jamk

# Organisaation tietoturvallisuus toimitta-jasuhteissa: Riskien arviointi ja IoT-toi-mittajan vastuut

Maija Virta

Opinnäytetyö, AMK
Huhtikuu 2024
Tieto- ja viestintätekniikan tutkinto-ohjelma

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

**Kuvailulehti**

**Virta, Maija**

**Organisaation tietoturvallisuus toimittajasuhteissa: Riskien arviointi ja IoT-toimittajan vastuut.**

Jyväskylä: Jyväskylän ammattikorkeakoulu. Huhtikuu 2024, 89 sivua

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

**Tiivistelmä**

Digita Oy operoi koko Suomen laajuisesti televisio- ja radioverkkoa ja on maan suurin riippumaton tietoliikennemastojen omistaja. Yhtiö on keskeinen osa Suomen huoltovarmuutta ja tarjoaa lisäksi nykyaikaisia teknologiapalveluita, kuten konesali- ja IoT-palveluita. Digita on sitoutunut kehittämään tietoturvallisuuden hallintajärjestelmäänsä Broadcasting- ja Telecom-pääliiketoiminta alueillaan.

Opinnäytetyön tavoitteena oli kehittää työn toimeksiantajan Digita Oy:n tietoturvallisuuden hallintajärjestelmää IoT-liiketoiminnan osalta, keskittyen erityisesti toimittajasuhteiden tietoturvallisuuteen. Tutkimuksen ensisijaisena päämääränä oli luoda toimittajan riskien arviointilomake organisaation käyttöön. Lomakkeen luomiseksi tutkimuksen ensimmäisenä tavoitteena oli tutkia toimittajasopimuksia ja niihin liittyviä tietoturvavaatimuksia. Tarvittavan taustatiedon saamiseksi tutkimus toteutettiin monimenetelmällisenä, yhdistäen sekä laadullista että määrällistä tutkimusta.

Laadullinen tutkimus toteutettiin teemahaastatteluna IoT-toimittajalle, jonka perusteella pyrittiin tarkastelemaan toimittajasopimuksen tietoturvallisuusvaatimusten täyttymistä sekä niiden päivittämisen tarvetta. Määrällinen tutkimus toteutettiin verkkokyselynä Digita Oy:ssä sisäisesti, jossa analysoitiin organisaation hankintaprosessin nykytilaa toimittajien riskien arvioinnin osalta.

Työn tuloksena havaittiin useita kehityskohteita, erityisesti organisaation sisäisen kyselyn perusteella toimittajahankinnan prosessin aktiiviseen seurantaan ja ylläpitämiseen liittyen. Tuloksissa ilmeni, että tietoturvakriittisiltä toimittajilta puuttui sopimuksesta tärkeitä tietoturvallisuusvaatimuksiin liittyviä liitteitä. Merkittävimpinä kehitystoimenpiteinä esitettiin yli kaksi vuotta vanhojen toimittajasopimusten tietoturvavaatimusten tarkastelua sekä IoT-toimittajan toimittajasopimuksen päivittämistä tietoturvavaatimuksien osalta.

Tutkimuksen lopputuloksena kehitettiin opinnäytetyöhön lisäarvoa tuottava toimittajan riskien arviointilomake, jonka avulla organisaatio voi tehokkaammin arvioida toimittajien tietoturvallisuutta ja riskejä. Lomake on kehitetty laadullisen ja määrällisen tutkimuksen tulosten pohjalta.

**Avainsanat (asiasanat)**

tietoturva, toimitusketju, riskienhallinta, esineiden internet, tietoturvan hallinta, ISMS, NIS2, ISO/IEC 27001

**Muut tiedot (salassa pidettävät liitteet)**

-

jamk

**Description**

**Virta, Maija**

**Organizational information security in supplier relationship: Risk assessment and IoT-supplier responsibilities.**

Jyväskylä: JAMK University of Applied Sciences, April 2024, 89 pages.

Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

**Abstract**

The thesis was commissioned by Digita Oy. Digita operates the television and radio network throughout Finland and is the largest independent owner of telecommunications towers in the country. The company is a key part of Finland's security of supply and also offers modern technology services, such as data center and IoT services. Digita is committed to developing its information security management system in its Broadcasting and Telecom main business areas.

The task of the thesis was to develop Digita Oy's information security management system for the IoT business, with a particular focus on information security in supplier relationships. The primary goal of the study was to create a supplier risk assessment form for use by the organization. In order to create the form, the first objective of the study was to study supplier agreements and the related information security requirements. To obtain the necessary background information, the research was carried out in a multi-method, combining both qualitative and quantitative research.

The qualitative research was conducted as a theme interview for an IoT supplier, on the basis of which the aim was to examine the fulfilment of the information security requirements of the supplier agreement and the need to update them. The quantitative research was carried out as an online survey at Digita Oy, which analysed the current state of the organization's procurement process in terms of supplier risk assessment.

As a result of the study, several areas of development were identified, especially in relation to the active monitoring and maintenance of the supplier acquisition process based on an internal survey of the organization. The results showed that security-critical suppliers lacked important attachments to the contract related to information security requirements. The most significant development measures were to review the information security requirements of supplier agreements that are more than two years old and to update the supplier agreement of the IoT supplier with regard to information security requirements.

The end result of the research was the development of a supplier risk assessment form that provides added value to the thesis, enabling the organisation to more effectively assess suppliers' information security and risks. The form has been developed based on the results of qualitative and quantitative research.

**Keywords/tags (subjects)**

information security, supply chain, risk management, internet of things, ISO/IEC 27001, NIS2

**Miscellaneous (Confidential information)**

-

**Sisältö**

**Kuviot**

**Taulukot**

# 1 Johdanto

## 1.1 Nykyaikaisen tietoturvan haasteet organisaation toimittajasuhteissa

Nykypäivänä tietoturvaa leimaa monimutkaisten, kehittyneiden ja globaalien uhkien lisääntyvät hyökkäykset, jota pahentavat nopeasti kehittyvän digitaalisen aikakauden sääntelyvaatimukset. Organisaatioiden on omaksuttava strateginen näkökulma ja tunnustettava ohjelmistojen, laitteistojen tai toimittajien ohjaamien itsenäisten ratkaisujen riittämättömyys vastata tietoturvan monitahoisiin haasteisiin. (Carder & Warkins 2020, luku 1.)

Organisaatioiden tietojärjestelmien turvallisuuteen luotetaan, vaikka karu todellisuus on, että useimmat organisaatiot toimivat haavoittuvaisessa tilassa. Tehottomasti suojatuilla organisaatioilla ei ole vain toiminnallisia vaikeuksia, vaan ne aiheuttavat myös riskejä vastuullisille yhteistyökumppaneilleen. (Carder & Warkins 2020, luku 1.) Data on arvokasta omaisuutta yrityksille kuten myös yksityishenkilöille, ja jatkuvasti lisääntyvät uhat tietojen varastamisesta, väärinkäytöstä ja tuhoamisesta, vaikuttaa suoraan kuluttajien, että yrityksien luottamukseen. Organisaatio, joka ylläpitää tietojärjestelmiensä turvallisuutta, sekä pystyy todistamaan sen tietoturvallisuuden hallintajärjestelmän kautta, erottuu alalla edukseen kilpailijoistaan.

Monilta organisaatioilta puuttuu edelleen tehokas tietoturvallisuuden hallintajärjestelmä (ISMS) tai ne toteutetaan puutteellisesti (Carder & Warkins 2020, luku 1). Digita Oy on kehittänyt tietoturvallisuuden hallintajärjestelmäänsä eri liiketoiminnoilleen jo pitkään. Uusimpien vaatimuksien päivittyessä, esimerkiksi ISO/IEC 27001- kansainvälisessä tietoturvallisuuden hallintajärjestelmän standardissa ja kyberturvallisuusdirektiivissä NIS2:ssa, on nostettu tietoturvallisuus toimittajasuhteissa tärkeään asemaan, jota myös Digita on lähtenyt tarkastelemaan.

Opinnäytetyöhön oli määritelty useita tavoitteita. Ensimmäisenä tavoitteena oli selvittää IoT-liiketoiminnan toimittajan tietoturvallisuuden taso toimittajasopimuksen tietoturvavaatimuksiin nähden: täyttyvätkö niihin liittyvät vaatimukset, ja onko vaatimuksia tarpeellista päivittää. Tietoturvavaatimuksien päivittämisen tarpeen tutkimisen lisäksi, haluttiin selvittää Digita Oy:n sisäisen hankintaprosessin nykytila toimittajien riskien arvioinnissa tietoturvan näkökulmasta, ja tunnistaa

siihen liittyvät kehityskohteet. Saatujen tulosten perusteella työn viimeinen tavoite oli luoda toimittajan riskien arviointilomake toimeksiantajalle, yhtenäistämään toimittajien tietoturvallisuuden arviointia osana tietoturvallisuuden riskienhallintaa.

Opinnäytetyön aihe valikoitui toimeksiantajan tarpeesta, sekä opiskelijan mielenkiinnosta tietoturvallisuuden hallinjärjestelmän kehittämiseen, ja erityisesti kiinnostuksesta toimittajasuhteisiin liittyvien tietoturvariskien tunnistamiseen. Aihe on ajankohtainen monelle yritykselle ja erityisesti niille, jotka kuuluvat Euroopan Unionin määrittelemän kyberturvallisuusdirektiivi NIS2 verkko- ja tietoturvadirektiivin piiriin. Direktiivin sääntöjen soveltamisen aloitusajankohta Suomessa on 18.10.2024 (What is NIS2? 2024). Toimeksiantajan organisaatio kuuluu näihin toimijoihin, joita direktiivi koskettaa.

## 1.2 Toimeksiantaja

Opinnäytetyön toimeksiantaja Digita Oy operoi koko Suomen laajuisesti maanpäällistä televisio- ja radioverkkoa. Digita on myös Suomen suurin riippumaton tietoliikennemastojen omistaja. Digita on muuttunut viestintäverkkoyhtiöstä nykyajan moderniksi teknologiataloksi, jonka palveluihin kuuluvat tietoliikennemastojen lisäksi nyt konesali- ja esineiden internet (IoT) -palvelut sekä tulevaisuuden broadcasting-palvelut. Digitan pääviestinä on ”Huomisen arvoinen digitaalinen toimintaympäristö" (ks. kuvio 1). Palveluitaan Digita Oy tarjoaa useille isoille organisaatioille kuten Suomen suurimmille matkapuhelinoperaattoreille, internet- ja mediayhtiöille, infrastruktuuriyhtiöille ja lisäksi yksityisille kiinteistöjen omistajille. (Digita yhtiönä n.d.)


Kuvio 1. Digita (Huomisen arvoinen digitaalinen toimintaympäristö 2023).

Digita Oy on myös tärkeässä roolissa osana Suomen huoltovarmuutta. Digita vastaa merkittävästä osasta Suomen kriittistä infrastruktuuria, kuten televisio- ja radio lähetyksistä sekä tietoliikenneverkoista. Näin ollen Digita on tärkeä toimija varmistettaessa maan toimintakykyä myös poikkeusoloissa. Huoltovarmuuden näkökulmasta Digita varmistaa, että tietoliikenne ja viestintäpalvelut ovat saatavilla myös häiriötilanteissa tai poikkeusoloissa, mikä on keskeistä yhteiskunnan toimivuuden kannalta. (Digita varmistaa luotettavan tiedonkulun jokaiselle suomalaiselle – myös poikkeusoloissa 2023.)

Vuonna 2012 perustettu Digita Oy on osakeyhtiö, ja omistaa yhdysvaltalainen pörssiyhtiö Digital Bridge. Digitan kotipaikka on Helsinki, ja yhtiön toimitusjohtajana toimii Vesa Tykkyläinen. Yrityksen liikevaihto vuonna 2022 oli 87 miljoonaa euroa, ja tilikauden tulos oli -6,2 miljoonaa euroa. Liikevaihto nousi 4,6 %, kun taas liikevoittoprosentti oli -7,1 %. Tilikauden päättyessä joulukuussa 2022 yhtiöllä oli yhteensä 212 työntekijää, mikä merkitsi 9,3 % kasvua verrattuna edelliseen tilikauteen. (Digita Oy n.d.)

# 2 Tutkimusasetelma

## 2.1 Tutkimuksen tarkoitus ja tavoitteet

Tutkimuksen tarkoituksena oli selvittää IoT-toimittajan nykytila-analyysin avulla, täyttyykö toimittajasopimuksen tietoturvavaatimukset kyseisellä toimittajalla, sekä onko organisaation toimittajasopimusta tietoturvavaatimuksien osalta ajankohtaista päivittää. Lisäksi haluttiin selvittää Digitan sisäisen kyselyn avulla nykyisen hankintaprosessin toimivuus ja kehityskohteet toimittajien tietoturvariskien arviointiin.

Lisäarvona opinnäytetyölle haluttiin tuottaa toimeksiantajalle toimittajan riskien arviointilomake. Lomakkeen avulla saatiin ratkaisu tutkimusongelmaan siitä, ettei organisaatiolla ollut tehokasta työvälinettä arvioida toimittajan toimittajasopimukseen sisällytettyjen tietoturvallisuusvelvoitteiden täyttymistä, eikä yhtenäistä tapaa teettää toimittajille riskien arviointia.

Toimeksiantajan organisaation toimittajasopimuksen tietoturvavaatimukset on määritelty ISO27001:2013 standardin vaatimuksien pohjalta, ja haluttiin selvittää, mitä uuden version ISO27001:2022 keskeiset muutokset ovat, ja onko niiden perusteella ajankohtaista päivittää tietoturvavaatimuksia toimittajasopimuksissa. Kehitystarpeita analysoitaessa otettiin lisäksi huomioon, miten voidaan täyttää NIS2 – kyberturvallisuusdirektiivin vaatimukset liittyen toimittajasuhteisiin.

Tutkimustyön tavoitteet:

1. Selvittää tapaustutkimuksena IoT-toimittajan avulla toimittajasopimuksen päivittämisen tarve tietoturvallisuusvelvoitteiden osalta.
2. Selvittää IoT-toimittajan nykytila-analyysin avulla toimittajasopimuksen velvoitteiden täyttyminen.
3. Selvittää organisaation nykytila-analyysin avulla nykytilanne toimittajien tietoturvariskien arviointiin sekä mahdolliset kehityskohteet.
4. Luoda edellisten tuloksien pohjalta toimittajan riskien arviointilomake, jonka avulla organisaatio pystyy tehokkaasti tekemään toimittajien riskiarvioinnin osana tietoturvallisuuden hallintajärjestelmän riskienhallintaa. Riskien arviointilomakkeen luominen tehtiin huomioiden ISO/IEC 27001:2022 ja NIS2-direktiivin vaatimukset toimittajasuhteiden osalta.

Esiolettamuksina tuloksina haluttiin saada organisaation sekä toimittajan nykytila-analyysin tulosten perusteella toimittajasopimuksen kehitysehdotus, sekä organisaation käyttöön osana hankinnan prosessia toimittajan riskien arviointilomake. Lomakkeen avulla organisaatio voi tehdä toimittajien tietoturvallisuuden riskien arvioinnin, osana tietoturvallisuuden riskienhallintaa.

## 2.2 Tutkimuskysymykset ja työn rajaus

Tutkimuskysymykset muokkautuivat toimeksiantajan ongelman pohjalta:

1. **Toimiiko IoT-toimittaja tietoturvavaatimuksien osalta toimittajasopimuksen mukaisesti?**
2. **Onko IoT-toimittajan toimittajasopimusta tietoturvavaatimusten osalta tarpeellista päivittää?**
3. **Tarvitseeko toimeksiantajan nykyprosessia toimittajien tietoturvallisuuden riskien arvioinnin tekemiseen kehittää?**

Laadullinen tutkimus rajattiin yhteen IoT-toimittajaan toimittajasopimuksen katselmusten osalta, koska kaikkia toimittajia katseltaessa työ olisi paisunut liikaa. Yhden IoT-liiketoiminnan strategisen toimittajan haastattelun koettiin tarjoavan tärkeää tietoa toimittajan tietoturvallisuuden nykytilasta, mitä toimittajilta on realistista odottaa, jos toimittajasopimuksen tietoturvavaatimuksia toimittajia kohtaan tiukennetaan.

Määrällisen tutkimuksen kysely, eli Digitan nykytila-analyysin datan saamiseksi kysely rajattiin viimeisen vuoden aikana tehtyihin toimittajasopimuksiin. Rajaus tehtiin siksi, että haluttiin saada relevanttia ja ajantasaisinta tietoa siitä, miten toimittajahankinnan prosessia noudatetaan toimittajien tietoturvallisuuden vaatimuksien osalta. Organisaatiossa oli tehty vuoden 2023 aikana päivityksiä Code of Conduct eli organisaation omiin hyvän liiketavan periaatteisiin, sekä toimittajan tietoturvallisuusvaatimuksiin, joten viimeisin hankinnan prosessi on ollut nyt käytössä noin vuoden ajan.

Toimittajan riskien arviointilomakkeen luomisessa rajaus tehtiin pohjan rakentamiseen. Kysymykset päätettiin määritellä käyttämällä apuna IoT-toimittajan teemahaastattelun ja organisaation sisäisen kyselyn tuloksia, joiden avulla saataisiin yleisesti toimiva kysymysrunko, jota myöhemmin eri liiketoiminnan osa-alueet voisivat lähteä itse kehittämään tarvitsemaansa suuntaan.

## 2.3 Tutkimusote

### 2.3.1 Monimenetelmäinen tutkimus

Opinnäytetyön tutkimusmenetelmäksi valittiin monimenetelmällinen tutkimusote, koska haluttiin saada tutkittavasta ilmiöstä tietoa kahdesta eri näkökulmasta, sen ymmärtämiseksi kokonaisvaltaisesti. Tutkimuksessa voidaan käyttää useita tutkimusmenetelmiä, jolloin voidaan tarkastella tutkittavaa ilmiötä eri näkökulmista. Tätä kutsutaan monimenetelmälliseksi tutkimukseksi (Kananen 2015, 323). Opinnäytetyössä käytettiin laadullista-, sekä määrällistä tutkimusta, sekä kahta erilaista aineistonkeruumenetelmää: teemahaastattelua ja kyselyä.

Kanasen (2015) mukaan, laadullinen tutkimus on useimmiten monimenetelmällisessä tutkimuksessa ymmärrystä tuottava, joten se teetetään esitutkimuksena. Esimerkiksi teemahaastattelun

avulla voidaan saada paljon esitietoa ilmiöstä ja sen välisistä suhteista ja riippuvuuksista. (Kananen 2015, 325.)

Laadullinen tutkimus toteutettiin ensin IoT-toimittajalle, mikä auttoi hahmottamaan toimittajasopimuksen tietoturvavaatimusten nykytilanteen ja antoi pohjan määrälliselle tutkimukselle ja siihen määriteltäville kysymyksille.

Monimenetelmällinen tutkimus mahdollisti laajan näkökulman saamisen tutkittavaan ilmiöön ja auttoi kattavan ymmärryksen muodostamisessa. Käytettyjen tutkimusmenetelmien yhdistelmä tarjosi monipuolista tietoa, jota voitiin hyödyntää yrityksen IoT-liiketoiminnan toimittajasuhteiden riskienhallinnan kehittämisessä.

### 2.3.2 Kvalitatiivinen

Tuomi ja Sarajärvi (2018) kuvaavat kvalitatiivista eli laadullista tutkimusta tutkimusmenetelmänä, joka keskittyy ilmiöiden syvälliseen ymmärtämiseen ja tulkintaan. Laadullisessa tutkimuksessa keskitytään ihmisten kokemusten ja merkitysten ymmärtämiseen. Tämä tulkinnallinen näkökulma tuo esille yksilöiden subjektiiviset kokemukset ja antaa tilaa moninaisille tulkintatavoille. (Tuomi & Sarajärvi 2018, 10-15.)

Laadullinen tutkimus korostaa avointa ja joustavaa lähestymistapaa eikä tutkimusprosessi ei ole tiukasti etukäteen määritelty, vaan tutkijalla on mahdollisuus sopeutua tutkimuksen edetessä ja ottaa huomioon uudet näkökulmat ja löydökset. Tämä dynaaminen lähestymistapa mahdollistaa tutkimuksen rikastuttamisen ja kehittymisen tutkimusprosessin aikana. (Tuomi & Sarajärvi 2018, 10-15.)

Tuomi ja Sarajärvi (2018) korostavat, että laadullisessa tutkimuksessa käytetään monipuolisesti erilaisia aineistotyyppejä, kuten haastatteluja, havaintoja ja dokumentteja. Tavoitteena on saada kattava ja monipuolinen kuva tutkittavasta ilmiöstä eri näkökulmista. Laadullisen aineiston monimuotoisuus antaa tutkimukselle syvyyttä ja rikkautta. (Tuomi & Sarajärvi 2018, 62.)

Laadullista tutkimusta tarkastellaan prosessina, joka etenee vaiheittain. Tutkijan rooli on Tuomen ja Sarajärven (2018) mukaan olla tietoinen omista ennakko-oletuksistaan ja olla avoin uusille näkökulmille ja oivalluksille tutkimuksen edetessä. Tutkimusprosessin dynaamisuus ja vuorovaikutteisuus korostuvat, kun tutkijat pyrkivät ymmärtämään ilmiöitä niiden omista konteksteista käsin. (Tuomi & Sarajärvi 2018, 69.)

Kuten Tuomi ja Sarajärvi (2018) totesivat, laadullisessa tutkimuksessa tiedonhankintamenetelmänä käytetään asiantuntijahaastatteluiden lisäksi osallistuvaa havainnointia sekä dokumenttien analysointia, ja siksi laadullinen tutkimus tähän opinnäytetyön tarpeeseen yhdeksi tutkimusmenetelmäksi. Laadullinen tutkimus toteutettiin puolistrukturoituna teemahaastatteluna IoT-toimittajan edustajalle.

### 2.3.3 Kvantitatiivinen

Kanasen (2015) mukaan, kvantitatiivisen eli määrällisen tutkimuksen toteuttamiseksi on olennaista hallita tutkittava ilmiö perusteellisesti. Tämä edellyttää vankkaa taustatietoa ja selittäviä teorioita ilmiöstä, jotka toimivat pohjana tutkimusongelman määrittelylle ja tutkimuskysymysten laadinnalle. (Kananen 2015, 73.)

Tutkimuskysymysten ratkaisemiseksi tarvitaan apukysymyksiä, jotka ilmenevät yksityiskohtaisina kysymyksinä kyselylomakkeessa. Apukysymykset voivat olla joko faktapohjaisia tai mielipidekysymyksiä, riippuen tutkimuksesta. Kananen (2015) jatkaa, että kvantitatiivisessa tutkimuksessa yleisin tapa kerätä aineistoa on kyselyiden avulla. (Kananen 2015, 73.)

Kvantitatiivinen tutkimus toteutettiin strukturoituna verkkokyselynä, ja sen tarkoituksena oli saada kokonaiskuva organisaation toimittajasopimuksien tietoturvallisuusvaatimuksien riskien arvioinnin nykytilasta. Kysely teetettiin Microsoft Forms sovelluksen avulla sisäisesti toimeksiantajan organisaatiossa, jossa otantana olivat asiantuntijat ja liiketoimintajohtajat, jotka neuvottelevat uudet hankintasopimukset. Kyseinen ryhmä valikoitui otannaksi, koska heillä on vankka taustatieto sekä tarvittava tietämys tutkittavasta ilmiöstä.

## 2.4 Aineistonkeruu ja analyysimenetelmät

Laadullisessa tutkimuksessa aineistonkeruumenetelminä ovat havainnointi, haastattelut ja dokumentit (Kananen 2015, 89). IoT-toimittajan haastattelu toteutettiin teemahaastatteluna, jonka kysymysrunko rakentui toimittajasopimuksen tietoturvallisuusvaatimuksista, sekä ISO27001:2022 standardin vaatimuksista. Teemahaastattelu sopi hyvin aineistonkeruumenetelmäksi, koska sen avulla haluttiin selvittää toimittajan nykyiset toimintamallit ja käytänteet. Teemahaastattelu järjestettiin toimittajan tietoturvallisuusasiantuntijan kanssa yksilöhaastatteluna.

Teemahaastattelun aineiston tallentaminen digitaaliseen muotoon, joka myöhemmin puretaan tekstiksi, kutsutaan litteroinniksi (Kananen 2015, 129). Teemahaastattelu tallennettiin osallistujien luvalla ja se pidettiin Teams sovelluksessa videokokouksena, koska haastateltavan toimipiste on ulkomailla. Teemahaastattelu litteroitiin jälkikäteen tekstimuotoon sekä käännettiin haastattelukielestä englannista, suomen kielelle.

Tuomi ja Sarajärvi (2018) käsittelevät laadullisen tutkimuksen aineiston analyysia erilaisilla menetelmillä, ja yksi niistä on sisällönanalyysi. Sisällönanalyysi on laadullisen tutkimuksen menetelmä, jonka avulla tutkija pyrkii löytämään ja ymmärtämään aineiston sisältämät merkitykset, teemat ja rakenteet. Se voidaan jakaa induktiiviseen ja deduktiiviseen sisällönanalyysiin, ja molemmilla on omat lähestymistapansa aineiston käsittelyyn. (Tuomi & Sarajärvi 2018, 80–83.) Toimittajan edustajan teemahaastattelun pohjalta tehdyn aineiston analyysiin käytettiin perusanalyysimenetelmää, eli sisällönanalyysiä.

Aineistonkeruu kvantitatiivisessa tutkimuksessa aloitettiin toimeksiantajan organisaation sisäisellä kyselyllä. Kysely toteutettiin käyttäen Microsoft Forms sovellusta, strukturoituna verkkokyselynä. Verkkokysely sopi aineistonkeruumenetelmänä parhaiten, koska tutkimus kohdistettiin henkilöille, joilla on vahva käsitys aiheesta. Lisäksi tavoitteena oli saada tietoa, miten hankintaprosessissa arvioidaan toimittajan riskien arviointia tietoturvallisuuden näkökulmasta.

Tutkimuksessa käytettiin harkinnanvaraista otantaa, joten kysely teetettiin vain niille, jotka asemassaan tekevät tai vastaavat toimittajahankinnoista. Kyselyyn osallistuneille kerrottiin etukäteen, miksi kysely toteutetaan ja mitä sen avulla tutkitaan, joten he pystyivät valmistautumaan kyselyyn.

Kvantitatiivisen tutkimuksen kyselyn vastaukset analysoitiin käyttäen tilastollisista menetelmistä suoraa jakaumaa.

Hyödyntäen suoraa jakaumaa, tutkimuksen kysymykset esitetään suhteellisina lukuarvoina, eli prosentteina vastausten jakautumisesta. Tämä tarkoittaa, että vastausten esittämisessä käytetään prosenttilukuja, jotka antavat selkeän käsityksen vastausten suhteellisesta esiintymisestä. Havaintoyksiköiden kokonaismäärästä (N) lasketaan vastausten prosentuaalinen osuus, jotta saadaan käsitys vastausten suhteellisesta merkityksestä koko aineistossa. (Kananen 2015, 290.)

Kyselyn strukturoiduista kysymyksistä kerätyt vastaukset esitettiin suorina jakaumina. Näistä jakaumista muodostettiin ympyrä- ja pylväskuvaajia, jotka auttoivat tulosten hahmottamisessa selkeämmin. Tämä visuaalinen esitystapa teki tulosten analysoinnista ja vertailusta helpompaa.

## 2.5 Tiedonhaku ja lähdeaineisto

Teoreettisen viitekehyksen kerääminen on toteutettu systemaattisella tiedonhankinnalla. Tiedonhankinnan kokonaisprosessi on esitetty kuviossa 2. Prosessin vaiheet olivat aihevalinnan jälkeen tiedontarpeen määrittely; mitä haetaan, millä tavalla ja millä termeillä (Tiedonhankinnan opas: Tiedonhaun suunnittelu 2023).


Kuvio 2. Tiedonhakuprosessi (Tiedonhankinnan opas: Tiedonhaun suunnittelu 2023, muokattu)

Tiedonhaun suunnittelun jälkeen eteneminen jatkui tiedonhaun aloittamiseen, aikaisemmin tehdyn suunnitelman perusteella, josta taas edelleen hakutulosten arviointiin. Arvioinnissa prosessiin kuului arvioida, kuinka hyvin aiheeseen osuvia hakuja löytyi sekä niiden määrä. Lopuksi tarkastelu,

mistä lähde löytyy, ja edelleen lähteen arviointi tutkimusetiikan mukaisesti sekä lähdekriittisesti. (Tiedonhankinnan opas: Tiedonhaun suunnittelu 2023.)

Tiedonhaussa aineiston etsimiseen ja keräämiseen käytettiin Google Scholaria, Jyväskylän Ammattikorkeakoulun kirjastoa, IEEE Xplore digitaalista kirjastoa, sekä Janet Finna tiedonhakukantaa. Lähdeaineiston hakusanoihin on käytetty monia erilaisia yhdistelmiä hakusanoista, riippuen mistä tietoa haettiin, kuten esimerkiksi ”ISMS OR Information Security Management System", "ISO” AND ”ISMS", "RISK MANAGEMENT AND ISMS", ”TIETOTURVA OR INFORMATION SECURITY”, ”INFORMATION SECURITY AND SUPPLIER, ISMS AND SUPPLIER, INFORMATION SECURITY AND AUDIT.

Tiedon hakeminen aloitettiin hyvissä ajoin keräämällä monipuolisesti suomalaista, sekä kansainvälistä kirjallisuutta, tutkimusartikkeleita, verkkojulkaisuja sekä blogeja. Teoriaa löytyi monipuolisesti kansainvälisistä sekä suomalaisista lähteistä, kuitenkin kansainvälisiä lähteitä on opinnäytetyössä merkittävin osuus niiden ajantasaisuuden takia. Teorian kerääminen laajalla haulla eri lähteistä, tarjosi kattavan käsityksen tutkittavasta aiheesta sekä kokonaiskuvan direktiivien ja standardien sitoutumisesta yhteen, monien yhdistävien vaatimuksien osalta.

Valitut lähteet pyrittiin pitämään mahdollisimman laadukkaina, ja erityisesti standardeista ja direktiiveistä on kerätty monipuolisesti erilaisia lähteitä, mutta samalla otettiin kriittisesti huomioon, miten niitä voidaan tulkita kaupallisessa näkökulmassa eri tavoin. Täten luottaviksi lähteiksi valikoitui mm. Suomen Standardisoimisliitto SFS ry, joka on taloudellista voittoa tavoittelematon järjestö, sekä henkilöiden kirjallisuutta, jotka ovat alan asiantuntijoita, sekä ovat olleet mukana kehittämässä kansainvälisiä standardeja.

Blogikirjoituksia sekä kaupallisten tahojen materiaaleja on käytetty lähteinä käsitteiden selittämiseen. Niistä hankittua tietoa on verrattu useisiin verkkoartikkeleihin sekä tutkimusartikkeleihin, jotta on pystytty varmistamaan teorian paikkansapitävyys.

Koska IT-alan kehitys on nopeaa, erityisesti standardien ja direktiivien osalta on käytetty vain tuoreita lähteitä, sekä käytetty kriittistä ajattelua lähteiden paikkansa pitävyyteen ja ajankohtaisuuteen.

# 3 Organisaation tietoturvallisuus toimittajayhteistyössä

## 3.1 Laadunhallintajärjestelmä

Laadunhallintajärjestelmä ohjaa ja valvoo organisaation toimintoja tavoitteenaan parantaa toimintaa ja tuoda johdonmukaisuutta prosesseihin. Se tarjoaa kehyksen laatuun liittyvien asioiden hallintaan ja resurssien tehokkaaseen hyödyntämiseen. Sen avulla siis vähennetään virheitä ja resurssien hukkaa, mikä automaattisesti tehostaa organisaation toimintaa. Järjestelmä keskittyy ohjaamaan toimintaa laadun näkökulmasta varmistaen, että tuotteet tai palvelut vastaavat asiakkaiden tarpeita ja odotuksia (Robitaille 2015, 4–5.)

Laadunhallintajärjestelmä koostuu organisaation suunnitelluista ja järjestelmällisistä toimenpiteistä laadunhallinnan varmistamiseksi ja parantamiseksi. Keskeisimmät osat järjestelmässä sisältävät suunnitelman, organisaatiorakenteen, prosessit, dokumentoinnin, valvonnan ja seurannan sekä jatkuvan parantamisen periaatteen. Se voi perustua kansainvälisiin ISO 9000 -sarjan standardeihin ja soveltua kaikenkokoisille ja -tyyppisille yrityksille eri toimialoilla. (Laadunhallintajärjestelmä 2024.)

Järjestelmän tavoitteena on varmistaa organisaation toiminnan systemaattinen ohjaus ja valvonta, asiakastyytyväisyys sekä tuotteiden korkea ja tasainen laatu. Laadunhallintajärjestelmä on johtamisjärjestelmä, jonka avulla organisaatio voi tehdä toiminnan ohjauksesta ja valvonnasta systemaattista, toteuttaa asiakkaiden vaatimukset ja odotukset, varmistaa asiakastyytyväisyyden ja tuotteiden korkean laadun, luoda yhtenäisiä käytäntöjä ja innovatiivisia ratkaisuja, kehittää henkilöstön osaamista, motivaatiota ja tehokkuutta, hallita laatukustannuksia, parantaa työn tuottavuutta ja kasvattaa kilpailukykyä. (Laadunhallintajärjestelmä 2024.)

Laadunhallintajärjestelmissä hyödynnetään usein ISO 9000 -sarjan standardeja, erityisesti ISO 9001 -standardia. Tämän standardin avulla organisaatio voi hankkia sertifikaatin, joka osoittaa sen toiminnan täyttävän sidosryhmien vaatimukset, tarpeet ja odotukset. (Laadunhallintajärjestelmä 2024.) ISO 9000 -sarjan kansainvälisiä standardeja käytetään maailmanlaajuisesti organisaatioiden laadunhallintajärjestelmissä ja sarjan standardeja on ollut jo vuodesta 1986 lähtien, eli yli 37 vuoden ajan. ISO 9000 -sarjan standardit on laatinut International Organization for Standardization (ISO). (ISO 9000 Laadunhallinnan standardisarja n.d.)

Seitsemää laadunhallinnan periaatetta voidaan soveltaa organisaatiossa parantamaan sen suorituskykyä. Nämä periaatteet muodostavat perustan ISO 9000 -standardisarjalle, joka kattaa laadunhallintajärjestelmät (Laadunhallinnan periaatteet n.d.). Nämä seitsemän periaatetta ovat:

- **Asiakaskeskeisyys:** Tärkeimpänä tavoitteena on täyttää asiakkaiden vaatimukset ja ylittää heidän odotuksensa, mikä luo perustan jatkuvan menestyksen saavuttamiselle. Asiakastyytyväisyys ja -uskollisuus parantavat organisaation mainetta ja markkinaosuutta. (Laadunhallinnan periaatteet n.d.; Pulkkanen 2019, 3)

- **Johtajuus:** Organisaation ylimmän johdon rooli on määritellä yhteinen tarkoitus ja suunta sekä luoda edellytykset täyteen osallistumiseen laadunhallintatavoitteiden saavuttamiseksi (Pulkkanen 2019, 3).

- **Ihmisten täysipainoinen osallistuminen**: Kaikilla organisaation tasoilla olevien ihmisten osallistuminen ja pätevyys edistävät parempaa luovuutta, aloitteellisuutta ja organisaation laatutavoitteiden ymmärtämistä ja saavuttamista (Pulkkanen 2019, 3).

- **Prosessimainen toimintamalli**: Johdonmukaiset ja ennustettavissa olevat tulokset saavutetaan hallitsemalla toimintoja prosesseina, jotka toimivat yhtenäisenä järjestelmänä. (Pulkkanen 2019, 5).

- **Parantaminen:** Jatkuva parantaminen on keskeinen osa organisaation menestystä, ja se auttaa ylläpitämään suorituskykyä, reagoimaan muutoksiin ja luomaan uusia mahdollisuuksia (Pulkkanen 2019, 5).

- **Näyttöön perustuva päätöksenteko**: Päätöksentekoprosessit perustuvat tietoon ja analyysiin, mikä johtaa parempiin päätöksiin ja suorituskyvyn arviointiin (Pulkkanen 2019, 6.)

- **Suhteiden hallinta**: Organisaation on hallittava suhteitaan olennaisiin sidosryhmiin, kuten asiakkaisiin, toimittajiin ja yhteistyökumppaneihin, jotta se voi saavuttaa jatkuvaa menestystä (Pulkkanen 2019, 6).

Sarjan standardeista yleisimmin käytetty on ISO 9001-standardi. ISO 9001 on kansainvälinen standardi, joka määrittelee vaatimukset organisaation ja prosessien hallintajärjestelmän perustamiselle ja se on toiminut prosessimallin perustana kaikille uudemmille erityisesti ISO-pohjaisille standardeille jo vuodesta 1987 lähtien. (Robitaille 2015, 2.)

Standardi tarjoaa loogisen menetelmän liiketoiminnan johtamiseen ja tuo johdonmukaisuutta ja hallintaa päivittäisiin käytäntöihin. Sen perusfilosofiana on "Tee mitä sanot ja sano mitä teet", ja se tarjoaa viitekehyksen riskien tunnistamiseen ja käsittelyyn. (Robitaille 2015, 2.) ISO 9001:2015-standardissa käytetään PDCA-sykliä, joka on prosessilähtöinen ja sillä kannustetaan riskeihin perustuvaan ajatteluun (Robitaille 2015, 32). PDCA-sykli esitetty tarkemmin kuviossa 4.

Digitalisaation aikakaudella tietoturva on noussut elintärkeäksi osaksi yritysten liiketoimintaa, erityisesti arkaluonteisen tiedon suojaamisen näkökulmasta. Yritykset pyrkivät varmistamaan asiakastietojen luottamuksellisuuden ja säilyttämään tietoturvansa keskeisenä haasteena. Krugerkin (2022) mainitsee blogissaan, että yritykset, joilla on jo käytössään ISO 9001 -standardin mukainen laadunhallintajärjestelmä, ovat luoneet hyvän perustan tehokkaan tietoturvan vähittäiselle käyttöönotolle. (Krueger 2022.)

## 3.2 Tietoturvallisuus

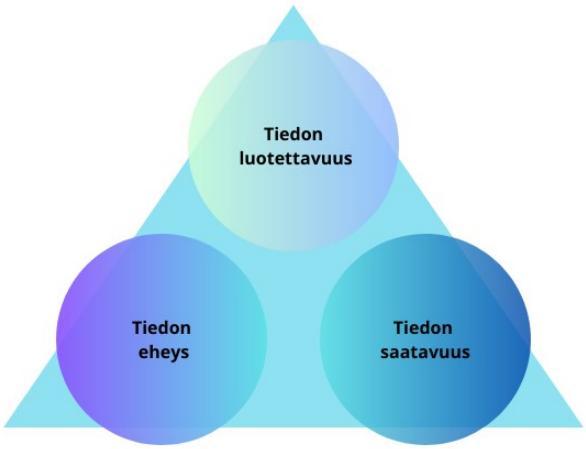
Tietoturvan olemuksen ymmärtämiseksi, Watkins (2022) tekee helposti ymmärrettävän vertauksen kolmella eri näkökulmalla yleisesti tunnustettuun arvoon; rahaan.

Kukaan meistä ei halua kenenkään luvattoman henkilön kuluttavan rahojamme, joten rajoitetun pääsyn varmistaminen tai luottamuksellisuuden säilyttäminen on ratkaisevan tärkeää tietojen käsittelyssä Watkins (2022) toteaa. Pelkästään pääsyn rajoittaminen ei kuitenkaan riitä, kuten vaikka rahan säilyttäminen lukittuna sisätiloissa. (Watkins 2022, luku 1.)

Watkins (2022) jatkaa ja korostaa, että arvostus rahojen saatavuuteen ja joustavuuteen, että rahat ovat käytettävissä silloin kun niitä tarvitsee, edellyttää luottamuksellisuuden ja saatavuuden tasapainottamista. Halutaan tietojen olevan turvassa, mutta myös että ne ovat saatavilla käyttökelpoisessa muodossa silloin, kun niille on tarve. (Watkins 2022, luku 1.)

Viimeisenä Watkins (2022) lisää, että rahoitustoimissa tarkkuus on tärkeää. Samoin tietojen on oltava täydellisiä ja tarkkoja eri yhteyksissä, kuten esimerkiksi pörssitiedot sijoittajille tai lääketieteelliset terveystiedot potilaalle. Tätä täydellisyyttä ja tarkkuutta kuvataan tietoturvallisuuden eheydeksi. (Watkins 2022, luku 1.)

Tietoturvan hallinnassa painopiste ulottuu siis luottamuksellisuuden lisäksi saatavuuteen sekä eheyteen. Luottamuksellisuudella varmistetaan, ettei tietoihin pääse käsiksi kukaan luvattomasti. Saatavuudella taas varmistetaan tietojen saatavuus tarvittaessa ja eheydellä taataan tietojen tarkkuus ja täydellisyys. (Watkins 2022, luku 1.) Tätä kolmiosaista mallia kutsutaan CIA-kolmioksi (ks. kuvio 3).




Kuvio 3. CIA-kolmio (Watkins 2022, luku 1, muokattu)

Tietoturvan ymmärtäminen tietojen luottamuksellisuuden, eheyden ja saatavuuden (CIA) säilyttämisenä selventää sen merkitystä yksilöille, yrityksille ja organisaatioille. Yksilöt haluavat varmuutta siitä, että heidän tietojaan hallitaan asianmukaisesti varkauden tai petoksen kaltaisten ongelmien estämiseksi. Organisaatiot sidosryhmien ja asiakkaiden odotusten, kilpailukyvyn ja viranomaisvaatimusten pohjalta asettavat tietoturvan etusijalle suojellakseen hallussaan olevia tietoja ja ylläpitääkseen vahvaa turvallisuusasennetta. (Watkins 2022, luku 1.)

Organisaatiot suojaavat näitä näkökohtia tietoturvan hallintajärjestelmillä (ISMS), jotka kattavat ohjeet, menettelyt, käytännöt, ja niihin liittyvät toimet (Watkins 2022, luku 1).

## 3.3 Tietoturvallisuuden hallintajärjestelmä (ISMS)

Tiedonhallintakäytäntöjä edellytetään useilla sektoreilla, erityisesti johtuen keskinäisriippuvuudesta toimittajista sekä immateriaalioikeuksien ja organisaation maineen turvaamisen tarpeesta. Tehokkaan tietoturvan avulla saavutettu kilpailuetu ulottuu muuhunkin kuin kustannusten tai liikesalaisuuksien paljastamisen estämiseen. (Watkins 2022, luku 1.)

Nykypäivän digitaaliriippuvuuden ympäristössä organisaatiotietojen turvaaminen on ensiarvoisen tärkeää. Tietoturvan hallintajärjestelmä on strateginen välttämättömyys kriittisten tietojen saatavuuteen, eheyteen ja luottamuksellisuuteen kohdistuvien lisääntyvien uhkien torjumiseksi. (Carder & Watkins 2020, luku 1.)

Pohjimmiltaan tietoturvallisuuden hallintajärjestelmä menee perinteisiä lähestymistapoja pidemmälle tarjoamalla järjestelmällisen ja strategisen viitekehyksen organisaatioille. Hallintajärjestelmä käsittelee tietoturvan monitahoisia haasteita tarjoamalla työkaluja ja strategioita nykyaikaisen liiketoiminnan perustan, eli tiedon suojaamisen vahvistamiseen. Kun organisaatiot aloittavat matkansa turvatakseen digitaalisen omaisuutensa, ISMS toimii suunnan näyttäjänä, joka ohjaa kohti kestävää ja turvallista tietoinfrastruktuuria. (Carder & Watkins 2020, luku 1.)

ISMS:n käyttöönotto on ennen kaikkea Chopran ja Chaudharyn (2020) mukaan organisaatiolle strateginen päätös, ja se kattaa ihmiset, prosessit ja IT-järjestelmät. Se auttaa kaikenkokoisia yrityksiä kaikilla erilaisilla toimialoilla turvaamaan omaisuutensa. (Chopra & Chaudhary 2020, luku 1.)

Chopra ja Chadhary (2020) toteavat, että organisaatiot eivät voi enää sulkea silmiään tietoturvan oikeudellisilta vaatimuksilta. Sääntely-ympäristö kehittyy, ja yhä useammat lait muokkaavat organisaatioiden velvollisuuksia liittyen tietoturvallisuuteen. Vuoden 2018 EU:n yleinen tietosuoja-asetus (GDPR) on viimeaikaisen lainsäädännön kulmakivi. Se velvoittaa sekä julkiset että yksityiset organisaatiot toteuttamaan tietoturvatoimenpiteitä, jotka suojaavat henkilötietojen luvattomalta käsittelyltä, katoamiselta tai vahingoittumiselta. Tietosuojalain rikkomisesta voi aiheutua mittaviakin sakkoja, jotka voivat olla enintään neljä prosenttia organisaation maailmanlaajuisesta liikevaihdosta. (Chopra & Chaudhary 2020, luku 1.)

Toimialojen johtajien on esitettävä ennakoivasti toimenpiteet tietovarojen luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi. Riskeihin perustuva tietoturvapolitiikka, joka toteutetaan tietoturvan hallintajärjestelmän kautta, on vakuuttava todiste organisaation sitoutumisesta lakisääteisten velvoitteiden täyttämiseen ja tietovarojensa turvaamiseen. (Chopra & Chaudhary 2020, luku 1.)

## 3.4 ISO/IEC 27001 & ISO/IEC 27002 -standardit

ISO/IEC 27000 muodostaa laajan tietoturvan hallintaan omistettujen kansainvälisten standardien sarjan. Kansainvälisen standardointijärjestö (ISO) ja kansainvälisen sähköteknisen komission (IEC) yhteistyössä kehittämät standardit luovat maailmanlaajuisesti tunnustetun perustan tehokkaalle tietoturvan hallinnalle. (Carder & Watkins 2020, luku 3.)

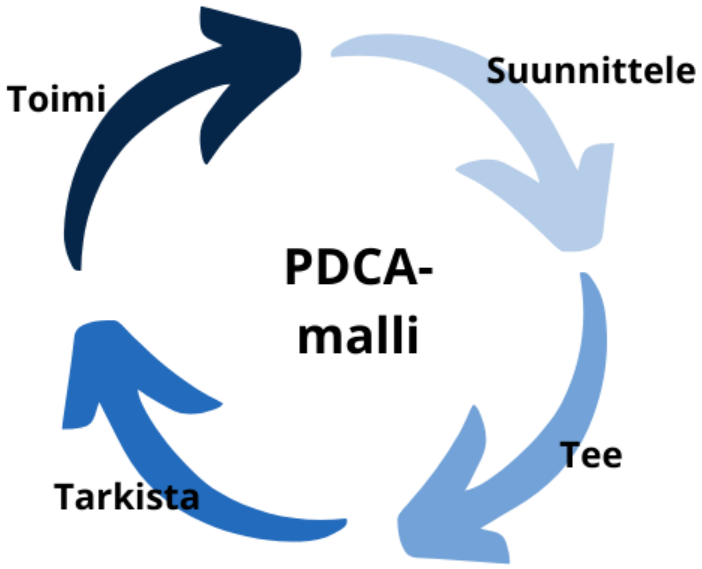
ISO/IEC 27001 määrittää vaatimukset ISMS:n luomiselle, toteuttamiselle, ylläpidolle ja jatkuvalle parantamiselle organisaatiossa. Kun taas ISO/IEC 27002 tietoturvallisuuden hallintakäytännesäännöt, tarjoten ohjeita ja yleisiä periaatteita tietoturvallisuuden hallintajärjestelmän käynnistämiseen, toteuttamiseen, ylläpitoon ja parantamiseen. (Carder & Watkins 2020, luku 3.)

### 3.4.1 ISO/IEC 27001

ISO/IEC 27001 on kansainvälinen tietoturvallisuuden hallintajärjestelmien standardi, joka toimii kattavana viitekehyksenä käsitellen eri puolia ISMS:n perustamisesta jatkuvaan tarkistamiseen ja mukauttamiseen (Watkins 2022, luku 3).

Vaikka standardi noudattaa lineaarista rakennetta, Watkins (2022) muistuttaa, ettei tietyn järjestyksen noudattaminen ole pakollista, mikä mahdollistaa joustavuuden ISMS:n toteutuksessa. Yksi laajalti tunnustettu lähestymistapa on Plan-Do-Check-Act (PDCA) -sykli, joka korostaa jatkuvaa parantamista. (Watkins 2022, luku 3.) Aikaisemmin mainitussa ISO 9001:2015-standardissa käytetään PDCA-sykliä, ja se on toiminut myös perustana tälle ISO-pohjaisille standardille. (Robitaille 2015, 2).

PDCA-lähestymistapa (ks. kuvio 4) helpottaa jatkuvien parannussyklien aloittamista, jolloin seuraavat PDCA-syklit etenevät rinnakkain eri aikajanalla (Watkins 2022, luku 3).




Kuvio 4. PDCA-sykli (Watkins 2022, luku 3, muokattu)

- **Suunnittele (Plan)**: Tavoitteiden määrittely, mukaan lukien saavutettavat asiat ja ISMS-vaatimusten määrittäminen.
- **Tee (Do)**: Suunniteltujen toimien toteuttaminen.
- **Tarkista (Check)**: Varmistetaan, ovatko toteutetut toimet tavoitteiden mukaisia, ja havaitaan mahdolliset puutteet tai puutteet.
- **Toimi (Act):** Puutteiden korjaaminen, tehokkuuden parantaminen ja suunnitelmien laatiminen lisäjalostusta varten. (Watkins 2022, luku 3.)

Tietoturvallisuuden hallintajärjestelmän toteutuksessa resurssi-intensiivisiä vaiheita ovat suunnitteluvaihe sekä toteutus. Suunnitteluvaihe ulottuu kuitenkin projektin suunnittelua pidemmälle, sisältäen ISMS-vaatimusten ja toteutustapojen määrittelyn. Siksi vaihe voi kuluttaa merkittävän osan projektin aikajanasta. (Watkins 2022, luku 3.)

Watkins (2022) painottaa, että yhteisiin hallintajärjestelmävaatimuksiin kuuluvat dokumentoitu tieto, sisäinen tarkastus ja johdon katselmus. Dokumentoidulla tiedolla tarkoitetaan ajantasaisten hyväksyttyjen asiakirjojen saatavuuden varmistaminen ISMS:ssä. Tämä sisältää yritystason käytän-

nöt, toimintatavat, työohjeet ja asiakirjat. Asiakirjojen hallinnan tavoitteena on varmistaa asianmukaisten viranomaisten hyväksyntä ja uusimpien versioiden saatavuus valtuutetulle henkilökunnalle. (Watkins 2022, luku 3.)

Sisäistä tarkastusta käytetään valvomaan johtamisjärjestelmän vaatimusten ja todellisten käytäntöjen noudattamista. Organisaation teettämät sisäiset auditoinnit auttavat arvioimaan ISMS:n noudattamista, tehokkuutta ja tunnistamaan parannuskohteita. (Watkins 2022, luku 3.)

Johdon katselmukset ovat kuuden tai kahdentoista kuukauden välein suoritettavat katsaukset, jotka arvioivat ISMS:n käyttöönoton edistymistä ja tehokkuutta. Raportit kattavat auditoinnin tulokset, tietoturvahäiriöt, muutokset ulkoisissa tai sisäisissä tekijöissä, jotka vaikuttavat ISMS:ään, tietoisuusindikaattoreita sekä tehokkuutta ja jatkuvaa parantamista koskevia toimenpiteitä. (Watkins 2022, luku 3.)

### 3.4.2 ISO/IEC 27001 5.19 Tietoturvallisuus toimittajasuhteissa

ISO/IEC 27001:2022 - standardin tietoturvallisuuden hallintakeinot käsittelevät toimittajan tuotteiden tai palveluiden käyttöön liittyviä tietoturvariskejä. Tämän hallintakeinon päätarkoituksena on ylläpitää sovittua tietoturvallisuuden tasoa toimittajasuhteissa. Standardissa esitetään ohjeistus, jonka mukaan organisaation tulisi laatia kohdennetut toimintaperiaatteet toimittajasuhteisiin ja viestittää ne kaikille olennaisille sidosryhmille. (SFS-EN ISO/IEC 27002:2022, 43–44.)

Organisaation on tarkoitus yksilöidä ja toteuttaa prosessit ja menettelyt, joilla käsitellään toimittajan tuotteiden ja palveluiden käyttöön liittyviä tietoturvariskejä. Tämä koskee myös organisaation käyttämiä pilvipalvelun tuottajien resursseja. Näiden prosessien ja menettelyjen tulisi sisältää ne toimet, joita organisaation on tarkoitus toteuttaa, sekä ne toimet, joita organisaatio edellyttää toimittajalta toimittajan tuotteiden tai palveluiden käyttöön otettaessa tai poistettaessa käytöstä. (SFS-EN ISO/IEC 27002:2022, 43–44.)

Lisäksi hallintakeino edellyttää tarkastelua menettelyistä tietojenkäsittelyn jatkamiseen siinä tapauksessa, että toimittaja ei kykene enää toimittamaan tuotteitaan tai palveluitaan, jotta voidaan

välttää viiveet korvaavien tuotteiden tai palveluiden hankinnassa. Tähän voi kuulua vaihtoehtoisten toimittajien tunnistaminen etukäteen tai korvaavien toimittajien säännöllinen käyttö. (SFS-EN ISO/IEC 27002:2022, 43–44.)

### 3.4.3 ISO/IEC 27001 5.20 Toimittajasopimusten tietoturvallisuus

Tämä hallintakeino käsittelee toimittajasopimusten tietoturvallisuutta. Hallintakeinon tarkoituksena on ylläpitää sovittua tietoturvallisuuden tasoa organisaation ja toimittajien välisissä suhteissa. (SFS-EN ISO/IEC 27002:2022, 45.)

Kunkin toimittajan kanssa tulisi laatia ja sopia asianmukaiset tietoturvavaatimukset, jotka perustuvat kyseisen toimittajasuhteen tyyppiin. Tämän tarkoituksena on varmistaa sovittu tietoturvallisuuden taso toimittajasuhteissa. Toimittajasopimukset olisi laadittava ja dokumentoitava selkeän ymmärryksen takaamiseksi osapuolten velvoitteista tietoturvavaatimusten täyttämisessä. (SFS-EN ISO/IEC 27002:2022, 45–46.)

Organisaation tulee luoda ja jatkuvasti ylläpitää rekisteriä sopimuksista kolmansien osapuolten kanssa (sopimusrekisteri), ja säännöllisesti katselmoida ja päivittää näitä sopimuksia tietoturvavaatimusten mukaisiksi (SFS-EN ISO/IEC 27002:2022, 45–46).

### 3.4.4 ISO/IEC 27002

Carder ja Watkins (2020) tähdentävät, että pohjimmiltaan ISO/IEC 27002 on huolellisesti muotoiltu toimimaan kompassina parhaille käytännöille tietoturvan hallinnassa ja järjestelmien yhteen toimivuudessa. Standardi tarjoaa ohjeita, joihin ulkoiset tarkastajat luottavat arvioidessaan valvonnan toteutusta sertifioitavan tietoturvan hallintajärjestelmän sisällä. On kuitenkin tärkeää huomata, että ISO/IEC 27002 ei nykyisessä muodossaan ole kansainvälisen sertifiointijärjestelmän perusta. (Carder & Watkins 2020, luku 3.)

ISO/IEC 27002:n antamat ohjeet liittyvät olennaisesti ISO27001-vaatimuksiin. ISMS:n käyttöönottoprosessissa ISO/IEC 27002 -standardin puoleen käännytään näkemyksien saamiseen erilaisista toiminnoista, joita voidaan soveltaa valittuihin kohteisiin. (Carder & Watkins 2020, luku 3.)

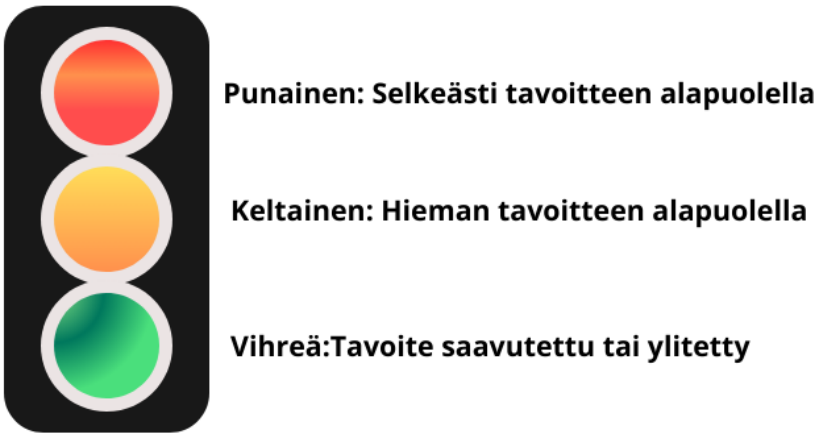
Tietoturvaympäristön dynaamisuuden tunnustaessa korostetaan, että vaikka vuosien varrella ISO/IEC 27002 -standardia on uudistettu, ei se silti välttämättä aina vastaa viimeisimpiä muutoksia. Carder ja Watkins (2020) toteavat, miten tietotekniikan nopea kehitys tuo jatkuvasti uusia uhkia ja haavoittuvuuksia, mikä antaa alan ammattilaisille tilaa täydentää ISO/IEC 27002 -standardia lisätoimenpiteillä ja käytännöillä. Kuitenkin kattavan ymmärryksen ja optimaalisten projektien tulosten saamiseksi kehotetaan käyttämään vuorovaikutuksellisesti ISO27001- ja ISO27002-standardeja yhdessä. (Carder & Watkins 2020, luku 3.)

## 3.5 Auditointi

Kun organisaatio on aloittanut tietoturvallisuuden hallinnan kehittämisen, ja tulee ajankohtaiseksi, että halutaan arvioida ISMS tehokkuutta, prosessien noudattamista sekä tunnistaa parannuskohteet, voi organisaatio teettää sisäisen tai ulkoisen auditoinnin. Auditointi on objektiivinen arviointiprosessi, jonka avulla puolueettomasti arvioidaan noudattaako organisaatio sille asetettuja vaatimuksia. Sen ydin on varmistaa, että organisaation toiminta vastaa sen ilmoitettuja käytäntöjä. (Kriik 2019.)

Auditointiprosessissa pitää ottaa huomioon organisaation omien prosessien lisäksi mahdolliset viranomaisvaatimukset. Sekä Kriikin (2019) että Allenin, Bapstin ja Hicksin (2024) mukaan, järjestelmällisyys ja riippumattomuus ovat keskeisiä auditoinnin tekemisen edellytyksiä, ja sen tarkoituksena on vahvistaa, että organisaatio täyttää erilaiset vaatimukset, jotka voivat tulla viranomaisilta tai asiakkailta. Auditoinnissa hyödynnetään yleisiä standardeja, kuten laatustandardeja, jotka määrittelevät, miten tietyt asiat tulisi suorittaa. (Kriik 2019; Allen, Bapst & Hicks 2024, 57.)

Kriik (2019) toteaa, että standardit auttavat parantamaan organisaation toimintaa ja lisäämään asiakkaiden luottamusta. Auditointi on systemaattinen ja dokumentoitu prosessi, jossa arvioidaan, täyttyvätkö asetetut kriteerit. Se perustuu näytteenottoperiaatteeseen, ja sen tulokset tallennetaan visuaaliseen muotoon, esimerkiksi liikennevalomenetelmällä (ks. kuvio 5). (Kriik 2019.)




Kuvio 5. Auditoinnin arviointi – liikennevalomenetelmä (Kriik 2019, muokattu).

Allen, Bapst ja Hicks (2024) luettelevat kolme alan standardia, jotka ohjaavat toimivaan hallintokehykseen, jota organisaation tulisi kehittää ja tarkastaa säännöllisesti. Yksi näistä standardeista on ISO 31000:2018, joka on standardi ohjeistamaan organisaatioiden kohtaamien riskien hallintaan. ISO 31000:2018 edellyttää riskienhallintakehyksen tehokkuuden säännöllistä arviointia sekä selvittämistä, onko kehystä ajankohtaista päivittää, eli tukeeko se organisaation tavoitteita. (Allen ym. 2024, 57.)

Allen ja muut kannustavat organisaatiota ottamaan käyttöön kattavat kyberturvallisuuden käytännöt ja menettelyt, jotta organisaatio pystyy tuottamaan tarvittavat ajankohtaiset riskituotokset osana ISMS:n jatkuvaa kehittämistä. (Allen ym. 2024, 57).

Auditoinnin toteuttajana voi olla joko ulkopuolinen taho tai se voidaan toteuttaa organisaatiossa sisäisesti, kunhan varmistetaan objektiivisuus ja tasapuolisuus. Sertifikaatti toimii todistuksena siitä, että organisaatio täyttää tietyn standardin vaatimukset, ja sen myöntävät sertifiointialan yritykset. (Kriik 2019.) Organisaatio voi sertifiointialan yrityksien avulla esimerkiksi sertifioida tietoturvallisuuden hallintajärjestelmän ISO 27001 -standardia vasten.

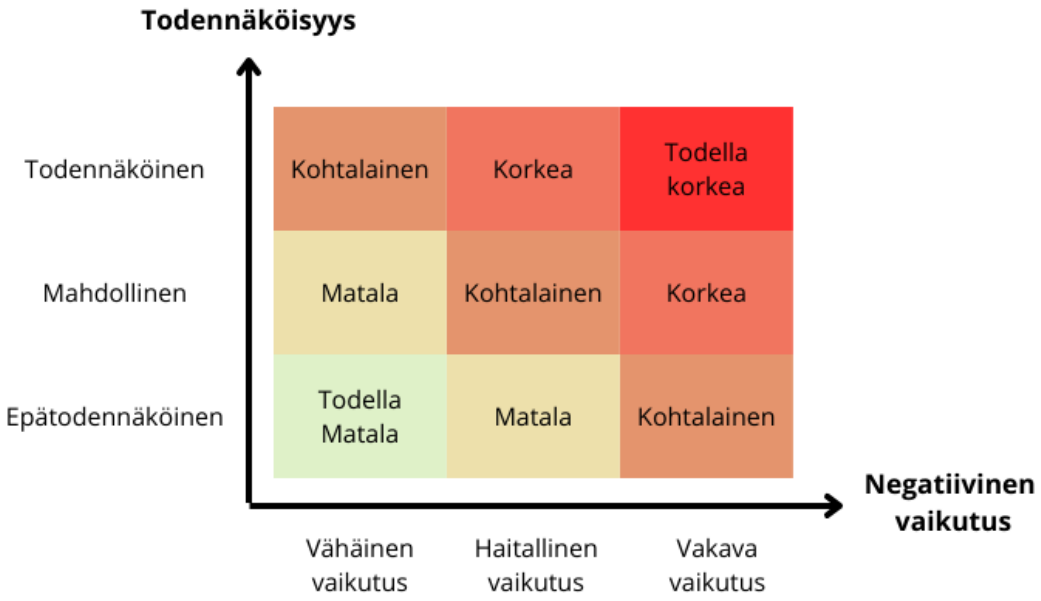
## 3.6 Riskienhallinta

Huttusen (2019) mukaan, tietoturvariskien hallinta on keskeinen osa laajempaa tietoturvallisuuden hallintajärjestelmää. Sen puitteissa tarkastellaan erilaisia uhkia ja arvioidaan riskien potentiaalisia seurauksia. Päätökset siitä, miten toimia ja milloin, tehdään vasta perusteellisen analyysin jälkeen, jotta riskit voitaisiin minimoida hyväksyttävälle tasolle. Sekä Huttunen (2019) että Watkins (2022) korostavat miten riskienhallinnan tavoitteena on varmistaa, että organisaatio voi hallita riskinsä tehokkaasti suhteessa tietoturvallisuuden keskeisiin tavoitteisiin. (Huttunen 2019; Watkins 2022, luku 4.)

Watkins (2022) nostaa esille, miten tietoturvan hallintajärjestelmä suunnitellaan samaan linjaan organisaation liiketoiminnan ja tavoitteiden kanssa. Sen määrittelemiseksi organisaatio tunnistaa asianomaiset osapuolet sidosryhmistä ja henkilöstöstä asiakkaisiin ja yleisöön. Heidän tietoturvavaatimustensa ymmärtäminen, organisaation laki-, säädös- ja sopimusvelvoitteiden lisäksi, toimii perustana ISMS-tietoturvakehykselle. Nämä näkökohdat yhdistettynä tietoturvariskien arvioinnin tuloksiin muokkaavat organisaation toteuttamien turvatoimien valintaa. (Watkins 2022, luku 4.)

Riskinarviointiprosessin ensimmäinen vaihe sisältää ISMS:n laajuuden määrittelyn, asianomaisten osapuolten kannalta merkityksellisten kysymysten tunnistamisen ja ISMS-alueen liiketoiminnan määrittämisen. Kaikki tietoon kohdistuvat mahdolliset riskit huomioon ottaen ISMS:n suojatoimet ovat ratkaisevan tärkeitä, ja ne kattavat tiedot, käsittely- ja tallennuslaitteet, järjestelmät, henkilöstön ja ulkoiset riippuvuudet. (Watkins 2022, luku 4.) Watkins (2022) jatkaa, että riskit tunnistetaan, arvioidaan ja luokitellaan luottamuksellisuuden, eheyden ja saatavuuden (CIA) mukaan, mikä muodostaa perustan klassiselle riskikaavalle. (Watkins 2022, luku 4.)

Kullekin riskille on määritetty seurausarvot, jotka edustavat organisaation kokonaiskustannuksia riskin toteutuessa. Nämä arvot yhdessä todennäköisyysarvioiden kanssa määrittävät riskitason riskinarviointikaavion (ks. kuvio 6) mukaisesti.  Riski = Todennäköisyys × Vaikutus (Watkins 2022, luku 4.)




Kuvio 6. Riskinarviointikaavio (Watkins 2022, luku 4, muokattu).

Tietoturvallisuuden hallintajärjestelmän ensisijainen tavoite on hallita kaikkia riskejä johdonmukaisesti, mikä edellyttää johdon määrittelevän hyväksyttävät riskitasot organisaation riskinottohalun perusteella. Jokaiselle riskille tulee nimetä riskinomistaja, joka on vastuussa riskien käsittelyn hyväksymisestä ja jäännösriskin hyväksymisestä ennalta määriteltyjen riskien hyväksymiskriteerien mukaisesti. (Watkins 2022, luku 4.)

Watkins (2022) kuvaa, miten hyväksytyn tason ylittävät riskit saavat aikaan päätöksiä asianmukaisista toimista, jotka ovat riskienhallinnan 4T:tä (ks. kuvio 7) (Watkins 2022, luku 4).

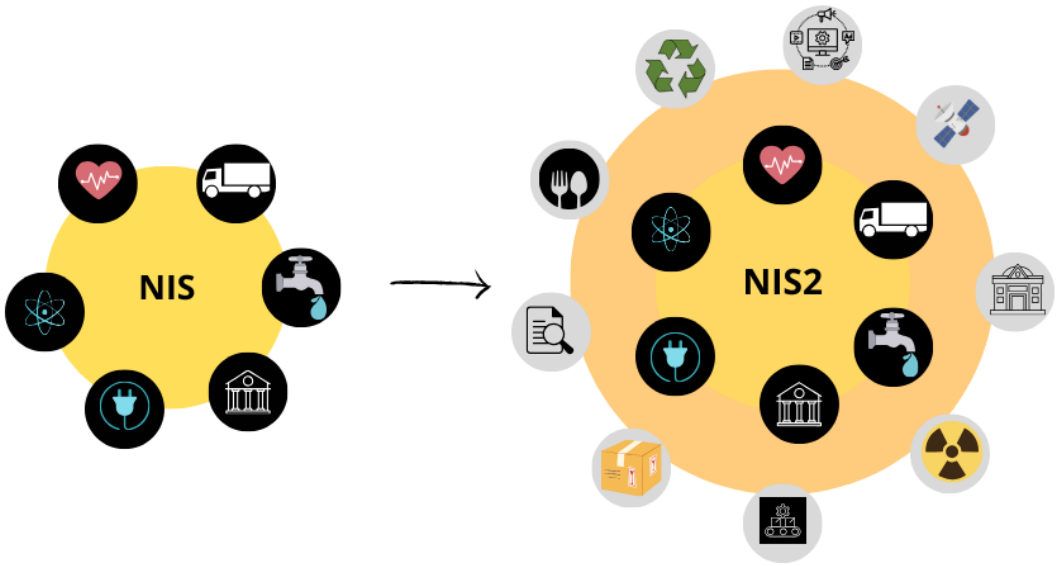

Kuvio 7. Riskienhallinnan 4T:tä (Watkins 2022, luku 4, muokattu)

Päätöksiä ja valvontaa arvioidaan jatkuvasti uudelleen, kunnes kaikki riskit täyttävät hyväksymiskriteerit (Watkins 2022, luku 4).

## 3.7 NIS2-direktiivi (2022/2555)

Euroopan Unionin (EU) määrittelemä kyberturvallisuusdirektiivi NIS2, tarkemmin kuvailtuna verkko- ja tietoturvadirektiivi, on suunniteltu vahvistamaan kyberturvallisuuden tasoa yhdenmukaistamalla unioniin kuuluvien jäsenvaltioiden toimenpiteitä ja raportointivelvoitteita keskeisillä toimialoilla. Lisäksi direktiivin tavoitteena on yhdenmukaistaa eri toimijoiden kyberturvallisuuskäytänteitä. (Direktiivi toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa (NIS2-direktiivi) 2023.)

NIS2 -direktiivi on laajennus aikaisempaan Network and Information Security (NIS) -direktiiviin. Se on tiukempi versio, ja se kattaa laajemman toimialajoukon (ks. kuvio 8). (Direktiivi 2022/2555/EU; Who Does NIS2 Apply To? 2024.)




- Terveydenhuolto
- Digitaalinen infrastruktuuri
- Kuljetus
- Vesihuolto
- Digitaaliset palveluntarjoajat
- Pankki- ja rahoitusmarkkinoiden infrastruktuuri
- Energia

NIS2-direktiiviin lisätyt:

- Jätevesi ja jätehuolto
- Tiettyjen kriittisten tuotteiden valmistus
- Kemikaalit
- Ruoka
- Digitaaliset palvelut, kuten sosiaalisen verkostoitumisen alustat ja datakeskuspalvelut
- Avaruus ja ilmailu
- Posti- ja kuriiripalvelut
- Julkishallinto
- Tutkimus

Kuvio 8. Muutokset toimialajoukkoihin NIS2-direktiiviin (Direktiivi 2022/2555/EU, muokattu)

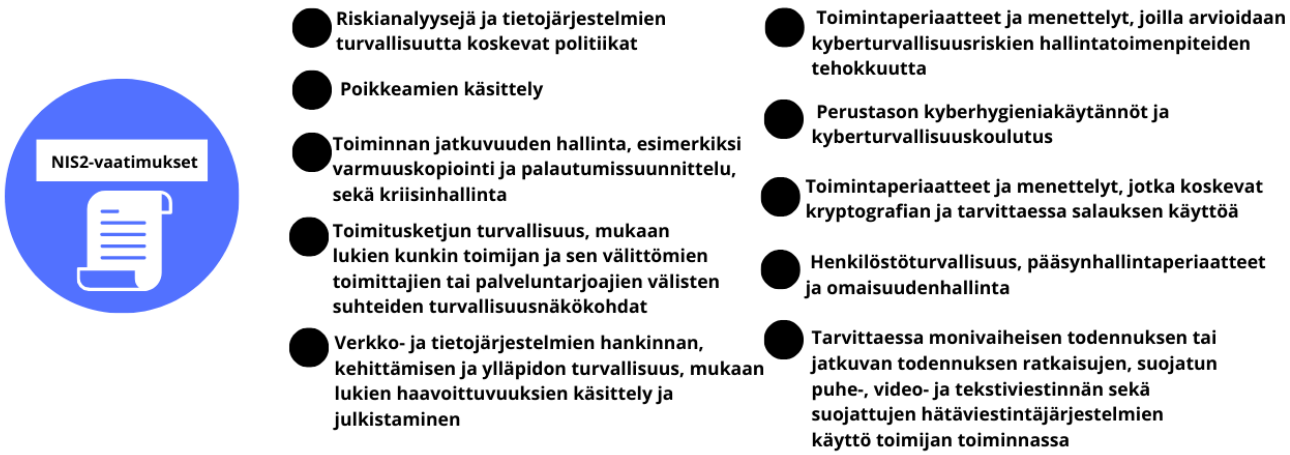
Keskeisiin toimijoihin lukeutuvat yleensä Essential Entity (EE), mikä käsittää kriittiset yhteiskunnan palvelut, joilla on vähintään 250 työntekijää, vuosiliikevaihto ylittää 50 miljoonaa euroa tai taseen loppusumma on yli 43 miljoonaa euroa. Vastaavasti tärkeiksi toimijoiksi kutsutaan Important Entity (IE), joka voidaan ajatella yhteiskunnan toiminnan kannalta tärkeiden palveluiden tukipalveluiksi tai kriittisiksi toimijoiksi. Näissä organisaation koko vaihtelee toimialoittain, mutta yleisesti niissä on 50 työntekijää, vuosiliikevaihto tai tase vähintään 10 miljoonaa euroa. (Who Does NIS2 Apply To? 2024.)

Ne organisaatiot, jotka kuuluvat NIS2:n soveltamisalaan, tulisi jo olla aloittaneet valmistelut direktiivin vaatimuksia varten, sillä joitakin siihen kuuluvia keskeisiä vaatimuksia on hidasta toteuttaa.

Direktiivi on astunut voimaan tammikuussa 2023, ja jäsenvaltioiden tulee sisällyttää se osaksi kansallista lainsäädäntöään lokakuun 17. päivä 2024 mennessä. Suomessa sääntöjen soveltamisen aloitusajankohta on 18. lokakuuta 2024. (What is NIS2? 2024.)

NIS2-direktiivi asettaa uusia vaatimuksia ja sitoumuksia organisaatioille neljällä keskeisellä osa-alueella: riskienhallinta, yritysvastuu, raportointivelvoitteet ja liiketoiminnan jatkuvuus. Näiden neljän vaatimusalueen lisäksi direktiivi edellyttää, että olennaiset ja tärkeät toimijat pitävät huolta perusturvatoimenpiteistä voidakseen torjua tunnetuimpia kyberuhkia, joiden tiedetään olevan todennäköisiä. (NIS2 Requirements 2024.)

NIS-direktiivin kohteena olevien organisaatioiden kyberturvallisuuden riskienhallinnassa ja siihen perustuvissa hallintatoimenpiteissä on olennaista sisällyttää ja pitää ajan tasalla vähintään NIS2-direktiivissä (21 artiklassa) mainitut kymmenen kohtaa (Traficom 2024). Kymmenen keskeistä kohtaa esitetty kuviossa 9.




Kuvio 9. NIS2-vaatimukset (Traficom 2024, muokattu)

Lisäksi organisaatioilla on ilmoitusvelvollisuus merkittävistä poikkeamista tärkeänä osana tietoturvan hallintaa. Merkittävällä poikkeamalla tarkoitetaan tapahtumaa, joka voi aiheuttaa vakavan toimintahäiriön palveluissa, taloudellisia tappioita tai merkittävää haittaa muille henkilöille tai organisaatioille. NIS2-direktiivin mukaan toimijan, joka kuuluu direktiivin soveltamisalaan, on

ilmoitettava viipymättä valvovalle viranomaiselle palveluun kohdistuvasta merkittävästä poikkeamasta. Ilmoitusvelvollisuus on jaettu kolmeen vaiheeseen: ensi-ilmoitus, joka on toimitettava 24 tunnin kuluessa poikkeaman havaitsemisesta, jatkoilmoitus, joka on toimitettava 72 tunnin kuluessa poikkeaman havaitsemisesta, ja loppuraportti, joka on toimitettava poikkeamatilanteen päätyttyä. (Traficom 2024.)

Lisäksi toimijan on ilmoitettava viipymättä merkittävästä poikkeamasta palvelujensa vastaanottajille, jos poikkeama todennäköisesti haittaa palvelujen tarjoamista. Tämä kolmivaiheinen ilmoitusvelvollisuus auttaa varmistamaan, että poikkeamat käsitellään asianmukaisesti ja että asianomaiset tahot saavat tarvittavat tiedot poikkeamatilanteen hallitsemiseksi ja mahdollisten vaikutusten minimoimiseksi. (Traficom 2024.)

Kuten Chopra ja Chadhary (2020) totesivat, organisaatiot eivät voi enää sulkea silmiään tietoturvallisuuden oikeudellisilta vaatimuksilta. Carder ja Watkins (2020) kehottavat käyttämään viitekehyksenä ISMS:n luomiseen ISO/IEC 27001 standardia, joka antaa perustan tehokkaalle tietoturvan hallinnalle. (Chopra & Chaudhary 2020, luku 1; Carder & Watkins 2020, luku 3.)

Tärkeänä lisäyksenä NIS2-direktiiviin on nostettu toimitusketjujen turvallisuus ja suhde suoriin toimittajiin, mikä kannustaa organisaatioita määrittelemään turvatoimenpiteet vastaamaan suorien toimittajien haavoittuvuuksia ja arvioimaan kaikkien toimittajien yleistä turvallisuustasoa. (NIS2 Requirements 2024.)

Jos organisaatio aloittaa kehittämään tietoturvallisuuden hallintajärjestelmää ISO27001-standardin viitekehyksen ja vaatimuksien pohjalta, otetaan standardissa jo huomioon tietoturvallisuus toimittajasuhteissa sekä toimittajasopimuksissa. Hallintakeinot opastavat käsittelemään ja arvioimaan toimittajan tuotteiden tai palveluiden käyttöön liittyviä tietoturvariskejä. (SFS-EN ISO/IEC 27002:2022, 43–44; SFS-EN ISO/IEC 27002:2022, 45.)

# 4 Tutkimustulokset

## 4.1 IoT-toimittajan tietoturvallisuuden taso ja sopimuksen päivitystarve

IoT-liiketoiminnan strategisen IoT-toimittajan nykytila-analyysillä haluttiin selvittää, millainen on toimittajan tietoturvallisuuden taso, ja vastaako se toimittajasopimukseen määriteltyjä tietoturvallisuusvaatimuksia. Samalla katselmoitiin IoT-toimittajan toimittajasopimus, ja analysoitiin sopimuksen päivittämisen tarve tietoturvallisuusvaatimuksien osalta.

Teemahaastattelun avulla haluttiin kartoittaa kokonaiskuva toimittajan yleisestä tietoturvallisuuden tasosta, prosesseista ja valmiustasosta poikkeamiin sekä häiriöihin. Digitan tavoitteena on IoT-liiketoiminnan tietoturvallisuuden hallintajärjestelmän kehittäminen ISO/IEC 27002:2022-standardin ja NIS2-direktiiviin vaatimuksien mukaiseksi, joten toimittajasuhteen arviointiin oli ajankohtainen tarve.

Digita Oy haluaa kehittää tietoturvallisuuden tasoaan sen, ja toimittajien välisissä suhteissa, sekä päivittää kullekin toimittajalle tietoturvavaatimukset toimittajasuhteen tyypin mukaisesti. Yhden strategisesti tärkeän toimittajan sopimuksen katselmoinnilla sekä teemahaastattelulla, organisaatiolle saatiin monipuolista dataa toimittajasuhteen tilasta, sekä tietoa sopimuksen päivittämisen tarpeen ajankohtaisuudesta. Kerättyä tietoa haluttiin lisäksi hyödyntää harkittaessa sopivia kysymyksiä uuden toimittajan riskien arviointilomakkeeseen.

### 4.1.1 Teemahaastattelun toteutus

Aineistonhankintamenetelmänä tutkimuksessa toimi teemahaastattelu, joka toteutettiin puolistrukturoituna haastatteluna. Menetelmä sopi parhaiten tutkittavaan aiheeseen, sekä siihen, miten haastattelu haluttiin toteuttaa. Haastattelun aikana haluttiin mahdollisuus selventää tai tarkentaa kysymyksiä, sekä keskustella haastateltavan asiantuntijan kanssa syvemmin annettujen vastausten perusteella.

Tuomi ja Sarajärvi (2018) toteavat, että teemahaastattelut vaihtelevat avoimesta haastattelutyypistä ihan strukturoituun haastatteluun. Kysymykset eivät kuitenkaan voi olla ihan mitä tahansa, vaan ne aina etsivät vastauksia tutkimustehtävän mukaisesti. (Tuomi & Sarajärvi 2018, 65.)

IoT-toimittajan teemahaastattelun kysymysrunko rakentui tutkimuskysymyksien perusteella; noudattaako IoT-toimittaja toimittajasopimuksen mukaisia tietoturvallisuusvaatimuksia, ja onko toimittajasopimusta tarvetta päivittää tietoturvallisuuden vaatimusten osalta. Lisäksi kysymyksissä otettiin huomioon jo alustavasti ISO/IEC 27002:2022-standardin ja NIS2-direktiiviin vaatimukset kehityskohteita ajatellen.

Teemahaastattelu toteutettiin rentona vuoropuheluna ja sen tarkoituksena oli myös kehittää organisaation ja toimittajan yhteistä vuorovaikutusta sekä rakentaa luottamusta. Teemahaastatteluun valittiin toimittajan organisaatiosta asiantuntija, joka on vastuussa tutkittavasta aihealueesta ja sen myötä omaa eniten kokemusta ja tietoa tutkittavasta aiheesta.

Haastatteluun osallistujille ilmoitettiin teemahaastattelun kysymyksien sisällöstä etukäteen, jotta toimittajan edustaja pystyi valmistautumaan käsiteltäviin aiheisiin. Kysymysrunko teemahaastatteluun (ks. liite 1) rakensi pohjan keskustelun etenemiselle, mutta keskustelu haluttiin pitää avoimena kommentoinnille ja avoimelle keskustelulle lisätiedon saamiseksi. Keskustelua kuitenkin ohjattiin jatkuvasti tutkijan toimesta kysymysrungon mukaisesti.

Teemahaastattelu eteni kysymysrungon mukaisesti koko haastattelun ajan, vaikkakin aiheista keskusteltiin hieman eri järjestyksessä. Teemahaastatteluun osallistui Digita Oy:stä IoT-Engineer Trainee eli tutkija, sekä IoT-liiketoiminnan Development Manager, joka toimi haastattelun ajan havainnoitsijana. IoT-toimittajan organisaatiota edustivat Project Director, sekä Network Operations Manager, joka toimi teemahaastattelun asiantuntijana vastaten kysymyksiin.

Haastattelun alussa kerrattiin vielä haastattelun agenda ja tavoitteet, sekä pyydettiin lupa haastattelun tallentamiseen videolle. Teemahaastattelu tallennettiin, litteroitiin ja käännettiin suomen kielelle englanninkielisestä litteroidusta tekstistä. Käännöksen laadun varmistamiseksi, sen vielä oikoluki Digitan asiantuntija, jotta kääntäessä kokonaisuus pysyisi mahdollisimman autenttisena sisällönanalyysiä varten. Haastattelun kokonaiskesto oli noin neljäkymmentä minuuttia.

### 4.1.2 Teemahaastattelun aineiston analyysi

Sisällönanalyysin avulla Tuomi ja Sarajärvi (2018) painottavat tiedon jäsentämistä, teemojen tunnistamista ja merkitysten rakentumista aineistosta. Analyysivaiheessa tutkija pyrkii löytämään aineistosta toistuvia kuvioita, trendejä ja merkityksiä, jotka voivat vastata tutkimuskysymyksiin tai tukea teoreettista viitekehystä. Sisällönanalyysi tarjoaa järjestelmällisen tavan tulkita laadullista aineistoa ja tuottaa merkityksellistä tietoa tutkimuksen tavoitteiden saavuttamiseksi. (Tuomi & Sarajärvi 2018, 91.)

Teemahaastattelun aineiston analyysiin valikoitui aineistolähtöinen laadullinen eli induktiivinen aineiston analyysi, joka on karkeasti määriteltynä kolmevaiheinen prosessi (ks. kuvio 10) (Tuomi & Sarajärvi 2018, 89). Aineiston analysointi aloitettiin litteroimalla teemahaastattelun video sanasta sanaan, ja sen jälkeen kääntämällä se englannista suomeksi.


Kuvio 10. Induktiivinen aineiston analyysi - kolmivaiheinen prosessi (Tuomi & Sarajärvi 2018, 89, muokattu).

Sisällönanalyysi aloitettiin alkuperäisdatan pelkistämisestä eli redusoinnista. Pelkistäminen tapahtuu siten, että aineistosta karsitaan kaikki tutkimukselle epäolennainen pois. Se voi olla datan pilkkomista tai tiivistämistä osiin (Tuomi & Sarajärvi 2018, 89). Analysoitava data oli sanasta sanaan auki kirjoitettu teemahaastattelu, joka tiivistettiin tutkimukselle oleellisimpiin tietoihin.

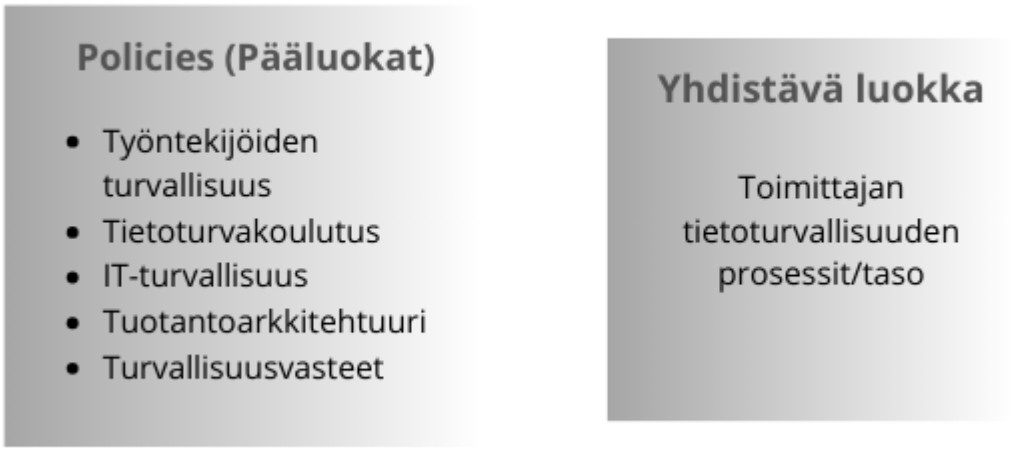
Datan pelkistämisen jälkeen siirryttiin sen klusterointiin, eli ryhmittelyyn. Samat käsitteet ryhmiteltiin ja yhdisteltiin eri luokiksi, joiden alle muodostui siten omat alaluokat (ks. kuvio 11).

Tuomi ja Sarajärvi (2018) opastavat ryhmittelemään alkuperäisdatasta muodostetut ilmaukset alaluokiksi, ja jatkaa siten luokittelua niin, että alaluokkia yhdistelemällä muodostetaan yläluokkia ja niitä edelleen yhdistämällä muodostuu pääluokkia, jotka nimetään aineiston nousevan ilmiötä kuvaavan aiheen mukaan. Lopuksi muodostetaan yhdistävä luokka, joka on yhteydessä tutkimustehtävään. (Tuomi & Sarajärvi 2018, 92.)

Alaluokkien ryhmittelyn jälkeen luokittelua jatkettiin siten, että muodostettiin yläluokkia, jotka on esitetty myös kuviossa 11. Osana aineiston klusterointia tehtiin myös abstrahointia, eli yleiskäsitteiden muodostamista pelkistämällä. Abstrahoinnissa yhdistetään empiirisen aineiston teoreettisiin käsitteisiin, jonka jälkeen esitetään tulokset, joissa esitellään muodostettu malli, käsitejärjestelmä, käsitteet tai aineistoa kuvaavat teemat. Tulosten osassa kuvataan myös luokittelujen perusteella muodostetut käsitteet tai kategoriat ja niiden sisällöt. (Tuomi & Sarajärvi 2018, 93.)


Kuvio 11. Ala- ja yläluokka

Luotujen yläluokkien avulla määriteltiin vielä pääluokat sekä lopuksi yhdistävä luokka (ks. kuvio 12), joka oli yhteydessä tutkimuskysymyksiin, joihin teemahaastattelussa haettiin vastauksia.




Kuvio 12. Pääluokka ja yhdistävä luokka

Tuomen ja Sarajärven (2018) mukaan, johtopäätöksissä on tärkeää pyrkiä ymmärtämään, mitkä asiat ovat merkityksellisiä tutkimuksen kannalta.

### 4.1.3 Laadullisen tutkimuksen tulokset

IoT-toimittajan toimittajasopimuksen tietoturvallisuusvaatimuksien katselmoinnin tarve oli todella ajankohtainen. Teemahaastattelun sisältöanalyysin avulla saatiin kattavasti tietoa siitä, mitkä ovat toimittajan tämänhetkiset toimintamallit, prosessit tai menettelyt. Tulosten avulla pystyttiin arvioimaan toimeksiantajan kanssa toimittajan toimintakykyä tarvittaessa vastata häiriötilanteisiin, mikä vaikuttaa toimittajan riskiarvioon.

Toimittajaketjun ymmärtäminen liittyy oleellisesti Digita Oy:n tavoitteeseen kehittää omaa tietoturvallisuuden hallintajärjestelmää vastaamaan NIS2-direktiivin, sekä ISO27001-standardin vaatimuksiin. Kun tiedostetaan riippuvuussuhde toimittajaan sekä siihen liittyvät riskit, pystytään analysoinnin avulla ottaa huomioon liiketoiminnalliset riskit, erityisesti liittyen palveluiden saatavuuteen, tietoturvaan sekä kyberturvallisuuteen.

Tietoturvavaatimukset IoT-toimittajan toimittajasopimuksessa olivat suppeat, mikä saattoi johtua siitä, että Digitalla ei ollut vielä otettu käyttöön toimittajan tietoturvallisuusvaatimuksia liitettä sopimuksen solmimishetkellä.

Tutkimustulosten perusteella IoT-toimittaja on aktiivisesti parantanut tietoturvaprosessejaan. Heillä on vakiintunut tietoturvallisuuden hallintajärjestelmä, ja he ilmoittivat kehittävänsä sitä ISO 27001-standardin vaatimusten mukaisesti. Lisäksi toimittaja avoimesti ilmaisi kiinnostuksensa parantaa yhteistä viestintää Digita Oy:n kanssa ja luoda yhteistyössä viestintäkanava, erityisesti häiriötilanteisiin liittyvää viestintää varten.

Tuloksia arvioitaessa on tärkeää ottaa huomioon mahdolliset riskit, joista merkittävimpänä nousi dokumentaation puute. Teemahaastattelun aikana nousi useasti esiin, että dokumentaatioon liittyen toimittajalla oli vielä selkeitä puutteita. Tämä herätti perusteltuja kysymyksiä siitä, miten prosessit todellisuudessa toimivat häiriötilanteissa, jos dokumentaatiota ei ole saatavilla tai se on puutteellista. Puutteellisen dokumentaation myötä herää myös epäilyksiä siitä, miten henkilöstöä on koulutettu toimimaan prosesseissa ja onko prosessien ja käytäntöjen tuntemus rajoittunut vain muutamiin avainhenkilöihin.

## 4.2 Digita Oy:n sisäinen kysely

Organisaation nykytila-analyysin tarve toimittajien tietoturvallisuuden ja riskien arvioinnin tasoon perustui tarpeeseen selvittää, miten organisaatiossa sisäisesti toimitaan toimittajan tietoturvallisuutta ja riskiarviointia tehdessä, sekä niihin liittyvät mahdolliset kehityskohteet. Tietojen avulla haluttiin pystyä tarkastelemaan organisaation toiminnan riskitaso toimittajasuhteisiin peilaten.

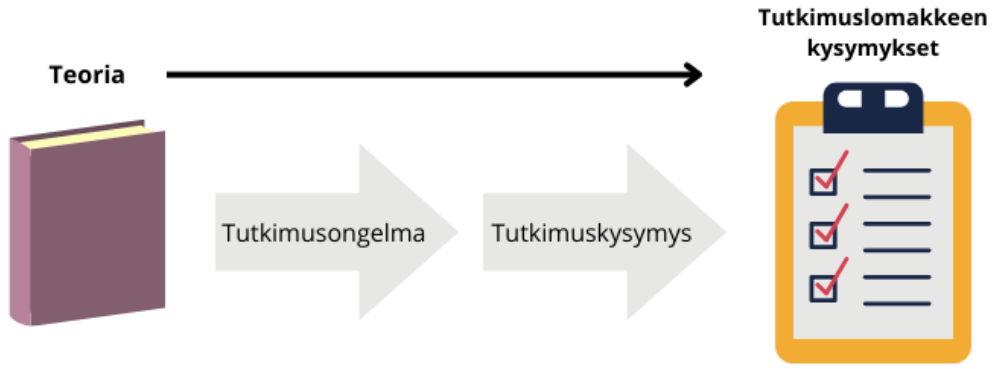
Digita Oy:ssä on tullut muutoksia vuoden 2023 alussa toimittajan tietoturvallisuusvaatimuksiin, joten otanta keskittyi vain viimeisen vuoden ajalta tehtyihin uusiin toimittajasopimuksiin relevanteimman datan saamiseksi.

### 4.2.1 Kyselytutkimuksen toteutus

Digita Oy:n toimittajien riskien arvioinnin nykytila-analyysi aloitettiin perehtymällä organisaation sisäisiin materiaaleihin, sekä tarkastelemalla IoT-toimittajalle teetetyn teemahaastattelun tuloksia.

Materiaalien pohjalta luotiin tarvittava kysymyspohja, johon sisällytettiin prosessikuvaukset toimittajahankintaan liittyen, organisaation Code of Conduct -periaatteet sekä toimittajan tietoturvallisuusvaatimukset. Perehtyminen mahdollisimman laajasti ja syvällisesti tarvittaviin tietolähteisiin, hyödytti tutkimusta ja kyselylomaketta tehdessä. Kanasenkin (2015) mukaan, tietolähteisiin perehtymällä voidaan lisätä työn luotettavuutta (Kananen 2015, 199).

Teorian jälkeen tutkimus eteni kysymyksien luomiseen, samalla keskittyen kyselyn otannan valintaan. Koska kysymykset kyselylomakkeeseen johdettiin teoriasta (ks. kuvio 13) ja määrällinen tutkimus edellyttää teorian ja tutkittavan ilmiön tuntemista, sekä vahvaa esiymmärrystä, niin otannaksi valikoitui ne asiantuntijat ja liiketoimintajohtajat, jotka neuvottelevat uudet hankintasopimukset. Heillä on tarvittava tietämys tutkittavasta ilmiöstä.




Kuvio 13. Kyselylomakkeen kysymyksien toteutus.

Tutkimuksen kysymykset rakennettiin perustuen tutkimuskysymyksiin, toimeksiantajan tarpeisiin ja määrittelemiin prosesseihin, sekä huomioiden voimassa olevat lainsäädännöt ja standardien vaatimukset. Ennen kyselylomakkeen luomista Microsoft Forms -sovelluksella, kysymykset tarkastettiin yhden liiketoimintajohtajan kanssa. Tämän katselmuksen avulla voitiin korjata mahdolliset kirjoitusvirheet, tarkentaa ja parantaa kysymysten sisältöä sekä rajata mukaan vain relevantit kysymykset tutkimusta varten.

Kyselyyn valikoitui 24 kysymystä, joista 20 kappaletta oli strukturoituja kysymyksiä, ja neljä avoimia kysymyksiä (ks. liite 3). Ensimmäiset kolme kysymystä eivät olleet opinnäytetyön kannalta olennaisia, koska niissä pyydettiin toimittajan nimeä, ID:tä ja sopimusnumeroa. Kyselyn aloittaminen näillä tunnistetiedoilla oli kuitenkin tärkeää, koska ne tarjosivat lisäarvoa toimeksiantajalle.

Kysely toteutettiin Microsoft Forms -sovelluksen avulla luodulla verkkokyselyllä, jossa vastattiin monivalintakysymyksiin. Kysymysten sisältö pyrittiin pitämään yleistasoisina, jotta tuloksista saataisiin kokonaiskuva useamman liiketoiminnan käytänteistä.

Kyselytutkimuksen kutsut lähetettiin sähköpostitse otantaan valituille henkilöille, ja viestissä esiteltiin kyselyn sisältö, tarkoitus ja tavoitteet (ks. liite 2). Viestin lopussa oli linkki, joka johti vastaajat Forms-kyselyyn. Tavoitteena oli saada dataa useammasta toimittajasta, joten kyselyyn oli määritelty mahdollisuus vastata useamman kerran saman henkilön toimesta. Kyselyn totutusprosessi on kuvattu tähän asti kuviossa 14.


Kuvio 14. Verkkokyselyn toteutus.

Kyselyn alussa vastaajan oli täytettävä toimittajan tiedot ennen kuin hän pääsi etenemään monivalintakysymyksiin. Kysymysten määrä vaihteli 17–23 kysymyksen välillä (ks. liite 3), riippuen toimittajan tyypistä. Kyselyn loppuun oli lisätty kaksi kysymystä järjestelmätoimittajiin liittyen, ja jos toimittaja ei ollut järjestelmätoimittaja, kysely päättyi kahta kysymystä aiemmin. Lisäksi kyselyn loppuun oli sisällytetty avoin tekstikenttä, johon vastaaja pystyi jättämään kirjallisen palautteen.

Kyselyyn asetettiin viikon vastausaika (7.3.2024 – 15.3.2024), ja tästä tiedotettiin organisaation sisällä laatupäällikön toimesta sekä sisäisessä uutiskanavassa. Kysely lähetettiin torstaina, ja seuraavana maanantaina lähetettiin vielä muistutusviesti kyselystä vastaajille paremman vastausmäärän saamiseksi. Kuten Kananen (2015) on huomauttanut, uusintakutsujen lähettämisellä voidaan kasvattaa vastausprosenttia (Kananen 2015, 219).

Toimeksiantajan kanssa oli sovittu etukäteen, että toimittajien nimiä ei mainita opinnäytetyössä. Näin ollen ensimmäisten kolmen kysymyksen tiedot pysyivät toimeksiantajan tiedossa. Kyselyn viimeiseen avoimeen kysymykseen tuli palautetta vain liittyen tarkennuksiin toimittajista, joten niiden tiedot eivät myöskään tulleet opinnäytetyön raporttiin.

### 4.2.2 Kyselytutkimuksen aineiston analyysi

Määrällisessä tutkimuksessa kaikki vastaajien vastaukset kysymyksiin kootaan havaintomatriisiin, jonka jälkeen aineisto tarkistetaan ja tulokset tiivistetään (Kananen 2015, 287). Kyselyn kysymyksiin saatiin suoraan ladattua Excel-taulukko Forms-sovelluksesta, joka toimi havaintomatriisina. Havaintomatriisin avulla aloitettiin aineiston tarkastus ja tiivistäminen. Tarkastuksen tarkoituksena oli poistaa turhat puutteelliset vastaukset, joita ei lopullisissa tuloksissa havaittu lainkaan. Tämän jälkeen jatkettiin aineiston tiivistämiseen.

Aineiston tiivistetty esittäminen toteutettiin käyttämällä jakaumia. Suora jakauma on yksi yksinkertainen analyysikeino kerätyn tiedon tiivistämiseen, ja sen avulla nähdään yksittäisen kysymyksen eri vaihtoehtojen vastaukset (Kananen 2015, 288). Kaikki strukturoiduista kysymyksistä saadut vastaukset esitettiin suoran jakauman avulla, koska se tarjosi yksinkertaisen ja selkeän tavan tiivistää aineisto.

### 4.2.3 Kyselytutkimuksen tulokset

Kyselyyn saatiin yhteensä 17 vastausta, mikä vastaa yli puolta (57 %) tehtyjen toimittajasopimusten (30 kpl) kokonaismäärästä viimeisen vuoden ajalta. Kyselyn ensimmäisessä strukturoidussa kysymyksessä selvitettiin, mihin toimittajakategoriaan vastaajan toimittaja kuuluu (ks. kuvio 15).

Suurin osa vastauksista (41 %) koski strategisia toimittajia, noin joka kolmas (35 %) yleisiä toimittajia, ja loput (24 %) kyvykkäitä toimittajia. Muihin kategorioihin kuuluvia toimittajia ei ilmennyt vastauksissa.


Kuvio 15. Kysymys 4. Mihin toimittajakategoriaan toimittaja kuuluu (N=17).

Seuraavassa kysymyksessä tarkasteltiin, kuuluuko vastaajan toimittaja tietoturvakriittisiin toimittajiin (ks. kuvio 16). Kaikista vastauksista (17 kpl) hieman yli puolet (53 %) toimittajista kuului tietoturvakriittisiin toimittajiin, kun taas loput (47 %) eivät kuuluneet. Tämän jälkeen kyselyssä ohjattiin "Kyllä" vastanneet vastaamaan kysymykseen toimittajan prioriteetista tietoturvakriittisenä toimittajana, kun taas "Ei" vastanneet siirtyivät suoraan kysymykseen seitsemän.


Kuvio 16. Kysymys 5. Kuuluuko toimittaja tietoturvakriittisiin toimittajiin (N=17).

Edellisen kysymyksen perusteella joka kolmas toimittaja (33 %) kuului tietoturvakriittisiin toimittajiin, joilla oli tietoturvaomaisuuden prioriteetti luokassa 1 (ks. kuvio 17). Yli puolet vastaajista, jotka siirtyivät vastaamaan tähän kysymykseen, eivät vastanneet mitään (67 %).


Kuvio 17. Kysymys 6. Mikä on toimittajan omaisuuden prioriteetti (N=9).

Kysymyksessä seitsemän tarkasteltiin, onko toimittajasopimuksen laatimisen yhteydessä käytetty Digitan vai toimittajan sopimuspohjaa (ks. kuvio 18). Vastaajista (17 kpl) selvästi lähes kaikki (80 %)

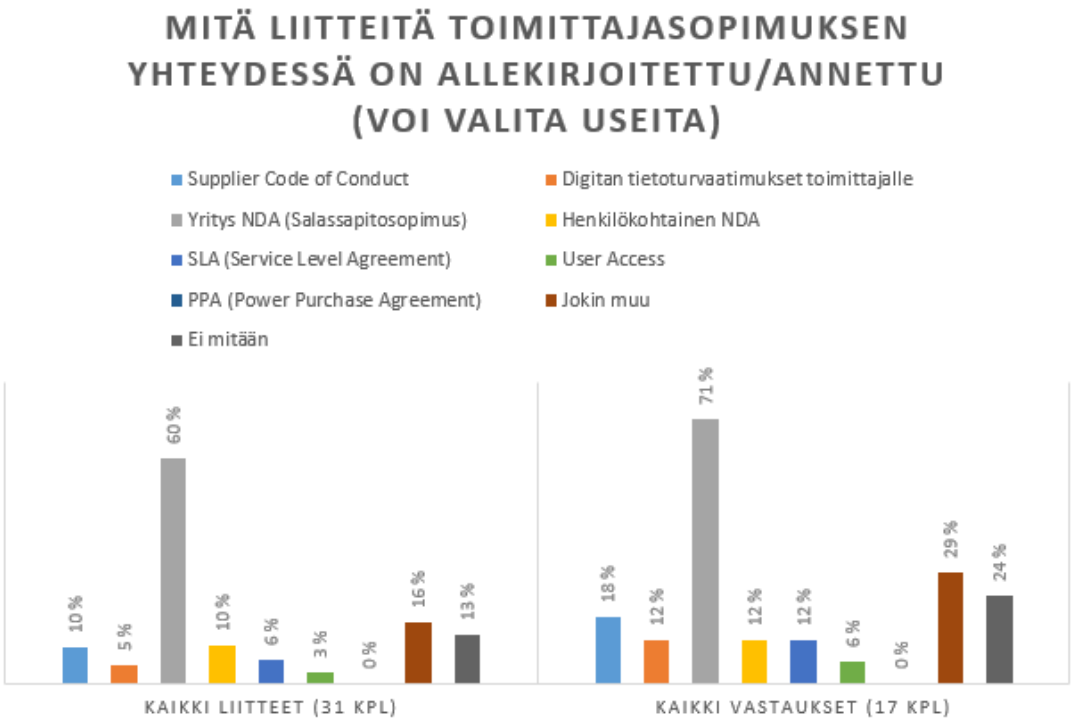
ilmoittivat käyttäneensä toimittajan sopimuspohjaa, kun taas vain noin joka viides (18 %) ilmoitti käyttäneensä Digitan sopimuspohjaa.


Kuvio 18. Kysymys 7. Kenen sopimuspohjaa toimittajasopimusta tehdessä on käytetty (N=17).

Kysymys liittyen toimittajasopimuksen yhteydessä allekirjoitettuihin tai annettuihin liitteisiin koski kaikkia vastauksia (17 kpl). Kuviossa 19 on esitetty pylväskaaviossa vasemmalla puolella kaikkien liitteiden kokonaismäärä vastauksissa (31 kpl), ja oikealla puolella vastauskohtaisesti (17 kpl). Neljäsosalle toimittajista (24 %) ei ollut allekirjoitettu tai annettu liitteitä osana toimittajasopimusta, ja PPA (Power Purchase Agreement) -liitettä ei ollut käytetty kertaakaan (0 %).

Osaan toimittajasopimuksista oli liitetty useampi kuin yksi liite. Liitteitä oli yhteensä 31 kappaletta (ks. kuvio 19), joista selkeästi yli puolet (60 %) olivat Yritys NDA-liitteitä, eli salassapitosopimuksia. Selkeä enemmistö toimittajasopimuksista (71 %) sisälsi Yritys NDA-liitteen (salassapitosopimus), ja kahdessa sopimuksessa (15 %) oli allekirjoitettu sekä Yritys NDA että henkilökohtainen NDA. Henkilökohtaisia NDA-liitteitä oli vain kahdessa tapauksessa (10 %) kaikista liitteistä.

Supplier Code of Conduct eli Digitan oman hyvän liiketavan periaatteet-liite oli annettu kolmelle toimittajalle, mikä vastasi lähes joka neljättä (18 %) kaikista vastauksista. Digitan tietoturvavaatimukset toimittajalle-liite oli liitteenä kahdessa sopimuksessa (12 %), ja User Access-liite yhdessä (6 %).




Kuvio 19. Kysymys 8. Liitteet, jotka annettu toimittajasopimuksen yhteydessä.

Pääsynhallinnan turvallisuutta mittaavassa kysymyksessä oli sisällytetty samaan kysymykseen sekä fyysisen että järjestelmäturvallisuuden mittaaminen. Suurimmassa osassa vastauksista ja yli puolessa tapauksista (59 %) tämä oli otettu huomioon, kun taas lähes joka kolmannessa vastauksessa (30 %) sitä ei ollut otettu huomioon (ks. kuvio 20).


Kuvio 20. Kysymys 9. Onko pääsynhallinnan turvallisuus otettu huomioon (N=17).

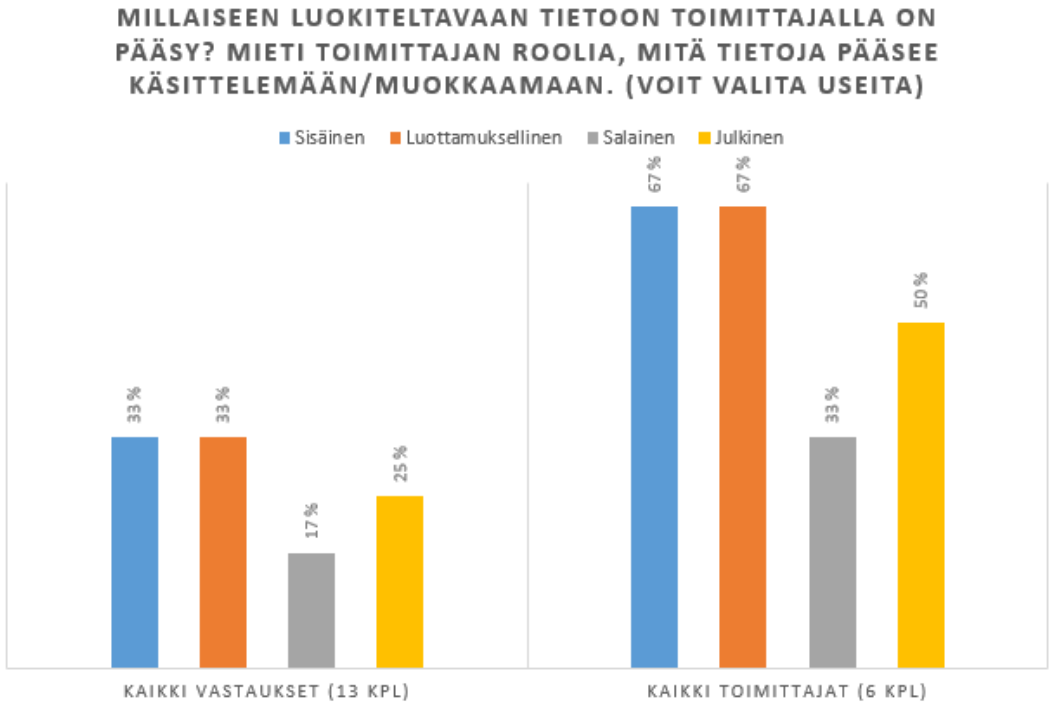
Loogisena jatkumona edellisestä kysymyksestä seuraavassa tarkasteltiin toimittajan työntekijöiden tai alihankkijoiden tarvetta liikkua Digitan tiloissa (ks. kuvio 21). Enemmistö vastaajista (88 %) vastasi, ettei ole lainkaan tarvetta, kun taas yhden toimittajan kohdalla (6 %) tarve on viikoittainen ja yhden toimittajan kohdalla (6 %) tarve oli satunnainen.


Kuvio 21. Kysymys 10. Toimittajan työntekijöiden/alihankkijoiden tarve liikkua Digitan tiloissa (N=17).

Kysymyksessä 11 tarkasteltiin toimittajan työntekijöiden pääsyä järjestelmien kautta Digitan omaisuuteen, tarkemmin määriteltynä tietoon (ks. kuvio 22). Kaikista vastauksista hieman yli puolet (65 %) ilmoitti, ettei ollut pääsyä tietoon, kun taas hieman alle puolet (35 %) ilmoittivat, että toimittajalla on pääsy tietoon. Tähän kysymykseen ”Kyllä” vastanneet ohjattiin seuraavaan kysymykseen, jossa tarkasteltiin, millaiseen tietoon toimittaja pääsee. ”Ei” vastanneet siirtyivät suoraan kysymykseen 13.


Kuvio 22. Kysymys 11. Onko toimittajan työntekijöillä pääsy omaisuuteen (tietoon) (N=6).

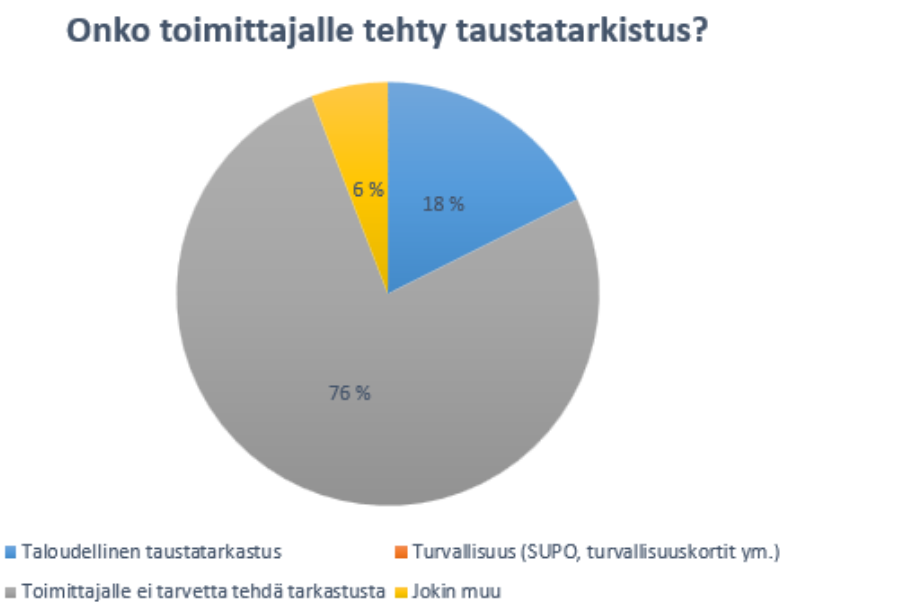
Seuraavaan kysymykseen vastattiin kuuden toimittajan osalta, jotka olivat vastanneet edelliseen kysymykseen ”Kyllä” (35 %). Kysymyksessä pyrittiin tarkentamaan, minkä tyyppiseen luokiteltavaan tietoon toimittajalla on pääsy, ja vastauksia sai olla useita. Kysymykseen saatiin yhteensä 13 vastausta, jotka liittyivät kuuden eri toimittajan luokiteltavaan tietoon pääsyyn (ks. kuvio 23).




Kuvio 23. Kysymys 12. Millaiseen luokiteltavaan tietoon toimittajalla on pääsy.

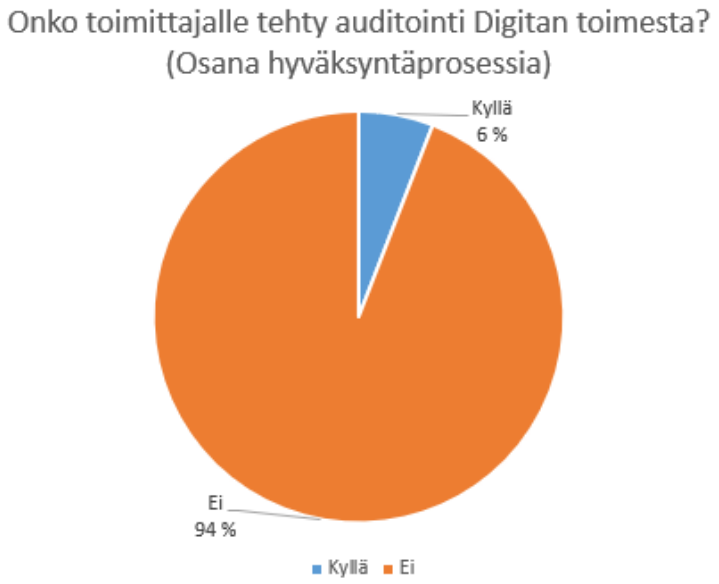
Suurimmalla osalla kuudesta toimittajasta (67 %) oli pääsy sekä sisäiseen että luottamukselliseen tietoon. Salaiseen tietoon pääsy oli kahdella toimittajalla (17 %), ja puolet, eli kolme toimittajaa (25 %), pääsivät muokkaamaan tai käsittelemään julkista tietoa.

Kysymyksessä 12 tiedusteltiin, oliko toimittajille tehty taustatarkastuksia (ks. kuvio 24). Vastausvaihtoehdoissa esitettiin erilaisia taustatarkastusmahdollisuuksia, ja vastaajat saivat valita useampia vaihtoehtoja. Jokainen vastaaja oli valinnut yhden taustatarkistuksen, joten kaikista vastauksista (17 kpl) suurin osa (76 %) ilmoitti, ettei toimittajille ollut tehty taustatarkastusta koska sille ei ole tarvetta. Hieman alle viidesosa vastaajista (18 %) valitsi, että toimittajalle oli tehty taloudellinen taustatarkastus, sekä vain yhdelle toimittajalle (6 %) oli tehty jokin muu taustatarkastus. Kenellekään vastauksien toimittajista ei ollut toteutettu turvallisuustarkastusta (0 %).




Kuvio 24. Kysymys 13. Onko toimittajalle tehty taustatarkistus (N=17).

Toimittajan auditointi Digitan toimesta oli tehty vain yhdelle (6 %) toimittajalle, kun taas suurimmalle osalle toimittajista (94 %), sitä ei ollut suoritettuna osana hyväksyntäprosessia (ks. kuvio 25).




Kuvio 25. Kysymys 14. Onko toimittajalle tehty auditointia Digitan toimesta (N=17).

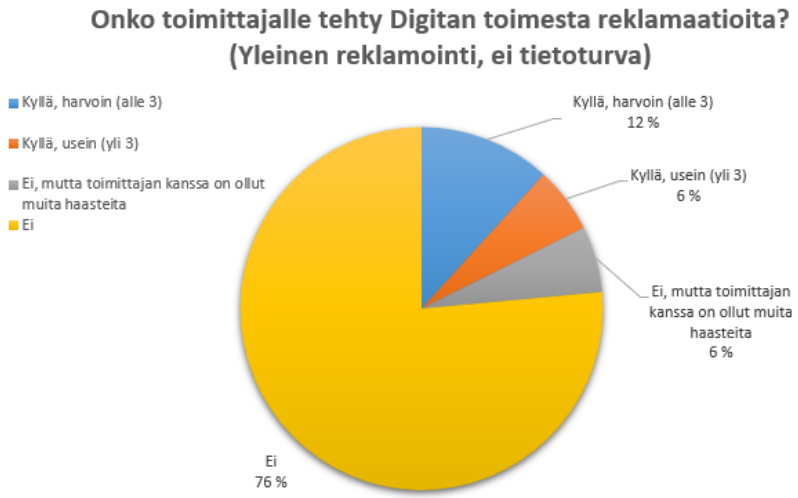
Seuraavaksi kysyttiin vastaajan mielipidettä siitä, olisiko toimittajalle tarpeellista tehdä auditointia riskienhallinnan näkökulmasta (ks. kuvio 26). Vastauksista selkeä enemmistö (88 %) ei kokenut sitä tarpeelliseksi, kun taas hieman yli kymmenesosa (12 %) vastasi, että kokisi toimittajan auditoinnin tarpeelliseksi.


Kuvio 26. Kysymys 15. Onko toimittajalle mielestäsi tarpeellista tehdä auditointi? (N=17).

Kysyttäessä, onko toimittajan kanssa määritelty laatu- ja/tai mahdollisesti muita vaatimustenmukaisuus toimitettaville tuotteille tai palveluille, tarkennettiin vastausvaihtoehtoja toimitusketjun turvaamisella, lainsäädännöllä, tai asiakkaan palvelutasosopimuksella (SLA). Hieman alle puolet vastaajista (41 %) vastasi ”Kyllä”, kun taas suurimmalla osalla toimittajista (59 %) tällaista ei ollut määritelty, ja vastaus oli ”Ei” (ks. kuvio 27).

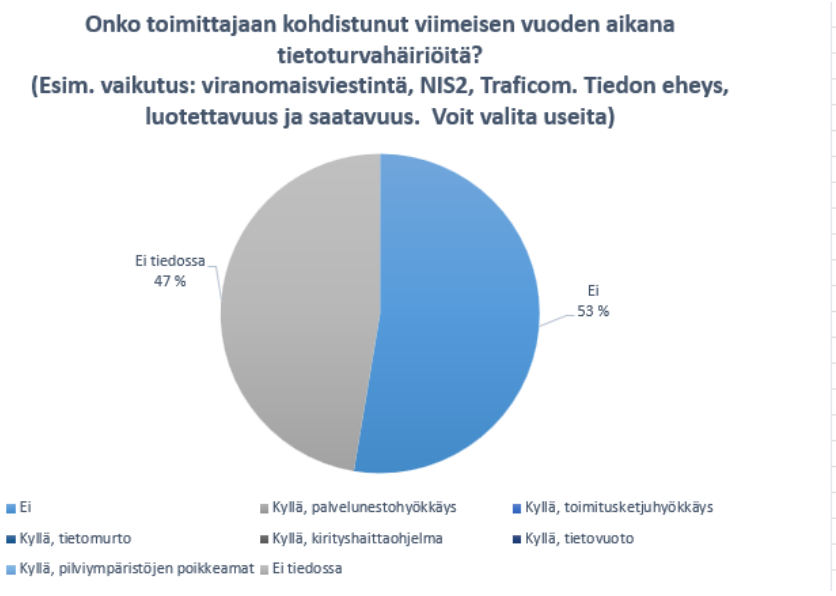

Kuvio 27. Kysymys 16. Onko toimittajan kanssa määritelty laatu- ja/tai jokin muu vaatimustenmukaisuus toimitettaville tuotteille/palveluille (N=17).

Kysymyksessä 17 selvitettiin, onko toimittajalle tehty viimeisen vuoden aikana Digitan toimesta reklamaatioita. Kysymys tarkennettiin yleiseen reklamointiin, ei tietoturvaan (ks. kuvio 28). Suurimmalle osalle (67 %) ei ollut tehty reklamaatioita, mutta yhdelle toimittajalle (6 %) niitä oli tehty usein, eli enemmän kuin kolme kappaletta. Yhden toimittajan kanssa oli ollut muita haasteita, jotka eivät olleet johtaneet reklamaation tekemiseen, ja kahdelle toimittajalle (12 %) oli tehty reklamaatio harvoin, eli alle kolme kertaa.




Kuvio 28. Kysymys 17. Onko toimittajalle tehty Digitan toimesta reklamaatioita (N=17).

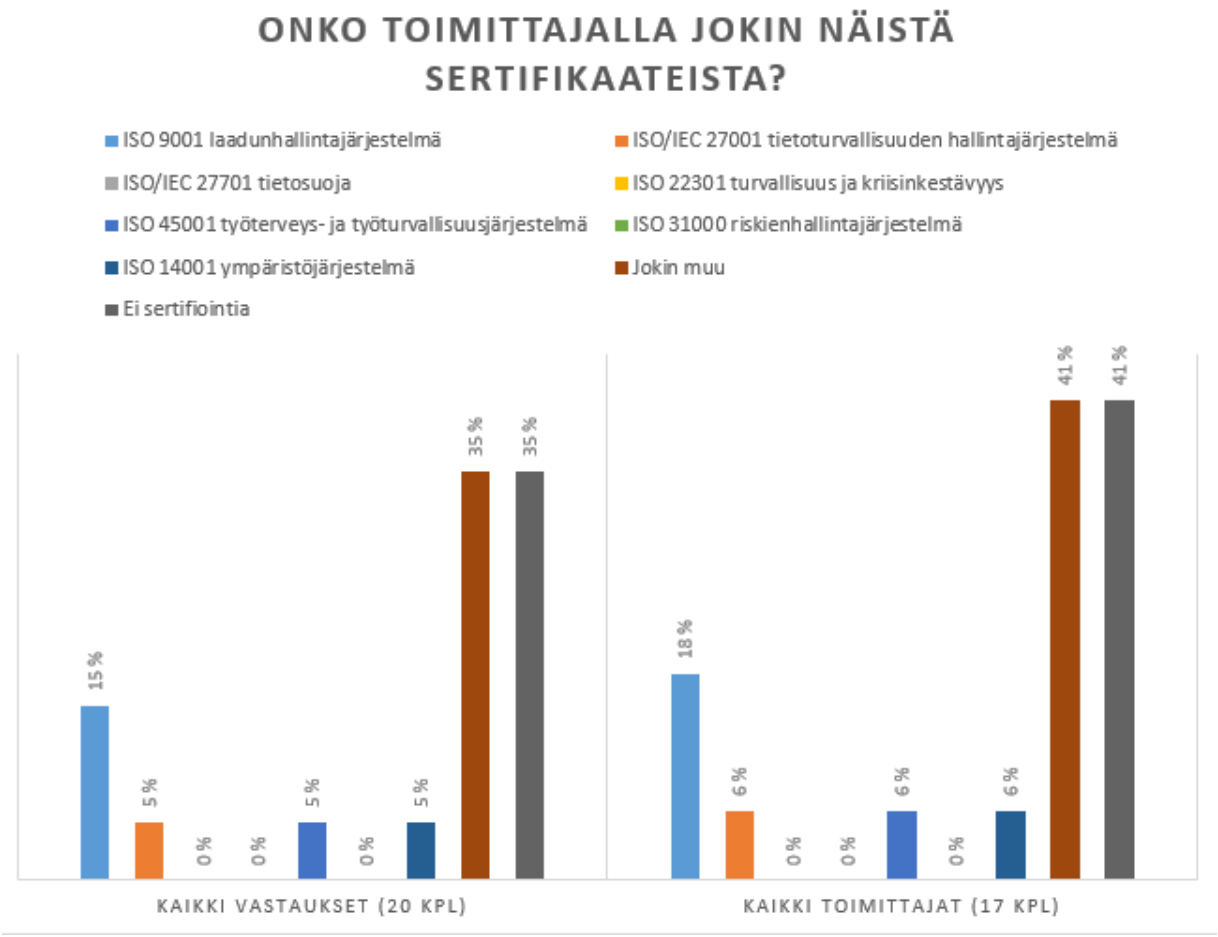
Toimittajan mahdollisia tietoturvahäiriöitä kysyttiin kysymyksessä 18, johon vastaajat pystyivät valitsemaan useita vaihtoehtoja. Kysymyksessä tarkennettiin, onko toimittajaan kohdistunut tietoturvahäiriöitä viimeisen vuoden aikana. Kysymyksessä annettiin selvennystä, joka sisälsi viranomaisviestinnän, NIS2:n, Traficomin, tiedon eheyden, luotettavuuden ja saatavuuden. Vastauksia saatiin yhteensä 19 kappaletta, ja ne jakautuivat melko tasaisesti "Ei" (53 %) ja "Ei tiedossa" (47 %) vastausten välille (ks. kuvio 29).




Kuvio 29. Kysymys 18. Onko toimittajaan kohdistunut tietoturvahäiriöitä (N=19).

Seuraavaksi kysyttiin, onko toimittajalla jokin listalla olevista sertifikaateista, tai ei sertifiointia (ks. kuvio 30). Koska toimittajalla saattoi olla useampi sertifikaatti, vastaaja pystyi valitsemaan useita vaihtoehtoja. Kaikista vastauksista (17 kpl) löytyi yhteensä 20 sertifikaattia. Kymmenellä toimittajalla (59 %) oli yksi tai useampi sertifikaatti, kun taas seitsemällä (41 %) toimittajalla ei ollut sertifiointia.

Eniten oli "jokin muu" vastauksia, joiden osuus oli hieman yli kolmannes (35 %), ja vastaavasti ei sertifiointia ollenkaan samansuuruisella osuudella (35 %). ISO 9001 laadunhallintajärjestelmä oli kolmella toimittajalla (18 %). ISO/IEC 27001 tietoturvallisuuden hallintajärjestelmä löytyi yhdeltä toimittajalta (6 %), samoin kuin ISO 45001 työterveys- ja työturvallisuusjärjestelmä (6 %) sekä ISO 14001 ympäristöjärjestelmä (6 %).

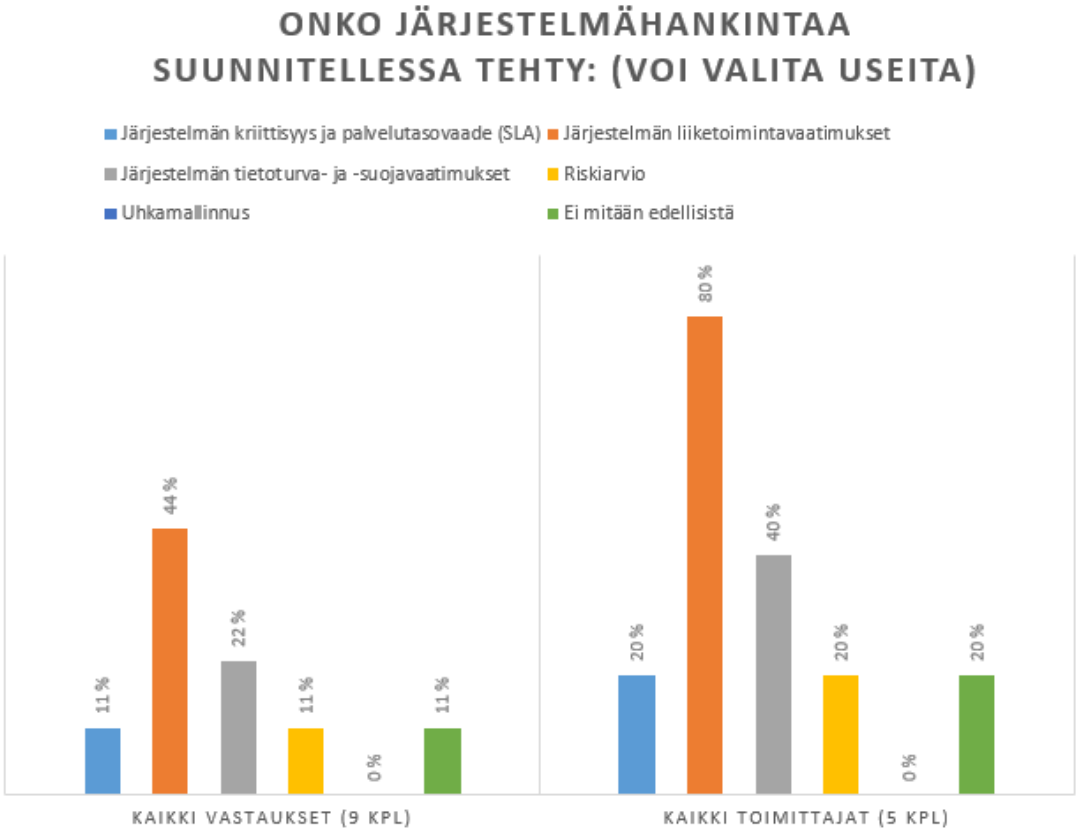



Kuvio 30. Kysymys 19. Onko toimittajalla jokin näistä sertifikaateista.

Seuraava kysymys oli kyselyn viimeinen osa joillekin vastaajille, ja se käsitteli, onko toimittaja järjestelmätoimittaja (ks. kuvio 31). ”Kyllä” vastanneet (29 %) ohjattiin vastaamaan vielä kahteen jatkokysymykseen, kun taas ”Ei” vastanneet (71 %) ohjattiin suoraan viimeiseen kysymykseen, joka oli vapaaehtoinen avoin palaute.


Kuvio 31. Kysymys 20. Onko toimittaja järjestelmätoimittaja (N=17).

Järjestelmätoimittajille suunnattu ensimmäinen kysymys pyrki selvittämään, mitä toimenpiteitä on tehty järjestelmähankinnan suunnitteluvaiheessa. Tähän kysymykseen vastasi viisi aiempaan kysymykseen ”Kyllä” vastannutta vastaajaa (ks. kuvio 32). Vastaajilla oli mahdollisuus valita useita vaihtoehtoja.




Kuvio 32. Kysymys 21. Mitä järjestelmähankintaa suunnitellessa on tehty.

Melkein kaikille toimittajille oli järjestelmähankintaa suunnitellessa määritelty järjestelmän liiketoimintavaatimukset (80 %). Järjestelmän tietoturva- ja suojavaatimukset oli tehty kahdelle (40 %) toimittajalle osana järjestelmähankinnan suunnittelua. Uhkamallinnusta ei ollut tehty järjestelmähankinnan suunnitteluvaiheessa yhdellekään toimittajalle (0 %). Riskiarvio sekä järjestelmän kriittisyys ja palvelutasovaatimukset (SLA) on tehty kumpikin yhdelle toimittajalle (20 %). Yhdelle toimittajalle (20 %) ei ole tehty mitään edellä mainituista toimenpiteistä (20 %).

Viimeisessä kysymyksessä haluttiin tietää, oliko järjestelmähankinnan aikana kartoitettu, että ulkoisella toimittajan henkilöstöllä ja sen mahdollisilla alihankkijoilla on riittävät tietoturva- ja suojamenettelyt, sekä kyky toteuttaa järjestelmä tietoturva- ja suojavaatimusten mukaisesti (ks. kuvio 33). Lisäksi haluttiin tietää, millä tavalla tämä oli kartoitettu.


Kuvio 33. Kysymys 21. Mitä järjestelmähankinnan aikana on kartoitettu (N=5).

Kaikista vastauksista (5 kpl) yli puolet oli todennettu jollain muulla tavalla (60 %). Loput (40 %) vastaajista vastasivat, että ei ole tehty tällaista todennusta.

## 4.3 Toimittajan riskien arviointilomake

IoT-toimittajan ja organisaation nykytila-analyysien tulosten perusteella haluttiin kehittää toimittajan riskien arviointilomake. Lomakkeen avulla organisaatio voi tehokkaasti arvioida toimittajan riskiluokan osana hankintaprosessia tulevaisuudessa.

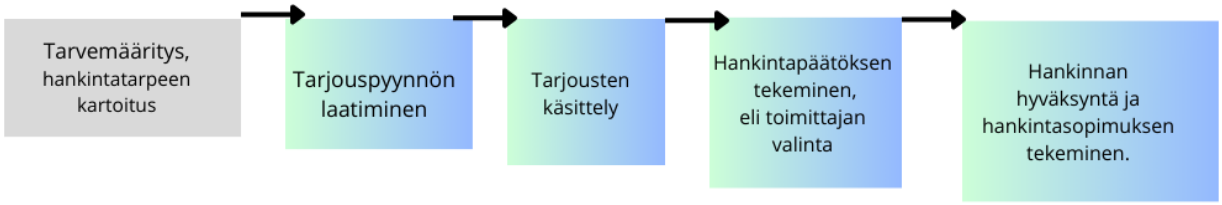
Tiedostettiin, että lomakkeen kehittäminen vaatii huolellista suunnittelua, sillä eri liiketoiminnoilla on omat tarpeensa. Tavoitteena oli kuitenkin tuottaa lisäarvoa opinnäytetyölle ja toimeksiantajalle. Tästä syystä päätettiin luoda riskien arviointilomakkeelle pohja, hyödyntämällä sekä määrällisen että laadullisen tutkimuksen tuloksia.

Relevanttien kysymysten valinta lomakkeelle tehtiin tutkimustulosten perusteella. Sekä laadullisen että määrällisen tutkimuksen tuloksista kävi ilmi, että organisaation tarpeisiin sopivin ratkaisu olisi

todennäköisesti kaksi erilaista riskien arviointilomaketta. Yksi lomake olisi suunnattu konsulttitoimittajille ja toinen järjestelmä- ja ylläpitotoimittajille. Tämä varmistaisi, että kunkin toimittajatyypin erityispiirteet ja riskit otetaan asianmukaisesti huomioon arvioinnissa.

Kuitenkin päätettiin pitäytyä alkuperäisessä suunnitelmassa ja luoda yksi riskien arviointilomake, joka olisi suunnattu erityisesti IoT-liiketoiminnan toimittajille. Tässä yhteydessä kysymysten valinnassa keskityttiin järjestelmä- ja ylläpitotoimittajiin, jotka ovat olennainen osa IoT-toimitusketjua.

Lomakkeen tarkoituksena on toimia osana hankintaprosessia ja mahdollisesti myös osana toimittajasuhteiden vuosittaista arviointia. Tämä helpottaa toimittajan riskien arviointia tehokkaasti samalla kun dokumentaatio tallennetaan jatkuvaa seurantaa varten. Digita Oy: toimittajien hankintaprosessi noudattaa samankaltaista runkoa kuin yleisimmät hankintaohjeet, jotka on kuvattu eri teoreettisissa lähteissä. Prosessin kuvaus on esitetty kuviossa 34.




Kuvio 34. Toimittajan hankinnan prosessi

Ensimmäinen vaihe hankintaprosessissa on hankintatarpeen kartoitus ja hankinnan suunnittelu. Tässä vaiheessa organisaatiossa määritellään tarvittavat tuotteet tai palvelut ja otetaan huomioon palveluiden hankinnassa tarvittavat näkökulmat. Yleensä tähän vaiheeseen kuuluu myös markkinakartoituksen tekeminen, jossa selvitetään erilaisia vaihtoehtoja ja määritellään palvelulta tai sen tarjoajalta vaadittavat ominaisuudet. (Huuhka 2022, 219.)

Seuraavana vaiheena on tarjouspyynnön laatiminen. Tarjouspyyntö on laadittava erittäin huolellisesti, jotta siitä ei jää epäselvyyksiä tai tulkinnanvaraisuuksia. Tarjouspyynnössä määritellään esimerkiksi haluttu palvelu, odotetut laatu- ja muut ominaisuudet sekä niiden painotukset tarjouksia

arvioitaessa. Lisäksi voidaan asettaa tarjoajille vähimmäisedellytyksiä, kuten luotettavuutta, taloudellista luottokelpoisuutta tai teknisiä vaatimuksia. (Huuhka 2022, 219.) Tässä vaiheessa toimittajan riskien arviointilomakkeen tarkoituksena on tarjota tietoa jo aikaisemmin hyväksytyistä toimittajista, joilla on kyseiset laatu- tai muut ominaisuudet. Tämä mahdollistaa sen, että hankintaprosessissa organisaatio voi kohdistaa tarjouspyynnöt jo tarkastetuille toimittajille, mikä voi säästää aikaa ja resursseja. Lisäksi se auttaa varmistamaan, että valituilla toimittajilla on tarvittavat ominaisuudet ja laatu täyttämään organisaation tarpeet ja vaatimukset.

Kun hankintailmoitus on julkaistu ja tarjousaika on umpeutunut, siirrytään tarjousten käsittelyvaiheeseen. Tarjoukset käsitellään luottamuksellisesti ja avataan, jotta organisaatio voi arvioida tarjoajien soveltuvuutta ja vertailla niitä keskenään. (Huuhka 2022, 219.) Toimittajan riskien arviointilomakkeen tarkoituksena on tässä vaiheessa mahdollistaa organisaation tarpeen arvioida tarjoajien soveltuvuutta ja vertailla tarjouksia keskenään luotettavasti ja systemaattisesti. Lomake tarjoaa strukturoidun kehyksen, jonka avulla voidaan kerätä ja analysoida tietoa eri toimittajista, kuten sertifikaateista, toimintatavoista sekä niihin liittyvistä riskeistä.

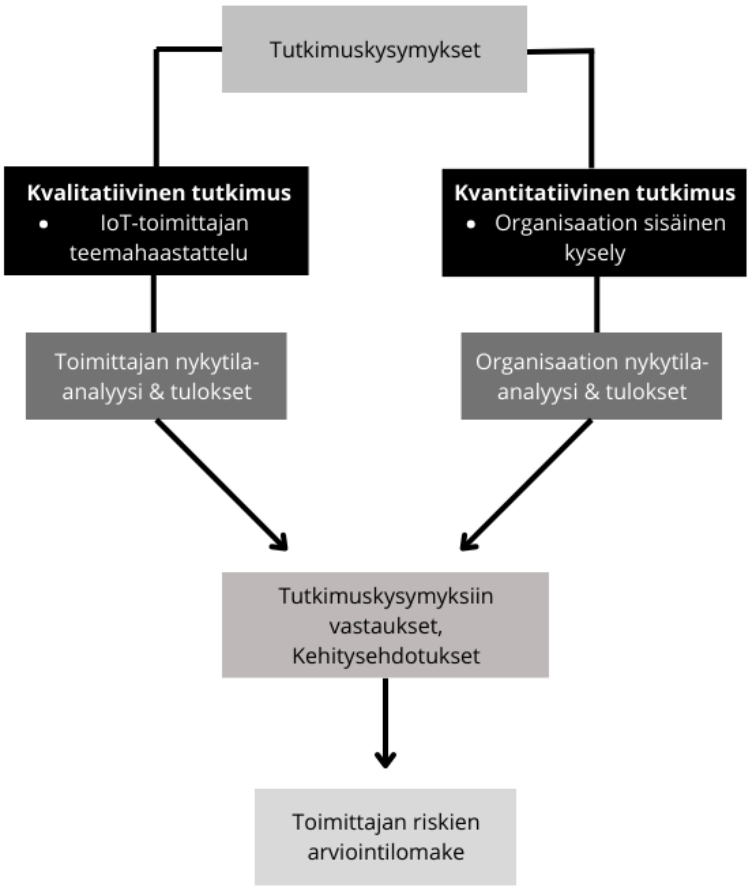
Tarjousten käsittelyn jälkeen siirrytään hankintapäätöksen tekemiseen eli toimittajan valintaan. Toimittajan valinnasta laaditaan kirjallinen perustelu, jossa perustellaan valitun tarjouksen valintaa. Tämän jälkeen siirrytään hankinnan hyväksymiseen organisaatiossa ja hankintasopimuksen tekemiseen. (Huuhka 2022, 219.) Toimittajan riskien arviointilomakkeen tiedot voivat tukea hankintapäätöksen tekemistä antamalla lisätietoa toimittajien riskiprofiileista ja auttamalla organisaatiota valitsemaan turvallisimmat ja luotettavimmat toimittajat.

Edellä mainitun prosessin lisäksi toimittajan riskien arviointilomake tulee osaksi hankinnan hyväksymistä. Lomakkeen täyttäminen ja tallentaminen järjestelmään mahdollistaa toimittajan riskien arvioinnin dokumentoinnin. Tämä varmistaa, että arviointi on suoritettu asianmukaisesti ja että organisaatio voi tarvittaessa osoittaa, että toimittajien riskit on otettu huomioon ja suoritettu asianmukaisesti. Lomakkeen avulla voidaan myös suorittaa säännöllisiä tarkastuksia ja päivityksiä toimittajien riskiprofiileihin. Tämä mahdollistaa riskienhallinnan jatkuvan parantamisen ja varmistaa, että toimittajat täyttävät jatkossakin organisaation asettamat vaatimukset.

### 4.3.1 Riskien arviointilomakkeen suunnittelu ja toteutus

Yhdessä toimeksiantajan kanssa päätettiin kehittää toimittajan riskien arviointilomaketta hyödyntäen Microsoft PowerApps-sovellusta. PowerApps valikoitui työkaluksi, koska se on ollut jo organisaatiossa käytössä, ja sen avulla organisaatio voi vaivattomasti integroida erilaisia tietolähteitä ja automatisoida prosesseja jatkokehityksessä.

Lomakkeen runkoon valikoitiin kysymykset sekä laadullisten että määrällisten tutkimustulosten perusteella. Kuviossa 35 esitetään opinnäytetyöprosessin eri vaiheet, joista viimeinen oli toimittajan riskien arviointilomakkeen luominen. Lomakkeen tavoitteena on myös tarjota työkalu opinnäytetyön kehitysehdotusten toteuttamiseen, ja se voidaan tarvittaessa kehittää vastaamaan eri liiketoimintojen yksilöllisiä tarpeita tulevaisuudessa.




Kuvio 35. Opinnäytetyöprosessin vaiheet - toimittajan riskien arviointilomakkeeseen asti.

Lomakkeeseen valittiin yhteensä kolmetoista erilaista kohtaa, joihin toimittajasopimuksesta vastaava henkilö vastaa (ks. liite 4). Etukäteen oli sovittu toimeksiantajan kanssa, että aluksi 10–15 kohdan määrä lomakkeella on sopiva ja että sitä voidaan kehittää käytännön kokemuksen myötä, kun lomake on otettu käyttöön.

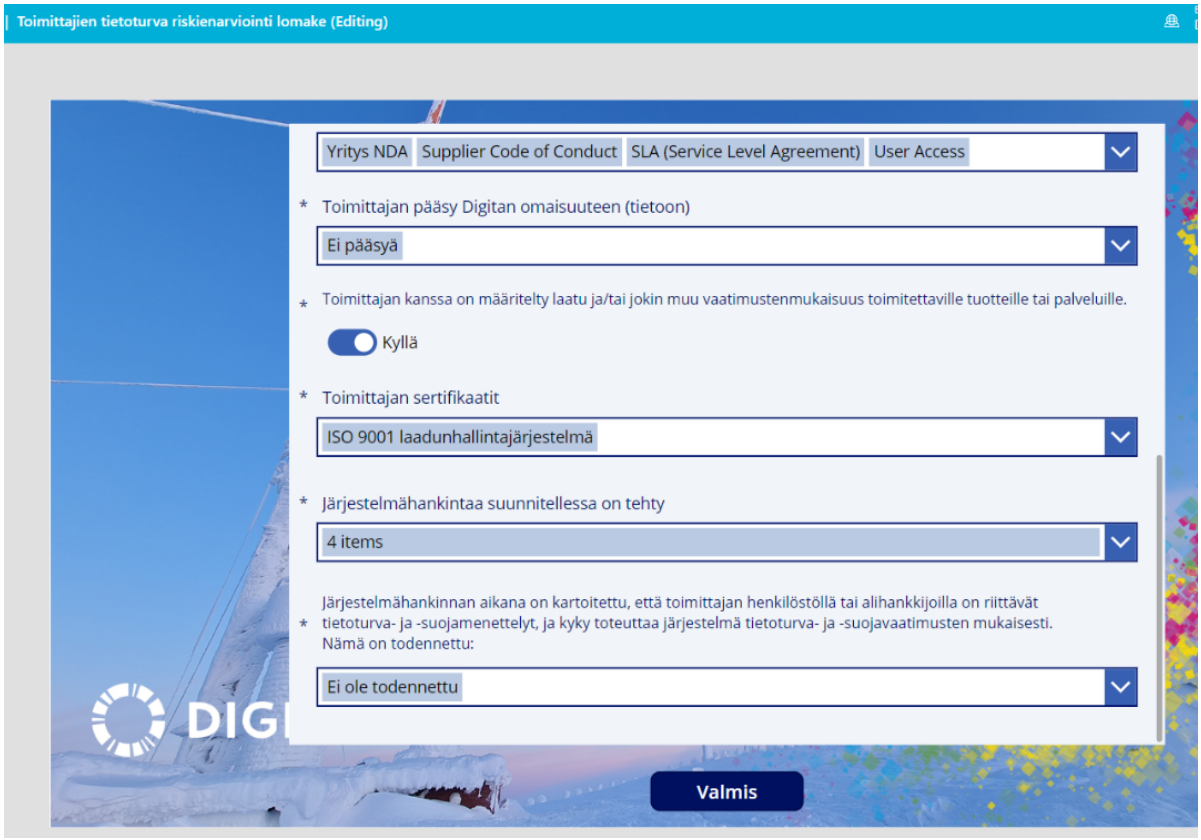
Lomakkeessa toistuu sama teema kuin määrällisessä tutkimuksessa. Kysymykset, jotka on valittu lomakkeelle, palvelevat Digitan asettamia toimittajan tietoturvallisuustason vaatimuksia. Lomake luotiin PowerApps-sovelluksella, ja sen data siirtyy automaattisesti organisaation SharePoint-järjestelmään, josta sitä jatkokehitetään tulevaisuudessa esimerkiksi automaation avulla.

Lomake toteutettiin siten, että ensin SharePoint-alustalla luotiin kysymyspohja, joka sisälsi kaikki valitut kysymykset ja niihin liittyvät tiedot. Tämä pohja määritti, mitä tietoja haluttiin kerättävän ja tallennettavan.

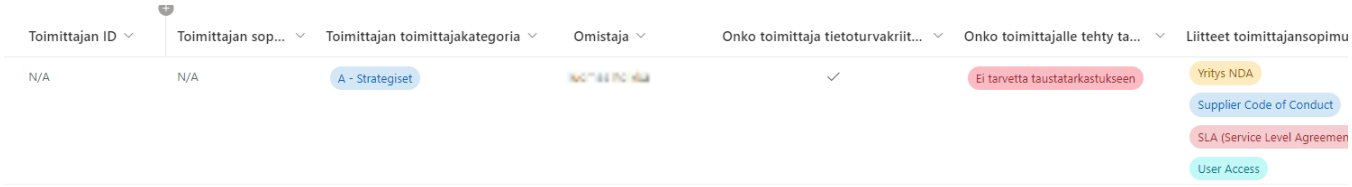
Seuraavaksi siirryttiin PowerApps-sovellukseen, jonka avulla luotiin uusi lomakepohja. Uuteen lomakkeeseen linkitettiin aiemmin SharePointiin luotu kysymyspohja. Linkitys mahdollisti kysymysten suoran tuonnin SharePointista lomakkeelle.

Lomakkeen pohjaa muokattiin halutunlaiseksi värimaailmaltaan, kenttien kokoa ja sisältöä hieman säädettiin, ja lisäksi siihen lisättiin toiminnallinen painike. Tämä painike oli niin sanottu ’Valmis’-painike, joka mahdollistaa vastausten tallentamisen SharePointiin.

Kokonaisuudessaan toteutetut toimenpiteet yhdistävät SharePointin ja PowerApps-sovelluksen toiminnan tehokkaasti, tarjoten organisaatiolle helpon tavan kerätä ja tallentaa tietoja. Lisäksi lomaketta voidaan helposti mukauttaa ja laajentaa toiminnallisuuksia tarpeiden mukaan. Tavoitteena oli luoda käyttäjäystävällinen, yksinkertainen, ja selkeä toimiva lomake. Lopuksi lomaketta testattiin yhdellä toimittajalla varmistaen, että lomakkeen täyttäminen ja tietojen siirtyminen tapahtuu sujuvasti ja ongelmitta SharePointin ja PowerApps-sovelluksen välillä. Testaus on esitetty kuvioissa 36 ja 37.




Kuvio 36. Toimittajan riskien arviointilomakkeen testausta.




Kuvio 37. Lomakkeen testaus - Tiedon siirtyminen PowerApps-sovelluksesta SharePointiin.

Lomakkeen täyttäminen sujui moitteettomasti, ja tiedon siirtyminen SharePointiin tapahtui välittömästi painikkeen 'Valmis' painamisen jälkeen. Koko lomake on esitetty tarkemmin liitteessä 5.

# 5 Johtopäätökset & keskeisten tulosten tarkastelu

## 5.1 Kvalitatiivinen tutkimus – IoT-toimittajan teemahaastattelu

Tärkeimpänä tutkimuksen tuloksena oli kahden toimittajaan kohdistuneen tutkimuskysymyksen vastausten saaminen. Tutkimuskysymykset ja niihin tiivistetyt vastaukset esitetään alla, sekä taulukossa 1 tiivistetään tutkimuksen keskeisimmät löydökset, sekä esitetään selkeä yhteenveto tuloksista.

1. **Toimiiko IoT-toimittaja tietoturvavaatimuksien osalta toimittajasopimuksen mukaisesti?**

   Kyllä, IoT-toimittajan tietoturvallisuudentaso vastaa toimittajasopimuksen vaatimuksia, koska käytössä olevat tietoturvallisuuden hallintakeinot olivat selkeästi laajemmat kuin toimittajasopimuksessa on vaadittu.

2. **Onko organisaation toimittajasopimusta tietoturvavaatimusten osalta tarpeellista päivittää?**

   Toimittajasopimusta katseltaessa riskiksi nousi, että tietoturvallisuuden vaatimukset toimittajalle ovat suppeat. Vaikka toimittaja on kehittänyt itse aktiivisesti tietoturvallisuuden hallintajärjestelmää, pitää nykyaikaiset vaatimukset olla selkeästi kirjattuna osaksi toimittajasopimuksen vaatimuksia.

   Lisäksi toimittajalla ei ole tällä hetkellä velvollisuutta seurata Digita Oy:n toimittajien tietoturvallisuusvaatimuksia, joka on yksi tärkeä osa Digitan tietoturvallisuuden ja riskien hallintaa. Toimittajasopimusta on jo pelkästään näiden tulosten perusteella ajankohtaista päivittää.

Tutkimuskysymyksien vastauksien lisäksi keskeiset tulokset ovat lisätiedot, jotka voidaan esittää toimeksiantajalle toimittajasuhteen parantamiseksi ja siihen liittyvien riskien arvioimiseksi. Seuraavassa taulukossa on vielä esitelty tiivistettynä saadut tulokset ja niistä tehdyt johtopäätökset IoT-toimittajan teemahaastattelusta.

Taulukko 1. Keskeiset tulokset – IoT-toimittajan teemahaastattelu.

| | Tulokset |
|---|---|
| **Toimittajan toimintamallit, prosessit ja menettelyt** | Teemahaastattelun sisältöanalyysi paljasti toimittajan nykyiset tietoturvallisuuden toimintamallit, prosessit ja menettelyt. |
| **Toimittajasopimuksen tietoturvavaatimukset** | Tietoturvavaatimukset IoT-toimittajan toimittajasopimuksessa olivat suppeat, mikä voi johtua siitä, että Digitalla ei ollut vielä otettu käyttöön toimittajan tietoturvallisuusvaatimuksia-liitettä sopimuksen solmimishetkellä. |
| **Toimittajan tietoturvallisuuden kehittäminen** | Toimittaja oli aktiivisesti kehittänyt tietoturvallisuuden prosessejaan ja oli kiinnostunut yhteistyöstä Digita Oy:n kanssa prosessien hallittavuuden ja läpinäkyvyyden parantamiseksi. |
| **Kommunikointi** | Toimittaja avoimesti ilmaisi kiinnostuksensa parantaa yhteistä viestintää Digita Oy:n kanssa ja luoda yhteistyössä viestintäkanava, erityisesti häiriötilanteisiin liittyvää viestintää varten. Tämä parantaisi reagointinopeutta ja valmiutta NIS2-direktiivin raportointivelvoitteita. |
| **Tietoturvallisuuden hallintajärjestelmä** | IoT-toimittaja oli aktiivisesti parantanut tietoturvaprosessejaan. He kehittävät tietoturvallisuuden hallintajärjestelmää, ja he ilmoittivat kehittävänsä sitä ISO 27001-standardin vaatimusten mukaisesti. Toimittajalla oli tavoitteena ISO 27001-sertifiointi tulevaisuudessa. |
| **Toimittajasopimuksen päivittämisen tarve** | Analyysi osoitti tarpeen päivittää toimittajasopimusta, erityisesti toimittajan tietoturvallisuusvaatimusten osalta, koska nykyiset vaatimukset eivät vastanneet Digita Oy:n nykyisiä tietoturvavaatimuksia toimittajille. |
| **Kehityskohteet** | Dokumentaatioon liittyen toimittajalla oli vielä selkeitä puutteita. Sen myötä heräsi kysymyksiä siitä, miten prosessit todellisuudessa toimivat häiriötilanteissa, jos dokumentaatiota ei ole saatavilla tai se on puutteellista. Puutteellisen dokumentaation myötä herää myös kysymys siitä, miten henkilöstöä on koulutettu toimimaan prosesseissa ja onko prosessien ja käytäntöjen tuntemus rajoittunut vain muutamiin avainhenkilöihin. |

## 5.2 Kvantitatiivinen tutkimus – Digita Oy:n sisäinen kysely

Kyselytutkimuksen keskeisin tulos oli saada tietoa Digita Oy:n nykyisen hankintaprosessin toimivuudesta toimittajien tietoturvariskien arviointiin, ja tunnistaa siihen liittyvät mahdolliset kehityskohteet. Tutkimuskysymys, johon pyrittiin tutkimuksella saamaan, vastaus oli seuraava:

3. **Tarvitseeko toimeksiantajan nykyprosessia toimittajien tietoturvallisuuden riskien arvioinnin tekemiseen kehittää?**

   Tulosten perusteella voidaan todeta, että suurin osa määritellyistä toimenpiteistä toimittajan tietoturvallisuuden tason riskien arvioinnissa toteutuu.

   Kuitenkin havaittiin, että liitteiden määrä sopimuksissa oli yllättävän alhainen. Erityisesti Supplier Code of Conduct-liite (Digitan hyvän liiketavan periaatteet), oli liitetty vain kolmen toimittajan sopimukseen (18 %), ja Digitan tietoturvavaatimukset toimittajalle-liite oli mukana vain kahdessa sopimuksessa (12 %). Vaikka yli puolet vastaajista (53 %) ilmoitti toimittajan kuuluvan tietoturvakriittisiin toimittajiin. Vastausten perusteella prosessin seurantaa on vaikea toteuttaa ja varmistaa, että vaaditut toimenpiteet suoritetaan asianmukaisesti. Tämän vuoksi prosessin seurantaa tulisi kehittää.

Taulukko 2 sisältää Digitan sisäisen kyselyn keskeisimmät tulokset, tiivistettynä selkeäksi yhteenvedoksi.

Taulukko 2. Keskeiset tulokset ja johtopäätökset – Organisaation sisäinen kysely.

| | **Tulokset** |
|---|---|
| **Toimittajien kategoriat** | Enemmistö vastauksista (41 %) oli strategisia toimittajia, kun taas noin kolmasosa (35 %) yleisiä toimittajia ja loput (24 %) kyvykkäitä toimittajia. Muita toimittajakategorioita ei mainittu vastauksissa. |
| **Tietoturvakriittiset toimittajat** | Hieman yli puolet vastaajista (53 %) ilmoitti toimittajan kuuluvan tietoturvakriittisiin toimittajiin.<br><br>Tämä korostaa tarvetta varmistaa näiden toimittajien tietoturvallisuuden riittävä taso. Tuloksia tarkemmin tarkasteltaessa, vain 2 toimittajalla oli liitteenä toimittajan tietoturvallisuusvaatimukset, mutta kriittisiä toimittajia oli 9 kpl, mikä viittaisi tarpeeseen tarkastella tehtyjä toimittajasopimuksia ja niiden vaatimuksia. |

| | |
|---|---|
| **Sopimuspohjat** | Selkeä enemmistö (80 %) vastanneista käytti toimittajan sopimuspohjaa toimittajasopimusten laatimisessa, kun taas vain noin viidesosa (18 %) käytti Digitan sopimuspohjaa.<br><br>Tämä tulos osoittaa luottamusta toimittajien valmiisiin sopimusehtoihin. Kuitenkin herättäen kysymyksen, miksi Digitan sopimuspohjaa käytetään selkeästi harvemmin. |
| **Liitteet sopimuksissa** | Neljänneksellä vastaajista (24 %) ei ollut lainkaan allekirjoitettuja tai annettuja liitteitä toimittajasopimuksissa. Yleisimmät liitteet olivat Yritys NDA (salassapitosopimus) ja Supplier Code of Conduct (Digitan hyvän liiketavan periaatteet).<br><br>Erityisesti Digitan tietoturvavaatimukset toimittajalle-liite oli liitteenä kahdessa sopimuksessa (12 %) mikä on huolestuttava tulos, kun yli 9 toimittajaa oli tietoturvakriittisiä toimittajia. |
| **Sertifikaatit** | Suurimmalla osalla toimittajista (59 %) oli yksi tai useampi sertifikaatti, kun taas noin 41 %:lla ei ollut sertifiointia lainkaan. Yleisimpiä sertifikaatteja olivat ISO 9001 laadunhallintajärjestelmä ja ISO/IEC 27001 tietoturvallisuuden hallintajärjestelmä.<br><br>Melko suurella osuudella toimittajista ei ollut yhtään sertifikaattia. Tämä voi osoittaa tarvetta selkeyttää ja tiukentaa toimittajien sertifiointivaatimuksia, jotta Digita voi varmistaa laadun ja turvallisuuden vaatimuksien täyttyminen kaikilta toimittajilta. |
| **Järjestelmätoimittajien toimenpiteet** | Lähes kaikille järjestelmätoimittajille (80 %) oli määritelty liiketoimintavaatimukset järjestelmähankinnan suunnitteluvaiheessa, mutta uhkamallinnusta ei ollut tehty yhdellekään toimittajalle.<br><br>Koska uhkamallinnusta ei ollut tehty useimmissa tapauksissa, tämä tulos voi viitata siihen, että riskien hallintaa ja turvallisuuden arviointia pitäisi kehittää järjestelmähankintojen suunnitteluvaiheessa. |
| **Ulkoisen toimittajan tietoturva- ja suojamenettelyt** | Yli puolet vastaajista (60 %) ilmoitti, että ulkoisten toimittajien henkilöstön ja alihankkijoiden tietoturva- ja suojamenettelyt sekä kyky toteuttaa järjestelmä tietoturva- ja suojavaatimusten mukaisesti oli todennettu jollain tavalla.<br><br>Kuitenkin, 40 %:lle todennusta ei ollut tehty lainkaan. Tämä tulos korostaa tarvetta vahvistaa ulkoisten toimittajien tietoturvavaatimuksia ja varmistaa, että kaikki toimittajat täyttävät organisaation asettamat vaatimukset. |

## 5.3 Kehittämisehdotukset

Laadullisen sekä määrällisen tutkimuksen tuloksissa tunnistettiin useita kehityskohteita liittyen toimittajahankintaprosessiin ja toimittajasopimusten hallintaan. Näiden kehitysehdotusten tavoitteena on parantaa toimeksiantajan organisaation kykyä hallita toimittajien tietoturvallisuusvaatimuksia ja niiden seurantaa sekä riskien arviointia. Kehitysehdotukset esitetty tiivistettynä taulukossa 3.

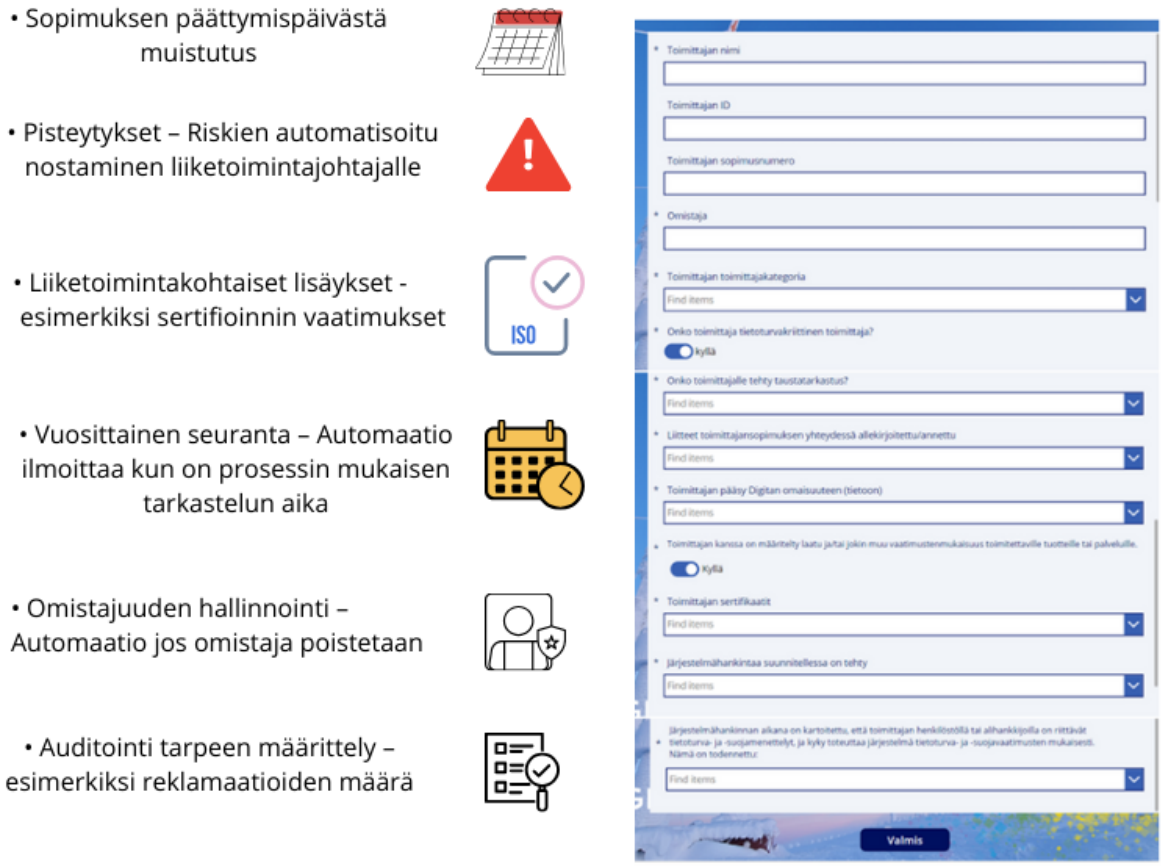
Taulukko 3. Tutkimuksien tulosten perusteella esitetyt kehittämisehdotukset.

| Kehittämisehdotukset | |
|---|---|
| **1. Toimittajahankinnan prosessin aktiivinen seuranta ja ylläpitäminen** | Organisaation tulisi seurata tarkemmin toimittajahankintaprosessin määriteltyjen vaatimusten toteutumista erityisesti strategisten ja tietoturvakriittisten toimittajien osalta. Hankintaan liittyvät vaatimukset on tarkasti määritelty, ja niiden aktiivinen seuranta ja ylläpitäminen on tärkeää, että voidaan varmistaa toimittajien noudattavan asetettuja vaatimuksia.<br><br>Lisäksi Digita voisi harkita tietoturvavaatimusten vakioimista ja niiden pakollista sisällyttämistä kaikkiin toimittajasopimuksiin. |
| **2. Toimittajasopimuksien ylläpito** | On tärkeää kehittää tehokkaampia menetelmiä toimittajasopimusten omistajuuden seurantaan ja ylläpitoon. Sopimuksissa esiintyi omistajuusongelmia, ja organisaatio voisi siksi esimerkiksi harkita automaation käyttöönottoa tässä prosessissa, jotta varmistetaan, että sopimukset ovat ajantasaisia ja vastaavat organisaation tarpeita. |
| **3. Yli kaksi vuotta vanhojen toimittajasopimusten tietoturvavaatimuksien tarkastelu** | Vanhojen toimittajasopimusten tarkastelu uusien toimittajan tietoturvavaatimusten osalta. Organisaation tulisi tarkastaa vanhat sopimukset vastaamaan nykyisiä vaatimuksia (ISO 27001 &NIS2), mikä parantaisi tietoturvaa ja vähentäisi riskejä. |
| **4. Läpinäkyvän viestinnän edistäminen toimittajien kanssa** | Läpinäkyvän viestinnän edistäminen toimittajien kanssa, erityisesti kriittisten tilanteiden hallinnassa. Organisaatio voisi rohkaista avointa viestintää toimittajien kanssa, erityisesti tietoturvahäiriöiden tai muiden ongelmien yhteydessä, jotta voidaan nopeasti reagoida ja minimoida mahdolliset haitat. (NIS2-raportointivelvoite) |

| | |
|---|---|
| **5. Toimittajan riskiarviointilomakkeen käyttöönotto osana hankintaprosessia ja mahdollisesti myöhemmin osana seurantaa.** | Toimittajan riskiarviointilomakkeen käyttöönotto riskienhallinnan kannalta. Lomake tarjoaa strukturoitua lähestymistapaa toimittajien arviointiin ja sen avulla voisi mahdollistaa automatisoidun seurannan ja päivityksen sopimuksille. Tämä parantaisi toimittajasopimuksien hallintaa, dokumentaatiota, prosessin vaatimuksien toteutumista ja mahdollisesti vähentäisi riskejä hankintaprosessissa. |
| **6. Sertifiointivaatimusten päivittäminen** | Koska osalla toimittajista ei ollut sertifikaatteja lainkaan, Digitan olisi hyvä tarkistaa ja tiukentaa sertifiointivaatimuksia varmistaakseen kaikkien toimittajien laadun ja turvallisuuden tason. Tämä voi auttaa parantamaan toimitusketjun vakautta ja luotettavuutta. |
| **7. Liitteiden käytön vahvistaminen toimittajasopimuksissa** | Koska tietoturvakriittisillä toimittajilla oli vähemmän liitteitä, Digitan tulisi varmistaa, että kaikki toimittajasopimukset sisältävät tarvittavat liitteet, erityisesti tietoturvaa koskevat vaatimukset. Tämä auttaa vähentämään riskejä ja parantamaan toimittajien vastuullisuutta. |
| **8. Ulkoisten toimittajien tietoturva- ja suojamenettelyjen vahvistaminen** | Vaikka suurin osa järjestelmätoimittajien vastaajista oli todentanut ulkoisten toimittajien tietoturva- ja suojamenettelyt, osalla ei ollut tehty tällaista arviointia lainkaan.<br><br>Digitan tulisi kehittää ja vahvistaa ulkoisten toimittajien tietoturvavaatimuksia ja varmistaa, että kaikki toimittajat täyttävät organisaation asettamat vaatimukset ja ne tarkistetaan sopimuksen tekovaiheessa. |

Toimittajan riskien arviointilomakkeen kehittämiseksi esitetään muutamia kehitysehdotuksia. Osa näistä toimenpiteistä olisi voitu ottaa käyttöön jo lomakkeen luontivaiheessa, mutta osa vaatimuksista sisältää luottamuksellista tietoa, minkä vuoksi niitä ei voitu sisällyttää.

Kuviossa 38 esitetään kehittämisehdotukset uudelle toimittajan riskien arviointilomakkeelle. Opinnäytetyön osana luotiin toimittajan riskien arviointilomakkeelle pohja, ja kehittämisehdotukset on suunniteltu parantamaan lomakkeen soveltuvuutta organisaation tulevaisuuden tarpeisiin entistäkin paremmin (ks. kuvio 38).




Kuvio 38. Toimittajan riskien arviointilomakkeen kehittämisehdotukset.

Kehittämisehdotuksena esitetään lomakkeelle liiketoimintakohtaisia lisäyksiä, jotka sisältäisivät esimerkiksi mahdollisen sertifioinnin vaatimukset. Lisäksi lomakkeen kysymysten pisteytys olisi tarpeellinen, jotta organisaatio voi havaita sen avulla mahdolliset riskit. Esimerkiksi jos lomakkeen tallennuksen yhteydessä puuttuu vaadittuja toimenpiteitä tai liitteitä kriittisen toimittajan sopimuksesta, hälytys voitaisiin automaattisesti nostaa. Tämä auttaisi tunnistamaan hankintaprosessiin liittyvät riskit ja varmistamaan, että kaikki olennaiset kohdat käsitellään prosessin ohjeiden mukaisesti.

Lisäksi kehitysehdotuksena esitetään vuosittaista seurantaa, jossa automaatio ilmoittaa, milloin sopimuksen tarkastelu on prosessin ohjeiden mukaisesti ajankohtainen. Omistajuuden hallinnointiin liittyen voitaisiin käyttää automaatiota, joka nostaisi hälytyksen, mikäli toimittajan omistajaa ei

ole määritelty. Auditoinnin tarpeen määrittely olisi myös tarpeellinen. Esimerkiksi useamman reklamaation määrän perusteella, mikä auttaisi resurssien priorisoinnissa ja auditointien kohdistamisella niihin toimittajiin, joille se olisi tarpeellinen toteuttaa.

Viimeisenä ehdotuksena sopimuksen lähestyvän päättymispäivän muistutus, joka auttaisi varmistamaan, että sopimukset uusitaan tai päivitetään ajoissa.

Toimittajan riskien arviointilomakkeen kehittäminen ja päivittäminen on myös organisaatiolle jatkuva prosessi, joka vaatii huolellista suunnittelua ja aikataulutusta. Kuviossa 39 on esitelty vuosikelloehdotus, jossa hahmotellaan askel askeleelta toimintoja, jotka ovat tarpeen lomakkeen kehittämiseksi ja sen tehokkaan käytön takaamiseksi organisaatiossa. Vuosikellon avulla voidaan varmistaa, että käyttäjien kehitysehdotukset otetaan huomioon ja että lomakkeen kehitystyö jatkuu sujuvasti ja aikataulutettuna. Kuviossa esitetään ehdotuksena millainen vuosikello lomakkeen kehitykseen voisi olla. Sen avulla organisaatio voi suunnitella ja toteuttaa toimenpiteitä riskienhallinnan parantamiseksi ja toimittajasuhteiden hallinnan tehostamiseksi.


Kuvio 39. Vuosikello lomakkeen kehitykseen ja ylläpitoon

# 6 Pohdinta

## 6.1 Tutkimustyön luotettavuus

Luotettavuutta voidaan määrällisessä tutkimuksessa tarkastella arvioimalla validiteettia ja reliabiliteettia. Validiteetilla tarkoitetaan, että tutkitaan oikeita asioita, kun taas reliabiliteetti tarkoittaa pysyvyyttä tutkimustuloksissa, eli samojen tuloksien saamiseen, jos tutkimus toistettaisiin. (Kananen 2015, 343–350.)

Kyselytutkimuksen osalta reliabiliteetti on korkea, sillä tutkimuksen tarkoitus, otanta ja kysymykset on kuvattu tässä työssä, mikä helpottaisi kyselyn toistamista. Kyselyn tuloksen voitaisiin odottaa olevan samankaltainen, sillä vastaajat vastaisivat kysymyksiin samalla tavalla, perustuen viimeisen vuoden aikana tehtyihin toimittajasopimuksiin. Otanta kyselyyn oli huolellisesti harkittu ja kohdennettu, joten kyselyn uusiminen ei todennäköisesti muuttaisi tutkimusaineiston tulosta, ellei vastausprosessi kyselyyn olisi korkeampi.

On kuitenkin tärkeää ottaa huomioon kyselytutkimuksen vastausprosentti, joka oli 57 %. Korkeammalla vastausprosentilla tulokset olisivat luotettavuudeltaan laadukkaammat. Puuttuvat 43 % tehdyistä toimittajasopimuksista viimeisen vuoden ajalta voivat vaikuttaa tuloksia suuntaan tai toiseen, tai nostaa uusia epäkohtia. Kuitenkin jo saadulla vastausprosentilla havaittiin selkeästi prosessissa olevat kehityskohteet ja tarpeet.

Kyselytutkimuksen validiteetti on selvitetty organisaation sisäisten prosessikuvausten ja tutkimuskysymysten näkökulmasta. Ennen kysymysten laatimista ohjeita ja dokumentaatiota toimittajiin ja hankintoihin liittyen on tarkasteltu. Lisäksi teoriapohjaa, joka liittyy aiheen standardeihin ja direktiiviin, on tarkasteltu eri luotettavista lähteistä.

Määrällisen kyselytutkimuksen laatuun vaikutti myös verkkokyselyn kysymyksien katselmointi liiketoimintajohtajan kanssa ennen kuin ne luotiin Microsoft Forms -sovelluksella. Kun kysymykset oli lisätty verkkosovellukseen, kokonaisuus testattiin vielä kerran. Katselmoinnin ja testauksen avulla voitiin korjata laadullisia virheitä, kuten kirjoitusvirheitä, tarkentaa ja parantaa kysymysten rakennetta sekä rajata kyselyyn vain relevantit kysymykset.

Luotettavuutta reliabiliteetin ja validiteetin avulla ei voida soveltaa laadullisessa tutkimuksessa. Sen sijaan laadullisen tutkimuksen luotettavuuden arvioinnissa voidaan käyttää tarkkaa dokumentaatiota, jota ulkopuoliset arvioijat tarkastelevat vertaisarvioinnin avulla. Dokumentaation kautta vertaisarviointia tehdessä, tekijöiden pitäisi päästä samaan lopputulokseen kuin tutkija. Tällöin tulkinta on ristiriidaton. Yksinkertaisin tapa arvioida luotettavuutta on antaa aineiston kohdehenkilöllä luettavaksi ja tulkittavaksi. Jos kohdehenkilö vahvistaa tutkijan tekemän tulkinnan ja tuloksen, tutkimuksen voidaan katsoa luotettavaksi. Toimeksiantaja voi tosin olla tulkinnassaan eri mieltä, mikä voi aiheuttaa ongelmia. (Kananen 2015, 352–353.)

Laadullisen tutkimuksen suunnitteluvaiheessa haastattelurungon kysymyksien sisällöstä keskusteltiin toimeksiantajan asiantuntijan kanssa, jotta saatiin kokonaiskuva millaisiin tutkimuskysymyksiin, toimeksiantaja haluaa vastauksia, kuitenkaan paljastamatta luottamuksellisia tietoja. Täten pystyttiin varmistamaan, että tutkimuksessa tutkitaan oikeita asioita. Laadullinen tutkimus dokumentoitiin tarkasti joka vaiheessa, kun se suunniteltiin etukäteen, toteutettiin ja analysoitiin yksityiskohtaisesti.

Tutkimuksen teemahaastattelun videon pohjalta kirjoitettu sanasta sanaan litterointi tarkistettiin toisella haastatteluun osallistuneella asiantuntijalla, jotta tutkijan omat näkemykset vastauksista ei vääristäisi haastattelun vastauksia. Tarkastus suoritettiin ennen sisällönanalyysin aloittamista, jotta käsiteltävä aineisto säilyisi mahdollisimman laadukkaana ja sanoma pysyisi muuttumattomana.

Sisällönanalyysin tulokset käytiin lisäksi läpi toimeksiantajan kanssa, jotta tutkijan tulkinnat eivät vääristäisi tuloksia. Litteroinnin vahvistaminen toisen tulkinnalla vahvisti materiaalin oikean tulkinnan luotettavuutta. Lisäksi käytetty vertaisarviointi vahvisti tutkimuksen tulosten luotettavuutta.

## 6.2 Tutkimustyön eettisyys

Tutkimustyön alussa toimeksiantajan kanssa sovittiin, että toimittajien anonymiteetti säilytetään, ja toimittajista puhutaan yleisellä tasolla, kuten "toimittajista" tai "IoT-toimittaja". Tämä päätös tehtiin eettisistä syistä, sillä opinnäytetyössä käsiteltiin tietoturvallisuusprosesseja. Laadullisessa teemahaastattelussa osallistujien nimiä ei myöskään mainittu, vaan esiteltiin heidän roolinsa organisaatiossa.

Kaikki laadullinen ja määrällinen tutkimusmateriaali, mukaan lukien kysymykset, käytiin läpi toimeksiantajan kanssa ennen niiden sisällyttämistä opinnäytetyöhön. Vaikka keskusteltiin myös liitteiden salaamisen tarpeesta opinnäytetyön alussa, päätettiin yhdessä toimeksiantajan kanssa, että salaamista tuskin tarvitaan. Tätä kysymystä kuitenkin tarkasteltiin aktiivisesti koko opinnäytetyön ajan mahdollisten muutosten varalta.

Laadullisen teemahaastattelun tallentamiseen käytettiin Teams-sovellusta, ja kaikilta haastatteluun osallistujilta pyydettiin lupa tallentamiseen. Lisäksi kaikki osallistujat informoitiin haastattelun sisällöstä ja kysymyksistä etukäteen. Teemahaastattelun tallenteen omistajuus on toimeksiantajalla, ja aineistoa säilytettiin heidän tietokoneellaan. Lisäksi tallenne ovat kaikkien osallistujien saatavilla.

Laadullisessa tutkimuksessa hyvän tieteellisen käytännön mukaisesti, käytettiin tarkkuutta teemahaastattelun kysymyksien luonnissa. Tutkimuksen suunnitteluvaiheessa haastattelurungon kysymyksien sisällöstä keskusteltiin toimeksiantajan asiantuntijan kanssa, jotta saatiin kokonaiskuva toimeksiantajan tarpeesta, kuitenkaan paljastamatta luottamuksellisia tietoja. Laadullinen tutkimus suunniteltiin etukäteen, toteutettiin ja raportointiin yksityiskohtaisesti.

Määrällisen tutkimuksen eettisyyteen kiinnitettiin erityistä huomiota, ja se korostui erityisesti kommunikaatiossa. Osallistujille kerrottiin kyselyn tarkoitus ja tavoitteet selvästi ennen kyselyn lähettämistä sisäisen uutiskanavan kautta, ja sama informaatio lisättiin myös Forms-kyselyn alkuun. Opinnäytetyön tuloksissa toimittajat ja kyselyyn vastanneet vastaajat käsiteltiin anonyymisti eettisistä ja tietoturvasyistä.

Forms-sovelluksen avulla toteutettu kysely tarjosi vastaajille joustavuutta vastata siihen omalla aikataulullaan, mutta vastaamiseen asetettiin kuitenkin aikaraja. Jokaiselle vastaajalle varattiin 7 arkipäivää aikaa vastaamiseen, ja tavoitteena oli, että kyselyyn vastaaminen veisi enintään 45 minuuttia. Tämä aika oli toimeksiantajan mukaan hyväksyttävä työaika kysymyksiin vastaamiseen. Kokonaisaikaa määriteltäessä otettiin huomioon, että osa vastaajista vastasi kyselyyn useamman kerran, ja keskimäärin yhden vastauksen kirjaaminen vei noin 10 minuuttia.

## 6.3 Kyselytutkimus & teemahaastattelu

Organisaation sisäinen kyselytutkimus rajattiin vuoden 2023 alusta vuoden 2024 alkuun asti tehtyihin uusiin toimittajasopimuksiin. Toimeksiantajan dokumentoinnin perusteella sopimuksia oli tehty yhteensä 30 kappaletta. Vastausprosenttia odotettiin kohtalaiseksi, koska kohderyhmä oli tarkasti harkittu, heitä oli informoitu, ja osallistettu kyselyn kehittämiseen, ja kysely oli lyhyt ja nopea täyttää.

Tiedostettiin kuitenkin, että kyselyn vastausmäärään saattoi vaikuttaa viikon vastausaika, joka oli ajallisesti rajallinen. Lopulta vastausprosentti laskettiin rajatun ajanjakson välillä tehtyjen toimittajasopimuksien kokonaismäärää verraten kyselyn vastausten määrään, eli 17 kappaleeseen. Kyselyn vastausprosentiksi muodostui 57 %, ja olimme siihen toimeksiantajan kanssa tyytyväisiä.

Kyselyn tuloksista saatiin monipuolista dataa toimittajien riskien arvioinnista ja tietoturvallisuuden tasosta. Tuloksiin oltiin tyytyväisiä, koska niiden avulla voitiin tarkastella prosessia itsessään ja sen kehityskohteita. Kokonaisuutena toimeksiantaja sai tärkeää tietoa prosessin tehokkuuden parantamiseksi, ja tunnistettiin selkeä tarve luoda toimittajan riskien arviointilomake prosessin seurantaa ja dokumentaation ylläpitoa varten.

IoT-toimittajan teemahaastattelun avulla saatiin luotua pohja kysymysten esittämiselle toimittajasopimuksia tarkasteltaessa. Haastattelun tulosten perusteella toimeksiantaja sai vahvistuksen tarpeelle päivittää yli vuoden vanhat toimittajasopimukset erityisesti tietoturvavaatimusten osalta. Lisäksi saatiin vastaus toiseen tutkimuskysymykseen, jonka tarkoituksena oli selvittää vastaako toimittajan tietoturvallisuuden taso toimittajasopimuksen vaatimuksien mukaisesti. Saatiin selville, että sopimus on allekirjoitettu silloin, kun Digitalla ei ole ollut vielä toimittajan tietoturvallisuusvaatimukset -liitettä, jonka takia sopimuksen päivittämistä suositeltiin, vaikka toimittajan tietoturvallisuuden taso vastasi sopimuksen vaatimuksia.

Haastattelu vaikutti positiivisesti Digitaan ja IoT-toimittajan väliseen viestintään, ja sen avulla saatiin keskustelu käyntiin yhteisen viestintäkanavan kehittämiseksi, erityisesti NIS2 raportointivelvoitetta ajatellen.

Määrällisen ja laadullisen tutkimuksen tuloksiin oltiin tyytyväisiä ja niiden tavoitteet toteutuivat. Haluttuihin tutkimuskysymyksiin saatiin vastaukset ja vielä lisäinformaatiota, jota organisaatio voi hyödyntää osana riskienhallintaa, IoT-liiketoiminnan tietoturvallisuuden hallintajärjestelmän kehittämistä, sekä sisäisten prosessien kehittämistä.

## 6.4 Toimittajan riskien arviointilomake

Toimittajan riskien arviointilomakkeen pohjan luominen oli haasteellista, erityisesti kysymysten rajaaminen melko pieneen määrään. Kuitenkin valittuihin kysymyksiin oltiin lopulta tyytyväisiä, ja erityisesti sisäisen kyselyn tulosten perusteella voitiin tunnistaa olennaiset seurannan kohteet sekä sisäisen prosessin vaatimukset, jotka olivat tärkeitä sisällyttää lomakkeeseen. Lomakkeen testaaminen sujui myös onnistuneesti, ja data siirtyi vaivattomasti PowerApps:in ja SharePoint:in välillä. Lomakkeen avulla toimeksiantajan on nyt helpompi lähteä toteuttamaan haluttuja toimenpiteitä, kun perusta on niin sanotusti valmiina.

Jatkoa ajatellen, toimittajan riskien arviointilomakkeen kehittäminen ja sen integroituminen osaksi toimittajahankintaprosessia olisi tärkeä askel organisaation riskienhallinnassa. Lomakkeen tavoitteena on yhtenäistää hankintaprosessia ja varmistaa toimittajan tietoturvallisuusvaatimusten täyttyminen sekä dokumentaation kattavuus. Aikaisemmin kaikkien toimittajien sopimusten tarkasteleminen sisäisestä järjestelmästä oli haasteellista. Lomakkeen avulla organisaatio voisi varmistaa, että tarvittavat tiedot olisivat helposti saatavilla ja dokumentoitu yhteen paikkaan.

Tulevaisuudessa, mikäli toimeksiantaja jatkaa lomakkeen kehittämistä, esimerkiksi ehdotetun automaation avulla, prosessin seuranta organisaatiossa tulee olemaan entistä tehokkaampaa ja läpinäkyvämpää. Näiden toimenpiteiden odotetaan vähentävän riskejä, jotka liittyvät uusien toimittajien arviointiin sekä olemassa olevien toimittajasopimusten ylläpitoon ja seurantaan.

Tutkijalla on mahdollisuus jatkaa työskentelyä toimeksiantajalle kehittämällä lomaketta organisaation tarpeisiin yksityiskohtaisemmaksi tulevaisuudessa. Kehitysvaihetta ei kuitenkaan aloitettu opinnäytetyön tekemisen aikana, koska sen rajaus oli tehty ajanhallinnallisista syistä lomakkeen pohjan luomiseen jo tutkimuksen suunnitteluvaiheessa. Lisäksi rajaus tehtiin eettisistä syistä, sillä jatkokehitykseen lisättävät tiedot ja tarkennukset ovat suurelta osin luottamuksellisia.

# Lähteet

Allen, B., Bapst, B. & Hicks, T.A. 2024. Building a Cyber Risk Management Program. E-Kirja. Sebastopol: O'Reilly Media. Viitattu 25.2.2024. https://janet.finna.fi, Ebook Central.

Calder, A. & Watkins, S. 2020. IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002, Seventh Edition. E-kirja. Kogan Page. Viitattu 28.1.2024. https://janet.finna.fi, Skillsoft Books ITPro.

Chopra, A. & Chaudhary, M. 2020. Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines. Viitattu 27.1.2024. https://janet.finna.fi, Skillsoft Books ITPro.

Digita Oy. N.d. Kauppalehti yrityshaku sivustolla. Viitattu 10.2.2024. https://www.kauppalehti.fi/yritykset/yritys/digita+oy/2488970-5.

Digita varmistaa luotettavan tiedonkulun jokaiselle suomalaiselle – myös poikkeusoloissa. 2023. Uutinen Digita Oy:n www-sivuilla. Viitattu 20.1.2024.https://www.digita.fi/ajankohtaista/digita-varmistaa-luotettavan-tiedonkulun-jokaiselle-suomalaiselle-myos-poikkeusoloissa/.

Digita yhtiönä. N.d. Tiedote Digita Oy:n www-sivuilla. Viitattu 20.1.2024. https://www.digita.fi/digita-oy/.

Direktiivi 2022/2555/EU. Euroopan parlamentin ja neuvoston kyberturvallisuusdirektiivi (NIS2-direktiivi). Euroopan unionin virallinen lehti 27.12.2022. Viitattu 16.4.2024. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32022L2555.

Direktiivi toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa (NIS2-direktiivi). 2023. Euroopan komission virallinen verkkosivusto. Viitattu 13.2.2024. https://digital-strategy.ec.europa.eu/fi/policies/nis2-directive.

Huomisen arvoinen digitaalinen toimintaympäristö. 2023. Digita Oy:n markkinointivideo YouTube-kanavalla 13.9.2023. Lataaja Digita Oy. Viitattu 20.1.2024. https://www.youtube.com/watch?v=7xXdWaP_PWc.

Huttunen, E. 2019. Riskienhallinta tietoturvassa. Uutinen Suomen Standardisoimisliitto SFS:n sivustolla 14.2.2019. Viitattu 3.2.2024. https://sfs.fi/riskienhallinta-tietoturvassa/.

Huuhka, K. 2022. Tehokkaan hankinnan työkalut. 6. uudistettu laitos. 8. painos. Helsinki: BoD - Books on Demand. Viitattu 20.3.2024.https://janet.finna.fi, Ellibs.

ISO 9000 Laadunhallinnan standardisarja. N.d. Suomen Standardisoimisliitto SFS ry www-sivuilla. Viitattu 13.4.2024. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-9000-laadunhallinnan-standardisarja/.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas. Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylän ammattikorkeakoulun julkaisuja 202. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kriik, G. 2019. Mitä on auditointi? Blogiteksti. Julkaistu 26.8.2019. Viitattu 21.2.2024. https://www.arter.fi/mita-on-auditointi/.

Krueger, G. 2022. DQS www-sivujen blogi. Julkaistu 25.10.2022. Viitattu 14.4.2024. https://www.dqsglobal.com/fi-fi/opi/blogi/tietoturva-kohtaa-laadunhallinnan.

Laadunhallintajärjestelmä. 2024. Digi- ja väestötietoviraston verkkosivut. Viitattu 14.4.2024. https://www.suomi.fi/yritykselle/liiketoiminnan-kehittaminen/laadunhallinta/opas/tuotteen-laatu/laadunhallintajarjestelma.

Laadunhallinnan periaatteet. N.d. Suomen Standardisoimisliitto SFS ry www-sivuilla. Viitattu 13.4.2024. https://sfs.fi/osallistu-ja-vaikuta/aihealueet/johtaminen/laadunhallinnan-periaatteet/.

NIS2 Requirements. 2024. The NIS2 Directive www-sivuilla. Viitattu 10.2.2024. https://nis2directive.eu/nis2-requirements/.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. 3.–4. painos. Helsinki: Sanoma Pro Oy. Viitattu 9.3.2024. https://janet.finna.fi, Ellibs.

Pulkkanen, R. 2019. Laadunhallinnan periaatteet: ISO 9000-sarja PDF-tiedosto. Suomen Standardisoimisliitto SFS ry www-sivuilla. Viitattu 13.4.2024. https://sfs.fi/wp-content/uploads/2020/11/Laadunhallinnan-periaatteet-ISO-9000-sarja.pdf.

Robitaille, E.D. 2015. ISO 9001:2015 Handbook for Small and Medium-Sized Businesses, 3rd edition. E-kirja. La Vergne: ASQ Quality Press. Viitattu 13.4.2024. https://janet.finna.fi, Ebook Central.

SFS-EN ISO/IEC 27001:2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS ry. Julk. 09.2023. Digita Oy:n intranet. Vain sisäiseen käyttöön. Viitattu 1.2.2024.

SFS-EN ISO/IEC 27002:2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. Helsinki: Suomen Standardisoimisliitto SFS ry. Julk. 12/2023. Digita Oy:n intranet. Vain sisäiseen käyttöön. Viitattu 1.2.2024.

Tiedonhankinnan opas: Tiedonhaun suunnittelu. 2023. Aalto-yliopiston oppimiskeskuksen www-sivut. Viitattu 10.1.2024. https://libguides.aalto.fi/tiedonhankinta.

Traficom. 2024. Tärkeää tietoa Euroopan unionin kyberturvallisuusdirektiivistä (NIS2). 2024. Viitattu 13.4.2024. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tarkeaa-tietoa-euroopan-unionin-kyberturvallisuusdirektiivista#68867-1.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällön analyysi. E-kirja. Uudistettu laitos. Helsinki: Tammi. Viitattu 19.2.2024. https://janet.finna.fi, Ellibslibrary.

Watkins, S.G. 2022.ISO/IEC 27001:2022: An Introduction to Information Security and the ISMS Standard. E-kirja. Viitattu 31.1.2024. https://janet.finna.fi, Skillsoft Books ITPro.

What is NIS2?. 2024. The NIS2 Directive sivustolla. Viitattu 10.2.2024. https://nis2directive.eu/what-is-nis2/.

Who Does NIS2 Apply To?. 2024.The NIS2 Directive sivustolla. Viitattu 10.2.2024. https://nis2directive.eu/who-are-affected-by-nis2/.

# Liitteet

## Liite 1. Laadullisen teemahaastattelun kysymykset

**Information Security Management Systems (ISMS) — ISO/IEC 27001:2022 standard**

**5.19 Information Security in Supplier Relationships**

**5.20 Addressing information security within supplier agreements**

1. What kind of information security controls or/and defined processes does the Supplier have?

**Security Risks and Management:**

- How does the Supplier prepare for security risks from catastrophic events or major software incidents?
- Does the Supplier have procedures to manage security risks from its products or services, including cloud resources?
- How does the Supplier manage security risks from its information and assets, and from faults or weaknesses in its supplied products or services?

**Data and Information Management:**

- Has the Supplier identified ICT components that could affect the security of Customer's data?
- Does the Supplier have procedures to ensure data availability and recovery if needed?
- Does the Supplier have a method to securely destroy Customer's information when it's no longer needed?

**Compliance and Non-Compliance:**

- How does the Supplier deal with non-compliance with security rules?

**Disruptions and Exceptional Situations**:

- Can the Supplier handle disruptions and exceptional situations have related to its products and services?
- Does the Supplier have procedures to continue data processing if it can no longer supply its products or services?
- Does the Supplier have procedures for managing and reporting disruptions?

**Supplier Relationship and Subcontracting:**

- What rules does the Supplier follow in subcontracting? Do they have a list of subcontractors, and do they notify customers of changes?

**Training and Security:**

- Could the Supplier provide information on how they manage and control access rights to customer data, specifically in relation to Customer's information?
- Does the Supplier train its employees on operating rules and procedures that are affected by Customer's characteristics and access rights?
- What level of personnel and physical security is required from the Supplier's staff and premises?

## Liite 2. Kyselyn saateviesti

Tervetuloa osallistumaan kyselyyn, liittyen Digitan tietoturvan hallintamallin kehittämiseen.

Olen Maija Virta, Digitan IoT-tiimistä, ja työstän parhaillaan opinnäytetyötäni Digitalle.
Opinnäytetyöni keskittyy toimittajasuhteiden riskienhallinnan kehittämiseen.
Työni tavoitteena on vahvistaa Digitan riskienhallintaa ja parantaa toimittajasuhteiden tasoa tietoturvallisemmaksi osana tietoturvan hallintamallin kehittämistä,
sekä NIS2-direktiivin ja määräys 67 (Traficom) vaatimuksiin vastaamista.

Kyselyn aiheena on **toimittajan tietoturvariskien kartoitus**.

Tähän kyselyyn ovat saaneet kutsun osallistua ne henkilöt, jotka ovat vastuussa toimittajasuhteiden sopimuksista. Täytättehän kyselyn aktiivisesti ja omatoimisesti.

Kyselyyn voi vastata useamman kerran, ja sen tavoitteena on kerätä dataa vuoden 2023 alusta tähän päivään asti tehtyjen uusien toimittajasopimusten pohjalta. Kyselyä **ei tarvitse täyttää niiden toimittajien osalta**, joiden sopimus on tehty aikaisemmin.

- Riskikartoitus tulisi tehdä jokaiselle toimittajalle, jolle on tehty toimittajasopimus ilmoitetun ajanjakson sisällä.
- Ensimmäisen riskikartoituksen tekemiseen menee enemmän aikaa (noin 20 minuuttia), mutta sen jälkeen vastaaminen nopeutuu huomattavasti.
- Kyselyssä on 19–23 kysymystä, riippuen toimittajasta.
- Kyselyyn tulee vastata 7.3.2024 – 14.3.2024 välisenä aikana.

Huomioithan, jos uusia toimittajasopimuksia ei ole tehty kyseisenä ajanjaksona, pyydän ilmoittamaan siitä minulle, jotta tiedän etten odota sinulta vastauksia.

**Linkki kyselyyn:** **Siirry kyselyyn**

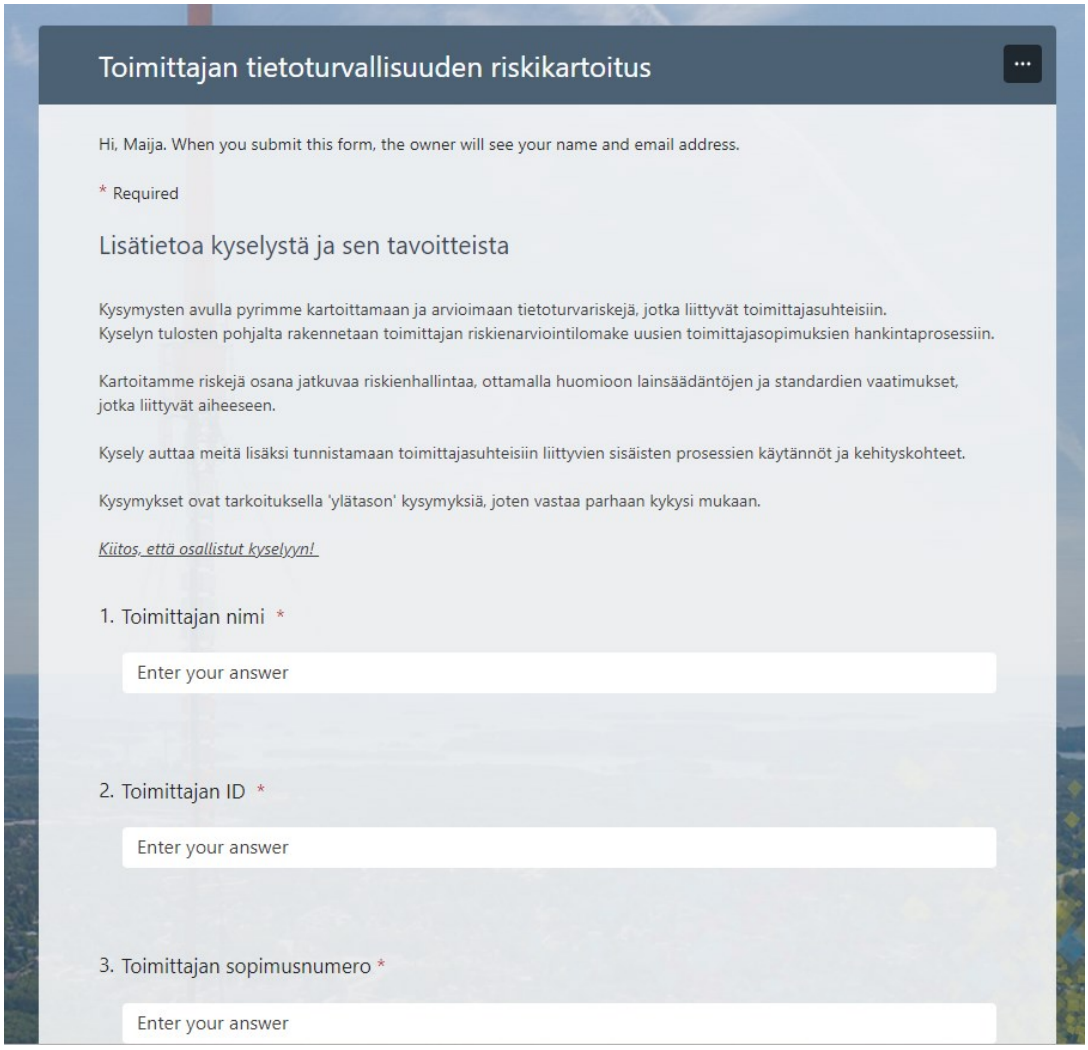
Toivon, että vastaat kyselyyn mahdollisimman pian, sillä se auttaa minua saamaan arvokasta tietoa toimittajasuhteiden nykytilasta ja kehitystarpeista.

Kiitos etukäteen osallistumisestanne ja yhteistyöstänne!

Ystävällisin terveisin,

Maija Virta

## Liite 3. Kyselytutkimuksen kysymykset

4. Mihin Digitan määrittelemään toimittajakategoriaan toimittaja kuuluu? *

- A - Strategiset
- B - Kyvykkäät
- C - Yleiset
- D - Poistettavat
- E - Muut

5. Kuuluuko toimittaja tietoturvakriittisiin toimittajiin? (Toimittaja voi kuulua esimerkiksi B toimittajakategoriaan ja olla tietoturvakriittinen toimittaja, siksi kysymys erikseen) *

- Kyllä
- Ei

6. Mikä on tietoturva omaisuuden toimittajan prioriteetti?

- Prioriteetti 1
- Prioriteetti 2
- Prioriteetti 3

7. Onko toimittajasopimuksen tekemisen yhteydessä käytetty Digitan vai toimittajan sopimuspohjaa? *

- Digitan sopimuspohja
- Toimittajan sopimuspohja

8. Mitä liitteitä toimittajansopimuksen yhteydessä on allekirjoitettu/annettu? *(Voit valita useita)* *

- [ ] Supplier Code of Conduct (Digitan vastuullisen toimintavan ohje toimittajille)
- [ ] Digitan tietoturvavaatimukset toimittajille
- [ ] Yritys NDA (Salassapitosopimus)
- [ ] Henkilökohtainen NDA
- [ ] SLA (Service Level Agreement)
- [ ] User Access
- [ ] PPA (Power Purchase Agreement)
- [ ] Jokin muu
- [ ] Ei mitään

9. Onko toimittajan kanssa otettu huomioon toimittajasopimusta tehdessä pääsynhallinnan turvallisuus? (Fyysinen turvallisuus sekä järjestelmäturvallisuus) *

- ◯ Kyllä
- ◯ Ei

10. Onko toimittajan työntekijöiden tai alihankkijoiden tarvetta liikkua Digitan tiloissa? *

- ◯ Kyllä, viikoittain
- ◯ Kyllä, kuukausittain
- ◯ Kyllä, kvartaaleittain
- ◯ Kyllä, kerran vuodessa
- ◯ Satunnaisesti
- ◯ Ei ollenkaan

11. Onko toimittajan työntekijöillä pääsy järjestelmän kautta Digitan omaisuuteen (tietoon)? *

- ◯ Kyllä
- ◯ Ei

12. Millaiseen luokiteltavaan tietoon toimittajalla on pääsy? Mieti toimittajan roolia, mitä tietoja pääsee käsittelemään/muokkaamaan. (Voit valita useita)

- [ ] Sisäinen
- [ ] Luottamuksellinen
- [ ] Salainen
- [ ] Julkinen

13. Onko toimittajalle tehty taustatarkastus? (Voit valita useita) *

- [ ] Taloudellinen taustatarkastus
- [ ] Turvallisuus (esim. SUPO, turvallisuuskortit ym.)
- [ ] Toimittajalle ei tarvetta tehdä taustatarkastusta
- [ ] Jokin muu

14. Onko toimittajalle tehty auditointi Digitan toimesta? (Osana hyväksyntäprosessia) *

- ◯ Kyllä
- ◯ Ei

15. Olisiko toimittajalle mielestäsi tarpeellista tehdä auditointi? (Riskienhallinnan näkökulmasta) *

- ◯ Kyllä
- ◯ Ei

16. Onko toimittajan kanssa määritelty laatu ja/tai mahdollisesti jokin muu vaatimustenmukaisuus toimitettaville tuotteille tai palveluille? (Toimitusketjun turvaaminen, lainsäädäntö, asiakas SLA) *

- ◯ Kyllä
- ◯ Ei

17. Onko toimittajalle tehty Digitan toimesta reklamaatioita? (Yleinen reklamointi, ei tietoturva) *

- ◯ Kyllä, harvoin (alle 3)
- ◯ Kyllä, usein (yli 3)
- ◯ Ei, mutta toimittajan kanssa on ollut muita haasteita
- ◯ Ei

18. Onko toimittajaan kohdistunut viimeisen vuoden aikana tietoturvahäiriöitä? (Esim. vaikutus: viranomaisviestintä, NIS2, Traficom. Tiedon eheys, luotettavuus ja saatavuus. *Voit valita useita)* *

- ☐ Ei
- ☐ Kyllä, palvelunestohyökkäys
- ☐ Kyllä, toimitusketjuhyökkäys
- ☐ Kyllä, tietomurto
- ☐ Kyllä, kiristyshaittaohjelma
- ☐ Kyllä, tietovuoto
- ☐ Kyllä, pilviympäristöjen poikkeamat
- ☐ Ei tiedossa

19. Onko toimittajalla jokin näistä sertifikaateista? *(voit valita useita)* *

- ☐ ISO 9001 laadunhallintajärjestelmä
- ☐ ISO/IEC 27001 tietoturvallisuuden hallintajärjestelmä
- ☐ ISO/IEC 27701 Tietosuoja
- ☐ ISO 22301 Turvallisuus ja kriisinkestävyys
- ☐ ISO 45001 työterveys- ja työturvallisuusjärjestelmä
- ☐ ISO 31000 riskienhallintajärjestelmä
- ☐ ISO 14001 ympäristöjärjestelmä
- ☐ Jokin muu
- ☐ Ei sertifiointia

20. Onko toimittaja järjestelmätoimittaja? *

- ◯ Kyllä
- ◯ Ei

21. Onko järjestelmähankintaa suunnitellessa tehty: *(voit valita useita)* *

- [ ] Järjestelmän kriittisyys ja palvelutasovaade (SLA)
- [ ] Järjestelmän liiketoimintavaatimukset
- [ ] Järjestelmän tietoturva- ja -suojavaatimukset
- [ ] Riskiarvio
- [ ] Uhkamallinnus
- [ ] Ei mitään edellisistä

22. Onko järjestelmähankinnan aikana kartoitettu, että ulkoisen toimittajan henkilöstöllä ja sen mahdollisilla alihankkijoilla on riittävät tietoturva- ja -suojamenettelyt, ja kyky toteuttaa järjestelmä tietoturva- ja -suojavaatimusten mukaisesti?

    Jos on, onko tämä todennettu:
    *

- [ ] Sertifikaatilla
- [ ] Auditoinnilla
- [ ] Jollain muulla tavalla
- [ ] Ei ole todennettu

23. **Kysely päättyy tähän.**

    **Kiitos paljon ajastasi ja kyselyyn vastaamisesta.**

    Avoin palaute (vapaaehtoinen)

    Enter your answer

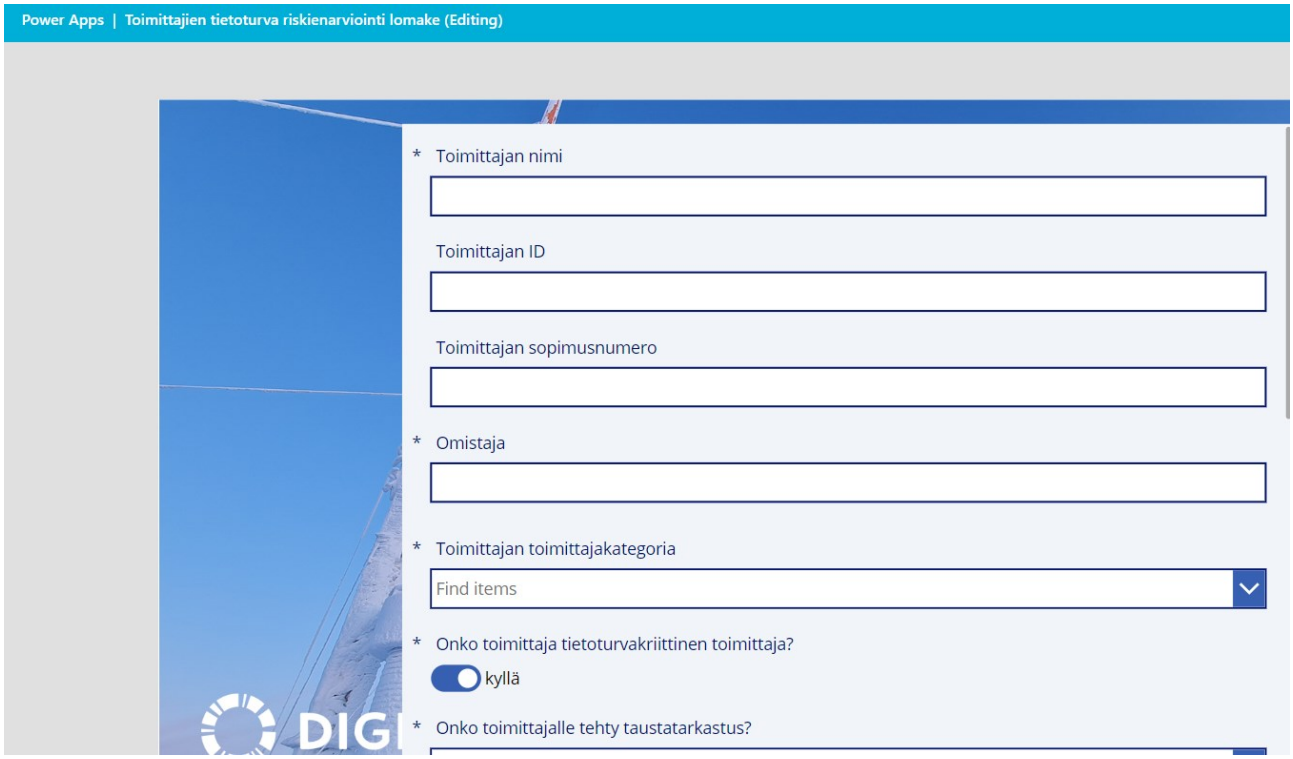
# Liite 4. Laadullisen teemahaastattelun kysymykset

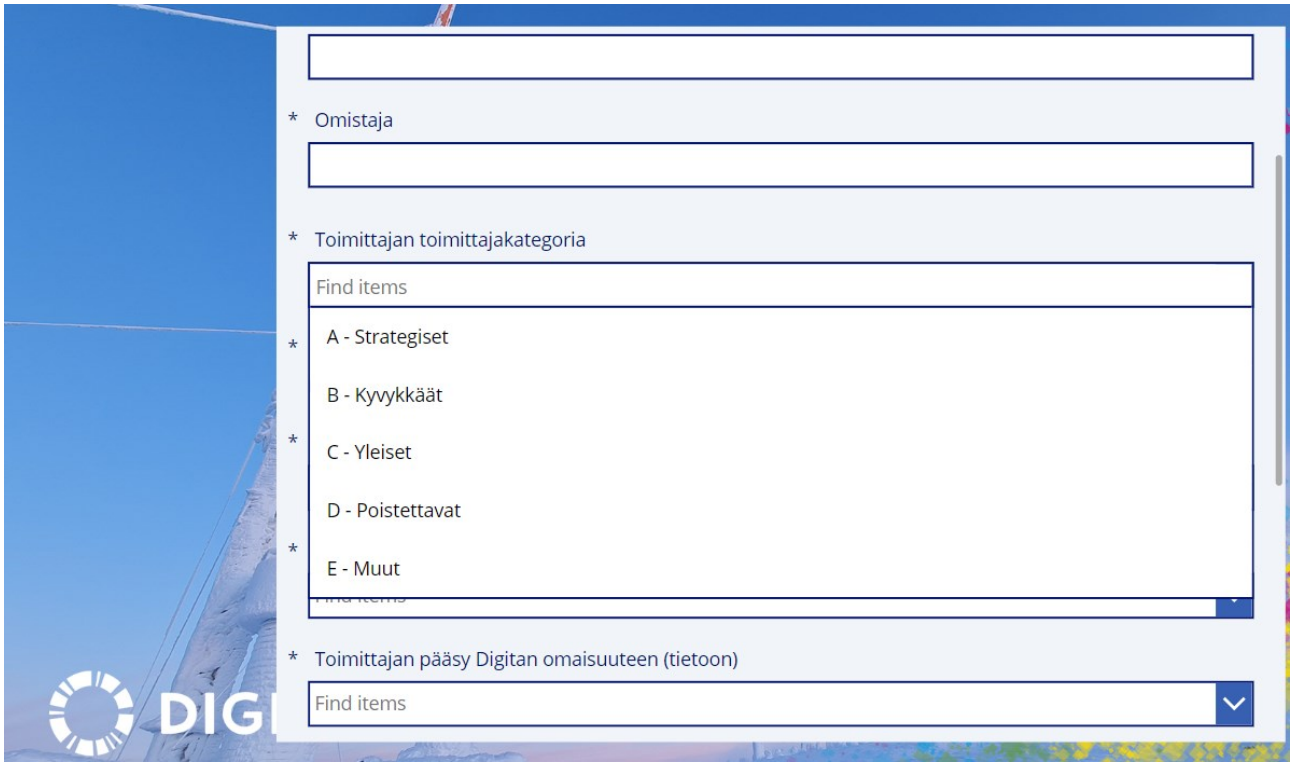
**Toimittajan riskiarviointilomakkeen sisältö**

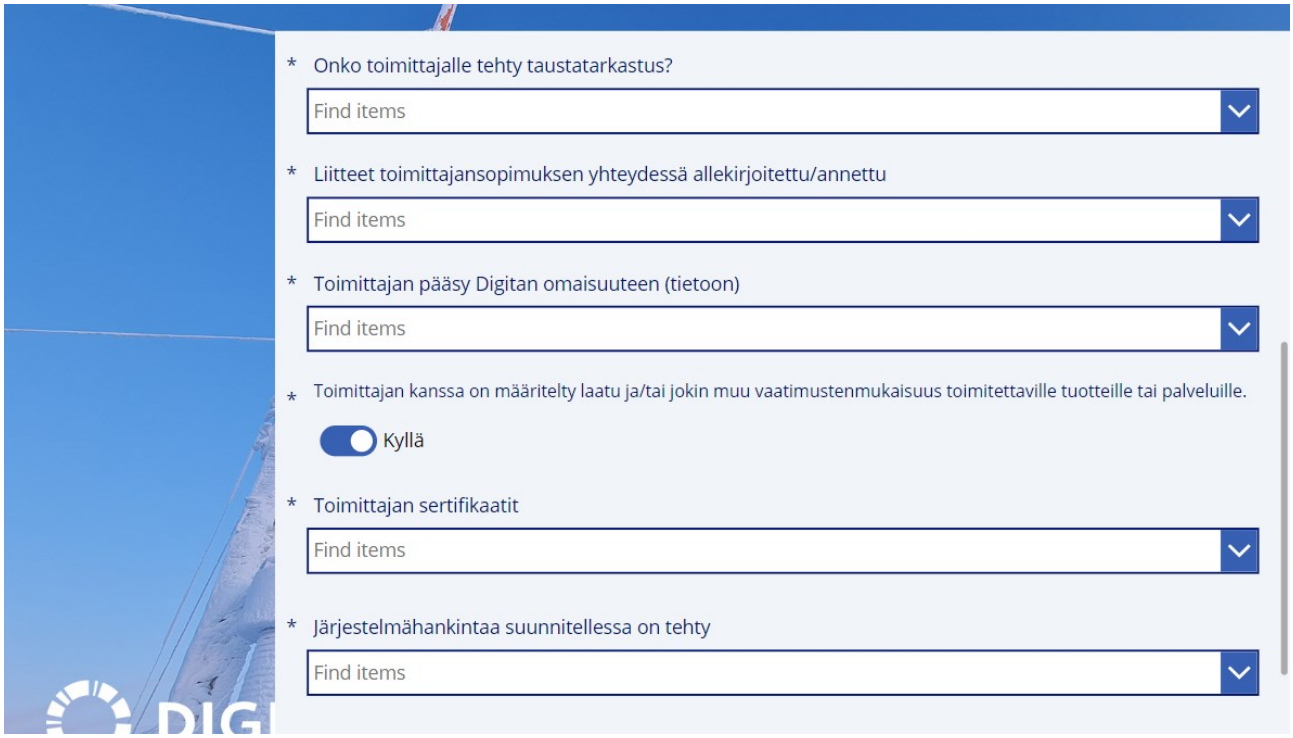
Järjestelmätoimittajat + ylläpitotoimittajat (järjestelmä- tai laitetoimittajat)

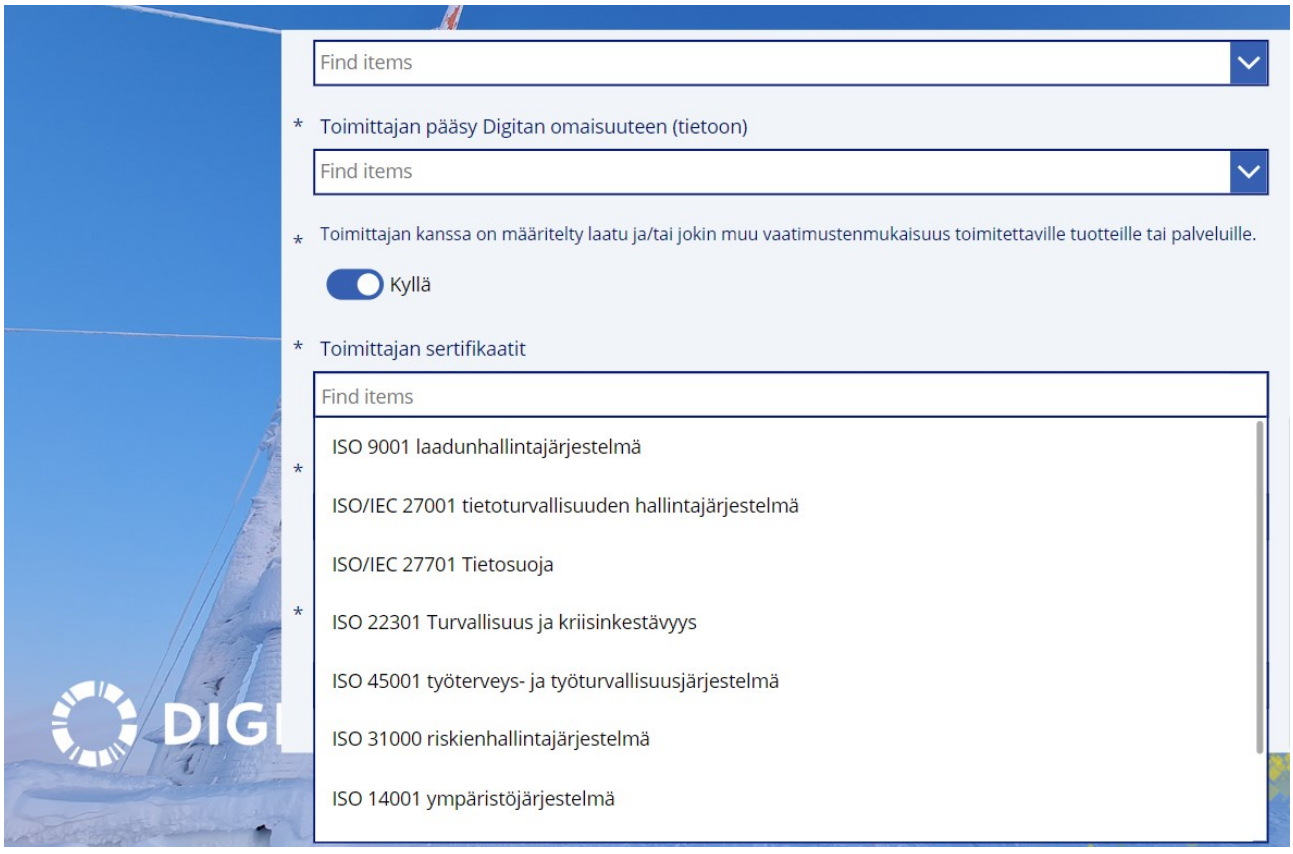
1. Toimittajan nimi
2. Toimittajan ID
3. Toimittajan sopimusnumero
4. Omistaja
5. Toimittajan toimittajakategoria
6. Onko toimittaja tietoturvakriittinen toimittaja?
7. Onko toimittajalle tehty taustatarkastus
8. Liitteet toimittajansopimuksen yhteydessä allekirjoitettu/annettu
9. Toimittajan pääsy Digitan omaisuuteen (tietoon)
10. Toimittajan kanssa on määritelty laatu ja/tai jokin muu vaatimustenmukaisuus toimitettaville tuotteille tai palveluille
11. Toimittajan sertifikaatit
12. Järjestelmähankintaa suunnitellessa on tehty
13. Järjestelmähankinnan aikana on kartoitettu, että toimittajan henkilöstöllä tai sen alihankkijoilla on riittävät tietoturva- ja suojamenettelyt, ja kyky toteuttaa järjestelmä tietoturva- ja suojavaatimusten mukaisesti. Nämä on todennettu:

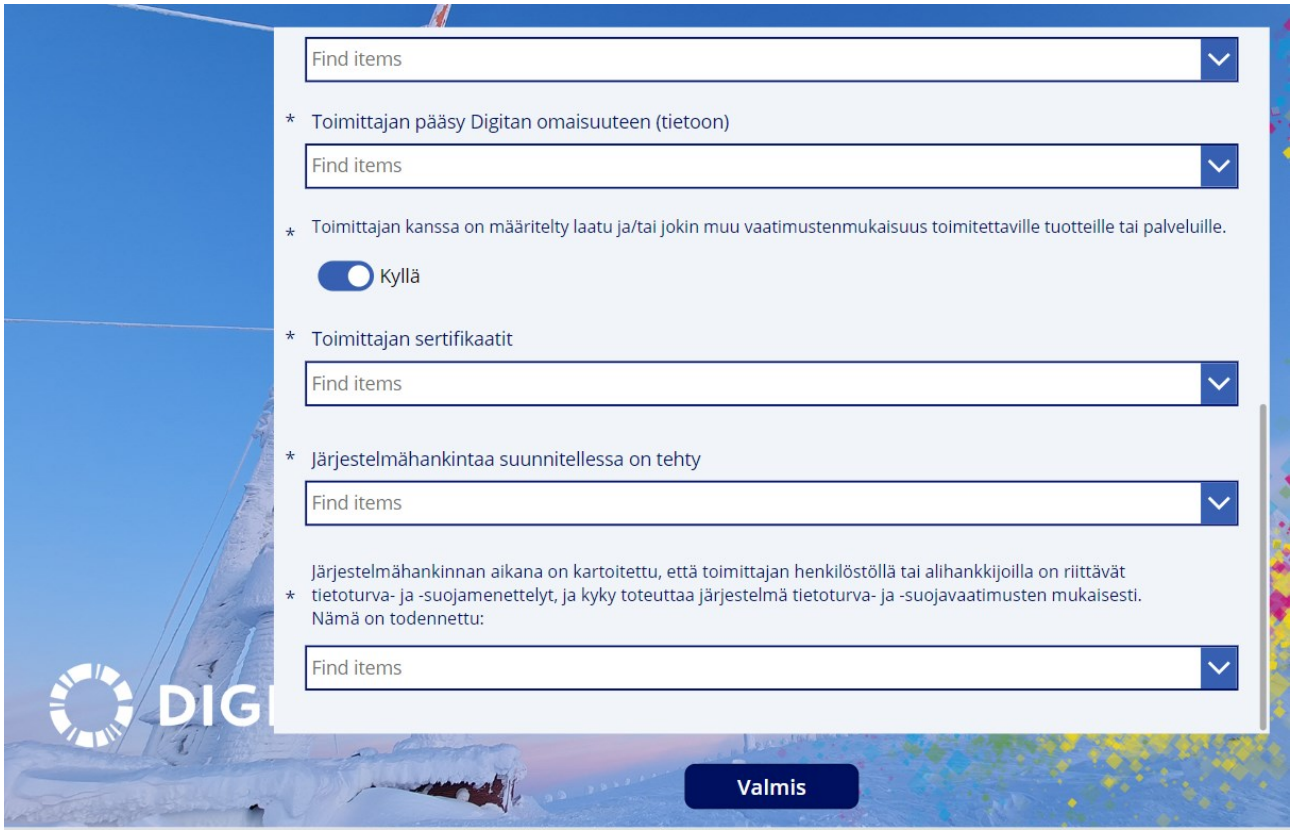
## Liite 5. Toimittajan riskiarviointilomakkeen pohja - Microsoft Power Apps

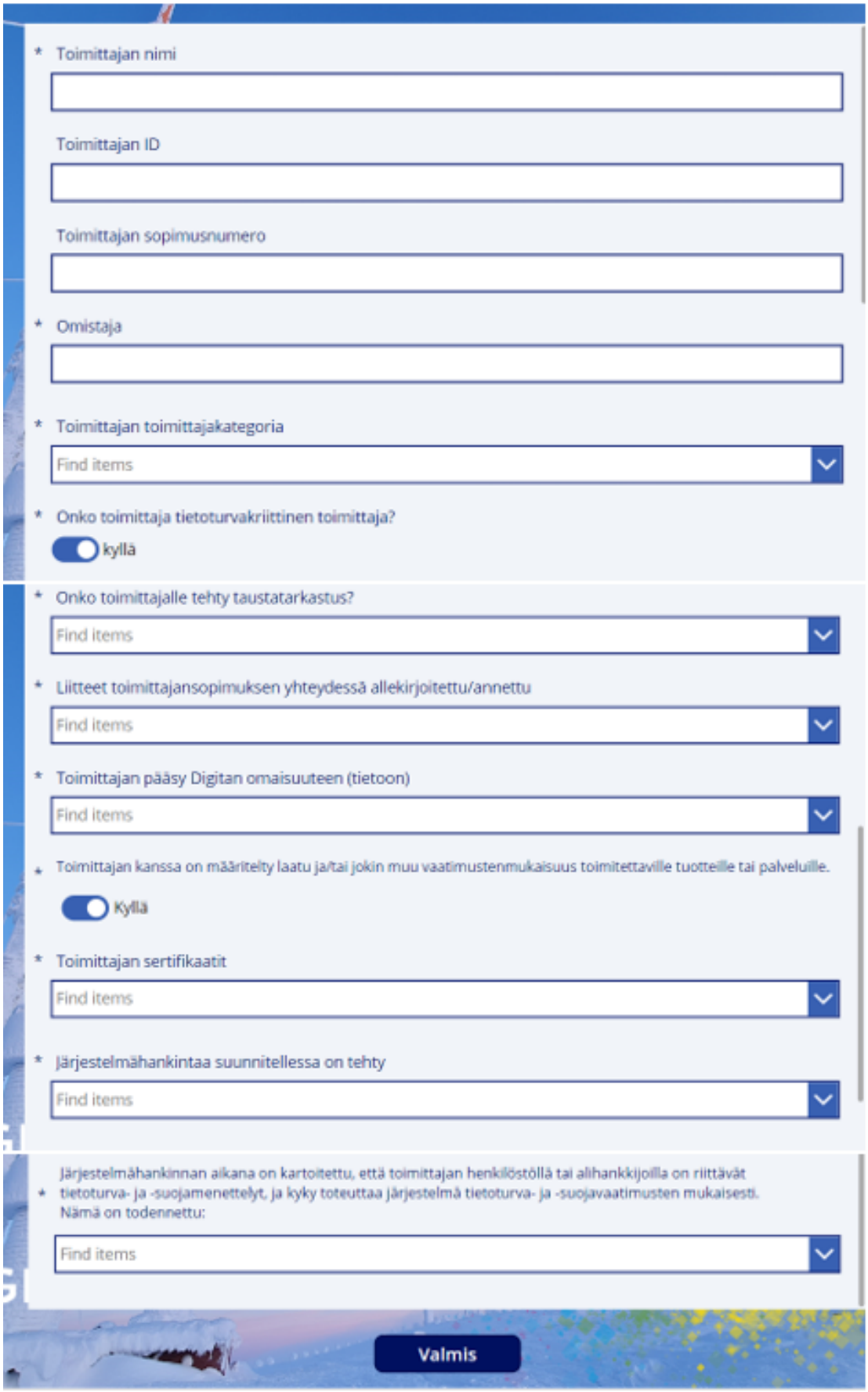



* Onko toimittajalle tehty taustatarkastus?
Find items
* Liitteet toimittajansopimuksen yhteydessä allekirjoitettu/annettu
Find items
* Toimittajan pääsy Digitan omaisuuteen (tietoon)
Find items
* Toimittajan kanssa on määritelty laatu ja/tai jokin muu vaatimustenmukaisuus toimitettaville tuotteille tai palveluille.
Kyllä
* Toimittajan sertifikaatit
Find items
* Järjestelmähankintaa suunnitellessa on tehty
Find items


Find items
* Toimittajan pääsy Digitan omaisuuteen (tietoon)
Find items
* Toimittajan kanssa on määritelty laatu ja/tai jokin muu vaatimustenmukaisuus toimitettaville tuotteille tai palveluille.
Kyllä
* Toimittajan sertifikaatit
Find items
ISO 9001 laadunhallintajärjestelmä
ISO/IEC 27001 tietoturvallisuuden hallintajärjestelmä
ISO/IEC 27701 Tietosuoja
ISO 22301 Turvallisuus ja kriisinkestävyys
ISO 45001 työterveys- ja työturvallisuusjärjestelmä
ISO 31000 riskienhallintajärjestelmä
ISO 14001 ympäristöjärjestelmä


Find items
* Toimittajan pääsy Digitan omaisuuteen (tietoon)
Find items
* Toimittajan kanssa on määritelty laatu ja/tai jokin muu vaatimustenmukaisuus toimitettaville tuotteille tai palveluille.
Kyllä
* Toimittajan sertifikaatit
Find items
* Järjestelmähankintaa suunnitellessa on tehty
Find items
* Järjestelmähankinnan aikana on kartoitettu, että toimittajan henkilöstöllä tai alihankkijoilla on riittävät tietoturva- ja -suojamenettelyt, ja kyky toteuttaa järjestelmä tietoturva- ja -suojavaatimusten mukaisesti. Nämä on todennettu:
Find items
Valmis


* Toimittajan nimi
Toimittajan ID
Toimittajan sopimusnumero
* Omistaja
* Toimittajan toimittajakategoria
Find items
* Onko toimittaja tietoturvakriittinen toimittaja?
kyllä
* Onko toimittajalle tehty taustatarkastus?
Find items
* Liitteet toimittajansopimuksen yhteydessä allekirjoitettu/annettu
Find items
* Toimittajan pääsy Digitan omaisuuteen (tietoon)
Find items
* Toimittajan kanssa on määritelty laatu ja/tai jokin muu vaatimustenmukaisuus toimitettaville tuotteille tai palveluille.
Kyllä
* Toimittajan sertifikaatit
Find items
* Järjestelmähankintaa suunnitellessa on tehty
Find items
* Järjestelmähankinnan aikana on kartoitettu, että toimittajan henkilöstöllä tai alihankkijoilla on riittävät tietoturva- ja -suojamenettelyt, ja kyky toteuttaa järjestelmä tietoturva- ja -suojavaatimusten mukaisesti. Nämä on todennettu:
Find items
Valmis