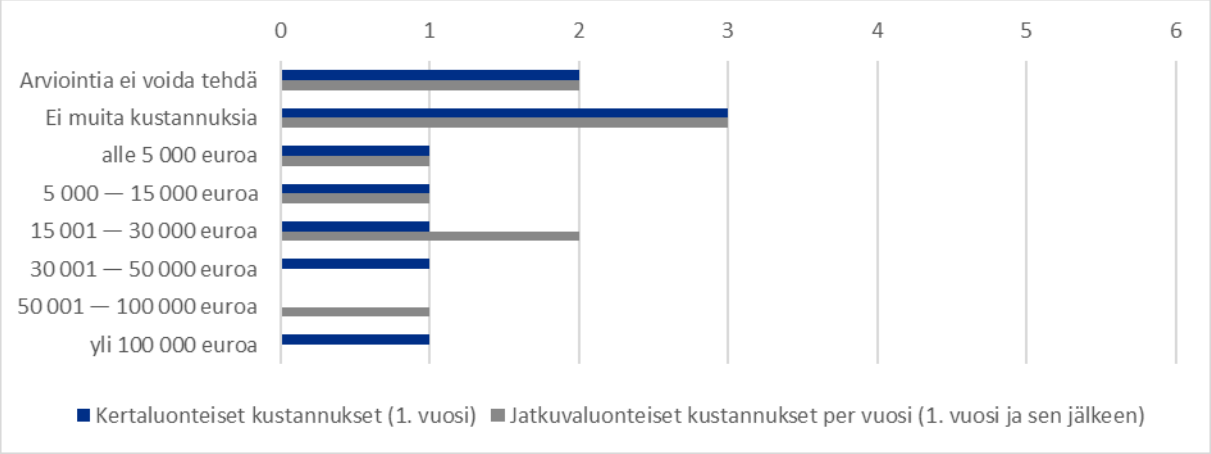
Elintarvikesektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10–20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli alle 10 henkilötyöpäivää.

KUVIO 17. Velvoite 5: elintarvikesektorille aiheutuvat henkilötyöpäivät



Elintarvikesektoriin kuuluvien yritysten yleisin arvio sekä kertaluonteisten kustannusten että jatkuvaluonteisten kustannusten osalta oli, ettei niille aiheudu tästä velvoitteesta muita kustannuksia.

KUVIO 18. Velvoite 5: elintarvikesektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 30 800 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 21 900 euroa vuosittain tämän jälkeen.

2.2.2.5.2 Valmistussektori

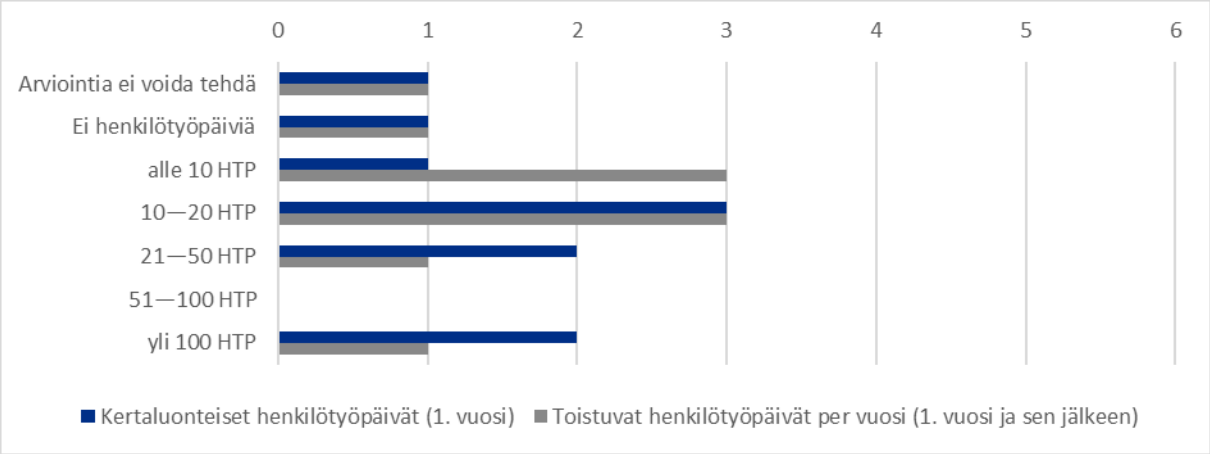
Asteikolla 1–5 valmistussektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 2,8. Yleisin arvio nykytilanteesta oli 2, jonka vastasi 50 % yrityksistä.

TAULUKKO 12. Velvoite 5: valmistussektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	5	50
3	3	30
4	1	10
5	1	10

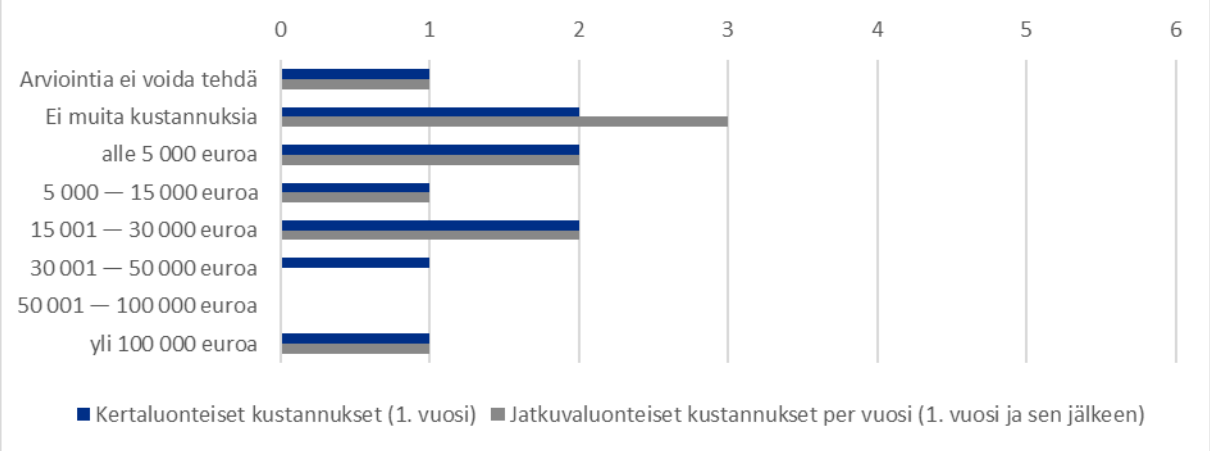
Valmistussektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10–20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisimmät arviot olivat alle 10 henkilötyöpäivää sekä 10–20 henkilötyöpäivää.

KUVIO 19. Velvoite 5: valmistussektorille aiheutuvat henkilötyöpäivät



Valmistussektoriin kuuluvien yritysten yleisimmät arviot niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista olivat ”Ei muita kustannuksia”, alle 5 000 euroa sekä 15 001–30 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia muita kustannuksia arvioidessa yleisin arvio oli, ettei tämän velvoitteen noudattamisesta aiheudu muita kustannuksia.

KUVIO 20. Velvoite 5: valmistussektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 34 200 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 25 100 euroa vuosittain tämän jälkeen.

2.2.2.6 Toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta

NIS2-direktiivin 21 artiklan 2 kohdan f alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta.

Instan asiantuntijoiden arvion mukaan tämän velvoitteen täyttäminen vaatii yrityksen toiminnasta riippuen sekä yleisiä että hallintakeinokohtaisia mittareita, joilla tietoturvan tehokkuutta voidaan mitata. Yrityksen olisi myös seurattava mittareita säännöllisesti. Lisäksi mittaustulokset tulisi arvioida ja raportoida johdolle.

Hallintatoimenpiteiden tehokkuuden arvioinnin toimintaperiaatteisiin ja menettelyihin liittyvät myös jatkuvan parantamisen käytänteet, joiden avulla suunnitellaan ja toteutetaan kehittämistoimenpiteitä mittaustulosten pohjalta. Yritysten tulisi myös arvioida ja ottaa huomioon toiminnassaan hallintatoimenpiteiden toteuttamisen jälkeinen jäännösriski.

2.2.2.6.1 Elintarvikesektori

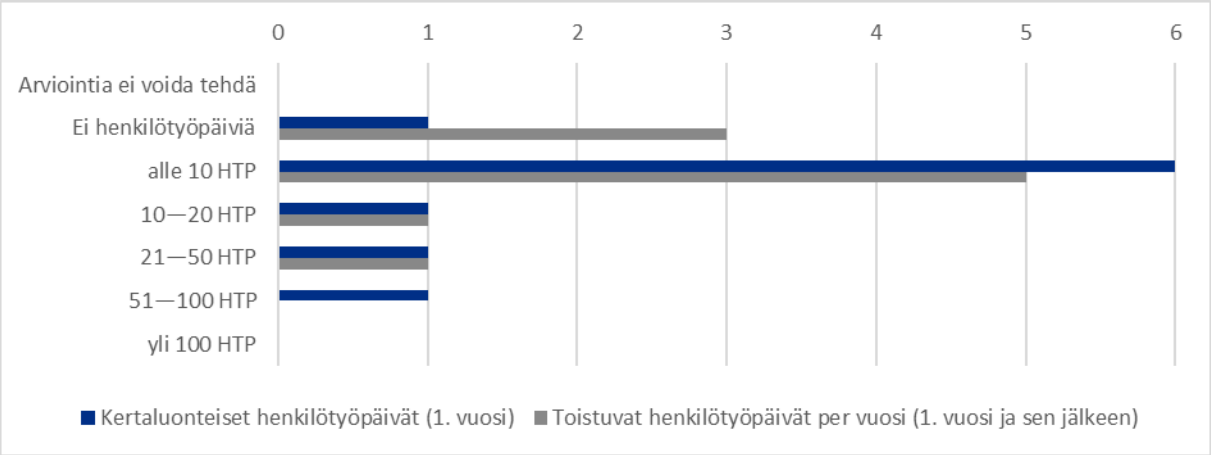
Asteikolla 1–5 elintarvikesektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 2,8. Yrityksistä 30 % antoi vastaukseksi 2, 3 tai 4, jotka olivat yleisimmät arviot nykytilanteesta.

TAULUKKO 13. Velvoite 6: elintarvikesektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	1	10
2	3	30
3	3	30
4	3	30
5	0	0

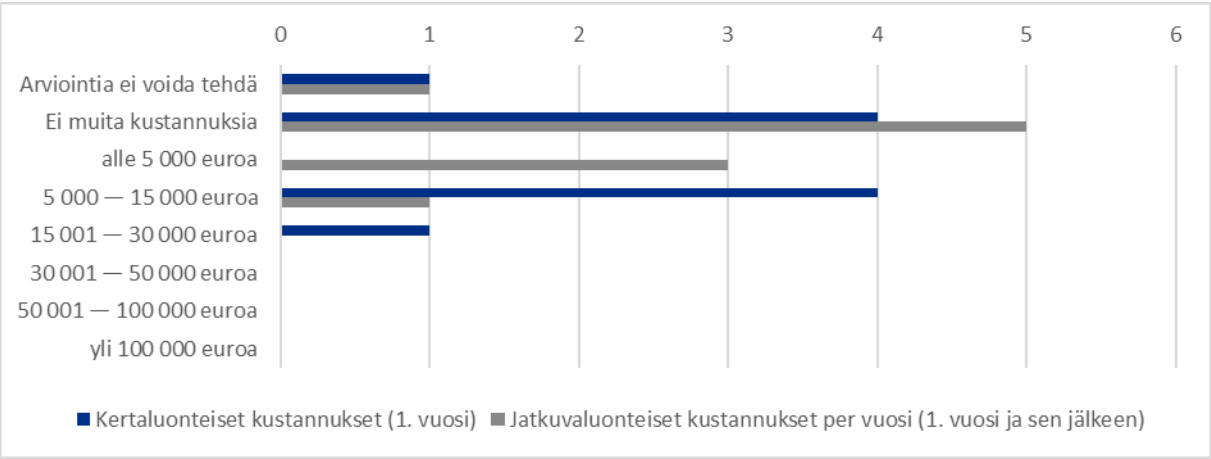
Elintarvikesektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli alle 10 henkilötyöpäivää. Myös vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli alle 10 henkilötyöpäivää.

KUVIO 21. Velvoite 6: elintarvikesektorille aiheutuvat henkilötyöpäivät



Elintarvikesektoriin kuuluvien yritysten yleisimmät arviot niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista olivat ”Ei muita kustannuksia” sekä 5 000–15 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia muita kustannuksia arvioidessa yleisin arvio oli, ettei tämän velvoitteen noudattamisesta aiheudu muita kustannuksia.

KUVIO 22. Velvoite 6: elintarvikesektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 12 100 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 4 500 euroa vuosittain tämän jälkeen.

2.2.2.6.2 Valmistussektori

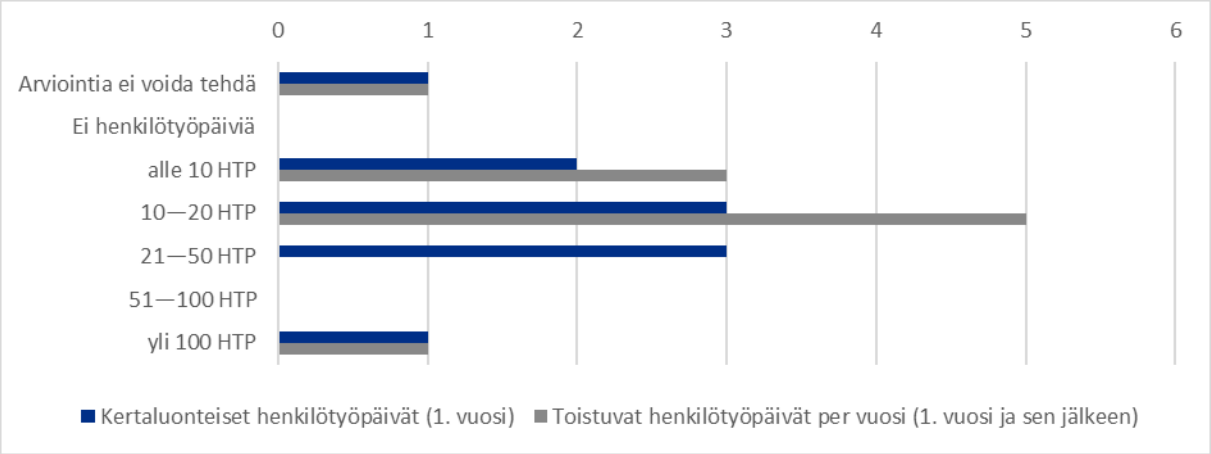
Asteikolla 1–5 valmistussektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 2,5. Yrityksistä 30 % antoi vastaukseksi 2 tai 3, jotka olivat yleisimmät arviot nykytilanteesta.

TAULUKKO 14. Velvoite 6: valmistussektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	2	20
2	3	30
3	3	30
4	2	20
5	0	0

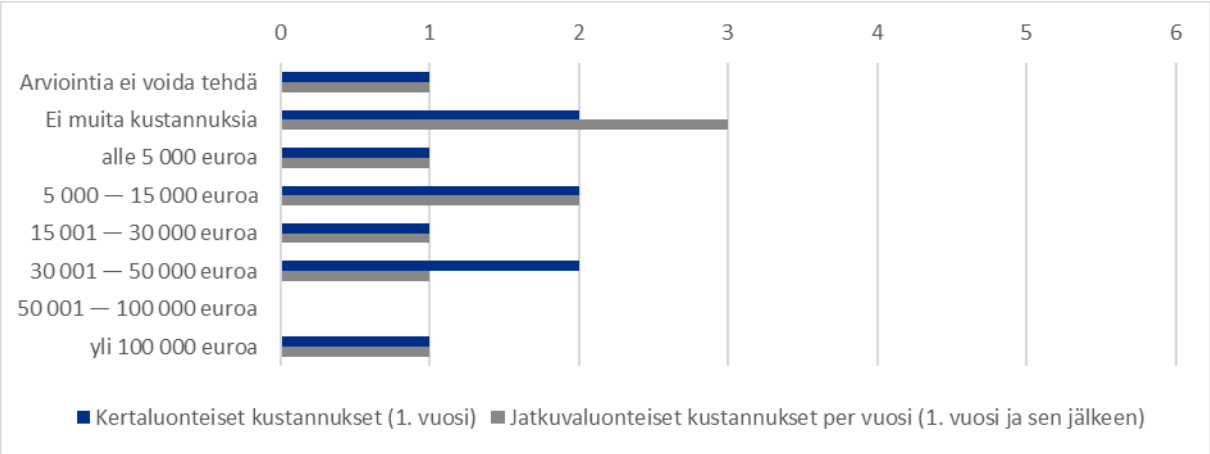
Valmistussektoriin kuuluvien yritysten yleisimmät arviot niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä olivat 10–20 henkilötyöpäivää sekä 21–50 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli 10–20 henkilötyöpäivää.

KUVIO 23. Velvoite 6: valmistussektorille aiheutuvat henkilötyöpäivät



Valmistussektoriin kuuluvien yritysten yleisimmät arviot niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista olivat ”Ei muita kustannuksia”, 5 000–15 000 euroa sekä 30 001–50 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia muita kustannuksia arvioidessa yleisin arvio oli, ettei tämän velvoitteen noudattamisesta aiheudu muita kustannuksia.

KUVIO 24. Velvoite 6: valmistussektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 34 700 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 27 600 euroa vuosittain tämän jälkeen.

2.2.2.7 Perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus

NIS2-direktiivin 21 artiklan 2 kohdan g alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus.

NIS2-direktiivin johdanto-osan 89 kohdan mukaan yritysten ”olisi otettava käyttöön monenlaisia perustason kyberhygieniakäytäntöjä, kuten nollaluottamuksen periaate, ohjelmistopäivitykset, laitteiden konfigurointi, verkon segmentointi, identiteetin- ja pääsynhallinta ja käyttäjien tietoisuuden lisääminen, ja järjestettävä henkilöstölleen koulutusta kyberuhkista, verkkourkinnasta ja käyttäjän manipuloinnista.”

Haastatteluissa havaittiin, että NIS2-direktiivissä luetellaan esimerkkeinä perustason kyberhygieniakäytännöistä joitakin sellaisia menettelytapoja, jotka saattavat olla haasteellisia toteuttaa etenkin direktiivin soveltamisalaan kuuluvissa pienemmissä yrityksissä. Esimerkkinä tällaisista menettelyistä mainittiin erityisesti nollaluottamuksen periaate eli ns. Zero Trust.

2.2.2.7.1 Elintarvikesektori

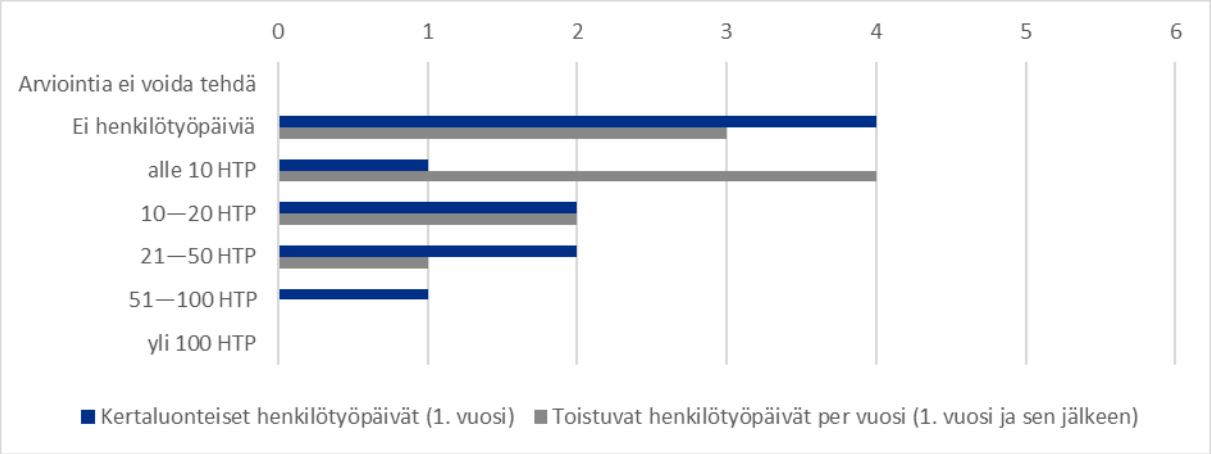
Asteikolla 1–5 elintarvikesektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 3,6. Yleisin arvio nykytilanteesta oli 4, jonka vastasi 40 % yrityksistä.

TAULUKKO 15. Velvoite 7: elintarvikesektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	2	20
3	2	20
4	4	40
5	2	20

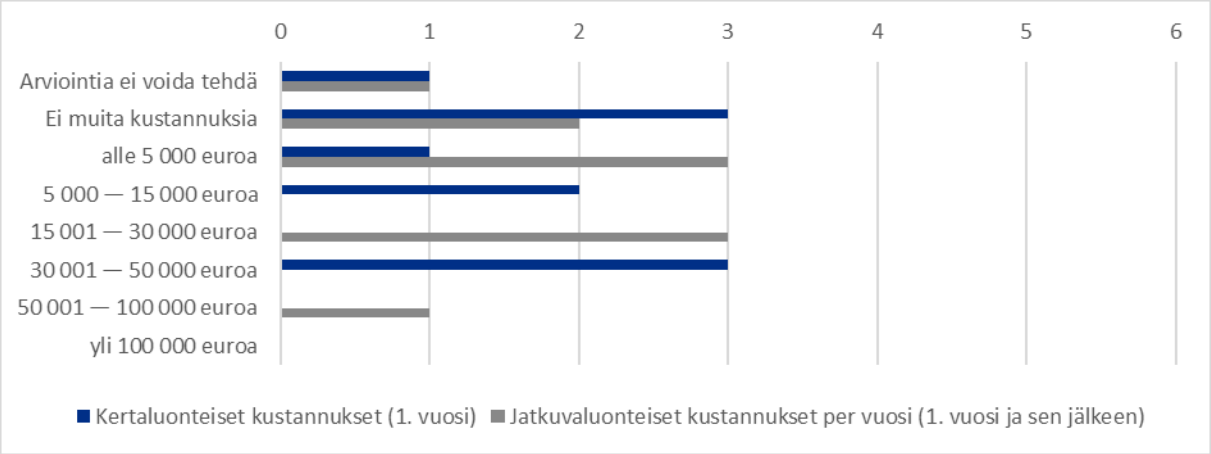
Elintarvikesektoriin kuuluvien yritysten yleisin arvio kertaluonteisten henkilötyöpäivien osalta oli, ettei niille aiheudu tähän velvoitteeseen sopeutumista henkilötyöpäiviä. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli alle 10 henkilötyöpäivää.

KUVIO 25. Velvoite 7: elintarvikesektorille aiheutuvat henkilötyöpäivät



Elintarvikesektoriin kuuluvien yritysten yleisimmät arviot kertaluonteisten muiden kustannusten osalta olivat ”Ei muita kustannuksia” sekä 30 001–50 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia muita kustannuksia arvioidessa yleisimmät arviot olivat alle 5 000 euroa sekä 15 001–30 000 euroa.

KUVIO 26. Velvoite 7: elintarvikesektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 21 900 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 19 500 euroa vuosittain tämän jälkeen.

2.2.2.7.2 Valmistussektori

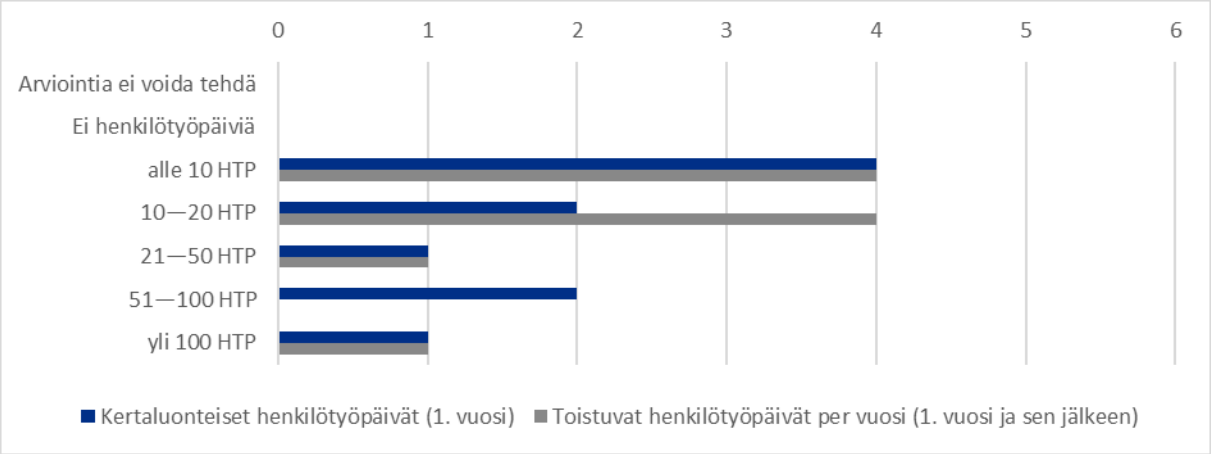
Asteikolla 1–5 valmistussektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 3,4. Yleisin arvio nykytilanteesta oli 4, jonka vastasi 40 % yrityksistä.

TAULUKKO 16. Velvoite 7: valmistussektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	2	20
3	3	30
4	4	40
5	1	10

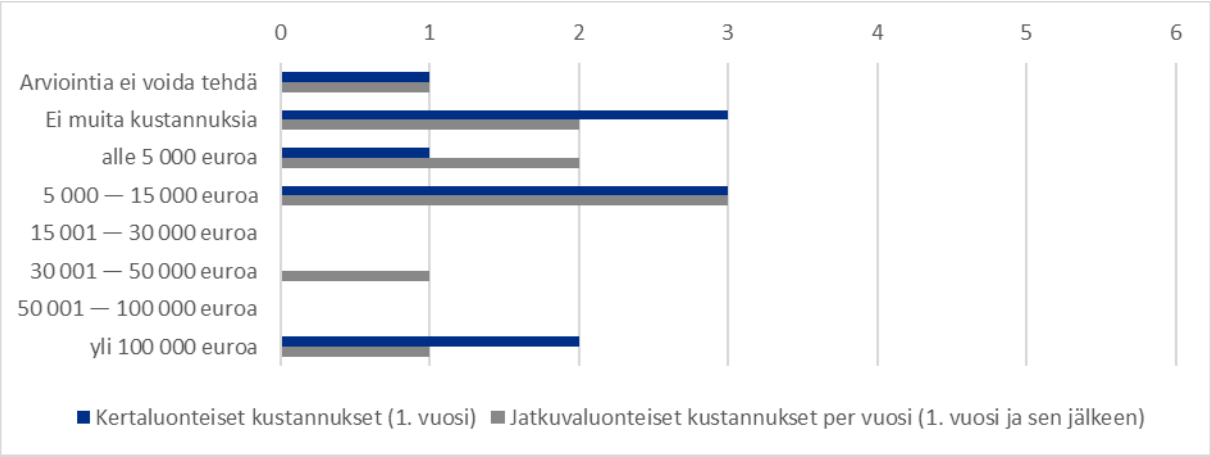
Valmistussektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli alle 10 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisimmät arviot olivat alle 10 henkilötyöpäivää sekä 10–20 henkilötyöpäivää.

KUVIO 27. Velvoite 7: valmistussektorille aiheutuvat henkilötyöpäivät



Valmistussektoriin kuuluvien yritysten yleisimmät arviot niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista olivat ”Ei muita kustannuksia” sekä 5 000–15 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia kustannuksia arvioidessa yleisin arvio oli 5 000–15 000 euroa.

KUVIO 28. Velvoite 7: valmistussektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 37 100 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 26 700 euroa vuosittain tämän jälkeen.

2.2.2.8 Toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä

NIS2-direktiivin 21 artiklan 2 kohdan h alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä.

Instan asiantuntijoiden arvion mukaan tämän velvoitteen arvioinnissa yritykset voivat ottaa erityisesti huomioon, onko niillä dokumentoidut kryptografian ja salauksen toimintaperiaatteet, jotka ottavat huomioon aitouden, eheyden sekä luottamuksellisuuden näkökulmat. Lisäksi yritykset voivat arvioida, onko algoritmien, protokollien, avainten pituuksien sekä salaustuotteiden valinnat tehty voimassa olevien suositusten mukaisesti, ja onko avainten ja sertifikaattien hallinta ja suojaaminen dokumentoitu.

2.2.2.8.1 Elintarvikesektori

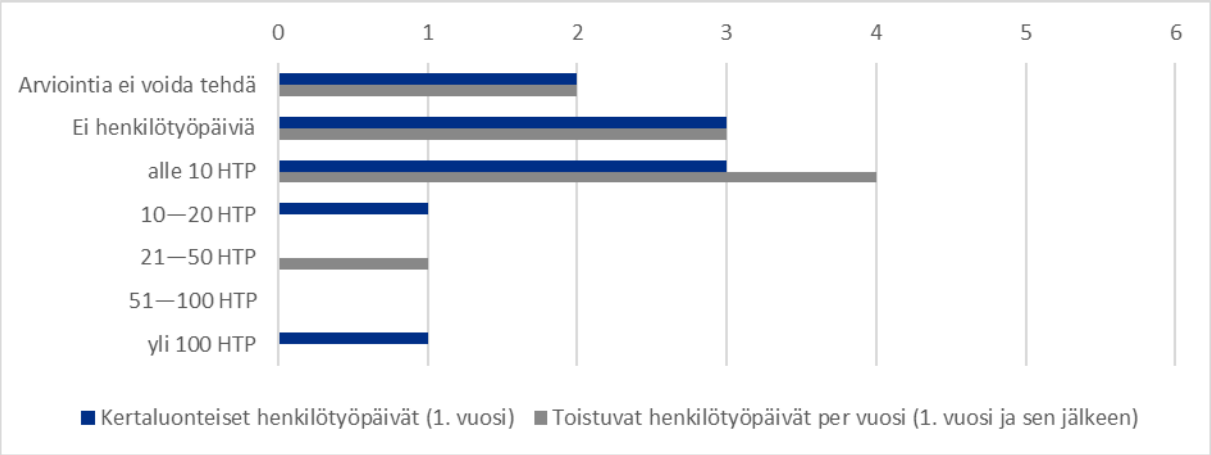
Asteikolla 1–5 elintarvikesektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 2,89. Yleisin arvio nykytilanteesta oli 4, jonka vastasi 44 % arvion antaneista yrityksistä. Lisäksi yksi osallistuneista yrityksistä ei osannut arvioida nykytilannetta.

TAULUKKO 17. Velvoite 8: elintarvikesektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	3	33
3	4	44
4	2	22
5	0	0

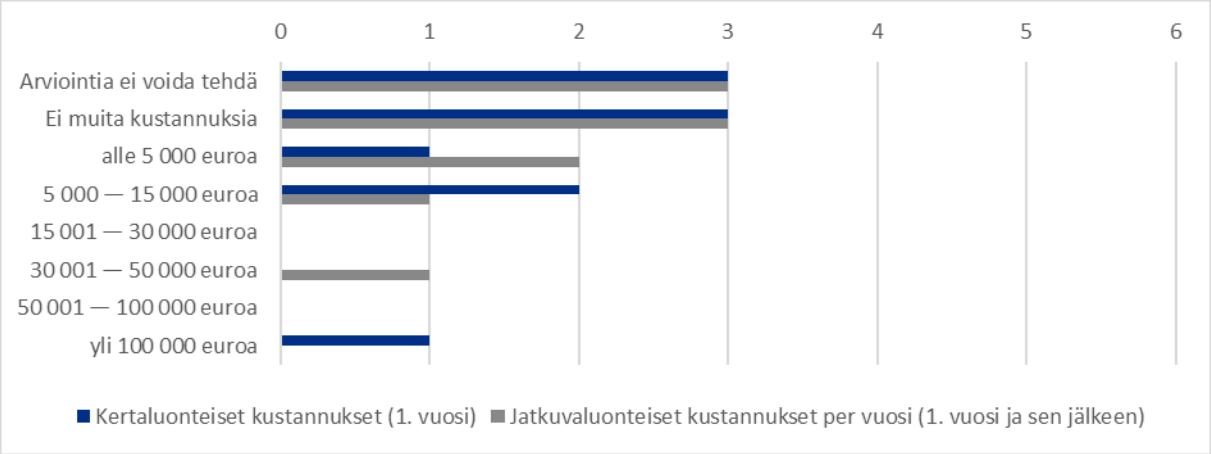
Elintarvikesektoriin kuuluvien yritysten yleisimmät arviot niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä olivat ”Ei henkilötyöpäiviä” sekä alle 10 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli alle 10 henkilötyöpäivää.

KUVIO 29. Velvoite 8: elintarvikesektorille aiheutuvat henkilötyöpäivät



Elintarvikesektoriin kuuluvien yritysten yleisin arvio sekä kertaluonteisten kustannusten että jatkuvaluonteisten kustannusten osalta oli, ettei niille aiheudu tästä velvoitteesta muita kustannuksia.

KUVIO 30. Velvoite 8: elintarvikesektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 23 000 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 10 200 euroa vuosittain tämän jälkeen.

2.2.2.8.2 Valmistussektori

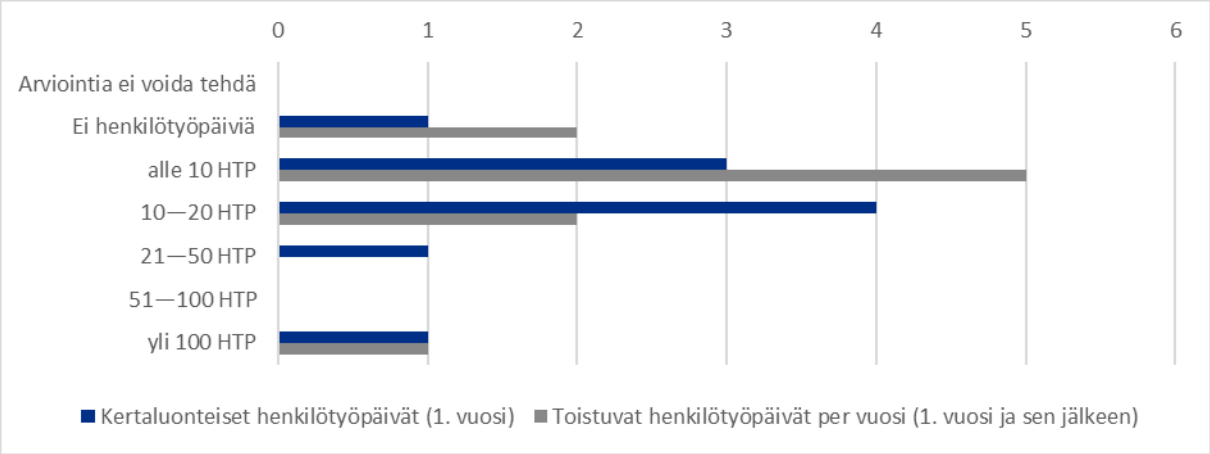
Asteikolla 1–5 valmistussektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 3,3. Yleisin arvio nykytilanteesta oli 4, jonka vastasi 40 % yrityksistä.

TAULUKKO 18. Velvoite 8: valmistussektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	1	10
2	1	10
3	3	30
4	4	40
5	1	10

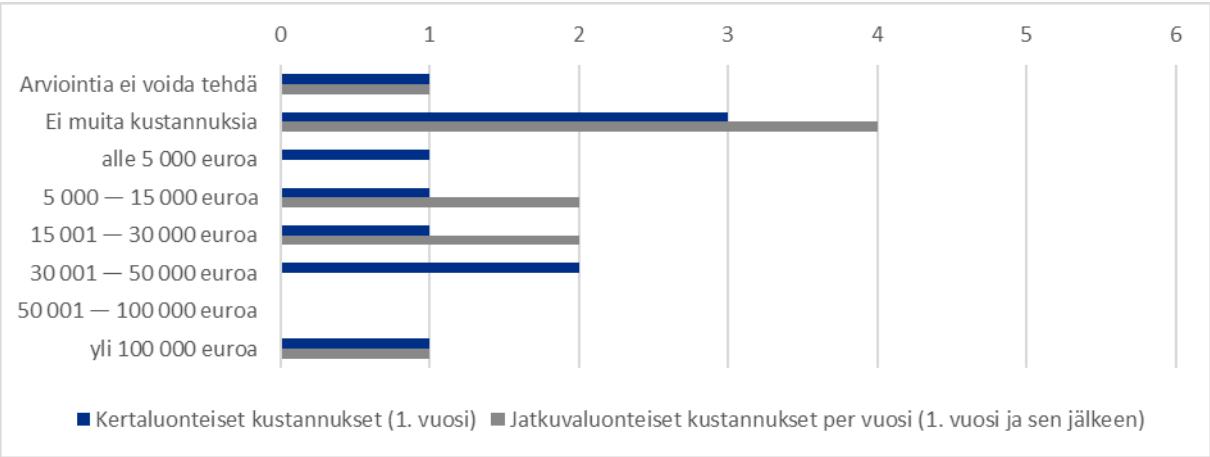
Valmistussektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10–20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli alle 10 henkilötyöpäivää.

KUVIO 31. Velvoite 8: valmistussektorille aiheutuvat henkilötyöpäivät



Valmistussektoriin kuuluvien yritysten yleisin arvio sekä kertaluonteisten kustannusten että jatkuvaluonteisten kustannusten osalta oli, ettei niille aiheudu tästä velvoitteesta muita kustannuksia.

KUVIO 32. Velvoite 8: valmistussektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 30 900 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 23 500 euroa vuosittain tämän jälkeen.

2.2.2.9 Henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta

NIS2-direktiivin 21 artiklan 2 kohdan i alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta.

NIS2-direktiivin johdanto-osan 79 kohdan mukaan ”toimijoiden olisi käsiteltävä kyberturvallisuusriskien hallintatoimenpiteissään myös henkilöstöturvallisuutta ja otettava käyttöön asianmukaiset pääsynhallintaperiaatteet. Näiden toimenpiteiden olisi oltava direktiivin (EU) 2022/2557 mukaisia.”

Direktiivin 2022/2557 (CER-direktiivi) 13 artiklan 1 kohdan e alakohdan mukaan kriittisten toimijoiden tulee ottaa käyttöön toimenpiteitä, jotka ovat tarpeen ”asianmukaisen henkilöstöturvallisuuden hallinnan varmistamiseksi, ottaen asianmukaisesti huomioon sellaiset toimenpiteet kuin kriittisiä tehtäviä hoitavien henkilöstöryhmien määrittäminen, pääsyoikeuksien vahvistaminen tiloihin, kriittiseen infrastruktuuriin ja arkaluonteisiin tietoihin pääsemiseksi, taustatarkastuksia koskevien menettelyjen käyttöönottaminen 14 artiklan mukaisesti ja sellaisten henkilöryhmien määrittäminen, joilta tällaisia taustatarkastuksia vaaditaan, sekä asianmukaisten koulutusvaatimusten ja pätevyyksien vahvistaminen”.

Edellisten lisäksi Instan asiantuntijoiden arvioiden mukaan pääsynhallintaperiaatteissa tulisi ottaa huomioon oikeuksien myöntäminen, muuttaminen ja poistaminen sekä asianmukainen valvonta. Pääsynhallintaperiaatteiden tulisi kattaa koko yrityksen kriittinen infrastruktuuri ja tilat sekä arkaluonteiset tiedot. Omaisuudenhallinnan tulisi kattaa sekä fyysinen että aineeton omaisuus. Lisäksi yrityksellä tulisi olla periaatteet koskien salassapito- ja vaitiolositoumuksia.

Kyselytutkimuksessa havaittiin, että vaatimus omaisuudenhallinnasta on osittain tulkinnanvarainen, koska NIS2-direktiivissä ei määritellä omaisuudenhallinta-termiä tarkasti. Yrityksiä haastateltaessa kävi ilmi, että omaisuudenhallintaa tarkasteltiin usein ISO 27001 -standardin tavoin kaikki tieto-omaisuus ja siihen liittyvät muut omaisuuserät huomioiden. Suppeasti tarkasteltuna omaisuudenhallinta olisi mahdollista tässä yhteydessä kuitenkin ymmärtää esimerkiksi henkilöstön hallussa olevan omaisuuden, kuten työvälineiden, hallinnoinniksi. Laaja tulkinta voisi sisältää kaiken omaisuuden, jolla on yritykselle arvoa.

On syytä huomioida, että omaisuudenhallinnan kehittämiseen liittyvän työn ja muiden kustannusten määrä vaihtelee merkittävästi riippuen siitä, missä laajuudessa omaisuudenhallintaan liittyviä toimenpiteitä toteutetaan. Haastatteluissa omaisuudenhallinnan osalta käytettiin ISO 27001 -standardin mukaista määritelmää.

2.2.2.9.1 Elintarvikesektori

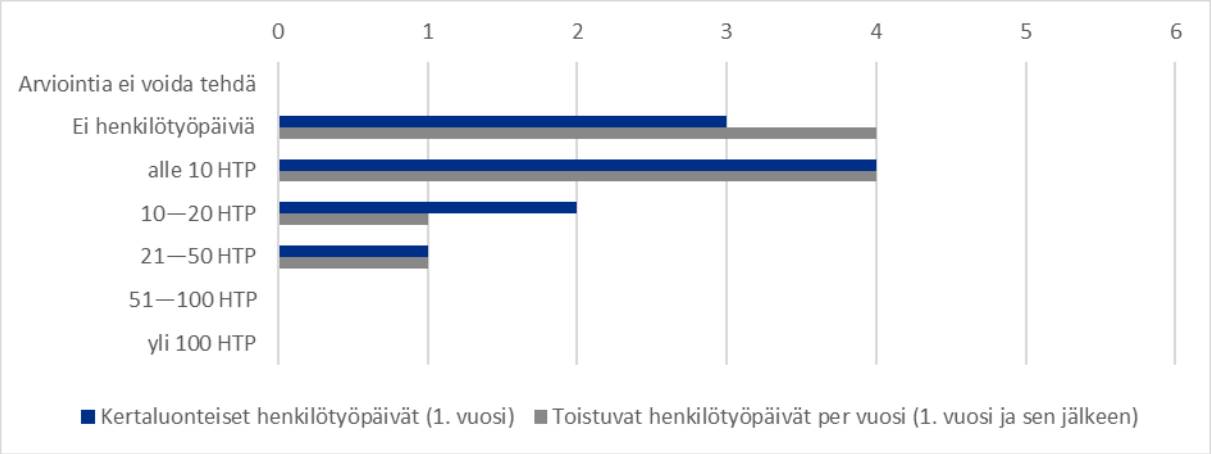
Asteikolla 1–5 elintarvikesektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 3,5. Yrityksistä 40 % antoi vastaukseksi 3 tai 4, jotka olivat yleisimmät arviot nykytilanteesta.

TAULUKKO 19. Velvoite 9: elintarvikesektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	1	10
3	4	40
4	4	40
5	1	10

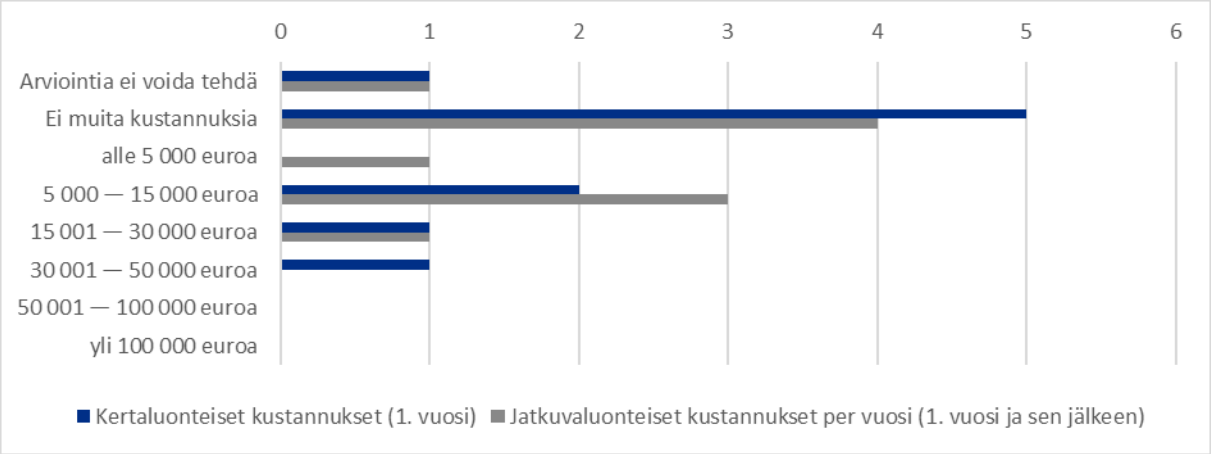
Elintarvikesektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli alle 10 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisimmät arviot olivat ”Ei henkilötyöpäiviä” sekä alle 10 henkilötyöpäivää.

KUVIO 33. Velvoite 9: elintarvikesektorille aiheutuvat henkilötyöpäivät



Elintarvikesektoriin kuuluvien yritysten yleisin arvio sekä kertaluonteisten kustannusten että jatkuvaluonteisten kustannusten osalta oli, ettei niille aiheudu tästä velvoitteesta muita kustannuksia.

KUVIO 34. Velvoite 9: elintarvikesektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 12 000 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 8 500 euroa vuosittain tämän jälkeen.

2.2.2.9.2 Valmistussektori

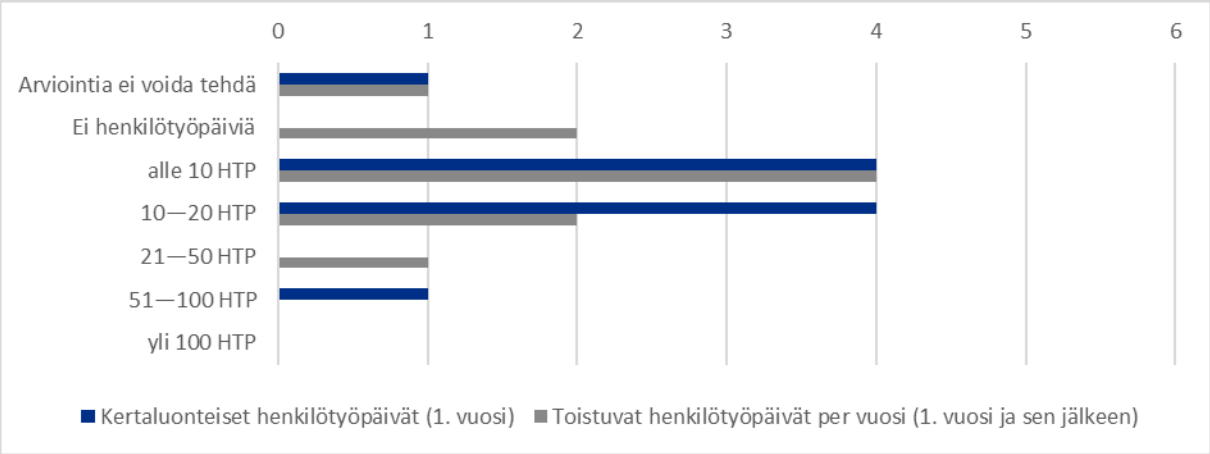
Asteikolla 1–5 valmistussektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 3,5. Yleisin arvio nykytilanteesta oli 4, jonka vastasi 50 % yrityksistä.

TAULUKKO 20. Velvoite 9: valmistussektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	2	20
3	2	20
4	5	50
5	1	10

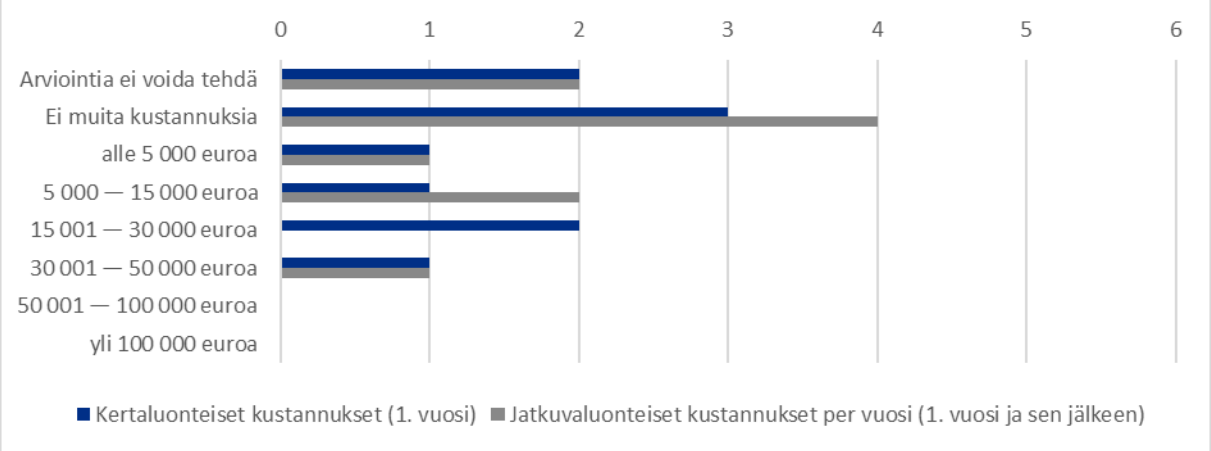
Valmistussektoriin kuuluvien yritysten yleisimmät arviot niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä olivat alle 10 henkilötyöpäivää sekä 10–20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisin arvio oli alle 10 henkilötyöpäivää.

KUVIO 35. Velvoite 9: valmistussektorille aiheutuvat henkilötyöpäivät



Valmistussektoriin kuuluvien yritysten yleisin arvio sekä kertaluonteisten kustannusten että jatkuvaluonteisten kustannusten osalta oli, ettei niille aiheudu tästä velvoitteesta muita kustannuksia.

KUVIO 36. Velvoite 9: valmistussektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 18 000 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 11 000 euroa vuosittain tämän jälkeen.

2.2.2.10 Tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa

NIS2-direktiivin 21 artiklan 2 kohdan j alakohdan mukaan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.

Haastattelujen yhteydessä nousi esille, että monivaiheisen tunnistautumisen käyttöönotto kaikissa suurten yritysten järjestelmissä saattaisi aiheuttaa kohtuuttoman suuria kustannuksia, koska sen tekninen toteuttaminen voi vaatia kalliimpien lisenssien käyttöönottoa esimerkiksi pilvipalveluissa. Kyseinen toiminto voi olla myös vaikea toteuttaa osaan vanhemmista järjestelmistä. Haastatteluissa kuitenkin nousi esille monivaiheisen tunnistautumisen hyödyllisyys ja kannatettavuus silloin, kun sen käyttöönotto perustuu riskiarviointiin, eikä sen käyttö ole pakollista kaikissa ympäristöissä.

Suojattujen hätä- ja muiden viestintäjärjestelmien osalta haastatteluissa kävi ilmi, että merkittävä osa yrityksistä ei osannut määritellä, millaisia kyseiset järjestelmät voisivat käytännössä olla kyseisessä yrityksessä. Tulkinnan helpottamiseksi lainsäädännössä olisi olennaista määritellä joko esimerkein tai muilla tavoin, mitä suojatuilla viestintäjärjestelmillä tarkoitetaan.

2.2.2.10.1 Elintarvikesektori

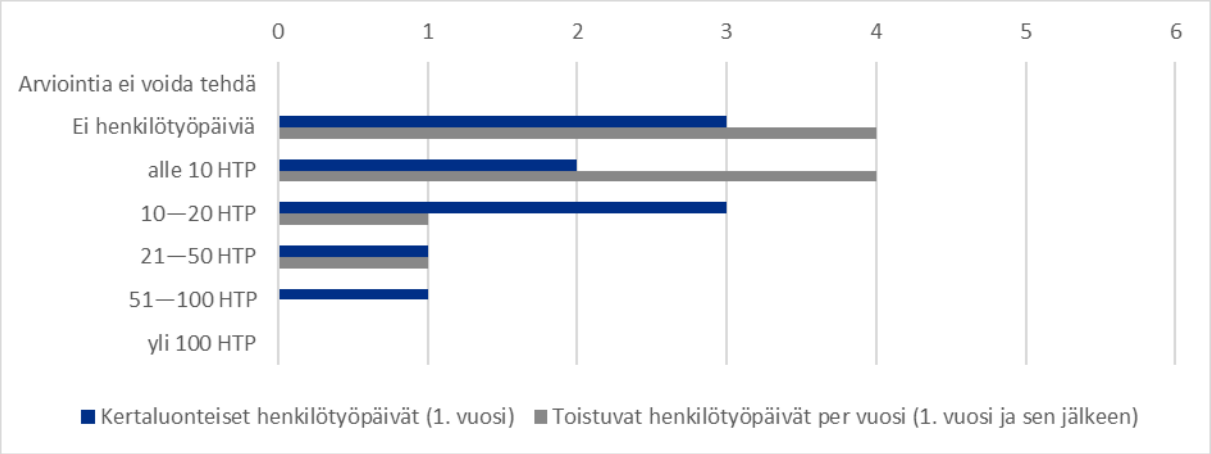
Asteikolla 1–5 elintarvikesektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 3,3. Yrityksistä 30 % antoi vastaukseksi 2 tai 3, jotka olivat yleisimmät arviot nykytilanteesta.

TAULUKKO 21. Velvoite 10: elintarvikesektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	3	30
3	3	30
4	2	20
5	2	20

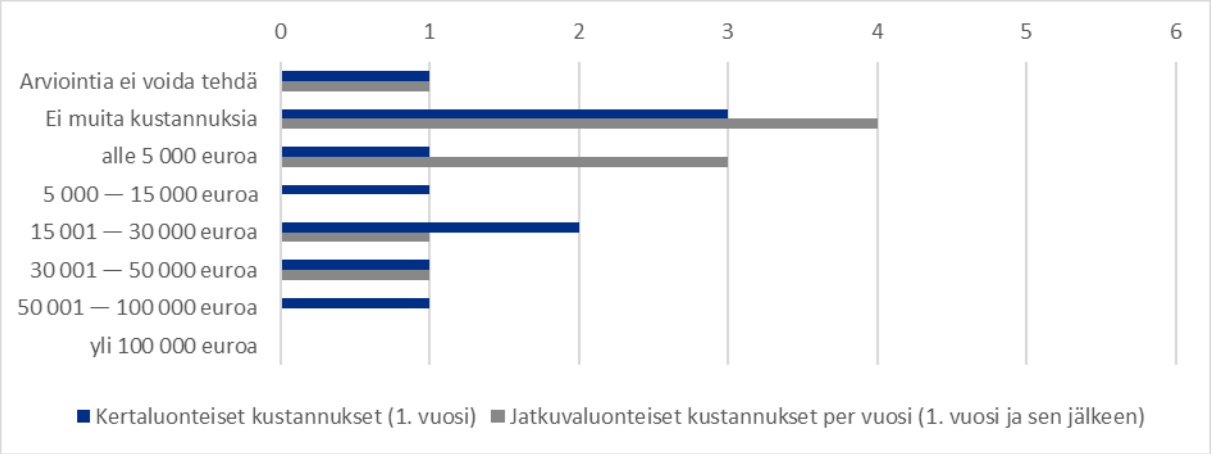
Elintarvikesektoriin kuuluvien yritysten yleisimmät arviot niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli ”Ei henkilötyöpäiviä” sekä 10–20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisimmät arviot olivat ”Ei henkilötyöpäiviä” sekä alle 10 henkilötyöpäivää.

KUVIO 37. Velvoite 10: elintarvikesektorille aiheutuvat henkilötyöpäivät



Elintarvikesektoriin kuuluvien yritysten yleisin arvio sekä kertaluonteisten kustannusten että jatkuvaluonteisten kustannusten osalta oli, ettei niille aiheudu tästä velvoitteesta muita kustannuksia.

KUVIO 38. Velvoite 10: elintarvikesektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille elintarvikesektorin yrityksille aiheutuu kertakustannuksena keskimäärin 24 700 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 10 100 euroa vuosittain tämän jälkeen.

2.2.2.10.2 Valmistussektori

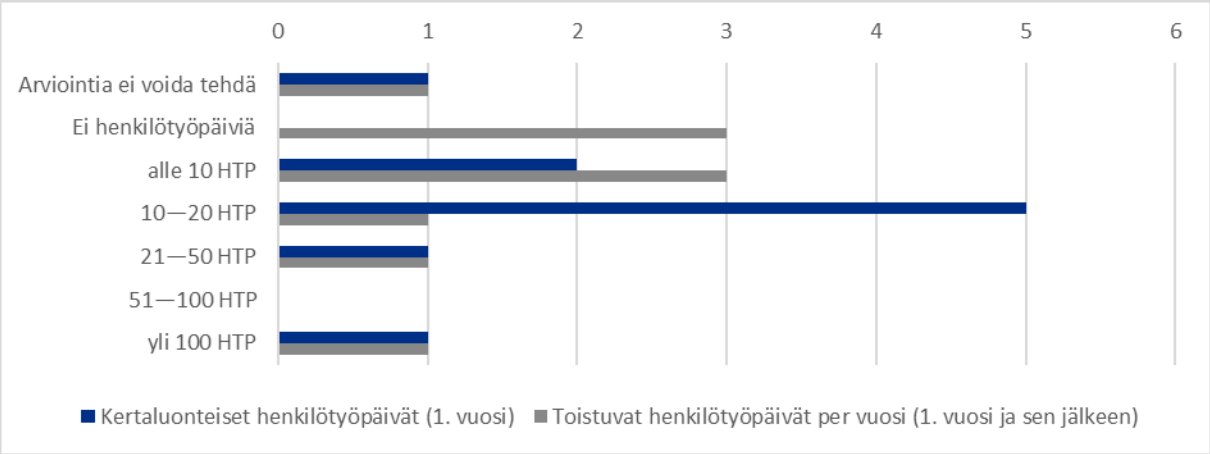
Asteikolla 1–5 valmistussektorin yritysten nykytilan arvioinnin keskiarvoksi saatiin 3,5. Yleisin arvio nykytilanteesta oli 4, jonka vastasi 60 % yrityksistä.

TAULUKKO 22. Velvoite 10: valmistussektorin nykytilanne

Asteikko (1 = merkittäviä puutteita, 5 = ei puutteita)	**Vastaukset**	
	Vastanneiden määrä (kpl)	Prosenttiosuus vastauksista (%)
1	0	0
2	1	10
3	3	30
4	6	60
5	0	0

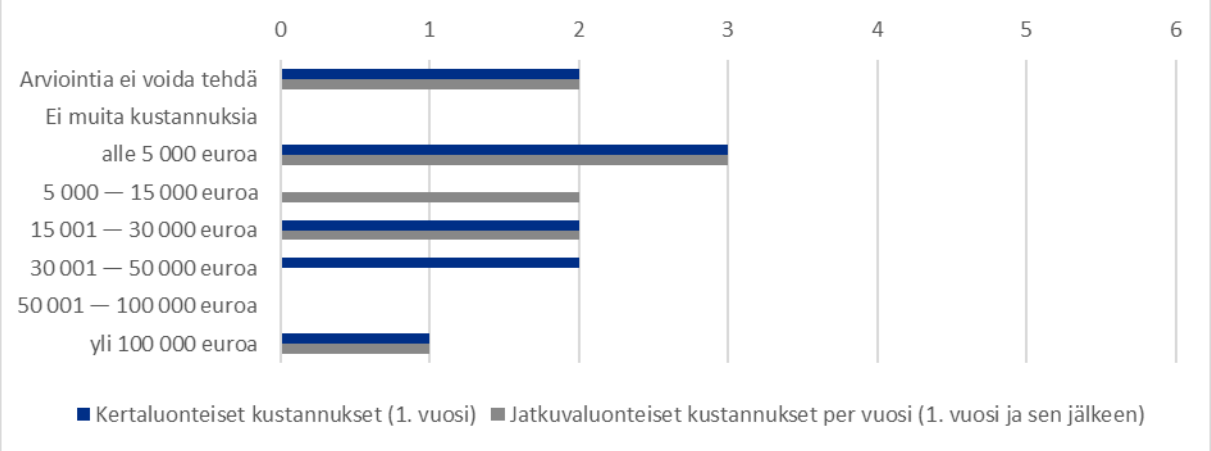
Valmistussektoriin kuuluvien yritysten yleisin arvio niiden tähän velvoitteeseen sopeutumiseen käytettävistä kertaluonteisista henkilötyöpäivistä oli 10–20 henkilötyöpäivää. Vuosittain aiheutuvia toistuvia henkilötyöpäiviä arvioidessa yleisimmät arviot olivat ”Ei henkilötyöpäiviä” sekä alle 10 henkilötyöpäivää.

KUVIO 39. Velvoite 10: valmistussektorille aiheutuvat henkilötyöpäivät



Valmistussektoriin kuuluvien yritysten yleisin arvio niille tähän velvoitteeseen sopeutumiseen kertaluonteisesti käytettävistä muista kustannuksista oli alle 5 000 euroa. Vuosittain aiheutuvia jatkuvaluonteisia kustannuksia arvioidessa yleisin arvio oli alle 5 000 euroa.

KUVIO 40. Velvoite 10: valmistussektorille aiheutuvat muut kustannukset



Sääntelytaakkalaskurin mukaan kyselytutkimukseen osallistuneille valmistussektorin yrityksille aiheutuu kertakustannuksena keskimäärin 37 300 euroa tähän velvoitteeseen sopeutumisesta ensimmäisenä vuonna ja 27 700 euroa vuosittain tämän jälkeen.

2.2.3 Keskeiset havainnot ja päätelmät

Yritysten velvoitteiden nykytilan arvioinneissa sekä elintarvike- että valmistussektorilla heikoimmat arviot asteikolla 1–5 saivat velvoitteet 3–6 (keskiarvo 2,5–2,8). Elintarvikesektorilla parhaimmat arviot saivat velvoitteet 7 ja 9 (keskiarvo 3,5–3,6) ja valmistussektorilla velvoitteet 9 ja 10 (keskiarvo 3,5).

TAULUKKO 23. Velvoitteiden täyttämisen nykytilanteen arvioiden keskiarvot

Riskienhallintavelvoite	Elintarvikesektori	Valmistussektori
Velvoite 1	3,00	3,20
Velvoite 2	3,10	3,30
Velvoite 3	2,50	2,80
Velvoite 4	2,60	2,80
Velvoite 5	2,50	2,80
Velvoite 6	2,80	2,50
Velvoite 7	3,60	3,40
Velvoite 8	2,89	3,30
Velvoite 9	3,50	3,50
Velvoite 10	3,30	3,50

Sekä elintarvikesektorilla että valmistussektorilla kertaluonteisia kustannuksia tulee eniten velvoitteista 1, 2 ja 4. Jatkuvaluonteisia kustannuksia elintarvikesektorilla aiheutuu eniten velvoitteista 2, 4 ja 5 sekä valmistussektorilla velvoitteista 1, 2 ja 4. Elintarvikesektorilla vähiten

kustannuksia aiheutuu velvoitteesta 6 ja 9. Valmistussektorilla vähiten kustannuksia aiheutuu velvoitteista 8 ja 9.

Elintarvikesektorille aiheutuvat yhteenlasketut kertaluonteiset kustannukset ovat noin 25 % matalammat kuin valmistussektorilla. Jatkuvaluonteisesti elintarvikesektorille aiheutuu noin 47 % matalammat kustannukset kuin valmistussektorille.

TAULUKKO 24. Riskienhallintavelvoitteista aiheutuvat keskimääräiset kustannukset per yritys sektoreittain

Riskienhallinta-velvoite	**Elintarvikesektori**		**Valmistussektori**	
	Kertaluonteiset kustannukset (€) (1. vuosi)	**Jatkuvat kustannukset (€) (1. vuosi ja sen jälkeen)**	**Kertaluonteiset kustannukset (€) (1. vuosi)**	**Jatkuvat kustannukset (€) (1. vuosi ja sen jälkeen)**
Velvoite 1	32 300	11 400	52 900	36 900
Velvoite 2	47 200	19 700	43 200	39 500
Velvoite 3	31 200	19 400	32 100	29 500
Velvoite 4	39 100	23 200	46 500	31 700
Velvoite 5	30 800	21 900	34 200	25 100
Velvoite 6	12 100	4 500	34 700	27 600
Velvoite 7	21 900	19 500	37 100	26 700
Velvoite 8	23 000	10 200	30 900	23 500
Velvoite 9	12 000	8 500	18 000	11 000
Velvoite 10	24 700	10 100	37 300	27 700
Yhteensä	**274 000**	**148 000**	**367 000**	**279 000**

Elintarvike- ja valmistussektoriin kuuluville yrityksille aiheutuu 21 artiklan riskienhallintavelvoitteista keskimäärin kertaluonteisesti noin 320 000 euron kustannukset, joista 27 % on työkustannuksia ja 73 % muita kustannuksia. Jatkuvaluonteisia kustannuksia aiheutuu keskimäärin noin 214 000 euroa, joista 26 % on työkustannuksia ja 74 % muita kustannuksia.

TAULUKKO 25. Riskienhallintavelvoitteista aiheutuvat keskimääräiset kustannukset elintarvike- ja valmistussektoreille per yritys kustannuslajeittain

Riskienhallinta-velvoite	Työkustannukset		Muut kustannukset	
	Kertaluonteiset kustannukset (€) (1. vuosi)	**Jatkuvat kustannukset (€) (1. vuosi ja sen jälkeen)**	**Kertaluonteiset kustannukset (€) (1. vuosi)**	**Jatkuvat kustannukset (€) (1. vuosi ja sen jälkeen)**
Velvoite 1	11 500	7 700	31 100	16 400
Velvoite 2	7 700	6 300	37 500	23 300
Velvoite 3	10 200	6 500	21 400	17 900
Velvoite 4	11 900	8 900	30 900	18 500
Velvoite 5	10 400	6 300	22 000	17 200
Velvoite 6	7 500	4 800	16 000	11 300
Velvoite 7	8 600	5 000	20 800	18 100
Velvoite 8	6 300	3 800	20 700	13 100
Velvoite 9	4 300	2 800	10 700	7 000
Velvoite 10	6 900	4 300	24 100	14 700
Yhteensä	**85 300**	**56 400**	**235 200**	**157 500**

2.2.3.1 Haastateltujen yritysten keskeisimmät huomiot

Yleisenä huomiona 21 artiklan riskienhallintavelvoitteiden kustannusvaikutuksista voidaan todeta ensinnäkin, että yritykset kokivat niiden arvioimisen *tarkasti* lähes poikkeuksetta hankalaksi yrityksen toimialasta ja koosta riippumatta. Suurten yritysten ja konsernien kohdalla arviointia hankaloitti erityisesti epätietoisuus siitä, kuinka laajasti niiden eri liiketoimintojen tai sidosyhtiöiden katsotaan lopulta kuuluvan NIS2-direktiivin soveltamisalan piiriin.

Kyselytutkimuksessa saatujen vastausten perusteella useat isot yritykset ja konsernit olivat tunnistaneet, että niiden eri toiminnoista osa todennäköisesti kuuluu NIS2-direktiivin soveltamisalaan ja osa ei. Tietyt yritykset olivat puolestaan linjanneet, että ne tulevat ulottamaan NIS2-direktiivin velvoitteet kaikkiin toimintoihinsa direktiivin soveltamisalasta riippumatta.

Yrityksiä kuultaessa toistui myös havainto siitä, että NIS2-direktiivin 21 artiklan riskienhallintatoimenpiteet vastaavat otsikkotasolla pääsääntöisesti ISO 27001 –standardin vaatimuksia. Niissä yrityksissä, joissa noudatetaan ISO 27001 –standardia, epätietoisuutta aiheutti kysymys siitä, missä määrin NIS2-direktiivin 21 artiklan vaatimukset menevät ISO 27001 –standardin vaatimuksia pidemmälle. Yhtä lailla niissä yrityksissä, joissa sertifiointityö

oli parhaillaan käynnissä, koettiin haastavaksi arvioida, kuinka paljon tulevasta lisätyöstä ja aiheutuvista kustannuksista olisi luettava NIS2-direktiivistä johtuvaksi.

Kyselytutkimukseen osallistuneiden yritysten joukossa oli myös toimijoita, joihin sovellettavassa EU:n alakohtaisessa sääntelyssä on jo vaadittu ottamaan käyttöön kyberturvallisuusriskien hallintatoimenpiteitä. NIS2-direktiivin johdanto-osan mukaan näiden yritysten olisi sovellettava kyseisiä alakohtaisia säännöksiä, jos alakohtaisen sääntelyn vaatimukset ovat vaikutukseltaan vähintään NIS2-direktiivissä säädettyjä velvoitteita vastaavia. Kyselytutkimuksen vastauksista kävi ilmi, että vaatimusten keskinäinen vertailu on haastavaa, mikä osaltaan hankaloitti NIS2-direktiivin 21 artiklasta aiheutuvien kustannusten arviointia.

NIS2-direktiivistä aiheutuvien kustannusten erottamista muista tietoturvaan liittyvistä tulevista kustannuksista vaikeuttaa saatujen vastausten perusteella myös se, että varsinkin suuremmissa yrityksissä tietoturvan tason kehittäminen on joka tapauksessa jatkuva prosessi niihin soveltuvasta sääntelykehikosta riippumatta.

Keskisuurissa yrityksissä kulujen arviointia hankaloitti ennen kaikkea sen määrittäminen, milloin riskienhallintatoimenpiteiden voidaan katsoa olevan oikeassa suhteessa riskeihin NIS2-direktiivin 21 artiklan tarkoittamalla tavalla. Selvitykseen osallistuneet keskisuuret yritykset nostivat esiin kysymyksen niiden mahdollisesti kohtaamien kyberturvallisuusriskien yhteiskunnallisista ja taloudellisista vaikutuksista verrattuna suuriin toimijoihin. Riskiperusteisen lähestymistavan oikeasuhtainen soveltaminen koettiin toisin sanoen haasteeksi etenkin keskisuurissa yrityksissä.

Suuria yrityksiä kuultaessa kävi ilmi, että selvityksessä käytetyt kustannusten ja työpäivien ylimmät asteikot, eli ”yli 100 000 euroa” ja ”yli 100 HTP", voivat olla maltillisia siihen verrattuna, kuinka paljon riskienhallintavelvoitteen implementointi voi tietyissä tapauksissa yritykselle kustantaa. Näin ollen *yli* 100 000 euroa tai *yli* 100 HTP:tä voi tarkoittaa suuryritysten kohdalla satojatuhansia euroja tai satoja henkilötyöpäiviä.

Yritysten vastauksissa toistui lisäksi huomio siitä, että niillä on paremmat edellytykset arvioida riskienhallintavelvoitteista aiheutuvia kustannuksia sen jälkeen, kun Suomessa on NIS2-direktiivin 3 artiklan 3 kohdan mukaisesti laadittu luettelo keskeisistä ja tärkeistä toimijoista viimeistään 17.4.2025 mennessä (eli noin puoli vuotta sen jälkeen, kun direktiivin säännökset on tullut saattaa osaksi kansallista lainsäädäntöä). Useat yritykset myös huomioivat, että EU-komissio voi NIS2-direktiivin 21 artiklan 5 kohdan mukaan hyväksyä täytäntöönpanosäädöksiä, joilla vahvistetaan riskienhallintavelvoitteiden tekniset ja menetelmiin liittyvät vaatimukset sekä tarvittaessa alakohtaiset vaatimukset.

Näin ollen varsinkin suurten yritysten joukossa pidettiin toivottavana, että riskienhallintavelvoitteista aiheutuvia kustannuksia arvioidaan uudestaan sen jälkeen, kun NIS2-direktiivin soveltamisala ja 21 artiklan toimialakohtaiset velvoitteet ovat mahdollisesti tarkentuneet. Kustannuksia uudelleen arvioitaessa voitaisiin myös tarkastella, kuinka hyvin EU-komission vaikutustenarvioinnissaan[5] esittämä arvio siitä, että uuden NIS-kehyksen

[5] Ks. tiivistelmä komission vaikutustenarvioinnista ehdotukseen NIS2-direktiiviksi (COM 2020/823 final).

soveltamisalaan tulevien yritysten olisi kasvatettava nykyisiä tieto- ja viestintätekniikan turvallisuuteen liittyviä menojaan enintään 22 % NIS-kehyksen ensimmäisinä vuosina, on toteutunut Suomeen sijoittautuneissa yrityksissä.

2.3 Riskienhallintavelvoitteista aiheutuvat kustannushyödyt

Koska NIS2-diretiivin tavoitteena on parantaa kyberturvallisuuden tasoa ja siten muun muassa ennaltaehkäistä kyberhäiriöitä ja niistä aiheutuvia haitallisia vaikutuksia, sääntelyllä on arvioitu olevan myös **välillisiä kustannushyötyjä** yrityksille. Tässä selvityksessä on arvioitu NIS2-direktiivin 21 artiklasta johtuvien velvoitteiden noudattamisesta syntyvistä kustannushyötyjä muun muassa kyberhäiriöiden vähentyessä.

Komission toteuttamassa NIS2-direktiivin vaikutustenarvioinnissa hyödyiksi oli tunnistettu esimerkiksi tietoturvaloukkauksista ja kyberrikoksista aiheutuneiden kulujen vähentyminen, asiakkaiden luottamuksen lisääntyminen, yrityksen maineen parantuminen, suojelu epäreilulta kilpailulta (teollisuusvakoilu), tyytymättömien asiakkaiden siirtymisen vähentyminen kilpailijoille sekä vaatimustenmukaisuuden lisääntyminen.

2.3.1 Kyselytutkimuksen toteutustapa

Kustannushyödyt jaettiin kyselytutkimuksessa komission vaikutustenarviointia mukaillen eri kategorioihin. Yrityksiä pyydettiin arvioimaan kustannushyötyjä vuositasolla.

Kyselytutkimuksessa kustannushyötyjen neljä kategoriaa olivat:

- asiakkaiden luottamuksen lisääntyminen
- tietoturvaloukkauksiin ja kyberrikoksiin liittyvien kustannusten vähentyminen
- kyberhäiriöiden väheneminen ja järjestelmien saatavuuden paraneminen
- muut kustannushyödyt.

Kussakin kategoriassa kustannushyödyille annettiin kuusi suuruusluokkaa:

- Ei kustannushyötyjä
- alle 10 000 euroa
- 10 000–20 000 euroa
- 20 001–50 000 euroa
- 50 001–100 000 euroa
- yli 100 000 euroa.

Lisäksi yrityksille annettiin mahdollisuus valita ”Arviointia ei voida tehdä”.

2.3.2 Tulokset

Kyselytutkimukseen osallistuneet yritykset kokivat kustannushyötyjen euromääräisen arvioinnin vaikeaksi. Kategoriasta riippumatta suurin osa yrityksistä vastasi ”Arviointia ei voida tehdä”. Helpoiten arvioitavaksi koettiin kyberhäiriöihin sekä saatavuuteen liittyvä

kustannushyöty, johon seitsemän yritystä 19:sta vastanneesta osasi antaa numeraalisen arvion. Tuloksista ei ole havaittavissa merkittäviä eroja eri sektorien välillä.

TAULUKKO 26. Arvioiden määrät riskienhallintavelvoitteista aiheutuvista kustannushyödyistä

	Asiakkaiden luottamuksen lisääntyminen	**Tietoturvaloukkauksiin ja kyberrikoksiin liittyvien kustannusten vähentyminen**	**Kyberhäiriöiden väheneminen ja saatavuuden paraneminen**	**Muut kustannus-hyödyt**
Arviointeja yhteensä	20	19	19	19
Arviointia ei voida tehdä	11	11	9	15
Arvion antaneet	9	8	10	4
Ei kustannus-hyötyjä	4	3	3	3
alle 10 000 euroa	0	1	2	0
10 000—20 000 euroa	0	1	0	1
20 001—50 000 euroa	2	2	3	0
50 001—100 000 euroa	1	1	1	0
yli 100 000 euroa	2	0	1	0

2.3.3 Keskeiset havainnot ja päätelmät

Kyselytutkimuksessa kävi ilmeiseksi, että mahdollisten kustannushyötyjen euromääräiseen arviointiin liittyy niin useita muuttujia, ettei suurin osa osallistuneista yrityksistä kyennyt esittämään tällaista arviointia.

Huolimatta siitä, että yritysten oli vaikea arvioida NIS2-direktiivistä syntyviä kustannushyötyjä euromääräisesti, toistui yritysten vastauksissa näkemys siitä, että kyberturvallisuustason paranemisella on väistämättä merkittäviä positiivisia liiketaloudellisia vaikutuksia. Kyberturvallisuuteen liittyvät vaatimukset näkyvät yritysten mukaan liiketoiminnassa monin tavoin.

Asiakkaiden luottamuksen lisääntymisen vuoksi kustannushyötyjä nähtiin syntyvän, sillä yhä useampi asiakas kiinnittää aikaisempaa enemmän huomiota kyberturvallisuuden tasoon hankinnoissa ja kilpailutuksissa. Yritysten vastauksissa toistui huomio siitä, että jo yhdenkin suuren asiakkaan menettämisellä tai voittamisella kybermaturiteettiin liittyvistä syistä voi olla pitkälti yli 100 000 euron vaikutus.

Asiakkaiden luottamuksen lisääntymisen osalta osa yrityksistä arvioi olennaiseksi sen, onko yrityksellä merkittäviä kilpailijoita EU:n ulkopuolella. NIS2-direktiivin asettamien velvoitteiden

täyttämisen arvioitiin mahdollisesti antavan kilpailuetua verrattuna niihin saman toimialan yrityksiin, joihin direktiiviä ei sovelleta.

Kuulluista yrityksistä vain muutama kertoi kohdanneensa vakavia kyberpoikkeamia lähimenneisyydessä. Näin ollen mahdollisten kustannushyötyjen arvioiminen jo tapahtuneisiin poikkeamiin peilaten ei ollut pääasiassa mahdollista. Yritykset tunnistivat joka tapauksessa, että potentiaalisten poikkeamatilanteiden välttämisellä on merkittävät kustannushyödyt esimerkiksi sitä kautta, että henkilötyötunteja ei jouduta sitomaan poikkeaman selvittämiseen ja toisaalta siten, että asiakkaiden luottamus yritykseen säilyy.

Yritysten vastauksista kävi myös ilmi näkemys siitä, että kybersääntelyn ja sitä kautta kybermaturiteetin vahvistuessa erilaiset kyberhyökkäykset tulevat vähenemään jo senkin vuoksi, että rikollisten on vaikeampi toteuttaa niitä ja hyödyt jäävät pienemmiksi. Tällä nähtiin olevan kustannushyötyjä, joskin vaikutusta on mahdoton arvioida euromääräisesti.

3 Yhteenveto

3.1 Kyselytutkimukseen osallistuneista yrityksistä

Selvityksen taustalla olevaan kyselytutkimukseen osallistui yhteensä 20 yritystä NIS2-direktiivin liitteessä II tarkoitetuilta elintarvike- ja valmistussektoreilta. Osallistuneista yrityksistä suureksi määriteltyjä yrityksiä oli 15 ja keskisuuria yrityksiä 5.

Selvityshankkeen perusteella voidaan vahvistaa, että NIS2-direktiivi ja siihen liittyvä kansallinen lainsäädäntöhanke herättää yrityksissä mielenkiintoa. Toisaalta havaintona on, että yrityksillä on merkittävä tarve saada lisätietoa direktiivin sisällöstä ja vaatimuksista.

Kyselytutkimuksen perusteella etenkin suuret konsernit olivat hyvin tietoisia direktiivistä ja kansallisesta lainvalmisteluprosessista. Sen sijaan keskisuurten yritysten keskuudessa NIS2-direktiivin tunnettuus oli heikompaa. Useamman keskisuuren yrityksen kohdalla selvitykseen osallistuminen oli ensimmäinen syvällisempi tutustuminen NIS2-direktiivin vaatimuksiin. Samoin oli tiettyjen suurten valmistussektorin yritysten kohdalla, joihin ei ole perinteisesti kohdistunut huolto- tai kybervarmuuteen liittyvää sääntelyä.

Kyselytutkimukseen osallistuneista yrityksistä suurin osa oli suuria yrityksiä ja konserneja. Saatujen vastausten ja Instan arvioiden perusteella keskisuurten yritysten osallistumishalukkuus selvityshankkeeseen oli pienempi erityisesti siksi, että keskisuuret yritykset eivät ole vielä keskimäärin tietoisia kyberturvallisuusdirektiivin soveltumisesta niiden toimintaan. On huomattava, että keskisuuren yrityksen raja-arvot – 50 työntekijää ja liikevaihto yli 10 miljoonaa – ylittyvät hyvin laajassa joukossa erilaisia Suomeen sijoittautuneita elintarvike- ja valmistussektorin yrityksiä.

3.2 Kyberturvaan kohdistuvista kuluista

Selvityksessä on arvioitu yritysten nykyisiä kyberturvallisuuteen liittyviä kuluja, jotka lukeutuvat tavallisesti laajemmin toimijoiden ICT-kokonaiskustannuksiin. EU-komission NIS2-direktiivin taustalla olevan vaikutustenarvioinnin mukaan yritysten yleiset ICT-kustannukset ovat keskimäärin 5,69 % yrityksen vuotuisesta liikevaihdosta ja kyberturvallisuuskustannukset (*ICT security spending*) 0,52 % vuotuisesta liikevaihdosta.

Kyselytutkimukseen osallistuneet valmistussektorin yritykset arvioivat nykyisiksi kyberturvallisuuskustannuksiksi keskimäärin 0,69 % vuotuisesta liikevaihdosta ja elintarvikesektorin yritysten arvio oli 0,28 % vuotuisesta liikevaihdosta. Kyselytutkimuksessa kävi ilmi, että puhtaasti kyberturvallisuuteen ja NIS2-direktiivin velvoitteisiin liittyviä kustannuksia on vaikea erotella yleisistä ICT-kustannuksista. Lisäksi on huomioitava, että kyselytutkimuksessa usean yrityksen arviot kyberturvallisuuskustannuksista eivät perustuneet tarkkoihin kirjanpidon lukuihin, vaan yritysten tietoturva-asiantuntijoiden arvioihin kustannuksista.

Arvioinnin haasteista huolimatta voitaneen todeta, että kyselytutkimuksen tulokset ovat linjassa EU-komission vaikutustenarvioinnissa esittämän arvion kanssa. On myös huomattava, että aivan kuten yleisten ICT-kustannusten kohdalla, myös kyberturvallisuuteen käytettyjen varojen määrään vaikuttaa yrityksen toimialan lisäksi muun muassa sen koko ja käytettävissä olevat resurssit.

3.3 Riskienhallintavelvoitteista aiheutuvista kustannuksista

Kyselytutkimuksessa yrityksiä pyydettiin arvioimaan, kuinka hyvin ne täyttävät kunkin NIS2-direktiivin 21 artiklan riskienhallintavelvoitteen nykyisellään. Nykytilanteen tarkastelu johdatteli yritykset arvioimaan 21 artiklan velvoitteista jatkossa aiheutuvia kustannuksia. Kyselytutkimuksen vastausten keskiarvon perusteella sekä valmistus- että elintarvikesektorin yritysten arvio velvoitteiden täyttämisen nykytilasta asteikoilla 1–5 oli noin 3.

Selvityksen perusteella NIS2-direktiivin 21 artiklan mukaiset riskienhallintavelvoitteet tulevat aiheuttamaan merkittävinäkin pidettäviä kustannuksia elintarvike- ja valmistussektoriin kuuluville yrityksille sekä lyhyellä että pitkällä aikavälillä. Elintarvikesektorin yrityksille aiheutuu 21 artiklan riskienhallintavelvoitteista keskimäärin kertaluonteisesti yhteensä noin 274 000 euron kustannukset. Jatkuvaluonteisia vuosittaisia kustannuksia elintarvikesektorin yrityksille aiheutuu keskimäärin yhteensä noin 148 000 euroa. Vastaavat luvut valmistussektorilla ovat 367 000 euroa ja 279 000 euroa.

Kyselytutkimuksen perusteella elintarvikesektorin yrityksille aiheutuu valmistussektoria vähemmän kustannuksia 21 artiklan riskienhallintavelvoitteiden noudattamisesta sekä lyhyellä että pitkällä aikavälillä. Elintarvikesektorilla kertaluonteisten kustannusten osalta kulut ovat noin 25 % matalammat ja jatkuvaluonteisten kustannusten osalta 47 % matalammat.

Vastauksia tarkasteltaessa voidaan huomata, että tietyt 21 artiklan vaatimukset erottautuvat sekä velvoitteen täyttämisen nykytilan että tulevien kustannusten arvioinnin osalta. Esimerkiksi sekä elintarvike- että valmistussektorilla matalimmat arviot nykytilanteesta asteikolla 1–5 saivat velvoitteet 3–6 (keskiarvo 2,5–2,8). Kustannusten osalta sekä elintarvikesektorilla että valmistussektorilla kertaluonteisia kustannuksia tulee eniten velvoitteista 1, 2 ja 4. Jatkuvaluonteisten kustannuksien osalta molemmissa sektoreissa erottuivat vastaavasti velvoitteet 2 ja 4.

Sekä suurten että keskisuurten yritysten vastausten taustalla toistui näkemys siitä, että kustannusten tarkka euromääräinen arviointi nykyisillä tiedoilla on hyvin haasteellista. Suurten yritysten kohdalla merkittävin haaste johtui direktiivin soveltamisalaan liittyvistä kysymyksistä. Moni kyselytutkimukseen osallistunut suuryritys arvioi, että ne harjoittavat toimintaa, josta osa todennäköisesti kuuluu NIS2-direktiivin soveltamisalaan ja osa ei. Monikansallisissa yrityksissä

sisäisiä tietoturvaan liittyviä palveluita saatetaan myös toteuttaa Suomen rajojen ulkopuolella, mikä aiheuttaa entisestään haasteita arvioida Suomeen sijoittuneen yrityksen kyberturvallisuuteen käytettäviä kustannuksia.

NIS2-direktiivin 21 artiklan riskienhallintavelvoitteista aiheutuvien kustannusten arviointia hankaloitti käytännössä kaikkien kyselytutkimukseen osallistuneiden yritysten kohdalla se, että yritysten on arvioitava vaadittavia toimenpiteitä riskiperusteisen lähestymistavan mukaisesti. Yritysten vastausten perusteella ne tulevat tarvitsemaan ohjausta siinä, milloin käyttöönotettujen riskienhallintatoimenpiteiden voidaan katsoa olevan oikeasuhtaisia huomioiden toimijan koko, niiden mahdollisesti kohtaamien riskien todennäköisyys, riskien vakavuus ja niiden yhteiskunnalliset ja taloudelliset vaikutukset.

3.4 NIS2-direktiivin kustannushyödyistä

Siinä missä 21 artiklan riskienhallintavelvoitteista yritykset pystyivät antamaan arvionsa kustannuksista, ei tämä ollut pääsääntöisesti mahdollista kustannushyötyjen kohdalla. Kyselytutkimukseen osallistuneet yritykset kuitenkin tunnistivat useita erilaisia liiketaloudellisia hyötyjä kybermaturiteetin parantuessa pakottavan lainsäädännön myötä.

Kyselytutkimuksen perusteella voidaan todeta, että pääasiassa jokainen estetty merkittävä kyberpoikkeama on yritykselle tuntuva kustannushyöty. Tämä voi näkyä esimerkiksi asiakkaiden luottamuksen säilymisenä tai menetettyjen työtuntien välttämisenä. Etenkin suurten yritysten kohdalla välilliset kustannushyödyt voivat olla satojatuhansia euroja.

Liitteet

1. TEM:n sääntelytaakkalaskuri, valmistussektori
2. TEM:n sääntelytaakkalaskuri, elintarvikesektori