Pyry Waldén

NIS2-DIREKTIIVI JA VALMISTAVA TEOLLISUUS

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus

2024

Kaakkois-Suomen ammattikorkeakoulu

South-Eastern Finland University of Applied Sciences

Tutkintonimike	Insinööri (AMK)
Tekijä/Tekijät	Pyry Waldén
Työn nimi	NIS2-direktiivi ja valmistava teollisuus
Toimeksiantaja	Sulzer Pumps Finland Oy
Vuosi	2024
Sivut	52 sivua, liitteitä 3 sivua
Työn ohjaaja	Jaakko Nurmi

TIIVISTELMÄ

Opinnäytetyön tarkoitus oli selvittää NIS2-direktiivin asettamia vaatimuksia valmistavalle teollisuudelle, sekä miten kyseisiä vaatimuksia voisi lähestyä. Tutkimusongelmana on se, että valmistavan teollisuuden toimijat eivät välttämättä tiedä, miten he voisivat käytännössä lähestyä NIS2-direktiivin asettamia vaatimuksia johtuen otsikkotasoisista ja epätarkoista vaatimuksista sekä IT- ja OT-järjestelmien vaatimuksista ja eroavaisuuksista.

Tutkimusongelmasta johdettiin seuraavat tutkimuskysymykset: mistä NIS2-direktiivissä on kyse, mitä vaatimuksia NIS2-direktiivi asettaa valmistavalle teollisuudelle ja miten valmistavan teollisuuden toimijat voivat lähestyä NIS2-direktiivin asettamia vaatimuksia. Ensimmäiseen kahteen tutkimuskysymykseen vastattiin kirjallisuuskatsauksella, kun taas viimeiseen tutkimuskysymykseen valittiin kvalitatiivinen kehittämistutkimus, sillä tarkoituksena on ymmärtää ilmiötä ja luoda käytännön ohjeistus.

NIS2-direktiiviin ja sen vaatimuksiin hallintoelimen koulutuksesta, riskienhallinnasta, toimijaksi ilmoittautumisesta ja raportointivelvollisuudesta perehdyttiin ja niitä käsiteltiin valmistavan teollisuuden näkökulmasta. Riskienhallinnan vaaditut otsikkotasoiset kymmenen toimenpidettä paloiteltiin osiin käyttämällä luonnosta Suomen lakiesitysestä NIS2-direktiivin täytäntöönpanemiseksi. Paloitellut vaatimukset yhdistettiin parhaita käytäntöjä edustaviin standardeihin ja ohjeistuksiin, jotta vaatimuksiin saataisiin käytännön ohjeistusta.

Standardit ja ohjeistukset valittiin edustamaan sekä IT- että OT-järjestelmiä, jotta voidaan ottaa huomioon molempien muuttujat ja tarpeet. ISO/IEC 27001 -standardi ja NIST SP 800-53 -ohjeistus edustavat IT-järjestelmiä, kun taas IEC 62443-2-1 -standardi ja NIST SP 800-82 -ohjeistus edustavat OT-järjestelmiä.

Opinnäytetyön tuloksena selvitettiin mistä NIS2-direktiivissä on kyse, mitä vaatimuksia se asettaa valmistavalle teollisuudelle sekä luotiin ohjeistus NIS2-direktiivin asettamien vaatimusten lähestymiseksi. Ohjeistus NIS2-direktiivin vaatimuksien lähestymiseen toteutettiin valmistavan teollisuuden toimijan näkökulmasta, ottamalla huomioon IT- ja OT-järjestelmien eroavaisuudet.

Asiasanat: NIS2, Direktiivi, valmistus, teollisuus

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author (authors)	Pyry Waldén
Thesis title	NIS2-directive and industrial manufacturing
Commissioned by	Sulzer Pumps Finland Oy
Time	2024
Pages	52 pages, 3 pages of appendices
Supervisor	Jaakko Nurmi

ABSTRACT

The objective of this thesis was to determine what requirements NIS2 directive sets for industrial manufacturing and how those requirements could be interpreted.

NIS2 directive sets requirements concerning the training of management bodies, risk management, as well as registering and reporting obligations. In this study, these aspects were examined from the perspective of industrial manufacturing. The ten minimum requirements of risk management were divided into smaller parts based on a draft of Finland's proposal for the law regarding NIS2 directive's execution. After that, they were linked to standards and guidelines that represent the best practices.

The standards and guidelines were chosen to represent both IT and OT systems so that the needs of both could be considered. ISO/IEC 27001 standard and NIST SP 800-53 guideline were chosen to represent the IT systems, whereas IEC 62443-2-1 standard and NIST SP 800-82 guideline were chosen to represent the OT systems.

As the results of this thesis, NIS2 directive and the requirements it sets for industrial manufacturing were explained, and a guide was created for industrial manufacturers on interpreting the requirements set by this directive. The guide was made from the perspective of the industrial manufacturer, and it takes into account both IT and OT systems.

Keywords: NIS2, directive, manufacturing, industrial

SISÄLLYS

1 JOHDANTO

Kyberturvallisuuden kannalta 17.10.2024 on merkittävä päivä EU:ssa, sillä silloin astuu voimaan Network and Information security 2 -direktiivi eli NIS2-direktiivi. NIS2-direktiivin tavoite on parantaa EU:n kyberturvallisuutta ja se laajentaa merkittävästi aiemman NIS-direktiivin sisältämiä toimialoja, sekä asettaa vaatimuksia direktiivin alaisille toimijoille (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555).

Vaatimusten kannalta valmistavan teollisuuden alalla tulee ottaa huomioon myös IT- ja OT-jakauma, sekä niiden kyberturvallisuustarpeiden erot. IT eli information technology tunnetaan usein myös nimellä tietotekniikka, ja se käsittelee tiedon prosessointiin ja tallennukseen käytettävää ohjelmistoa ja laitteistoa. OT eli operational technology viittaa taas fyysiseen järjestelmään vaikuttamiseen, esimerkiksi teollinen ohjausjärjestelmä joka monitoroi ja ohjaa teollisia prosesseja. OT-järjestelmillä on omia vaatimuksia kyberturvallisuuteen liittyen johtuen esimerkiksi siitä, että poikkeamat voivat uhata ihmisten terveyttä ja turvallisuutta.

Tässä opinnäytetyössä on tarkoitus selventää kirjallisuuskatsauksen kautta NIS2-direkiiviä valmistavan teollisuuden näkökulmasta: mistä siinä on kyse ja mitä vaatimuksia se tuo. Kvalitatiivisen kehittämistutkimuksen kautta luodaan ohjeistus toimista, joilla valmistavan teollisuuden toimija voi lähestyä NIS2-direktiivin asettamia vaatimuksia.

NIS2-direktiivin asettamia vaatimuksia lähestytään parhaita käytäntöjä noudattamalla, käyttämällä standardeja ja ohjeistuksia. IT- ja OT-jakauma valmistavalla teollisuudella otetaan huomioon valitsemalla molempia edustavia parhaita käytäntöjä. IT-järjestelmiä edustaa ISO/IEC 27001 -standardi ja NIST SP 800-53 -ohjeistus hallintakeinoista, kun taas OT-järjestelmiä edustaa IEC 62443-2-1 -standardi ja NIST SP 800-82 -ohjeistus OT-turvallisuudesta. Huomioimalla sekä IT että OT, voidaan varmistaa valmistavan teollisuuden järjestelmien kokonaisturvallisuus suhteessa NIS2-direktiivin asettamiin vaatimuksiin.

Aihe valittiin, sillä valmistavan teollisuuden toimijoille saattaa olla epäselvää, minkälaisia vaatimuksia heihin kohdistuu NIS2-direktiivistä. Toimijoille saattaa myös olla epäselvää se, miten he voisivat lähestyä vaatimuksia, sillä NIS2-direktiivi ei anna tarkkoja ohjeistuksia ja käytännön vaatimuksia. Hyöty opinnäytetyössä on se, että valmistavan teollisuuden toimijat ymmärtävät heihin kohdistuvia NIS2-direktiivin asettamia vaatimuksia, jonka lisäksi he saavat IT- ja OT-järjestelmät huomioonottavaa ohjeistusta vaatimuksien lähestymiseen.

TUTKIMUSASETELMA

1.1 Tutkimusongelma

Tutkimusongelmana opinnäytetyössä on se, että valmistavan teollisuuden toimijat eivät välttämättä tiedä, miten he voisivat käytännössä lähestyä erilaisia direktiivin asettamia vaatimuksia, sillä direktiivi ei määrittele tarkkoja käytännön toimenpiteitä.

1.2 Tutkimuskysymykset

Opinnäytetyön tutkimuskysymykset pohjautuvat opinnäytetyön tavoitteeseen selvittää tulevan NIS2-direktiivin vaatimuksia ja lähestymistapoja valmistavan teollisuuden näkökulmasta. Tutkimuskysymykset ovat siis tutkimusongelman pohjalta seuraavat:

1. Mistä NIS2-direktiivissä on kyse?
2. Mitä vaatimuksia NIS2-direktiivi asettaa valmistavalle teollisuudelle?
3. Miten valmistavan teollisuuden toimijat voivat lähestyä NIS2-direktiivin asettamia vaatimuksia?

Jotta voidaan ratkaista tutkimusongelma, täytyy ensiksi ymmärtää mistä NIS2-direktiivissä on kyse. Ensimmäisen tutkimuskysymyksen tarkoitus on siis selittää mikä NIS2-direktiivi on ja mitä se pitää sisällään. Kun NIS2-direktiiviä on avattu, seuraava vaihe on ymmärtää sen asettamat vaatimukset valmistavalle teollisuudelle, josta voidaan johtaa toinen tutkimuskysymys sen asettamista vaatimuksista valmistavalle teollisuudelle. Lopulta viimeinen tutkimuskysymys

koskee sitä, miten valmistavan teollisuuden yritykset voivat lähestyä niitä vaatimuksia, joita NIS2-direktiivi asettaa.

1.3 Tutkimusmenetelmä

Opinnäytetyössä on tarkoitus ymmärtää NIS2-direktiiviä sekä luoda ohjeistus, jonka avulla valmistavan teollisuuden toimijat voivat lähestyä direktiivin asettamia vaatimuksia. Ensimmäiset kaksi tutkimuskysymystä kysyvät, mistä NIS2-direktiivissä on kyse ja mitä vaatimuksia se asettaa valmistavalle teollisuudelle. Vastaus tutkimuskysymyksiin löytyy itse NIS2-direktiivistä sekä sitä käsittelevistä sekundääriaineistoista. Kirjallisuuskatsauksen avulla voidaan siis vastata ensimmäiseen kahteen tutkimuskysymykseen. Kirjallisuuskatsaus määritellään tutkimustavaksi, jolla voidaan tiivistää olemassa olevaa tietoa ja sen avulla luoda johtopäätöksiä tutkimuskysymykseen (Vilkka 2023, luku 1.1.1 Tutkimuskohteena tutkimukset).

Kolmas tutkimuskysymys pyrkii vastaamaan siihen, miten valmistavan teollisuuden toimijat voivat lähestyä NIS2-direktiivin asettamia vaatimuksia. Jotta kolmanteen tutkimuskysymykseen voidaan vastata, on tehtävä ohjeistus. NIS2-direktiivi astuu voimaan vasta 17.10.2024, eikä sitä koskevia lainsäädöksiä ole vielä luotu, eikä vaatimusten toteutusta ole käytännössä vielä valvottu. NIS2-direktiivi ei myöskään vaadi tiettyjen viitekehitysten tai standardien käyttöä. Lisäksi NIS2-direktiivin mukaan riskienhallintatoimenpiteiden tulisi olla oikeasuhtaisia, riippuen esimerkiksi tekijän koosta ja poikkeaman tapahtumisen todennäköisyydestä (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 21 artikla). Näistä syistä NIS2-direktiivin käsittely täytyy olla ilmiötä tulkitsevaa.

Tutkimusmenetelmäksi viimeisen tutkimuskysymykseen valitaan kvalitatiivinen kehittämistutkimus, sillä jotta kolmanteen tutkimuskysymykseen voidaan vastata, täytyy ymmärtää ilmiötä sekä luoda sen pohjalta ohjeistus toimista, joilla lähestyä NIS2-direktiivin vaatimuksia.

Määrällinen tutkimus perustuu numeeriseen analyysiin, kun taas kvalitatiivinen tutkimus perustuu tulkintaan (Vilkka 2021, osa 1: Opinnäytetyötyypit mahdollisuutena). Toimintatutkimus on tapa toteuttaa tutkimus niin, että siitä on käytännön hyötyä (Heikkinen ym. 2023, luku 1: Mitä toimintatutkimus on ja miten sitä tehdään). Toiminnallisen tutkimuksen toteutus voi olla esimerkiksi ohje tai opas (Vilkka 2021, osa 1: Toiminnallinen opinnäytetyö).

Toimintatutkimuksen ja kehittämistutkimuksessa on paljon yhteneväistä, mutta erona voidaan nähdä esimerkiksi se, että toimintatutkimuksessa tavoite on kehittää paikallisesti toimivaa ratkaisua, kun taas kehittämistutkimuksessa korostuu teorian luominen ja kehitettyjen asioiden voimakas yleistäminen suurempaan mittakaavaan (Pernaa 2013, 6). Tutkimusmenetelmäksi sopii siis tarkemmin kehittämistutkimus, sillä tarkoituksena on luoda yleinen ohjeistus valmistavan teollisuuden toimijoille.

Standardit ja NIST-ohjeistukset valittiin sen takia, että saataisiin parhaisiin käytäntöihin perustuvia ohjeistuksia vaatimusten täyttämiseksi. Valmistavan teollisuuden alalla täytyy ottaa huomioon sekä IT että OT, joten molempia edustamaan valitaan standardit.

1.4 Aineistonkeruumenetelmät

Tavoite on ymmärtää NIS2-direktiiviä sekä luoda standardien pohjalta ohjeistus sen vaatimusten täyttöön. Jotta voidaan ymmärtää NIS2-direktiiviä, sen vaatimuksia ja vaatimusten lähestymistä parhaiten käytäntöjen kautta, tulee perehtyä NIS2-direktiiviin sekä sitä käsittelevään sekundääriaineistoon. Sekundääriaineistoksi määritellään materiaalit, joita joku toinen henkilö on kerännyt (Vilkka 2021, osa 2: kohti aineistoin valintaa).

NIS2-direktiiviin perehtymisen jälkeen vaatimuksia koitetaan ymmärtää, jakaa ne osiin ja täyttää ne perehtymällä alan parhaita käytäntöjä edustaviin standardeihin. NIS2-direktiivi sisältää esimerkiksi riskienhallintaa, jonka vaatimuksien täyttämiseksi voidaan perehtyä ja käyttää riskienhallintaa ja hallintakeinoja koskevia standardeja, esimerkiksi ISO/IEC 31000, ISO/IEC 27001, ISO/IEC 27002 ja IEC 62443-2-1.

1.5 Analysointimenetelmät

Määrällisen tutkimuksen analyysillä pyritään ymmärtämään numeroiden ja tilastojen avulla, kun taas laadullisen tutkimuksen analyysillä pyritään tiivistämään ja täsmentämään hajanaiselta tuntuvaa aineistoa (Vilkka 2021, osa 3: Laadullinen analyysi; Jyväskylän yliopiston Koppa). Laadullisen analyysin avulla luodun kokonaisuuden pohjalta voidaan perustellusti tulkita ja luoda johtopäätöksiä tutkittavasti ilmiöstä (Puusa ym. 2020, kappale 4: Laadullisen aineiston analyysi). Opinnäytetyön tarkoitus on ymmärtää, yhdistää ja soveltaa NIS2-direktiiviä ja standardeja ohjeistuksen luomiseksi, joten siihen soveltuu parhaiten laadullinen analyysi.

NIS2-direktiiviin perehdytään ja sitä tutkitaan, jonka jälkeen sen asettamat vaatimukset jaetaan osiin. Kun vaatimukset on jaettu osiin, niitä lähestytään standardeilla ja viitekehyksellä, jotka edustavat parhaita käytäntöjä. NIS2-direktiivin riskienhallinnan toimenpeiden aihealueita käsitteleviin standardeihin ja viitekehykseen perehdytään, niitä tulkitaan ja sovelletaan, jotta saadaan ohjeistus ja lähestymistapa asetettuihin vaatimuksiin.

2 VALMISTAVAN TEOLLISUUDEN NYKYTILANNE

Koska valmistava teollisuus ei kuulunut ensimmäiseen NIS-direktiiviin, säätelystä koituvat kustannukset ovat sillä keskimäärin suurempia kuin ensimmäiseen direktiiviin kuuluvilla sektoreilla. Huoltovarmuuskeskuksen arvioinnin mukaan valmistavan teollisuuden kybermaturiteettitaso on alle perustason, jonka lisäksi sen nykytila vaatii kehittämistä. Puutteiksi valmistavan teollisuuden sektorilla esiin nousee varsinkin toimittajahallinnan kehittäminen ja sidonnaisuuksien tunnistaminen, riskienhallinta sekä johdon tuen ja kiinnostuksen puute. (Lausuntopalvelu 2023, 78.)

3 NIS2-DIREKTIIVI

Network and information security 2 -direktiivi eli NIS2-direktiivi on 17.10.2024 Euroopan unionissa voimaan astuva kyberturvallisuutta koskeva direktiivi, jota

täytyy noudattaa 18.10.2024 alkaen (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 41 artikla). NIS2-direktiivi kumoaa vanhan NIS-direktiivin, sekä lisää uusia toimialoja direktiivin alaiseksi. Direktiivin alaiset toimijat saavat vaatimuksia koskien esimerkiksi raportointia ja kyberturvallisuuden riskienhallintaa, joita heidän täytyy noudattaa sakkojen uhalla. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555.)

Suomen valtioneuvoksen arvion mukaan viikolla 21 hallitus julkaisee esityksen eduskunnalle NIS2-direktiin täytäntöönpanemiseksi, mutta esityksestä on julkaistu jo luonnos (Valtioneuvosto 2023; Lausuntopalvelu 2023).

Traficom valmistelee suositusta NIS2-direktiivin riskienhallintavelvoitteiden täyttämiseksi. Arvioituna julkaisuajankohtana suositukselle on vuoden kesällä 2024, kun laki NIS2-direktiivistä vahvistetaan. (Traficom 2023.)

Traficomin suosituksessa tulee olemaan esimerkkejä NIS2-direktiivin vaatimusten täyttämisen toteutuksesta sekä todennusmenetelmistä. Suosituksessa tullaan viittaamaan yleisimpiin standardeihin, mutta se ei edellytetä tiettyjen standardien tai viitekehysten käyttöä. (Traficom 2023.)

Koska Traficomin suositus ei tule edellyttämään tiettyjen standardien tai viitekehysten käyttöä, tässä opinnäytetyössä ehdotettuja hallintakeinoja pystytään hyödyntämään yhdessä tulevan Traficomin suosituksen kanssa.

3.1 NIS2-direktiivin toimialat

NIS2-direktiivi lisää huomattavasti toimialoja sen alaisiksi. NIS-direktiivissä toimialoja oli seitsemän: energia, liikenne, pankkiala, finanssimarkkinoiden infrastruktuurit, terveydenhuoltoala, juomaveden toimittaminen ja jakelu, sekä digitaalinen infrastruktuuri (Euroopan parlamentin ja neuvoston asetus (EU) 2016/1148, liite II).

NIS2-direktiivi jakaa toimialat kahteen kategoriaan: direktiivin liitteessä I määritellään erittäin kriittiset toimialat, kun taas liitteessä II määritellään muut kriittiset toimialat. NIS2-dirktiivin erittäin kriittiset toimialat sisältävät 11 toimialaa ja

muut kriittiset toimialat sisältävät seitsemän. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, liite I, II.)

NIS2-direktiivin erittäin kriittisiin toimialoihin kuuluvat seuraavat: energia, liikenne, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveys, juomavesi, jätevesi, digitaalinen infrastruktuuri, TVT-palvelujen hallinta (yritysten välinen), julkishallinto sekä avaruus. Muihin kriittisiin toimialoihin puolestaan kuuluvat seuraavat toimialat: posti- ja kuriiripalvelut, jätehuolto, kemikaalien valmistus, tuotanto ja jakelu, elintarvikkeiden tuotanto, jalostus ja jakelu, valmistus, digitaaliset palvelun tarjoajat sekä tutkimustoiminta
(Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, liite I, II).

Mikäli toimija kuuluu NIS2-direktiivin määrittelemälle toimialalle ja se täyttää keskisuuren yrityksen määritelmän, se luokitellaan NIS2-direktiivin alaiseksi toimijaksi, jonka pitää täyttää vaatimukset. Poikkeustilanteissa toimijat saattavat kuulua koosta riippumatta NIS2-direktiivin alaiseksi, jos esimerkiksi häiriö kyseisen toimijan palvelussa voisi vaikuttaa merkittävästi yleiseen järjestykseen, turvallisuuteen tai kansanterveyteen (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 2 artikla).

3.2 Keskeiset ja tärkeät toimijat

NIS2-direktiivi jakaa toimijat keskeisiin ja tärkeisiin toimijoihin. Mikäli erittäin kriittisen toimialan toimija täyttää keskisuuren yrityksen määrityksen, se lasketaan keskeiseksi toimijaksi. Tärkeitä toimijoita ovat taas ne toimijat, jotka ovat direktiivin alaisilla toimialoilla, mutta eivät täytä keskeisen toimijan määritelmää (Lausuntopalvelu 2023, 11).

Keskeisillä toimijoilla on tärkeitä toimijoita tiukempi valvonta ja isommat sakkorangaistukset, esimerkiksi keskeisille toimijoille toteutetaan valvontaa, mutta tärkeille toimijoille valvonta toteutetaan jälkikäteen toteutettuna, mikäli on syytä uskoa että puutteita löytyy. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 32, 33 artikla).

Valvonnan lisäksi myös sakkorangaistukset eroavat keskeisten ja tärkeiden toimijoiden välillä. Enimmäissakot keskeisille toimijoille on 10 miljoonaa euroa tai 2 % edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta, kumpi onkaan suurempi. Tärkeällä toimijalla sakot ovat taas enintään 7 miljoonaa tai 1,4 % (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 34 artikla).

3.3 Valmistava toimiala

Valmistava teollisuus ei ollut ensimmäisen NIS-direktiivin alainen, mutta NIS2-direktiivissä valmistus mainitaan direktiivin liitteessä II, eli kohdassa muut kriittiset toimialat. Tämä tarkoittaa sitä, että valmistavan teollisuuden toimija lasketaan NIS2-direktiivin alaiseksi tärkeäksi toimijaksi, mikäli se valmistaa direktiivissä määriteltyjä tuotteita, sekä on keskikokoinen tai suurempi toimija. Keskikokoinen toimija määritellään toimijaksi, jolla on yli 50 työntekijää tai yli 10 miljoonaa vuosittaista liikevaihtoa (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 2 artikla; Commission 2003).

Valmistus sisältää NIS2-direktiivissä seuraavat toimialan osat: lääkinnälliset laitteet ja in vitro-diagnostikkaan tarkoitetut lääkinnälliset laitteet, tietokoneet sekä elektroniset ja optiset tuotteet, sähkölaitteet, muut koneet ja laitteet, moottoriajoneuvot, perävaunut ja puoliperävaunut, muut kulkuajoneuvot (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, liite II).

Toimialan osat tarkennetaan muissa dokumenteissa, jotka määritellään direktiivin liitteessä II. Esimerkiksi direktiivissä tarkennetaan, että muiden koneiden ja laitteiden valmistus määräytyy NACE Rev. 2 luokituksen C jakson kaksinumerotasossa 28 määriteltyjen toimijoiden mukaan. Luokittelu sisältää monia erilaisia tuotteita, esimerkiksi hammaspyörät, pumput sekä yleiskäyttöön tarkoitetut voimakoneet (Eurostat 2006, 68; Lausuntopalvelu 2023, 40).

3.4 NIS2-direktiivin vaatimukset

Uusien toimialojen lisäksi NIS2-direktiivi sisältää velvoitteita jäsenmaille sekä keskeisten ja tärkeiden toimijoiden yrityksille. Jäsenmaiden velvoitteisiin kuu-

luu esimerkiksi velvoitteet hyväksyä kansalliset kyberturvallisuusstrategiat, järjestää toimivaltaiset ja kyberkriisinhallintaviranomaiset, tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-yksiköt) sekä keskitetyt yhteyspisteet (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 1 artikla).

Toimivaltaiset viranomaiset ovat vastuussa keskeisten ja tärkeiden toimijoiden valvonnasta (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 31 artikla). Suomessa valmistavan teollisuuden toimivaltainen viranomainen on Turvallisuus- ja kemikaalivirasto TUKES (Lausuntopalvelu 2023, 48).

NIS2-direktiivi asettaa keskeisille ja tärkeille toimijoille vaatimuksia riskienhallinnasta sekä toimenpiteistä, joita sen tulee sisältää. Merkittävistä poikkeamista toimijat saavat monivaiheisen raportointivelvoitteen. Lisäksi hallintoelimelle asetetaan vaatimuksia kouluttautumisesta ja riskienhallinnan hyväksymisestä. Toimijan täytyy myös itse ilmoittautua keskeiseksi tai tärkeäksi toimijaksi. Vaatimukset ovat samat keskeisillä ja tärkeillä toimijoilla, jonka takia tämän opinnäytetyön luvussa 11 NIS2-direktiivin vaatimukset valmistavalle teollisuudelle käsitellään vaatimuksia tarkemmin. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555.)

4 IT- JA OT-KYBERTURVALLISUUS

Kun aiheena on kyberturvallisuus ja valmistava teollisuus, nousee esiin kaksi termiä: IT ja OT. IT on lyhenne termistä information technology, usein tunnetaan myös nimellä tietotekniikka. IT viittaa ohjelmistoihin ja laitteistoihin, joiden tarkoitus on prosessoida ja tallentaa tietoa (Flaus 2019, 4).

OT on lyhenne termistä operational technology ja sen tarkoitus on vaikuttaa fyysiseen järjestelmään, esimerkiksi havaita sensoreilla ja toteuttaa toimenpide (Flaus 2019, 4). Esimerkkinä OT-järjestelmästä on teollinen ohjausjärjestelmä (ICS), joka monitoroi ja ohjaa teollisia prosesseja (Fortinet s.a).

Alunperin OT-järjestelmät pyörivät eristyksessä käyttäen patentoituja protokollia, jonka takia niillä ei ollut paljon yhteistä IT-järjestelmien kanssa. IT-tuotteiden, -järjestelmien ja -ominaisuuksien käyttö OT:n puolella yleistyy jatkuvasti,

sekä esimerkiksi asioiden internet (IoT) hämärtää rajaa IT:n ja OT:n välillä. IT-ominaisuuksien käyttö OT-ympäristössä tuo uusia mahdollisuuksia esimerkiksi etähallintaan liittyen, mutta se myös altistaa OT-järjestelmät kyberturvallisuuden vaaroille, sillä järjestelmät eivät ole enää eristyksessä. Jotta voidaan soveltaa IT-ympäristöön suunniteltuja kyberturvallisuuden toimenpiteitä OT-ympäristöön, täytyy ottaa huomioon OT-ympäristön vaatimuksia ja ominaispiirteitä. (ISAGCA 2021, 3, NIST 2023, 28.)

Luottamuksellisuus, eheys ja tiedon saatavuus takaavat sen, että tieto ei pääse vääriin käsiin, tieto pysyy eheänä ja se on saatavilla niille, joille sen kuuluu olla. Turvallisuuden näkökulmasta merkittävä ero IT- ja OT-järjestelmien välillä on OT-järjestelmien tiukemmat vaatimukset eheyteen ja saatavuuteen liittyen, kun taas IT-järjestelmissä luottamuksellisuus on usein tärkein. Eheys ja saatavuus ovat tärkeitä OT-järjestelmissä sen takia, että virheellinen toiminta voi aiheuttaa haittaa esimerkiksi ihmisten terveyteen tai ympäristölle. Virheellinen toiminta voi myös aiheuttaa taloudellisia tappioita tuotannon pysähtyessä. (Flaus 2019, 60; ISAGCA 2021, 3; NIST 2023, 28.)

OT-ympäristössä eheys ja saatavuus parantavat lisäksi järjestelmien turvallisuutta ja suorituskykyä, sillä niillä voidaan varmistaa esimerkiksi turvallisuus- ja hallintajärjestelmän toiminta (Flaus 2019, luku 3.1.1 The AIC criteria.)

OT-ympäristössä on usein käytössä legacy-laitteistoa, josta voi seurata esimerkiksi päivitysten puutteita. Myös omaisuuserien tunnistaminen OT-ympäristössä tuo lisähaasteita verrattuna IT-ympäristöön johtuen patentoiduista protokollista sekä riskistä että tuotantoprosessi häiriintyy. (Nozomi Networks 2024.)

5 RISKIENHALLINTA

NIS2-direktiivi asettaa toimijoille vaatimuksia kyberturvallisuuden riskienhallinnasta ja toimenpiteistä, joita siihen tulisi sisällyttää. Riskienhallinta tarkoittaa koordinoitua riskien suuntaamista ja hallintaa (Enisa 2022, 11). Riskienhallinta on jatkuva prosessi ja se sisältää monta eri vaihetta. Riskienhallinnan ensim-

mäisessä vaiheessa määritellään sen kattavuus, toimintaympäristö sekä riskikriteerit. Seuraavassa vaiheessa toteutetaan riskien arviointi, jonka jälkeen tapahtuu riskien käsittely. (Enisa 2022, 18.)

OT-riskienhallinta eroaa hieman IT-riskienhallinnasta, sillä OT-ympäristössä tulee ottaa huomioon erityisesti ihmisten turvallisuus ja järjestelmien vikasietoisuus, sillä digitaalisten vaikutusten lisäksi OT-ympäristöissä tapahtuvat poikkeamat saattavat vaikuttaa myös fyysiseen ympäristöön. OT-ympäristössä kyberturvallisuuden toimenpiteiden ei tulisi aiheuttaa vaaraa ihmisille. (NIST 2023, 28, 51)

5.1 Kattavuuden, toimintaympäristön ja riskikriteerien määrittely

Riskienhallinnan ensimmäinen vaihe on kattavuuden, toimintaympäristön ja riskikriteerien määrittely. Määrittelyn pohjalta voidaan tehdä valintoja riskienhallinnan vaiheisiin liittyen. (Enisa 2022, 18.)

Kattavuuden määrittelyssä selviää riskienhallintatoimenpiteiden laajuus. Toimintamallin suunnittelussa tulisi ottaa huomioon esimerkiksi riskienhallinnan tavoitteet, odotettavat tulokset, sekä työkalut ja tekniikat riskien arviointiin. (SFS-EN ISO/IEC 31000:2018, 15.) NIS2-direktiivin kannalta kattavuuden määrittelyssä tulisi ottaa huomioon direktiivin vaatimat kymmenen kyberturvallisuuden riskienhallinnan toimenpidettä.

Valmistavan teollisuuden toimijoiden tulisi ottaa kattavuuden määrittelyssä huomioon myös OT-järjestelmien erityistarpeet, esimerkiksi valmistusprosessin lämpötila tai OT-järjestelmän toiminnan sidoksissa oleminen fyysiseen ympäristöön. Ottamalla huomioon OT-järjestelmien erityistarpeet, voidaan tunnistaa niiden ainutlaatuiset riskit. (NIST 2023, 51.)

Toimintaympäristön määrittelyssä otetaan huomioon organisaation ulkoinen ja sisäinen toimintaympäristö, sekä organisaation tavoitteet (SFS-EN ISO/IEC 31000:2018, 15). Ulkoisella toimintaympäristöllä tarkoitetaan esimerkiksi kult-

tuurisia ja lakeihin liittyviä tekijöitä, kun taas sisäisellä toimintaympäristöllä tarkoitetaan esimerkiksi organisaation kykyihin ja työkulttuuriin liittyviä tekijöitä (Australian Department of Finance 2016, 2).

Riskikriteerien määrittelyssä käsitellään kuinka paljon ja minkälaisia riskejä organisaatio voi ottaa. Tulisi myös määritellä riskien merkittävyyden arvioinnin kriteerit, jotka auttavat riskeihin liittyvissä päätöksissä. (SFS-EN ISO/IEC 31000:2018, 16.)

5.2 Riskien arviointi

Kattavuuden, toimintaympäristön ja riskikriteerien määrittelyn jälkeen seuraava vaihe on toteuttaa riskien arviointi. Riskien arviointi pitää sisällään NIS2-direktiivin vaatiman riskien tunnistuksen, riskianalyysin sekä riskin merkityksen arvioinnin (SFS-EN ISO/IEC 31000:2018, 16).

OT-ympäristössä usein käytetään vikasietoisuuden takaamiseksi mekanismeja, jotka eivät ole digitaalisia, mutta jotka silti voivat lievittää digitaalisten poikkeamien vaikutuksia. Esimerkiksi kun poikkeama tapahtuu ja digitaaliset mittarit ovat epäkunnossa, voidaan käyttää analogisia mittareita. Riskien arvioinnissa tulisi huomioida kyseiset mekanismit. (NIST 2023, 52.)

NIS2-direktiivin kymmenen riskienhallinnan toimenpidettä tulisi toteuttaa asianmukaisesti ja oikeasuhtaisesti, johon vaikuttaa esimerkiksi toimijan koko, sekä poikkeamien todennäköisyys ja vakavuus (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 21 artikla). Toimijan tulisi siis sisältää riskien arviointiin NIS2-direktiivin vaatimat kymmenen riskienhallinnan toimenpidettä, jotta niille osataan toteuttaa asianmukaiset ja oikeasuhtaiset toimenpiteet.

Riskien tunnistuksessa pyritään löytämään, havaitsemaan ja kuvailemaan organisaatiota koskevat riskit. Riskien tunnistuksessa tulisi ottaa huomioon esimerkiksi riskien lähteet, omaisuuden arvo, haavoittuvuudet ja riskien seuraamukset. Riskit tulisi tunnistaa, vaikka niiden lähde ei olisi organisaation hallinnassa. (SFS-EN ISO/IEC 31000:2018, 16–17.)

Riskianalyysissä pyritään ymmärtämään riskin luonnetta ja vakavuutta. Riskianalyysissä tulisi ottaa huomioon esimerkiksi riskin todennäköisyys ja seuraamukset, sekä nykyisten hallintakeinojen tehokkuus riskin muuttamiseen. Riskianalyysin pohjalta riskiä ymmärretään syvemmin ja voidaan siirtyä seuraavaan vaiheeseen, eli riskin merkityksen arviointiin. (Enisa 2022, 20.)

Riskin merkityksen arvioinnin tarkoitus on auttaa riskiä koskevien päätöksen tekemisissä. Riskianalyysin tuloksia verrataan määriteltyihin riskikriteereihin, jonka perusteella voidaan valita riskiä koskevat toimenpiteet. (SFS-EN ISO/IEC 31000:2018, 18.)

5.3 Riskien käsittely

Riskiarvioinnin jälkeen käsitellään riski, eli valitaan sopiva toimenpide määritellyn hyväksyttävän riskikriteerin ylittävälle riskille. Riski voidaan käsitellä esimerkiksi lopettamalla riskin aiheuttava toiminta, muuttamalla sen todennäköisyyttä tai tietoisesti hyväksyä kyseinen riski. (Enisa 2022, 20.)

6 ISO/IEC 27000 -STANDARDISARJA

ISO/IEC 27000 on standardisarja, joka koostuu tietoturvallisuuden hallinnan standardeista. Sarjan keskiössä on ISO/IEC 27001, kansainvälinen standardi, joka asettaa vaatimukset tietoturvallisuuden hallintajärjestelmälle (ISMS). ISMS on kokoelma politiikoista, toimista ja ohjeistuksista, joiden tarkoitus on systemaattisesti hallinnoita tietoturvallisuutta (SFS-EN ISO/IEC 27000:2020, 16; Calder & Gerrard 2013, 12).

ISO/IEC 27001 sisältää hallintakeinoja, jotka määritellään riskiä muuttavina toimenpiteinä. (SFS-EN ISO/IEC 27002:2022, 7). Hallintakeinoista voidaan saada lisätietoa ISO/IEC 27002 -standardista, joka toimii viiteasiakirjana ISO/IEC 27001 -standardin mukaisten hallintakeinojen toteuttamiselle (SFS-EN ISO/IEC 27002:2022, 7).

Esimerkkinä yksi NIS2-direktiivin vaatimus koskee toimintaperiaatteita ja menettelyitä kryptografian suhteen, mutta kyseisestä vaatimuksesta ei anneta tarkkoja vaatimuksia ja toimia. ISO/IEC 27001 sisältää hallintakeinon A.8.24,

joka koskee kryptografian käyttöä (SFS-EN ISO/IEC 27001:2023, 24). ISO/IEC 27001 -standardista voidaan siis saada hallintakeinoja, joihin voidaan saada ISO/IEC 27002 -standardista yksityiskohtainen ohjeistus hallintakeinon toteuttamiseen (Calder & Gerrard 2013, 29). Käyttämällä ISO/IEC 27000 -standardisarjaa voidaan siis saada käytännön ohjeistus NIS2-direktiivin vaatimuksiin, joka perustuu kansainväliseen tietoturvastandardiin.

ISO/IEC 31000 on riskienhallinnan ohjeistuksen ja viitekehyksen sisältävä standardi (Enisa 2022, 17). ISO/IEC 31000 -standardin ohjeistus ei keskity pelkästään tietoturvallisuuden riskienhallintaan, vaan se on yleinen toimintamalli riskienhallinnalle (SFS-EN ISO/IEC 31000:2018, 6).

ISO/IEC 27005 on tietoturvallisuuden riskienhallintaa käsittelevä standardi, ja se sisältää ohjeistusta ISO/IEC 31000 -standardin mukaisen riskienhallinnan toteutuksesta tietoturvallisuuden näkökulmasta (ISO/IEC 27005:2022, 5).

7 IEC 62443 -STANDARDISARJA

IEC 62443 on OT-ympäristöön erikoistuva kyberturvallisuuden standardisarja. NIS2-direktiivin näkökulmasta standardisarjan oleellinen standardi on 62443-2-1, joka käsittelee tietoturvallisuusohjelman perustamista teollisuusautomaatio- ja ohjausjärjestelmiä varten (SFS-IEC 62443-2-1:2013).

IEC 62443-2-1 -standardin avulla valmistavan teollisuuden yritys voi siis saada OT:n näkökulmasta ohjeistusta NIS2-direktiivin riskienhallintavaatimusten toteutukseen. IEC 62443 sisältämät vaatimukset ovat hyvin samanlaisia kuin ISO/IEC 27001 -vaatimukset, jonka lisäksi se on yhteensopiva ISO/IEC 27000 -standardisarjan kanssa (SFS-IEC 62443-2-1:2013, 270; Flaus 2019, 168).

8 NIST SP 800-53 JA NIST SP 800-82

NIST SP 800-53 on ohjeistus, joka sisältää kattavan luettelon informaatiojärjestelmien hallintakeinoista. NIST SP 800-53 jakaa hallintakeinot 20 perheeseen, jotka sisältävät kyseisen aihealueen hallintakeinoja. Hallintakeinojen ni-

met koostuvat perheen mukaisesta etuliitteestä sekä numerotunnisteesta. Esimerkiksi SR-2 on toimitusketjun perheen sisällä oleva hallintakeino, joka käsittelee toimitusketjun riskienhallinnan suunnittelua. (NIST 2020, 2, 8.)

NIST SP 800-82 on ohjeistus OT-turvallisuudesta, ja sen avulla voidaan soveltaa NIST SP 800-53 -hallintakeinoja OT-ympäristöön sopivimmiksi. NIST SP 800-82 soveltaa NIST SP 800-53 -hallintakeinoja antamalla niihin OT-näkökulmasta lisätietoa ja/tai muokkauksia. Esimerkki NIST SP 800-82 antamasta lisätiedosta hallintakeinoon on sprinklerijärjestelmän mahdollinen vaarallisuus tietynlaisissa OT-ympäristöissä. (NIST 2023, 5, 6, 265.)

9 NIST CYBERSECURITY FRAMEWORK

NIST Cybersecurity Framework, eli NIST CSF, on kyberturvallisuuden viitekehys, jonka tarkoitus on antaa ohjausta kyberturvallisuuden riskien hallitsemiseen. NIST Cybersecurity Framework kuvastaa korkealla tasolla kyberturvallisuuden lopputuloksia, mutta ei suoraan opasta, miten kyseinen lopputulos tulisi saavuttaa. Viitekehys kuitenkin yhdistää itsensä muihin käytäntöihin ja hallintakeinoihin, joiden avulla voidaan saavuttaa tavoiteltu lopputulos kyberturvallisuudesta. (NIST 2024, i.)

NIST Cybersecurity Framework sisältää informatiivisia referenssejä, joiden tarkoitus on kuvata teknistä toteutusta, jonka avulla voidaan saavuttaa viitekehyksen kuvaama lopputulos. Informatiiviset referenssit eivät ole lista vaatimuksia, vaan niiden tarkoitus on antaa ohjausta käytännön toteutukseen. (NIST 2018; NIST 2024, iv.) NIST SP 800-53 -ohjeistus on yksi informatiivisista referensseistä, eli yhdistämällä NIST Cybersecurity Frameworkin osiot NIS2-direktiivin vaatimuksiin, saadaan informatiivisten referenssien kautta yhdistettyä NIST SP 800-53 -hallintakeinoja NIS2-direktiivin vaatimuksiin.

10 NIS2-DIREKTIIVIN VAATIMUKSET VALMISTAVALLE TEOLLISUUDELLE

10.1 Ilmoittautuminen

Toimijoiden täytyy itse ilmoittautua valvovalle viranomaiselle 1.1.2025 mennessä, mikäli he ovat keskeisiä tai tärkeitä toimijoita (Lausuntopalvelu 2023,

185). Ilmoittautumisessa tulisi antaa vaadittavat tiedot, jotka sisältävät toimijan nimen, osoitteet sekä yhteystiedot (mukaan lukien sähköpostiosoitteet ja puhelinnumerot), IP-osoitealueet, toimijan toimiala ja toimialan osa, sekä luettelo jäsenvaltioista, joissa toimija tarjoaa NIS2-direktiivin toimialan alaisia palveluita. Mikäli kyseisiin tietoihin tulee muutoksia, niistä täytyy ilmoittaa kahden viikon kuluessa. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 3 artikla.)

10.2 Vaatimukset hallintoelimille

20 Artiklassa määritellään vaatimuksia hallintoelimille. Keskeisten ja tärkeiden toimijoiden hallintoelimet joutuvat hyväksymään toimijan riskienhallintatoimenpiteet, sekä heidät voidaan asettaa vastuuseen, jos riskienhallinnan vaatimukset eivät toteudu. Hallintoelimillä on myös velvollisuus osallistua koulutukseen, jotta heillä on riittävä osaaminen tunnistamaan riskejä ja arvioida kyberturvallisuusriskien hallintakäytäntöjä. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 20 artikla).

10.3 Riskienhallinnan vaatimukset

21 artiklassa määritellään riskienhallinta vaatimuksia toimijoille. Keskeiset ja tärkeät toimijat joutuvat asianmukaisesti ja oikeasuhteisesti toteuttamaan toimenpiteitä, joilla hallitaan verkko- ja tietojärjestelmien riskejä, esimerkiksi poikkeamien käsittelyllä ja jatkuvuuden hallinnalla. Direktiivissä määritellään kymmenen riskienhallinnan toimenpidettä, jotka toimijan täytyy toteuttaa. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 21 artikla.)

Riskienhallinnan toimenpiteiden täytyy olla kaikki vaaratekijät huomioivia. Kaikkien vaaratekijöiden huomioimisen tarkennetaan sisältävän esimerkiksi varkauden, tulipalon ja tulvan. Riskienhallinnalla täytyy siis myös suojata verkko- ja tietojärjestelmien fyysinen ympäristö poikkeamilta. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, johdantokappale 79.)

NIS2-direktiivin asettamat kymmenen riskienhallinnan toimenpidettä ovat seuraavat (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 21 artikla):

a. Riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat.

Ensimmäinen NIS2-direktiivin riskienhallintavaatimus koskee riskianalyysejä ja tietoturvajärjestelmien turvallisuutta koskevia politiikkoja. Suomen julkaiseman luonnoksen hallituksen esityksestä koskien NIS2-direktiivin täytäntöönpanemista arvioidaan, että tämä vaatimus tulee tuottamaan eniten menoja valmistavan yrityksen aloille. (Lausuntopalvelu 2023, 69, 77.)

b. Poikkeamien käsittely.

Toinen vaadittu toimenpide koskee poikkeamariskien tunnistusta sekä poikkeamien ehkäisyä, havainnointia sekä palautumista. Poikkeamalla tarkoitetaan verkko- ja tietojärjestelmien tietojen tai palveluiden saatavuuden, eheyden tai luottamuksellisuuden vaarantumista. (Lausuntopalvelu 2023, 69.)

Poikkeamien käsittelyn vaatimukseen liittyen tulisi olla prosessit tapahtumien kirjaamisen havainnointiin, sekä lokitiedot ylläpidosta, muutoksista, käytöstä ja virheistä. Poikkeamiin tulisi reagoida, ne tulisi arvioida sekä niistä tulisi oppia. (Lausuntopalvelu 2023, 123.)

c. Toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta.

Kolmas vaatimus koskee toiminnan jatkuvuuden hallintaa, ja hallituksen esityksen arvion mukaan vaatimukseen voi sisältyä muun muassa ICT-tuotteet ja -palveluiden jatkuvuus ja toipumissuunnitelmat sekä säännöllinen poikkeamien harjoitteleminen (Lausuntopalvelu 2023, 70).

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

Neljäs vaatimus koskee toimitusketjun turvallisuutta. Hallituksen esityksessä arvioidaan, että toimitusketjun turvallisuutta koskeva riskienhallintavaatimus

tulee vaatimaan toimijoita arvioimaan heidän itsensä lisäksi myös koko toimintaketjun sisältämien roolien vastuut ja velvollisuudet, ottaen huomioon toimintaympäristön (Lausuntopalvelu 2023, 71).

Omaan toimintaan vaikuttavista välittömistä toimittajista ja palveluntarjoajista täytyy olla tieto. Turvallisuusnäkökohtaa tarvitaan välittömiin laite- ja palveluntarjoajiin, sekä tulee ottaa huomioon heidän haavoittuvaisuutensa, riskienhallintatoimenpiteet ja kyberturvallisuuskäytännöt. Hallitakseen toimitusketjujen kyberturvallisuusriskiä, toimijat voivat sisällyttää kyberturvallisuuden hallintatoimenpiteitä toimittajiensa ja palveluntarjoajiensa sopimusjärjestelyihin. (Lausuntopalvelu 2023, 121.)

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

Viides vaatimus koskee verkko- ja viestintäjärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuutta, jota tulisi ylläpitää koko elinkaaren ajan. Turvalliset konfiguraatiot pitäisi määritellä, sekä luvattomat ja haitalliset muutokset tulisi estää. Uusien järjestelmien hankinnassa tulisi varmistaa hankittavien järjestelmien riittävä turvallisuus. (Lausuntopalvelu 2023, 120.) Verkon rakenne tulisi olla turvallinen, jonka voisi toteuttaa esimerkiksi segmentoimalla. Haitallinen liikenne tulisi havaita ja estää. (Lausuntopalvelu 2023, 121.)

f. Toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta.

Kuudes vaatimus koskee kyberturvallisuusriskien hallintatoimenpiteiden tehokkuuden arviointia. Hallituksen esityksen arvion mukaan tietoturvan tehokkuuden mittaamiseen tarvitaan mahdollisesti yleisten mittareiden lisäksi hallintakeinokohtaisia mittareita (Lausuntopalvelu 2023, 73).

g. Perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus.

Seitsemäs vaatimus koskee perustason kyberhygieniakäytäntöjä ja kyberturvallisuuskoulutusta. Esimerkkinä kyberhygieniakäytännöistä mainitaan direktiivissä ohjelmisto- ja laitteistopäivitykset, verkon segmentointi, salasanojen vaihtaminen ja uusien asennusten hallinta (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, johdantokappale 89; Lausuntopalvelu 2023, 124).

Henkilöstön tulisi olla tietoinen heidän tietoturvallisuuteensa liittyvistä vastuista ja velvoitteista, sekä heidän pitäisi käydä kyberturvallisuuskoulutusta. Kyberturvallisuuskoulutuksen tarkoitus on parantaa henkilöstön ymmärrystä kyberturvallisuudesta, sen ajantasaisista käytännöistä sekä tunnetuista kyberturvallisuusriskeistä. (Lausuntopalvelu 2023, 122.)

h. Toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä.

Kahdeksas vaatimus koskee kryptografiaa ja salausta. Toimijan tulisi luoda toimintaperiaatteet ja menettelyt, joiden avulla voidaan tarvittaessa suojata tietoa. Salauksen käyttö voisi olla tarpeen esimerkiksi silloin, kun tietoa siirretään avoimessa tietoverkossa. Arvion mukaan tulee erityisesti ottaa huomioon kryptografian ja salauksen toimintaperiaatteiden dokumentointi (Lausuntopalvelu 2023, 75, 123).

i. Henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta.

Yhdeksäs vaatimus koskee henkilöstöturvallisuutta, pääsynhallintaperiaatteita ja omaisuudenhallintaa. Hallituksen esityksen arvion mukaan tulee ottaa huomioon oikeuksien myöntäminen, muuttaminen sekä poistaminen. Omaisuudenhallinnalla tarkoitetaan fyysistä sekä aineetonta omaisuutta. (Lausuntopalvelu 2023, 75.)

Toimijan tulisi luetteloida omaisuus, sekä luoda menettelyt ja ohjeet omaisuudenhallintaan. Omaisuudenhallinnan tulisi tapahtua koko elinkaaren ajan, käyttöönotosta turvalliseen poistamiseen asti. Omaisuudella tarkoitetaan fyysisten resurssien, esimeriksi laitteet ja henkilöt, lisäksi myös aineetonta omaisuutta, esimerkiksi IP-osoitteet. (Lausuntopalvelu 2023, 121, 122.)

Pääsynhallinnan koskea henkilöstön lisäksi myös ulkoisia toimijoita ja järjestelmätunnuksia, sekä sen pitäisi kattaa ohjelmistolla toimivan pääsyn sekä fyysisen pääsyn. Oikeudet tulisi antaa vain toimiin, joita työtehtävä vaatii. Käyttäjätunnuksien ja käyttöoikeuksien menettely pitäisi tapahtua koko elinkaaren ajan, sekä niistä on pidettävä ajantasaista kirjaa. (Lausuntopalvelu 2023, 121, 122.)

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

Kymmenes vaatimus koskee todennusta ja suojattuja viestintäjärjestelmiä. Hallituksen esityksen arvion mukaan monivaiheisen tunnistautumisen käyttöönotto ei ole kaikissa ympäristöissä pakollista vaan se perustuu tarpeeseen, esimerkiksi riskiarvioinnin pohjalta (Lausuntopalvelu 2023, 71).

Varaviestintäjärjestelmällä tarkoitetaan viestintäjärjestelmää, joka ei ole riippuvainen tavanomaisista järjestelmistä, esimerkiksi puhelimesta ja sähköpostista. Mikäli toimija tulee riskiarviossa siihen tulokseen, että varaviestintäjärjestelmä on välttämätön, täytyisi määritellä kyseiset järjestelmät, niiden tarve ja tapa käyttöönotolle. (Lausuntopalvelu 2023, 124.)

NIS2-direktiivin kymmenen riskienhallinnan vaadittua minimitoimenpidettä asettaa otsikkotasolla vaatimuksia, mutta tarkkoja vaatimuksia tai toimenpiteitä ei määritellä. Toimenpiteiden tulee olla asianmukaisia ja oikeasuhtaisia (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 21 artikla).

Direktiivin mukaan asianmukaisuudessa ja oikeasuhtaisuudessa tulisi ottaa huomioon toimijan riskit joille se altistuu, toimijan koko sekä poikkeamien esiintymisen todennäköisyys, vakavuus sekä poikkeamien yhteiskunnalliset ja taloudelliset vaikutukset (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, johdantokappale 82).

10.4 Raportointivelvoitteet

23 artiklassa määritellään monivaiheinen raportointivelvoite merkittävistä poikkeamista. Poikkeama on merkittävä, jos se on aiheuttanut tai voi aiheuttaa vakavaa toimintahäiriötä palveluihin tai taloudellisia tappiota. Poikkeama lasketaan myös merkittäväksi, jos se on vaikuttanut tai voi vaikuttaa muihin aiheuttamalla huomattavaa vahinkoa. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 23 artikla.)

Raportointi tehdään valvovalle viranomaiselle tai CSIRT-yksikölle (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 23 artikla). Suomessa valmistavan toimialan toimija tekee raportoinnin merkittävästä poikkeamasta sen valvovalle viranomaiselle Turvallisuus- ja kemikaalivirastolle, tai CSIRT-yksikölle Traficomille (Lausuntopalvelu 2023, 48–49).

Kun merkittävä poikkeama tapahtuu, toimijan täytyy tehdä siitä varoitus ensimmäisen 24 tunnin aikana sen huomaamisesta, jolloin on mahdollisuus pyytää apua. Varoituksessa tulee myös arvioida se, että onko kyseessä vihamielinen teko tai voiko poikkeamalla olla rajanylittävä vaikutus. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 23 artikla.)

Seuraava askel raportoinnissa on poikkeamailmoituksen tekeminen 72 tunnin sisällä poikkeaman huomaamisesta. Poikkeamailmoitus tulisi sisältää päivittää varoitusta, esimerkiksi poikkeaman vakavuuden ja vaikutuksen arviointia, sekä mikäli mahdollista, vaaraantumisindikaattorit, eli mistä poikkeama huomattiin. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 23 artikla.)

Poikkeamailmoituksen jälkeen, mikäli CSIRT-yksikkö tai toimivaltainen viranomainen pyytää toimijalta tilannepäivitystä väliraportin muodossa, sellainen täytyy toimittaa. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 23 artikla.)

Viimeinen askel raportointivelvoitteessa on lopullinen raportti, joka täytyy toimittaa kuukauden sisällä poikkeaman huomaamisesta. Lopullisessa raportissa

tulisi sisältää tarkka kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksesta, arviointi siitä mikä aiheutti tai mahdollisti poikkeaman, turvatoimenpiteet sekä mikäli poikkeamalla oli rajanylittävä vaikutus. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 23 artikla.)

Toimijat voivat myös vapaaehtoisesti tehdä ilmoituksia läheltä piti -tilanteista, kyberuhkista tai poikkeamista, vaikka ne eivät olisi merkittäviä (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 30 artikla).

11 NIS2-DIREKTIIVIN RISKIENHALLINNAN TOIMENPITEIDEN YHDISTÄMINEN STANDARDEIHIN JA NIST CYBERSECURITY FRAMEWORKIIN

Tässä luvussa käsitellään yksityiskohtaisemmin tämän opinnäytetyön liitettä 1 ja 2. Liite 1 sisältää NIS2-direktiivin riskienhallinnan toimenpiteisiin yhdistettyjä ISO/IEC 27001- ja IEC 62443-2-1 -standardin hallintakeinoja ja vaatimuksia. ISO/IEC 27001- ja IEC 62443-2-1 -standardien hallintakeinojen ja vaatimusten yhdistelmää käyttäessä ei tarvitse toteuttaa jokaista hallintakeinoa tai vaatimusta, vaan toteuttamisessa tulisi ottaa huomioon tarpeet (ISAGCA 2021, 7).

ISO/IEC 27001- ja ISO/IEC 27002 -standardien hallintakeinot ovat samat, sillä ISO/IEC 27002 -standardi avaa yksityiskohtaisemmin ISO/IEC 27001 -standardin hallintakeinoja. Toimijat voivat siis käyttää ISO/IEC 27002 -standardia saadakseen yksityiskohtaisemman ohjeistuksen NIS2-direktiiviin riskienhallintavaatimuksiin liitetyistä hallintakeinoista.

Liite 2 käsittelee NIS2-direktiivin vaadittuja riskienhallinnan toimenpiteitä yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53 -ohjeistuksen hallintakeinoihin. NIST Cybersecurity Framework sisältää sen osioille informatiivisia referenssejä, eli halutun lopputuloksen saavuttamista tukevia teknisiä kuvauksia toteutuksesta (NIST 2018; NIST 2024). NIST tarjoaa Cybersecurity Frameworkin osioihin yhdistetyt informatiiviset referenssit Excel-tiedostossa (NIST 2024). Yhdistämällä NIST CSF -osiot NIS2-direktiiviin, informatiivisista referensseistä saadaan teknisiä kuvauksia, joiden avulla voi-

daan saavuttaa haluttu lopputulos liittyen NIS2-direktiivin vaatimuksiin toimenpiteistä. NIST SP 800-53 -ohjeistus on yksi näistä informatiivisista referensseistä.

Liitteiden tarkoitus on toimia ohjenuorana toimijoille siitä, miten he voisivat parhaiden käytäntöjen mukaisesti käytännössä toteuttaa NIS2-direktiivin vaadittuja riskienhallinnan toimenpiteitä.

Jotta voidaan yhdistää NIS2-direktiivin vaatimukset riskienhallinnan toimenpiteistä standardeihin ja NIST Cybersecurity Frameworkkiin, täytyy ymmärtää mitä asioita vaatimukset pitävät sisällään. Luonnos hallituksen esityksestä eduskunnalle NIS2-direktiivin täytäntöönpanemisesta avaa riskienhallintavaatimuksia antamalla esimerkkejä mitä ne voisivat pitää sisällään (Lausuntopalvelu 2023, 119-125).

Käyttäen hyväksi hallituksen luonnosta, jokaiset kymmenen NIS2-direktiivin riskienhallinnan toimenpidettä jaettiin osiin. Kun riskienhallinnan toimenpiteiden vaatimukset oli jaettu osiin, niihin etsittiin verrannollisia hallintakeinoja ja osuuksia ISO/IEC 27001- ja IEC 62443-2-1 -standardeista, sekä NIST Cybersecurity Frameworkista. NIST Cybersecurity Frameworkin informatiivisten referenssien avulla pystyttiin yhdistämään NIS2-direktiivin vaatimukset NIST SP 800-53 -hallintakeinoihin.

NIS2-direktiivin riskienhallinnan tulee olla kaikki vaaratekijät huomioivaa, esimerkiksi fyysinen turvallisuus. Näistä syistä myös fyysisen ympäristön turvallisuutta ja sen resursseihin kohdistuvia riskejä lähestytään hallintakeinoilla.

Fyysinen ympäristö tulisi suojata, sekä järjestelmät tulisi suojata luvattomalta fyysiseltä pääsyltä, vahingolta tai häiriöltä. Toimijoiden tulisi myös varautua välttämättömien resurssien häiriöihin, esimerkiksi sähkökatkoksiin. Kuvassa 1 on yhdistetty vaatimus ISO/IEC 27001- ja IEC 62443-2-1 -standardeihin. Kuvassa 2 näkyy vaatimus yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53:een.

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
Kaikkien vaaratekijöiden huomiointi (fyysinen ympäristö)		
Suojaa fyysinen ympäristö	A.7.1 Fyysiset turva-alueet	4.3.3.3.1 Laaditaan toisiaan täydentävät fyysisen ja verkkoon liittyvän tietoturvallisuuden politiikat
Suojaa järjestelmät luvattomalta fyysiseltä pääsyltä, vahingoilta ja häiriöiltä	A.7.2 Kulunvalvonta A.7.3 Toimistojen, tilojen ja laitteistojen suojaus A.7.4 Fyysisen turvallisuuden valvonta A.7.8 Laitteiden sijoitus ja suojaus	4.3.3.3.2 Perustetaan fyysisen tietoturvan ulkoraja(t) 4.3.3.3.3 Toteutetaan kulunvalvonta 4.3.3.3.6 Suojataan yhteydet
Varaudu välttämättömien resurssien häiriöihin, esimerkiksi sähkönjakelu ja tietoliikenneyhteys	A.7.5 Suojaus fyysisiä ja ympäristön aiheuttamia uhkia vastaan A.7.11 Tukipalvelut	4.3.3.4 Suojataan suojattavat kohteet ympäristön aiheuttamia vahinkoja vastaan 4.3.3.3.10 Määritellään menettelyt kriittisten suojattavien kohteiden tilapäistä suojaamista varten

Kuva 1. Fyysisen ympäristön NIS2-direktiivin vaatimus, ISO/IEC 27001 ja IEC 62443-2-1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
All-hazards approach, fyysinen ympäristö		
Suojaa järjestelmät luvattomalta fyysiseltä pääsyltä, vahingoilta ja häiriöiltä	**PR.AA-06** Physical access to assets is managed, monitored, and enforced commensurate with risk **PR.IR-02** The organization's technology assets are protected from environmental threats **DE.CM-02** The physical environment is monitored to find potentially adverse events	CA-07, PE-02, PE-03, PE-04,PE-05, PE-06, PE-08, PE-09, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-18PE-18, PE-19, PE-20, PE-23
Varaudu välttämättömien resurssien häiriöihin, esimerkiksi sähkönjakelu ja tietoliikenneyhteys	**PR.IR-03** Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	CP, IR, SA-08, SC-06 ,SC-24, SC-36, SC-39, SI-13

Kuva 2. Fyysisen ympäristön NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53

Ensimmäinen varsinainen vaadittu riskienhallinnan toimenpide koskee riskianalyysejä ja tietojärjestelmien turvallisuutta koskevia politiikkoja. Toimijalla tulisi olla kirjalliset periaatteet ja menettelyt viestintäverkkojen ja tietojärjestelmien turvallisuudesta, mutta direktiivissä ei yksityiskohtaisesti määritellä mitä politiikkoja tulisi vähintään olla. (Lausuntopalvelu 2023, 69, 119.)

Kuvassa 3 on yhdistetty vaatimus ISO/IEC 27001- ja IEC 62443-2-1 -standardeihin. Kuvassa 4 näkyy vaatimus yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53:een.

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
a. Riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat.		
Kirjalliset viestintäverkkojen ja tietojärjestelmien turvallisuusperiaatteet/-menettelyt	A.5.1 Tietoturvallisuutta koskevat toimintaperiaatteet A.5.2 Tietoturvaroolit ja -vastuut A.5.31 Lainsäädäntöön, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyvät vaatimukset	4.3.2.6.1 Kehitetään tietoturvapolitiikat 4.3.2.6.2 Kehitetään tietoturvamenettelyt 4.3.2.6.3 Ylläpidetään yhdenmukaisuutta riskien hallintajärjestelmien välillä 4.3.3.2.1 Laaditaan henkilöstön tietoturvapolitiikka

Kuva 3. Ensimmäinen NIS2-direktiivin vaatimus, ISO/IEC 27001 ja IEC 62443-2-1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
a. Riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat.		
Kirjalliset viestintäverkkojen ja tietojärjestelmien turvallisuusperiaatteet/-menettelyt	**GV.PO-01** Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced **GV.PO-02** Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01

Kuva 4. Ensimmäinen NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53

Toinen NIS2-direktiivin riskienhallintavaatimus koskee poikkeamien käsittelyä. Poikkeamien käsittely tulisi pitää sisällään esimerkiksi menettelyt ja roolit poikkeamien ehkäisemiseksi, havainnoimiseksi, analysoimiseksi, hallitsemiseksi sekä palautumiseksi sekä riittävät lokitiedot (Lausuntopalvelu 2023, 123).

Huomattava seikka on se, että IEC 62443-2-1 -standardista ei löytynyt vaatimusta käytäntöihin poikkeaman vakavuuden ja vaikutuksen arvioinnista. Kuvassa 5 on yhdistetty NIS2-direktiivin riskienhallintavaatimus ISO/IEC 27001 -standardiin. Kuvassa 6 näkyy vaatimus yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53:een.

.

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
b. Poikkeamien käsittely.		
Menettelyt ja roolit poikkeamien ehkäisemisestä, havainnoinnista, analysoinnista, hallitsemisesta ja palautumisesta	A.5.24 Tietoturvahäiriöiden hallinnan suunnittelu ja valmistelu	4.3.4.5.1 Toimeenpannaan häiriötilannesuunnitelma
Menettelyt poikkeamien raportoinnista	A.5.5 Yhteydet viranomaisiin A.6.8 Tietoturvatapahtumista raportointi A.5.28 Todisteiden kerääminen	4.3.4.5.3 Luodaan raportointimenettely tavallisesta poikkeavista toiminnoista ja tapahtumista 4.3.4.5.4 Opetetaan työntekijöitä raportoimaan tietoturvallisuushäiriöistä
Lokitiedot ylläpidosta, muutoksista, käytöstä ja virheistä, tapahtumien kirjaus ja havannointi	A.8.15 Lokikirjaukset	4.3.3.6.4 Kirjataan ja läpikäydään kaikki pääsy-yritykset kriittisiin järjestelmiin
Käytännöt poikkeaman vakavuuden ja vaikutuksen arviointiin	A.5.25 Tietoturvatapahtumien arviointi ja niistä koskevien päätösten tekeminen	
Käytännöt poikkeamaan reagoimiseksi	A.5.26 Tietoturvahäiriöihin reagointi	4.3.4.5.6 Tunnistetaan häiriöt ja reagoidaan niihin
Poikkeamien syyn arviointi ja niistä oppiminen	A.5.27 Tietoturvahäiriöistä oppiminen	4.3.4.5.10 Käsitellään ja korjataan havaitut ongelmat

Kuva 5. Toinen NIS2-direktiivin vaatimus, ISO/IEC 27001 ja IEC 62443-2-1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
b. Poikkeamien käsittely.		
Menettelyt ja roolit poikkeamien ehkäisemisestä, havainnoinnista, analysoinnista, hallitsemisesta ja palautumisesta	**DE.CM-01** Networks and network services are monitored to find potentially adverse events **DE.AE-02** Potentially adverse events are analyzed to better understand associated activities **DE.AE-08** Incidents are declared when adverse events meet the defined incident criteria **RS.MA-01** The incident response plan is executed in coordination with relevant third parties once an incident is declared	IR-04, IR-06, IR-07, SR-03, SR-08, IR-04, IR-08, AU-06, CA-07, IR-04, SI-04, AC-02, AU-12, CA-07, CM-03, SC-05, SC-07, SI-04
Menettelyt poikkeamien raportoinnista	**RS.CO-02** Internal and external stakeholders are notified of incidents **RS.CO-03** Information is shared with designated internal and external stakeholders	IR-04, IR-06, IR-07, SR-03, SR-08
Lokitiedot ylläpidosta, muutoksista, käytöstä ja virheistä, tapahtumien kirjaus ja havannointi	**PR.PS-04** Log records are generated and made available for continuous monitoring	AU-02, AU-03, AU-06, AU-07, AU-11, AU-12
Käytännöt poikkeaman vakavuuden ja vaikutuksen arviointiin	**DE.AE-04** The estimated impact and scope of adverse events are understood **RS.AN-08** An incident's magnitude is estimated and validated	IR-04, IR-08, RA-03, RA-07, PM-09, PM-11, PM-18, PM-28, PM-30
Käytännöt poikkeamaan reagoimiseksi	**ID.IM-04** Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	CP-02, IR-08, PL-02, SR-02
Poikkeamien syyn arviointi ja niistä oppiminen	**RS.AN-03** Analysis is performed to establish what has taken place during an incident and the root cause of the incident	AU-07, IR-04

Kuva 6. Toinen NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53

Kolmas riskienhallintavaatimus koskee toiminnan jatkuvuuden hallintaan. Toimijoiden tulisi luoda menettelyt toiminnan jatkuvuuteen ja häiriötilanteista palautumiseen, sekä heidän tulisi varmistaa jatkuvuus. (Lausuntopalvelu 2023, 124).

Kuvassa 7 on yhdistetty vaatimus ISO/IEC 27001- ja IEC 62443-2-1 -standardeihin. Kuvassa 8 näkyy vaatimus yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53:een.

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
c. Toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta.		
Menettelyt toiminnan jatkuvuuteen ja häiriötilanteista palautumiseen, jatkuvuuden varmistus	A.5.29 Tietoturvallisuus häiriötilanteessa A.5.30 Tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa	4.3.2.5.1 Määritellään toipumistavoitteet 4.3.2.5.3 Kehitetään ja toteutetaan liiketoimminnan jatkuvuussuunnitelmat
Määrittely varmuuskopioinnista	A.8.10 Tietojen poistaminen A.8.13 Tietojen varmuuskopiointi	4.3.2.5.6 Luodaan liiketoiminnan jatkuvuussuunitelmaa tukevat varmistusmenettelyt 4.3.4.3.9 Luodaan menettely varmuuskopioiden tekemistä ja palauttamista varten

Kuva 7. Kolmas NIS2-direktiivin vaatimus, ISO/IEC 27001 ja IEC 62443-2-1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
c. Toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta.		
Menettelyt toiminnan jatkuvuuteen ja häiriötilanteista palautumiseen, jatkuvuuden varmistus	**RS.MA-05** The criteria for initiating incident recovery are applied **RC.RP-01** The recovery portion of the incident response plan is executed once initiated from the incident response process **RC.RP-02** Recovery actions are selected, scoped, prioritized, and performed	CP-10, IR-04, IR-04, IR-08
Määrittely varmuuskopioinnista	**PR.DS-11** Backups of data are created, protected, maintained, and tested	CP-06, CP-09

Kuva 8. Kolmas NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53

Neljäs NIS2-direktiivin riskienhallintavaatimus koskee toimitusketjun turvallisuutta. Toimijoiden täytyy ottaa huomioon toimintaan vaikuttavat välittömät toimittajat ja palveluntarjoajat. Toimittajien ja palveluntarjoajien haavoittuvuudet, häiriönsietokyky, riskienhallintatoimenpiteet ja kyberturvallisuuskäytännöt tulisi myös ottaa huomioon (Lausuntopalvelu 2023, 121.)

Kuvassa 9 on yhdistetty vaatimus ISO/IEC 27001 -standardiin. Huomioitavaa on se, että 62443-2-1 -standardi ei sisällä vaatimuksia jotka käsittelevät suoraan toimitusketjua. Kuvassa 10 näkyy vaatimus yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53:een.

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
d. Toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat.		
Tieto kaikista omaan toimintaan vaikuttavista välittömistä toimittajista ja palveluntarjoajista. Turvallisuusnäkökohta välittömiin laite- ja palveluntarjoajiin	A.5.19 Tietoturvallisuus toimittajasuhteissa A.5.20 Toimittajasopimusten tietoturvallisuus A.5.21 Tietoturvallisuuden hallinta tietotekniikan toimitusketjussa	
Ota huomioon toimittajan/palveluntarjoajan haavoittuvuudet, häiriönsietokyky, riskienhallintatoimenpiteeet ja kyberturvallisuuskäytännöt	A.5.22 Toimittajien palvelujen seuranta, katselmointi ja muutoksenhallinta	

Kuva 9. Neljäs NIS2-direktiivin vaatimus, ISO/IEC 27001 ja IEC 62443-2-1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
d. Toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat.		
Tieto kaikista omaan toimintaan vaikuttavista välittömistä toimittajista ja palveluntarjoajista. Turvallisuusnäkökohta välittömiin laite- ja palveluntarjoajiin	**GV.SC-01** A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders **GV.SC-02** Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally **GV.SC-04** Suppliers are known and prioritized by criticality **GV.SC-05** Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties **ID.RA-10** Critical suppliers are assessed prior to acquisition	PM-30, SR-02, SR-03, SA-04, SR-05, SR-06, RA-09, SA-09, SR-10
Ota huomioon toimittajan/palveluntarjoajan haavoittuvuudet, häiriönsietokyky, riskienhallintatoimenpiteeet ja kyberturvallisuuskäytännöt	**GV.SC-06** Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships **GV.SC-07** The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	RA-09, SA-04, SA-09, SR-05, SR-06

Kuva 10. Neljäs NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53

Viides NIS2-direktiivin riskienhallintavaatimus koskee verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuutta. Toimijoiden tulisi ylläpitää viestintäverkkojen ja tietojärjestelmien turvallisuutta koko elinkaaren

ajan, sekä varmistaa että hankittavat järjestelmät ovat riittävän turvallisia. Turvalliset konfiguraatiot tulisi olla määritelty, sekä luvattomat ja haitalliset muutokset tulisi estää. Verkon rakenteen tulisi olla turvallinen, joka voidaan saavuttaa esimerkiksi segmentoimalla. Haitallinen liikenne tulisi havaita ja estää. (Lausuntopalvelu 2023, 120.)

Kuvassa 11 on yhdistetty vaatimus ISO/IEC 27001- ja IEC 62443-2-1 -standardeihin. Kuvissa 12 ja 13 näkyy vaatimus yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53:een.

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
e. Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen.		
Viestintäverkkojen ja tietojärjestelmien turvallisuuden ylläpito koko elinkaaren ajan	A.8.20 Verkkoturvallisuus A.8.25 Turvallinen kehittämisen elinkaari A.8.27 Turvallisen järjestelmäarkkitehtuurin- ja suunnittelun periaatteet A.8.8 Teknisten haavoittuvaisuuksien hallinta	4.3.4.3.2 Kehitetään ja toteutetaan muutostenhallintajärjestelmä 4.3.4.3.3 Arvioidaan teollisuusautomaatio- ja ohjausjärjestelmän muuttamiseen liittyvät riskit 4.3.4.3.4 Vaaditaan tietoturvapolitiikkoja järjestelmän kehittämis- tai ylläpitomuutoksille 4.3.4.3.5 Yhdistetään tietoturvallisuuden ja prosessiturvallisuuden muutostenhallinnan menettelyt 4.3.4.3.7 Luodaan ja dokumentoidaan paikkaustenhallintamenettely
Hankittavien järjestelmien riittävä turvallisuus	A.5.23 Pilvipalvelujen tietoturvallisuus A.8.30 Ulkoistettu kehittäminen	4.3.4.3.1 Määritellään ja testataan tietoturva toimintoja ja -kykyjä
Turvallisen konfiguraation määritelly ja luvattomien/haitallisten muutosten tekemisen esto	A.8.9 Konfiguraationhallinta	4.3.3.6.3 Vaaditaan vahvoja todennusmenetelmiä järjestelmänhallintaa ja sovellusten konfigurointia varten
turvallinen verkon rakenne, esimerkiksi vyöhykkeistäminen	A.8.22 Verkkojen eriyttäminen	4.3.3.4.1 Kehitetään verkon segmentointiarkkitehtuuri 4.3.3.4.2 Käytetään eristämistä tai segmentointia korkean riskitason teollisuusautomaatio- ja ohjausjärjestelmissä 4.3.3.4.3 Estetään tarpeeton tietoliikenne verkonerotuslaitteiden avulla
haitallisen liikenteen havaitseminen ja estäminen	A.8.23 Verkkosuodatus A.8.16 Valvontatoiminnot	

Kuva 11. Viides NIS2-direktiivin vaatimus, ISO/IEC 27001 ja IEC 62443-2-1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
e. Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen.		
Viestintäverkkojen ja tietojärjestelmien turvallisuuden ylläpito koko elinkaaren ajan	**ID.RA-08** Processes for receiving, analyzing, and responding to vulnerability disclosures are established **PR.PS-02** Software is maintained, replaced, and removed commensurate with risk **PR.PS-03** Hardware is maintained, replaced, and removed commensurate with risk **PR.PS-06** Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	CM-07(09), CM-11, MA-03(06), SA-03, SA-08, SA-10, SA-11, SA-15, SA-17, SC-03(01), SI-02, SC-39(01), SC-49, SC-51, SI-07, RA-05
Hankittavien järjestelmien riittävä turvallisuus	**GV.SC-06** Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships **ID.RA-09** The authenticity and integrity of hardware and software are assessed prior to acquisition and use **ID.RA-10** Critical suppliers are assessed prior to acquisition	SA-04, SA-05, SA-09, SR-05, SA-10, SA-11, SA-15, SA-17, SI-07, SR-05, SR-06, SR-10, SR-11

Kuva 12. Viides NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53 osa 1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
Turvallisen konfiguraation määritelly ja luvattomien/haitallisten muutosten tekemisen esto	**PR.PS-01** Configuration management practices are established and applied	CM-01, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-08, CM-09, CM-10, CM-11
turvallinen verkon rakenne, esimerkiksi vyöhykkeistäminen	**PR.IR-01** Networks and environments are protected from unauthorized logical access and usage	AC-03, AC-04, SC-04, SC-05, SC-07
haitallisen liikenteen havaitseminen ja estäminen	**ID.AM-03** Representations of the organization's authorized network communication and internal and external network data flows are maintained **DE.CM-09** Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events **RS.MI-01** Incidents are contained	AC-04, AC-09, AU-12,, CA-03, CA-07, CA-09, CM-03, CM-06, CM-10, CM-11, IR-04, PL-02, PL-08, PM-07, SC-34, SC-35, SI-04, SI-07

Kuva 13. Viides NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53 osa 2

Kuudes riskienhallintavaatimus koskee toimintaperiaatteita ja menettelyitä, joilla voidaan arvioida kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta. Kuvassa 14 on yhdistetty vaatimus ISO/IEC 27001- ja IEC 62443-2-1 -

standardeihin. Kuvassa 15 näkyy vaatimus yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53:een.

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
f. Toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta.		
Toimintaperiaatteen/toimenpiteiden vaikuttavuuden arviointi	A.5.35 Tietoturvallisuuden riippumaton katselmointi	4.4.2.2 Suoritetaan säännöllisin välein teollisuus- ja ohjausjärjestelmän auditointeja 4.4.3.2 Arvioidaan tietoturvallisuuden hallintajärjestelmä säännöllisin väliajoin 4.4.3.6 Seurataan ja arvioidaan teollisuuden tietoturvallisuuden hallintajärjestelmästrategioita

Kuva 14. Kuudes NIS2-direktiivin vaatimus, ISO/IEC 27001 ja IEC 62443-2-1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
f. Toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta.		
Toimintaperiaatteen/toimenpiteiden vaikuttavuuden arviointi	**GV.OV-03** Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed **ID.IM-01** Improvements are identified from evaluations **ID.IM-02** Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties **ID.IM-03** Improvements are identified from execution of operational processes, procedures, and activities	AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PM-04, PM-06, PS-01, PT-01, RA-01, RA-07, SA-01, SC-01, SI-01, SR-01, CA-02, CA-05, CA-07, CA-08, CP-02, IR-04, IR-08, PL-02, RA-03, RA-05, RA-07, SA-08, SA-11, SA-17(06), SI-02, SI-04, SR-05, , SR-06

Kuva 15. Kuudes NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53

Seitsemäs NIS2-direktiivin riskienhallintavaatimus koskee perustason kyberhygieniakäytäntöjä ja kyberturvallisuuskoulutusta. Kyberhygieniakäytännöt sisältävät esimerkiksi salasanojen vaihtoa, ohjelmistopäivityksiä ja verkon segmentointia. Jotkin määritellyt kyberhygieniakäytännöt, esimerkiksi verkon segmentointi, täytetään jo muissa vaatimuksissa. (Lausuntopalvelu 2023, 124.)

Kyberhygieniakäytäntöjen lisäksi vaatimuksen mukaan henkilöstön tulisi olla tietoisia heidän tietoturvallisuuteensa liittyvistä vastuista sekä velvoitteista, sekä heitä tulisi kouluttaa kyberturvallisuudesta. Kuvassa 16 on yhdistetty vaatimus ISO/IEC 27001- ja IEC 62443-2-1 -standardeihin. Kuvassa 17 näkyy

vaatimus yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53:een.

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
g. Perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus.		
Henkilöstön tiedotus vastuista ja velvotteista	A.5.37 Dokumentoidut toimintaohjeet A.6.2 Työsuhteen ehdot A.6.5 Työsuhteen päättymisen tai muuttumisen jälkeiset vastuut A.6.6 Salassapito- ja vaitiolositoumukset	4.3.2.6.6 Tiedotetaan politiikoista ja -menettelyistä organisaatiolle 4.3.3.2.4 Määritellään tietoturvavastuut 4.3.3.2.5 Dokumentoidaan ja tiedotetaan tietoturvaodotuksista ja -vastuista 4.3.3.2.5 Määritellään tietoturvallisuuteen liittyvät työsopimusehdot
kyberturvallisuuskoulutus	A.6.3 Tietoturvatietoisuus, -opastus ja -koulutus	4.3.2.4.1 Kehitetään koulutusohjelma 4.3.2.4.2 Annetaan koulutusta menettelyistä ja välineistä
Perustason kyberhygieniakäytännöt	A.5.17 Tunnistautumistiedot A.8.1 Käyttäjien päätelaitteet A.8.7 Haittaohjelmilta suojautuminen	4.3.4.3.8 Luodaan ja dokumentoidaan virusten ja haittaohjelmien torjunnan hallintamenettely 4.3.3.5.7 Muutetaan oletussalasanat

Kuva 16. Seitsemäs NIS2-direktiivin vaatimus, ISO/IEC 27001 ja IEC 62443-2-1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
g. Perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus.		
Henkilöstön tiedotus vastuista ja velvotteista	**GV.RR-04** Cybersecurity is included in human resources practices	PM-13, PS-01, PS-07, PS-09
kyberturvallisuuskoulutus	**PR.AT-01** Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	AT-02, AT-03
Perustason kyberhygieniakäytännöt	**PR.AA-03** Users, services, and hardware are authenticated **PR.PS-05** Installation and execution of unauthorized software are prevented	AC-07, AC-12, CM-07(02), CM-07(04), CM-07(05), SC-34, IA-02, IA-03, IA-05, IA-07, IA-08, IA-09, IA-10, IA-11

Kuva 17. Seitsemäs NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53

Kahdeksas riskienhallintavaatimus koskee toimintaperiaatteita ja menettelyitä, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä. Kuvassa 18 on yhdistetty vaatimus ISO/IEC 27001- ja IEC 62443-2-1 -standardeihin. Kuvassa 19 näkyy vaatimus yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53:een.

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
h. Toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä.		
kryptografian toimintaperiaatteet ja menettelyt	A.8.24 Salauksen käyttö	

Kuva 18. Kahdeksas NIS2-direktiivin vaatimus, ISO/IEC 27001 ja IEC 62443-2-1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
h. Toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä.		
kryptografian toimintaperiaatteet ja menettelyt	**PR.DS-01** The confidentiality, integrity, and availability of data-at-rest are protected **PR.DS-02** The confidentiality, integrity, and availability of data-in-transit are protected	AU-16, CA-03, CP-09, MP-08, SC-04, SC-07, SC-08, SC-11, SC-12, SC-13, SC-16, SC-28, SC-32, SC-39, SC-40, SC-43, SI-03, SI-04, SI-07

Kuva 19. Kahdeksas NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53

Yhdeksäs NIS2-direktiivin riskienhallintavaatimus koskee henkilöstöturvallisuutta, pääsynhallintaperiaatteita sekä omaisuudenhallintaa. Toimijoiden tulisi luoda periaatteet pääsynhallintaan, luetteloida omaisuutensa, sekä luoda menettelyt ja ohjeet omaisuudenhallintaan. Henkilöstöturvallisuus tarkoittaa esimerkiksi tarvittaessa taustatarkastuksen toteuttamista. (Lausuntopalvelu 2023, 121-122.)

Kuvassa 20 on yhdistetty vaatimus ISO/IEC 27001- ja IEC 62443-2-1 -standardeihin. Kuvissa 21 ja 22 näkyy vaatimus yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53:een.

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
i. Henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta.		
Omaisuudenhallinnan menettelyt ja ohjeet	A.5.10 Tietojen ja niihin liittyvien omaisuuserien hyväksyttävä käyttö	A.2.3.3.8.3 Laitteiden ja järjestelmien ryhmittely ja luettelon tekeminen
Omaisuuden luettelointi	A.5.9 Tietojen ja niihin liittyvien omaisuuserien luettelo	A.2.3.3.8.3 Laitteiden ja järjestelmien ryhmittely ja luettelon tekeminen
Pääsynhallinta	A.5.15 Pääsynhallinta A.5.18 Pääsyoikeudet	4.3.3.5.1 Käyttäjätilien avulla toteutetaan valtuutuksia koskevaa tietoturvapolitiikkaa 4.3.3.5.4 Pidetään kirjaa käyttäjätileistä 4.3.3.6.1 Kehitetään todennusstrategia 4.3.3.6.5 Todennetaan kaikki etäkäyttäjät tarkoituksemukaisella vahvuudella 4.3.3.6.7 Estetään pääsy käyttäjätiliin epäonnistuneiden kirjautusmisyritysten jälkeen 4.3.3.7.2 Luodaan tarkoituksenmukaiset loogiset ja fyysiset pääsynsallimismenetelmät teollisuusautomaatio- ja ohjausjärjestelmän laitteisiin pääsyä varten 4.3.3.7.4 Käytetään useita valtuutusmenetelmiä kriittisiä teollisuusautomaatio- ja ohjausjärjestelmiä varten
Työsuhteen päättymisen tai työtehtävien muutoksen huomiointi	A.5.11 Omaisuuden palauttaminen	
Taustatarkastus mikäli vaaditaan erityistä luotettavuutta	A.6.1 Taustatarkistus	4.3.3.2.2 Seulotaan henkilöstöä aluksi 4.3.3.2.3 Seulotaan henkilöstöä jatkuvasti
Menettelyt vahvojen oikeuksien käyttäjätilien ja pääkäyttäjätilien hallintaan	A.8.2 Ylläpito-oikeudet	4.3.3.7.1 Määritellään tietoturvan valtuutuspolitiikka 4.3.3.7.3 Hallitaan pääsyä tietoihin ja järjestelmiin rooleihin perustuvien käyttäjätilien avulla

Kuva 20. Yhdeksäs NIS2-direktiivin vaatimus, ISO/IEC 27001 ja IEC 62443-2-1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
i. Henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta.		
Omaisuudenhallinnan menettelyt ja ohjeet	**ID.AM-05** Assets are prioritized based on classification, criticality, resources, and impact on the mission **ID.AM-07** Inventories of data and corresponding metadata for designated data types are maintained **ID.AM-08** Systems, hardware, software, services, and data are managed throughout their life cycles	CM-09, CM-12, CM-13, MA-02, MA-06, PL-02, PM-22, PM-23, RA-03, RA-09, RA-02, SA-03, SA-04, SA-08, SA-22, SI-12, SI-18, SR-05, SR-12
Omaisuuden luettelointi	ID.AM-01 Inventories of hardware managed by the organization are maintained ID.AM-02 Inventories of software, services, and systems managed by the organization are maintained	AC-20, CM-08, PM-05, SA-05, SA-09

Kuva 21. Yhdeksäs NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53 osa 1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
Pääsynhallinta	**PR.AA-05** Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	CM-09, CM-12, CM-13, MA-02, MA-06, PL-02, PM-22, PM-23, RA-03, RA-09, RA-02, SA-03, SA-04, SA-08, SA-22, SI-12, SI-18, SR-05, SR-12
Työsuhteen päättymisen tai työtehtävien muutoksen huomiointi	**PR.AA-01** Identities and credentials for authorized users, services, and hardware are managed by the organization	AC-01, AC-02, AC-14, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-07, IA-08, IA-09, IA-10, IA-11
Taustatarkastus mikäli vaaditaan erityistä luotettavuutta	**GV.RR-04** Cybersecurity is included in human resources practices	PM-13, PS-01, PS-07, PS-09
Menettelyt vahvojen oikeuksien käyttäjätilien ja pääkäyttäjätilien hallintaan	**PR.AA-01** Identities and credentials for authorized users, services, and hardware are managed by the organization	AC-01, AC-02, AC-14, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-07, IA-08, IA-09, IA-10, IA-11

Kuva 22. Yhdeksäs NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53 osa 2

Kymmenes NIS2-direktiivin riskienhallintavaatimus koskee tarvittaessa monivaiheisen todennuksen, suojatun viestinnän ja hätäviestintäjärjestelmien toteuttamista. Vahvojen oikeuksien käyttäjätilit ja pääkäyttäjätilit tulisi suojata vahvalla suojausmenetelmällä. Mikäli esimerkiksi tietoa siirretään avoimessa verkossa, se tulisi salata riittävällä salaustekniikalla. (Lausuntopalvelu 2023, 123-124.)

Kuvassa 23 on yhdistetty vaatimus ISO/IEC 27001- ja IEC 62443-2-1 -standardeihin. Kuvassa 24 näkyy vaatimus yhdistettynä NIST Cybersecurity Frameworkin osioihin ja NIST SP 800-53:een. Huomattavaa on, että ISO/IEC 27001, IEC 62443-2-1 tai NIST Cybersecurity Framework eivät sisällä osioita suojatusta varaviestintäkanavasta.

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
j. Tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.		
Vahvojen oikeuksien käyttäjätilit ja pääkäyttäjätilit vahvalla suojausmenetelmällä (Esimerkiksi MFA)	A.8.5 Turvallinen todentaminen	4.3.3.6.3 Vaaditaan vahvoja todennusmenetelmiä järjestelmänhallintaa ja sovellusten konfigurointia varten
Jos esimerkiksi tietoa siirretään avoimessa tietoverkossa, sitä tulisi salata riittävällä salaustekniikalla	A.8.24 Salauksen käyttö	A.3.4.4.3.2 Lisäkäytännöt d) 4.3.3.6.9 Käytetään todennusta tehtävien välisessä liikenteessä
Tarvittaessa suojattu varaviestintäkanava joka ei ole riippuvainen muusta järjestelmästä ja jossa on riittävä saatavuus ja luottamuksellisuus		

Kuva 23. Kymmenes NIS2-direktiivin vaatimus, ISO/IEC 27001 ja IEC 62443-2-1

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
j. Tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.		
Vahvojen oikeuksien käyttäjätilit ja pääkäyttäjätilit vahvalla suojausmenetelmällä (Esimerkiksi MFA)	**PR.AA-03** Users, services, and hardware are authent	AC-07, AC-12, IA-02, IA-03, IA-05, IA-07, IA-08, IA-09, IA-10, IA-11
Jos esimerkiksi tietoa siirretään avoimessa tietoverkossa, sitä tulisi salata riittävällä salaustekniikalla	**PR.DS-02** The confidentiality, integrity, and availabili	AU-16, CA-03, SC-04, SC-07, SC-08, SC-11, SC-12, SC-13, SC-16, SC-40, SC-43, SI-03, SI-04, SI-07
Tarvittaessa suojattu varaviestintäkanava joka ei ole riippuvainen muusta järjestelmästä ja jossa on riittävä saatavuus ja luottamuksellisuus		

Kuva 24. Kymmenes NIS2-direktiivin vaatimus, NIST CSF ja NIST SP 800-53

12 TULOKSET

NIS2-direktiivi on EU:n kyberturvallisuuden parantamiseen pyrkivä direktiivi, joka asettaa vaatimuksia valmistavan teollisuuden toimijoille, mikäli he ovat keskisuuria tai suurempia toimijoita, sekä valmistavat direktiivin alla määritel-

tyjä tuotteita. NIS2-direktiivi asettaa sen alaisille valmistavan teollisuuden toimijoille vaatimuksia hallintoelimen koulutuksesta, kyberturvallisuuden riskienhallinnasta, raportointivelvollisuudesta ja toimijaksi ilmoittautumisesta. Tämän luvun alaluvuissa käsitellään tarkemmin miten valmistavan teollisuuden toimijat voivat käytännössä lähestyä NIS2-direktiivin asettamia vaatimuksia.

12.1 Hallintoelimen koulutus

Hallintoelimen täytyy NIS2-direktiivin mukaan osallistua koulutukseen kyberturvallisuuden riskienhallinnasta, sekä hyväksyä toimijoiden toteutus kymmenestä NIS2-direktiivin vaatimasta riskienhallinnan toimenpiteestä (Lausuntopalvelu 2023, 45). Hallintoelimen tulisi siis perehtyä NIS2-direktiivin asettamiin vaatimuksiin, sekä osallistua koulutukseen riskienhallinnasta. Kun hallintoelin on saanut koulutusta riskienhallinnasta, sen tulisi hyväksyä toimijan toimenpiteet riskienhallinnasta.

12.2 Kyberturvallisuuden riskienhallinnan toimenpiteet

NIS2-direktiiviä varten toimijalla tulisi olla jatkuva, kaikki vaaratekijät huomioiva kyberturvallisuuden riskienhallinnan toimintamalli, jonka avulla voidaan tunnistaa, analysoida, arvioida ja käsitellä riskejä säännöllisesti. Riskit tulisi käsitellä, jotta niiden todennäköisyys on minimoitu, poistettu tai ulkoistettu, ja mahdolliset hyväksytyt riskit tulisi perustella. (Lausuntopalvelu 2023, 119-120.)

NIS2-direktiivin riskienhallinnan toimenpiteiden lähestymiseen voidaan käyttää tämän opinnäytetyön liitettä 1 ja 2, jotta saadaan käytännön toteutukseen ohjeistusta. Hallintakeino määritellään toimenpiteenä, joka säilyttää tai muuttaa riskiä (SFS-EN ISO/IEC 31000:2018, 7).

Liitteessä 1 on kerättynä hallintakeinoja ja vaatimuksia ISO/IEC 27001- ja IEC 62443-2-1 -standardeista. ISO/IEC 27002 -standardi sisältää yksityiskohtaista ohjeistuista ISO/IEC 27001 -hallintakeinoista, jota voidaan käyttää apuna hallintakeinojen toteutukseen. IEC 62443-2-1 -standardi soveltuu OT-ympäristöön.

Liitteessä 2 on yhdistetty NIST Cybersecurity Frameworkin osioita NIS2-direktiivin vaatimuksiin, jonka informatiivisten referenssien kautta on yhdistetty NIST SP 800-53 -hallintakeinot. NIST SP 800-53 -hallintakeinoja voi soveltaa OT-ympäristöön käyttämällä NIST SP 800-82 -ohjeistusta (NIST 2023, 5).

NIS2-direktiiviä koskevan suosituksen mukaan riskienhallinta kannattaa toteuttaa ajankohtaisten parhaiden käytäntöjen ja standardien avulla (Lausuntopalvelu 2023, 120). Riskienhallinnan toimintamallin toteuttamiseen toimija voi siis käyttää esimerkiksi ISO/IEC 31000 -standardia, joka kuvailee viitekehyksen riskienhallinnalle (Enisa 2022, 11). Toimija voi käyttää myös ISO/IEC 27005 -standardia, joka antaa ohjeistusta riskienhallinnan toteuttamiseen ISO/IEC 31000 -standardin mukaisesti, erityisesti tietoturvallisuuden näkökulmasta (ISO/IEC 27005:2022, 5).

OT-järjestelmien riskienhallintaan valmistavan teollisuuden toimija voi käyttää esimerkiksi NIST Risk Management Framework (RMF) viitekehystä, jonka sopeutus OT-järjestelmiin kuvataan julkaisussa NIST SP 800-82r3. (NIST 2023, 41).

12.2.1 Riskienhallinnan toimenpiteiden ohjeistusta hallintakeinojen tueksi

NIS2-direktiivin vaatimuksiin liittyviksi puutteiksi teollisuudessa havaittiin riskienhallinnan ja johdon vähäisen tuen lisäksi toimittajahallinnan kehittäminen ja sidonnaisuuksien tunnistaminen, joka liittyy toimitusketjun turvallisuutta koskevaan riskienhallinnan toimenpiteeseen (Lausuntopalvelu 2023, 78). OT-kyberturvallisuuden riskienhallinnan erityistarpeissa esiin nousee ihmisten turvallisuuden lisäksi toimitusketjun turvallisuuden tärkeys (NIST 2023, 54).

Suurin osa organisaatioista, joilla on käytössä OT-järjestelmiä ovat riippuvaisia toimittajista ja kolmannen osapuolen palveluntarjoajista, jotka voivat vahingossa tai tahallisesti vaikuttaa esimerkiksi OT-järjestelmän saatavuuteen ja eheyteen. Toimittajien ja kolmansien osapuolien palveluntarjoajien kyvykkyys, luotettavuus ja heidän toimitusketjunsa suhteet ja riippuvaisuuksiin liittyvät riskit tulisi selvittää. (NIST 2023, 54.)

Parantaakseen toimitusketjun turvallisuutta, valmistavan teollisuuden toimijat voivat käyttää esimerkiksi NIST SP 800-161-ohjeistusta kyberturvallisuuden toimitusketjun riskienhallinnasta. NIST SP 800-161 antaa yksityiskohtaisen kuvauksen toimitusketjun kyberturvallisuuden riskienhallinnan toteutuksesta, mukaan lukien ohjeistusta toimitusketjun riskien arvioinnista, ja se soveltuu sekä IT- että OT-ympäristöihin. (NIST 2022, 2; NIST 2023, 55.)

Poikkeamien käsittelyn hallintakeinojen tukemiseksi toimija voi käyttää Enisan luomaa ohjeistusta, Good Practice Guide for Incident Management. Ohjeistus käsittelee informaatioteknologiaan ja tietoturvallisuuteen liittyvää poikkeamien hallintaa, painottaen poikkeamien käsittelyä. Ohjeistuksen kohdeyleisö on Computer emergency response team (CERT), mutta sen lukemisesta hyötyvät myös muut tietoturvapoikkeamia käsittelevät ryhmät (Enisa 2010, 10, 11).

Enisan ohjeistuksen lisäksi toimija voi käyttää NIST:n luomaa ohjeistusta poikkeamien käsittelystä, NIST SP 800-61r2 - Computer Security Incident Handling Guide. Ohjeistuksen tarkoitus on tukea organisaatioita antamalla ohjeistusta poikkeamien hallinnasta, ja sen kohdeyleisö on ryhmät, jotka ovat vastuussa poikkeamien käsittelystä (NIST 2012, 4).

Kyberhygienian vaatimukseen liittyen toimija voi käyttää Traficomin suositusta perustason kyberhygieniakäytännöistä, jonka arvioitu julkaisu on vuoden 2024 alussa (Traficom 2023).

12.2.2 Riskienhallinnan dokumentointi

Mikäli valmistavan teollisuuden toimijoita epäillään rikkeistä, valvova viranomainen voi pyytää riskienhallinnan vaatimuksista dokumentointia (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 33 artikla). Toimijan täytyy siis voida perustella riskienhallinnan oikeasuhtaisuus ja toteutus, jonka takia dokumentointi on tärkeää.

OT-järjestelmissä esimerkiksi järjestelmien vaatimukset ja riski toimenpiteiden vaikuttamisesta järjestelmän toimintaan tarkoittaa sitä, että valittavat toimenpiteet riskien käsittelyyn saattavat olla rajatut (NIST 2023, 53). NIS2-direktiivi

vaatii oikeasuhtaista riskienhallintaa, joten mahdolliset OT-ympäristön rajoitteet ja niistä johtuvat toteutusmenetelmät tulee mahdollisesti perustella ja ne olisi hyvä dokumentoida.

Sen lisäksi että dokumentoinnilla voidaan todistaa NIS2-direktiivin vaatimusten täyttö, riskienhallinnan ja sen tulosten dokumentoinnilla voidaan esimerkiksi kehittää riskienhallintatoimia. Dokumentoinnista, sen säilytyksestä ja käsittelystä tulisi määritellä toimintaperiaatteet. (SFS-EN ISO/IEC 31000:2018, 20.)

12.3 Toimijaksi ilmoittautuminen

Mikäli kuuluu NIS2-direktiivin alaisiin toimijoihin, täytyy ilmoittautua 1.1.2025 mennessä valvovalle viranomaiselle. (Lausuntopalvelu 2023, 154). Valmistavan toimialan valvova viranomainen on Suomessa Turvallisuus- ja kemikaalivirasto TUKES (Lausuntopalvelu 2023, 48). Ilmoituksessa tulee olla toimijan nimi, osoitteet, yhteystiedot, IP-osoitealueet, toimijan toimiala ja toimialan osa, sekä luettelo jäsenvaltioista, joissa toimija tarjoaa NIS2-direktiivin toimialan palveluita. (Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555, 3 artikla)

12.4 Raportointivelvollisuuksiin perehtyminen

NIS2-direktiivi sisältää monivaiheisen raportointivelvollisuuden merkittävistä poikkeamista. Toimijoiden tulisi perehtyä kyseisiin velvollisuuksiin, jotta he osaavat raportoida vaatimuksien mukaisesti. Jotta raportointivelvollisuuden eri vaiheet saadaan toteutettua aikarajojen mukaisesti, toimija voi suunnitella etukäteen menetelmän merkittävien poikkeamien raportoimisesta, kenelle ilmoitetaan, mitä ilmoitetaan, missä ajassa ja raportoinnin eri vaiheet. Tämän opinnäytetyön luvussa 10.4 Raportointivelvoitteet, käsitellään tarkemmin toimijoiden raportointivelvollisuutta.

13 JOHTOPÄÄTÖKSET

Opinnäytetyössä selvitettiin mistä NIS2-direktiivissä on kyse, mitä vaatimuksia se asettaa valmistavalle teollisuudelle ja miten kyseisiä vaatimuksia voitaisiin

lähestyä. NIS2-direktiivin asettamien vaatimuksien lähestymistä käsitellään valmistavan teollisuuden toimijan näkökulmasta, sekä annetaan käytännön toimia ja ohjeistuksia.

Vaatimusten lähestymisessä on otettu huomioon sekä IT- että OT-järjestelmät, jotta valmistavan teollisuuden toimija saa ohjeistusta järjestelmiensä kokonaisturvallisuuteen. NIS2-direktiivin riskienhallinnan vaadittujen toimenpiteiden lähestymiseen tarjotaan käytännön ohjeistusta tarjoamalla hallintakeinoja standardeista ja NIST -ohjeistuksista. Hallintakeinojen lisäksi tarjotaan standardeja ja ohjeistuksia NIS2-direktiivin vaatimuksiin liittyen, esimerkiksi NIST -ohjeistusta toimitusketjun turvallisuudesta, sillä kyseiseen vaatimukseen liittyen on arvioitu olevan puutteita.

14 POHDINTA

Opinnäytetyön tarkoitus oli selvittää mitä vaatimuksia NIS2-direktiivi asettaa valmistavalle teollisuudelle, sekä miten kyseisiä vaatimuksia voitaisiin lähestyä. NIS2-direktiivi ja sen asettamat vaatimukset saatiin hyvin selvitettyä, sekä saatiin luotua käytännön ohjeistus toimista, joita valmistavan teollisuuden toimijan täytyy toteuttaa. Erityisesti ohjeistuksessa onnistuttiin vastaamaan hallintoelimen koulutukseen, riskienhallintaan, toimijaksi ilmoittautumiseen ja raportointivelvollisuuksiin liittyviin vaatimuksiin.

Riskienhallinnan sisältävien kymmenen vaaditun toimenpiteen ohjeistus jäi kuitenkin toivottua epämääräisemmäksi. Toimijoilla on omat ympäristönsä ja riskinsä, jonka lisäksi esimerkiksi toimijan koko vaikuttaa oikeasuhtaisuuteen. Koska NIS2-direktiivin vaatimien kymmenen riskienhallinnan toimenpiteiden tulee olla oikeasuhtaisia, tutkimuksen perusteella ei voi luoda yksityiskohtaista ja yleispätevää ohjeistusta.

NIS2-direktiivin kymmenen vaadittua riskienhallinnan toimepidettä ovat oikeasuhtaisesti toteutettavia, otsikkotasolla olevia toimenpiteitä. Tutkimuksen perusteella vaatimukset eivät ole yksityiskohtaisia, joka tarkoittaa sitä että valvova viranomainen tulee loppukädessä päättämään toimijan kyberturvallisuu-

den riittävyyden. Tämä tarkoittaisi myös sitä, että ohjeistuksen luominen aiheesta vaikeutuu entisestään, sillä vaatimukset itsessään eivät ole objektiivisia.

Vaikka riskienhallinnan kymmenestä vaaditusta toimenpiteestä ei tarkkaa ohjeistusta saatu, pystyttiin kuitenkin tarjoamaan parhaita käytäntöjä käyttämällä standardeja ja ohjeistuksia, jonka avulla toimija voi saada käytännön lähestymistavan vaatimuksiin.

Koska tarkoituksena oli luoda yleispätevä ohje, parempi lähestymistapa riskienhallinnan toimenpiteiden ohjeistukseksi olisi mahdollisesti ollut yhdistää NIS2-direktiivin vaadittujen toimenpiteiden aihealueita ohjeistuksiin parhaista käytännöistä. Tällä tavalla toimija saisi ohjeistuksen, jonka avulla he voisivat räätälöidä toimenpiteitä omiin tarpeisiinsa. Opinnäytetyössä kuitenkin haluttiin antaa ohjeistuksessa käytännön toimenpiteitä, joten hallintakeinojen valitsemista lähestymistavaksi voidaan perustella.

Vaikka opinnäytetyössä liitettyjä hallintakeinoja ei toteuttaisi, niistä voidaan kuitenkin nähdä se, että NIS2-direktiivin riskienhallinnan vaatimukset eivät ole täysin uutta asiaa. Riskienhallinnan alla määriteltyjä toimenpiteitä käsitellään esimerkiksi ISO/IEC 27001 -standardissa ja NIST Cybersecurity Frameworkissa. Vaikka toimija olisi esimerkiksi ISO/IEC 27001 -sertifioitu, sen täytyy kuitenkin ottaa huomioon riskienhallinnan lisäksi muutkin vaatimukset, esimerkiksi toimijaksi ilmoittautuminen. Kyseiset vaatimukset, jotka asetetaan riskienhallinnan lisäksi, käsitellään myös tässä opinnäytetyössä.

Vaikka opinnäytetyö ei välttämättä omineen ole riittävä tapa saavuttaa NIS2-direktiivin vaatimusten täyttämistä, se onnistui sen tavoitteessa tarjota ohjeistusta NIS2-direktiivin vaatimusten ymmärtämisestä ja niiden lähestymisestä.

14.1 Luotettavuustarkastelu

Opinnäytetyössä oli kvalitatiivinen eli ilmiötä tulkitseva lähestymistapa tulevaan direktiiviin, jota ei vielä käytännössä ole toteutettu. Tutkijan oma tulkinta vaatimuksista vaikuttaa siis tulosten luotettavuuteen, mutta tulokset kuitenkin

pohjautuvat NIS2-direktiivissä oleviin vaatimuksiin, Suomen lakiehdotuksen luonnokseen ja alan parhaita käytäntöjä edustaviin standardeihin ja ohjeistuksiin.

Opinnäytetyön tulokset ovat toistettavissa, lukuun ottamatta pientä mahdollista eroavaisuutta tekijän tulkinnassa liittyen NIS2-direktiivin otsikkotason vaadittuihin toimenpiteisiin, sekä standardien ja ohjeistuksien hallintatoimenpiteisiin, joita niihin voidaan yhdistää.

14.2 Jatkokehitysideat

Opinnäytetyön jatkokehitysideana on esimerkiksi vastaavan, tietyn toimialan näkökulmasta ohjeistuksen tekeminen NIS2-direktiivin vaatimusten lähestymiseksi. Lisäksi voitaisiin myös tarkentaa opinnäytetyötä yhdelle toimijalle, sillä oikeasuhtaisuuteen ja käytännön toimiin saataisiin tarkemmat ja konkreettisemmat ohjeet, kun toimijan ympäristö ja muuttujat ovat tiedossa.

ISO/IEC 27001- ja IEC 62443-2-1 -standardin ja NIST SP 800-53- sekä NIST SP 800-82 -ohjeistuksien lisäksi voitaisiin myös valita muita hallintakeinoja NIS2-direktiivin riskienhallinnan toimenpiteisiin lähestymiseksi.

Jatkokehitysideana voisi myös olla lähestymistapa, jossa hallintakeinojen sijaan yhdistetään NIS2-direktiivin riskienhallintavaatimuksia erilaisiin ohjeistuksiin, joiden kautta saataisiin käytännön toimenpiteitä. Esimerkiksi kryptografiaan liittyvää vaatimusta voitaisiin lähestyä NIST:n luomalla kryptografiaa käsittelevällä ohjeistuksella. Lisäksi voitaisiin luoda tarkempi ohjeistus riskien arvioimisesta, jotta toimijat osaavat toteuttaa oikeasuhtaisesti vaaditut toimenpiteet.

LÄHTEET

Australian Department of Finance. 2016. An Overview of the Risk Management Process. PDF-dokumentti. Saatavissa: https://www.finance.gov.au/sites/default/files/2019-11/Risk-Management-Process.pdf [viitattu 28.3.2024].

Calder, A & Gerrard, L. 2013. ISO27001 / ISO27002: A Pocket Guide. Second edition. Cambridge: IT Governance Publishing. E-kirja. Saatavissa: https://kaakkuri.finna.fi/Record/nelli29_mamk.2670000000432496?sid=4195145007 [viitattu 19.3.2024].

Commission. 2003. Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. PDF-dokumentti. Saatavissa: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF [viitattu 5.3.2024].

Enisa. 2010. Good Practice Guide for Incident Management. PDF-dokumentti. Saatavissa: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management [viitattu 31.3.2024].

Enisa. 2022. Risk Management Standards. PDF-dokumentti. Saatavissa: https://www.enisa.europa.eu/publications/risk-management-standards [viitattu 28.3.2024].

Euroopan parlamentin ja neuvoston asetus (EU) 2016/1148.

Euroopan parlamentin ja neuvoston asetus (EU) 2022/2555.

Eurostat. 2006. NACE Rev. 2 Statistical classification of economic activities in the European Community. PDF-dokumentti. Saatavissa: https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF [viitattu 5.3.2024].

Flaus, J-M. 2019. Cybersecurity of Industrial Systems. Hoboken: Wiley Data and Cybersecurity. E-Kirja. Saatavissa: https://kaakkuri.finna.fi/Record/nelli29_mamk.4100000008701109?sid=4195388247 [viitattu 19.3.2024].

Fortinet. Information Technology (IT) vs. Operational technology (OT) Cybersecurity. WWW-dokumentti. Saatavissa: https://www.fortinet.com/resources/cyberglossary/it-vs-ot-cybersecurity [viitattu 7.3.2024].

Heikkinen, H., Kaukko, M., Friman M., Salo, P., Kiilakoski, I., Huttunen, R., Mutaen, A., Nuutinen, L., Niemi, R. & Kemmis, S. 2023. Toimintatutkimus: käytännön opas. Tampere: Vastapaino. E-Kirja. Saatavissa: https://kaakkuri.finna.fi/Record/kaakkuri.230447?sid=4197831588 [viitattu 18.3.2024].

ISAGCA. 2021. Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments Whitepaper. PDF-dokumentti. Saatavissa: https://gca.isa.org/applying-iso/iec-27001/2-and-the-isa/iec-62443-series-for-operational-technology-environments [viitattu 7.3.2024].

ISO/IEC 27005. 2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Ohjeita tietoturvariskien hallintaan.

Jyväskylän yliopiston Koppa. Laadullinen analyysi. WWW-dokumentti. Päivitetty 28.10.2021. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/laadullinen-analyysi [viitattu 19.3.2024].

Jyväskylän yliopiston Koppa. Määrällinen analyysi. WWW-dokumentti. Päivitetty 28.10.2021. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/maarallinen-analyysi [viitattu 19.3.2024].

Lausuntopalvelu. 2023. Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. PDF-dokumentti. Saatavissa: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=4433cf2a-00ca-412e-8f47-20c55031b8dd [viitattu 19.3.2024].

NIST. 2012. NIST SP 800-61r2, Computer Security Incident Handling Guide. PDF-dokumentti. Saatavissa: https://csrc.nist.gov/pubs/sp/800/61/r2/final [viitattu 31.3.2024].

NIST. 2018. Informative References: What are they, and how are they used? WWW-dokumentti. Saatavissa: https://www.nist.gov/cyberframework/online-learning/informative-references [viitattu 29.3.2024].

NIST. 2020. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations. PDF-dokumentti. Saatavissa: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final [viitattu 31.3.2024].

NIST. 2022. SP 800-161r1. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. PDF-dokumentti. Saatavissa: https://csrc.nist.gov/pubs/sp/800/161/r1/final [viitattu 29.3.2024].

NIST. 2023. SP 800-82r3, Guide to Operational Technology (OT) Security. PDF-dokumentti. Saatavissa: https://csrc.nist.gov/pubs/sp/800/82/r3/final [viitattu 29.3.2024].

NIST. 2024. CSF 2.0 Informative References. Excel-tiedosto. Saatavissa: https://www.nist.gov/cyberframework/online-learning/informative-references [viitattu 28.3.2024].

NIST. 2024. The NIST Cybersecurity Framework (CSF) 2.0. PDF-dokumentti. Saatavissa: https://www.nist.gov/cyberframework [viitattu 31.3.2024].

Nozomi Networks. 2024. A CISO’s Guide to OT Security & Risk Management. WWW-dokumentti. Saatavissa: https://www.nozominetworks.com/blog/ot-cybersecurity-risk-management-for-cisos [viitattu 7.3.2024].

Pernaa, J. 2013. Kehittämistutkimus tutkimusmenetelmänä. Helsingin yliopiston tutkimusartikkelit. PDF-dokumentti. Saatavissa: http://hdl.handle.net/10138/317958 [viitattu 15.3.2024]

Puusa, A., Juuti, P. & Aalto, I. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. Helsinki: Gaudeamus. Saatavissa: https://kaakkuri.finna.fi/Record/kaakkuri.225650?sid=4228678509 [viitattu 25.3.2024].

SFS-EN ISO/IEC 27000. 2020. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto.

SFS-EN ISO/IEC 27001. 2023. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

SFS-EN ISO/IEC 27002. 2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot.

SFS-IEC 62443-2-1. 2013. Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 2-1: Tietoturvallisuusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten.

SFS-ISO 31000. 2018. Riskienhallinta. Ohjeet.

Traficom. 2023. Traficom laatii suositusta NIS2-direktiivin kyberturvallisuuden riskienhallinnan toimenpiteistä. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-laatii-suositusta-nis2-direktiivin-kyberturvallisuuden-riskienhallinnan [viitattu 5.3.2024].

Valtioneuvosto. 2023. Hallituksen esitys Euroopan unionin kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. WWW-dokumentti. Saatavissa: https://valtioneuvosto.fi/hanke?tunnus=LVM027:00/2023 [viitattu 27.3.2024].

Vilkka, H. 2021. Näin onnistut opinnäytetyössä: ratkaisut tutkimuksen umpikujiin. Jyväskylä: PS-kustannus. E-kirja. Saatavissa: https://kaakkuri.finna.fi/Record/kaakkuri.227174?sid=4197398637 [viitattu 15.3.2024].

Vilkka, H. 2023. Kirjallisuuskatsaus metodina, opinnäytetyön osana ja tekstilajina. Helsinki: Art House. E-kirja. Saatavissa: https://kaakkuri.finna.fi/Record/kaakkuri.229784?sid=4197281565 [viitattu 15.3.2024].

Liite 1

NIS2-direktiivin riskienhallintavaatimuksiin yhdistetyt ISO/IEC 27001 ja IEC 62443 -standardien hallintakeinot ja vaatimukset

NIS2-direktiivin vaatimus	ISO/IEC 27001/2:2022 hallintakeino	IEC 62443-2-1:2009 vaatimus
Kaikkien vaaratekijöiden huomiointi (fyysinen ympäristö)	A.7.1 Fyysiset turva-alueet A.7.2 Kulunvalvonta A.7.3 Toimistojen, tilojen ja laitteistojen suojaus A.7.4 Fyysisen turvallisuuden valvonta A.7.5 Suojaus fyysisiä ja ympäristön aiheuttamia uhkia vastaan A.7.8 Laitteiden sijoitus ja suojaus A.7.11 Tukipalvelut	4.3.3.3.1 Laaditaan toisiaan täydentävät fyysisen ja verkkoon liittyvän tietoturvallisuuden politiikat 4.3.3.3.2 Perustetaan fyysisen tietoturvan ulkoraja(t) 4.3.3.3.3 Toteutetaan kulunvalvonta 4.3.3.3.6 Suojataan yhteydet 4.3.3.3.10 Määritellään menettelyt kriittisten suojattavien kohteiden tilapäistä suojaamista varten 4.3.3.4 Suojataan suojattavat kohteet ympäristön aiheuttamia vahinkoja vastaan
a. Riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat.	A.5.1 Tietoturvallisuutta koskevat toimintaperiaatteet A.5.2 Tietoturvaroolit ja -vastuut A.5.31 Lainsäädäntöön, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyvät	4.3.3.2.1 Laaditaan henkilöstön tietoturvapolitiikka 4.3.2.6.1 Kehitetään tietoturvapolitiikat 4.3.2.6.2 Kehitetään tietoturvamenettelyt 4.3.2.6.3 Ylläpidetään yhdenmukaisuutta riskien hallintajärjestelmien välillä
b. Poikkeamien käsittely.	A.5.5 Yhteydet viranomaisiin A.5.24 Tietoturvahäiriöiden hallinnan suunnittelu ja valmistelu A.5.25 Tietoturvatapahtumien arviointi ja niistä koskevien päätösten tekeminen A.5.26 Tietoturvahäiriöihin reagointi A.5.27 Tietoturvahäiriöistä oppiminen A.5.28 Todisteiden kerääminen A.6.8 Tietoturvatapahtumista raportointi A.8.15 Lokikirjaukset	4.3.4.5.1 Toimeenpannaan häiriötilannesuunnitelma 4.3.4.5.3 Luodaan raportointimenettely tavallisesta poikkeavista toiminnoista ja tapahtumista 4.3.4.5.4 Opetetaan työntekijöitä raportoimaan tietoturvallisuushäiriöistä 4.3.4.5.6 Tunnistetaan häiriöt ja reagoidaan niihin 4.3.4.5.10 Käsitellään ja korjataan havaitut ongelmat 4.3.3.6.4 Kirjataan ja läpikäydään kaikki pääsy-yritykset kriittisiin järjestelmiin
c. Toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta.	A.5.29 Tietoturvallisuus häiriötilanteessa A.5.30 Tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa A.8.10 Tietojen poistaminen A.8.13 Tietojen varmuuskopiointi	4.3.2.5.1 Määritellään toipumistavoitteet 4.3.2.5.3 Kehitetään ja toteutetaan liiketoimminnan jatkuvuussuunnitelmat 4.3.2.5.6 Luodaan liiketoiminnan jatkuvuussuunitelmaa tukevat varmistusmenettelyt 4.3.4.3.9 Luodaan menettely varmuuskopioiden tekemistä ja palauttamista varten
d. Toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat.	A.5.19 Tietoturvallisuus toimittajasuhteissa A.5.20 Toimittajasopimusten tietoturvallisuus A.5.21 Tietoturvallisuuden hallinta tietotekniikan toimitusketjussa A.5.22 Toimittajien palvelujen seuranta, katselmointi ja muutoksenhallinta	
e. Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen.	A.5.23 Pilvipalvelujen tietoturvallisuus A.8.8 Teknisten haavoittuvaisuuksien hallinta A.8.9 Konfiguraationhallinta A.8.16 Valvontatoiminnot A.8.20 Verkkoturvallisuus A.8.22 Verkkojen eriyttäminen A.8.23 Verkkosuodatus A.8.25 Turvallinen kehittämisen elinkaari A.8.27 Turvallisen järjestelmäarkkitehtuurin- ja suunnittelun periaatteet A.8.30 Ulkoistettu kehittäminen	4.3.3.4.1 Kehitetään verkon segmentointiarkkitehtuuri 4.3.3.4.2 Käytetään eristämistä tai segmentointia korkean riskitason teollisuusautomaatio- ja ohjausjärjestelmissä 4.3.3.4.3 Estetään tarpeeton tietoliikenne verkonerotuslaitteiden avulla 4.3.3.6.3 Vaaditaan vahvoja todennusmenetelmiä järjestelmänhallintaa ja sovellusten konfigurointia varten 4.3.4.3.1 Määritellään ja testataan tietoturva toimintoja ja -kykyjä 4.3.4.3.2 Kehitetään ja toteutetaan muutostenhallintajärjestelmä 4.3.4.3.3 Arvioidaan teollisuusautomaatio- ja ohjausjärjestelmän muuttamiseen liittyvät riskit 4.3.4.3.4 Vaaditaan tietoturvapolitiikkoja järjestelmän kehittämis- tai ylläpitomuutoksille 4.3.4.3.5 Yhdistetään tietoturvallisuuden ja prosessiturvallisuuden muutostenhallinnan menettelyt 4.3.4.3.7 Luodaan ja dokumentoidaan paikkaustenhallintamenettely
g. Perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus.	A.5.17 Tunnistautumistiedot A.5.37 Dokumentoidut toimintaohjeet A.6.2 Työsuhteen ehdot A.6.3 Tietoturvatietoisuus, -opastus ja -koulutus A.6.5 Työsuhteen päättymisen tai muuttumisen jälkeiset vastuut A.6.6 Salassapito- ja vaitiolositoumukset A.8.1 Käyttäjien päätelaitteet A.8.7 Haittaohjelmilta suojautuminen	4.3.2.4.1 Kehitetään koulutusohjelma 4.3.2.4.2 Annetaan koulutusta menettelyistä ja välineistä 4.3.2.6.6 Tiedotetaan politiikoista ja -menettelyistä organisaatiolle 4.3.3.2.4 Määritellään tietoturvavastuut 4.3.3.2.5 Dokumentoidaan ja tiedotetaan tietoturvaodotuksista ja -vastuista 4.3.3.2.6 Määritellään tietoturvallisuuteen liittyvät työsopimusehdot 4.3.3.5.7 Muutetaan oletussalasanat 4.3.4.3.8 Luodaan ja dokumentoidaan virusten ja haittaohjelmien torjunnan hallintamenettely
h. Toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä.	A.8.24 Salauksen käyttö	
i. Henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta.	A.5.10 Tietojen ja niihin liittyvien omaisuuserien hyväksyttävä käyttö A.5.9 Tietojen ja niihin liittyvien omaisuuserien luettelo A.5.15 Pääsynhallinta A.5.18 Pääsyoikeudet A.5.11 Omaisuuden palauttaminen A.6.1 Taustatarkistus A.8.2 Ylläpito-oikeudet	A.2.3.3.8.3 Laitteiden ja järjestelmien ryhmittely ja luettelon tekeminen 4.3.3.2.2 Seulotaan henkilöstöä aluksi 4.3.3.2.3 Seulotaan henkilöstöä jatkuvasti 4.3.3.5.1 Käyttäjätilien avulla toteutetaan valtuutuksia koskevaa tietoturvapolitiikkaa 4.3.3.5.4 Pidetään kirjaa käyttäjätileistä 4.3.3.6.1 Kehitetään todennusstrategia 4.3.3.6.5 Todennetaan kaikki etäkäyttäjät tarkoituksemukaisella vahvuudella 4.3.3.6.7 Estetään pääsy käyttäjätiliin epäonnistuneiden kirjautusmisyritysten jälkeen 4.3.3.7.1 Määritellään tietoturvan valtuutuspolitiikka 4.3.3.7.2 Luodaan tarkoituksenmukaiset loogiset ja fyysiset pääsynsallimismenetelmät teollisuusautomaatio- ja ohjausjärjestelmän laitteisiin pääsyä varten 4.3.3.7.3 Hallitaan pääsyä tietoihin ja järjestelmiin rooleihin perustuvien käyttäjätilien avulla 4.3.3.7.4 Käytetään useita valtuutusmenetelmiä kriittisiä teollisuusautomaatio- ja ohjausjärjestelmiä varten
j. Tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.	A.8.5 Turvallinen todentaminen A.8.24 Salauksen käyttö	4.3.3.6.3 Vaaditaan vahvoja todennusmenetelmiä järjestelmänhallintaa ja sovellusten konfigurointia varten 4.3.3.6.9 Käytetään todennusta tehtävien välisessä liikenteessä A.3.4.4.3.2 Lisäkäytännöt d)

NIS2-direktiivin riskienhallintavaatimuksiin yhdistetyt NIST CSF -osiot ja NIST SP 800-53 -hallintakeinot

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1 hallintakeino
Kaikkien vaaratekijöiden huomiointi (Fyysinen ympäristö)	PR.AA-06 PR.IR-02 DE.CM-02 PR.IR-03	CP, IR, SA-08, SC-06 ,SC-24, SC-36, SC-39, SI-13, CA-07, PE-02, PE-03, PE-04,PE-05, PE-06, PE-08, PE-09, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-18PE-18, PE-19, PE-20, PE-23
a. Riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat.	GV.PO-01 GV.PO-02	AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01
b. Poikkeamien käsittely.	DE.CM-01 RS.CO-02 RS.CO-03 PR.PS-04 DE.AE-04 RS.AN-08 ID.IM-04 RS.AN-03 DE.AE-02 DE.AE-08 RS.MA-01 RS.MI-01 RS.MI-02	PL-02, CP-02, IR-04, IR-06, IR-07, SR-02, SR-03, SR-08, IR-04, IR-08, AU-06, CA-07, IR-04, SI-04, AC-02, AU-02, AU-03, AU-06, AU-07, AU-11, AU-12, CA-07, CM-03, SC-05, SC-07, SI-04
c. Toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta.	RS.MA-05 RC.RP-01 RC.RP-02 PR.DS-11	CP-06, CP-09, CP-10, IR-04, IR-04, IR-08
d. Toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat.	GV.SC-01 GV.SC-02 GV.SC-04 GV.SC-05 ID.RA-10 GV.SC-06 GV.SC-07	PM-30, SR-02, SR-03, SA-04, SR-05, SR-06, RA-09, SA-09, SR-10
e. Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen.	ID.RA-08 PR.PS-02 PR.PS-03 PR.PS-06 GV.SC-06 ID.RA-09 ID.RA-10 PR.PS-01 PR.IR-01 ID.AM-03 DE.CM-09 RS.MI-01	AC-03, AC-04, AC-09, AU-12, CA-03, CA-07, CA-09, CM-01, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-07(09), CM-08, CM-09, CM-10, CM-11, IR-04, MA-03(06), PL-02, PL-08, PM-07, SA-03, SA-04, SA-05, SA-08, SA-09, SA-10, SA-11, SA-15, SA-17, SC-03(01), SC-04, SC-05, SC-07, SC-34, SC-35, SC-39(01), SC-49, SC-51, SI-02, SI-04, SI-07, SR-05, SR-06, SR-10, SR-11, RA-05
f. Toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta.	GV.OV-03 ID.IM-01 ID.IM-02 ID.IM-03	AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PM-04, PM-06, PS-01, PT-01, RA-01, RA-07, SA-01, SC-01, SI-01, SR-01, CA-02, CA-05, CA-07, CA-08, CP-02, IR-04, IR-08, PL-02, RA-03, RA-05, RA-07, SA-08, SA-11, SA-17(06), SI-02, SI-04, SR-05, , SR-06

NIS 2 Vaatimus	NIST Cybersecurity Framework	NIST SP 800-53 Rev 5.1.1
g. Perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus.	GV.RR-04 PR.AT-01 PR.AA-03 PR.PS-05	AC-07, AC-12, AT-02, AT-03, CM-07(02), CM-07(04), CM-07(05), IA-03, IA-05, IA-07, IA-08, IA-09, IA-10, IA-11, PM-13, PS-01, PS-07, PS-09, SC-34
h. Toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä.	PR.DS-01 PR.DS-02	AU-16, CA-03, CP-09, MP-08, SC-04, SC-07, SC-08, SC-11, SC-12, SC-13, SC-16, SC-28, SC-32, SC-39, SC-40, SC-43, SI-03, SI-04, SI-07
i. Henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta.	ID.AM-05 ID.AM-07 ID.AM-08 ID.AM-01 ID.AM-02 PR.AA-05 PR.AA-01 GV.RR-04 PR.AA-01	AC-01, AC-02, AC-14, AC-20, CM-08, CM-09, CM-12, CM-13, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-07, IA-08, IA-09, IA-10, IA-11, MA-02, MA-06, PL-02, PM-05, PM-13, PM-22, PM-23, PS-01, PS-07, PS-09, RA-03, RA-09, RA-02, SA-03, SA-04, SA-05, SA-08, SA-09, SA-22, SI-12, SI-18, SR-05, SR-12
j. Tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.	PR.AA-03 PR.DS-02	AC-07, AC-12, AU-16, CA-03, IA-02, IA-03, IA-05, IA-07, IA-08, IA-09, IA-10, IA-11, SC-07, SC-08, SC-11, SC-12, SC-13, SC-16, SC-40, SC-43, SI-03, SI-04, SI-07