Eero Vento

TIETOTURVATIETOISUUSOHJELMAN VAATIMUKSET KELAN TIETOTURVAYKSIKÖSSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Vento, Eero
Tietoturvatietoisuusohjelman vaatimukset Kelan tietoturvayksikössä
Jyväskylä: Jyväskylän yliopisto, 2024, 64 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Frantti, Tapio

Elämme maailmassa, jossa romanssihuijarit kalastelevat rahaa viattomilta ihmisiltä, terveystietoja kaupitellaan internetin pimeällä puolella ja kyberhyökkäysvoi estää pääsyn pankkitilille jopa tunneiksi. Tänä päivänä myös digitaalinen ulottuvuus on jatkuvasti läsnä elämässämme. Arkiset askareet kytkeytyvät internetiin tavalla tai toisella. Lähes kaikissa tietoverkkohyökkäyksissä avainasemassa on ihmisen toiminta. Suunnitelmallinen hyökkäys alkaa usein täysin tavalliselta vaikuttavalla sähköpostiviestillä tai puhelinsoitolla. Tietoturvallisuudessa inhimillinen näkökulma on kiistatta yksi keskeisimmistä näkökulmista, joka kaikkien organisaatioiden on otettava tietoturvallisuuden hallinnassa huomioon. Yhteiskuntamme ei toimi ilman internetin varaan rakennettuja palveluita, jotka riippuvat yritysten tai julkishallinnon organisaatioiden toiminnasta. Eräs yhteiskunnan elintärkeistä toiminnoista on sosiaaliturvan toteutuminen, jossa Kelalla on itsenäisenä julkisoikeudellisena laitoksena keskeinen roolinsa. Kelassa tietoturvallisuus otetaan vakavasti ja sen hallintaan sovelletaankin kansainvälisesti tunnettua ISO/IEC 27001 -standardia. Standardi edellyttää sen mukaisesti toimivilta organisaatioilta henkilöstön tietoturvatietoisuudesta huolehtimista. Tätä varten Kelassa on tavoitteena suunnitella ja toteuttaa koko organisaan kattava tietoturvatietoisuusohjelma. Työ on aloitettu tietoturvayksiköstä, jonka tietoisuusohjelmaa koskevia standardeihin, viitekehyksiin, lainsäädäntöön, määräyksiin, sisäisiin ja sidosryhmien odotuksiin perustuvia vaatimuksia on lähdetty selvittämään tämän pro gradu -tutkielman muodossa. Tutkielman tutkimusstrategiana on käytetty tapaustukimusta, jossa keskeisinä menetelminä toimivat haastattelut sekä dokumenttianalyysi. Tutkimusmenetelmissä on hyödynnetty laajaa tutkimustietoon nojaavaa teoreettista viitekehystä. Tutkimustyön aineistona toimivat sen lisäksi Kelan laatima julkinen dokumentaatio, tietoturvayksikön asiantuntijat sekä sidosryhmät, Kelaa koskeva lainsäädäntö sekä kansainväliset standardit ja viitekehykset. Tutkielman tuloksena muodostettiin aineiston pohjalta vaatimuskehikko, jota Kelassa on tarkoitus käyttää perustana tietoturvatietoisuusohjelman suunnittelussa. Tutkielman keskeisiä havaintoja olivat johdon tukeen, ohjelman resursointiin, suunnitteluun, sisältöön, toteutukseen sekä jatkuvaan parantamiseen liittyvät vaatimukset. Vaatimuksissa korostuivat tietoisuusohjelman kytkeminen organisaation strategiaan, riittävän ajankäytön mahdollistaminen, riskienarvioinnin merkitys suunnittelussa sekä monipuolisen viestinnän toteuttaminen.

Asiasanat: tietoturva, tietoisuusohjelma, tietoisuus, osaaminen, kehittäminen, vaatimukset

ABSTRACT

Vento, Eero
Requirements for the information security awareness program in Kela's Information Security Unit
Jyväskylä: University of Jyväskylä, 2024, 64 pp.
Cyber Security, Master's Thesis
Supervisor: Frantti, Tapio

We live in a world where romance scammers exploit innocent people for financial gain, sensitive health information is sold on the dark web, and cyberattacks can disrupt access to bank accounts. Today, the digital dimension is an integral part of our lives. Daily tasks are connected to the internet in one way or another. In almost all cyberattacks, human behavior plays a crucial role. The human factor is undoubtedly one of the most critical aspects that organizations must consider in security management. Society depends on internet-based services supported by the operations of companies and public sector organizations. One essential function is the implementation of social security, in which Kela, as an independent public institution, plays a significant role. Kela applies the internationally recognized ISO/IEC 27001 standard for managing information security. The standard sets requirements for information security awareness. To meet the requirements, Kela aims to design and implement an information security awareness program. This work has begun within Kela's Information Security Unit, which has started to identify program requirements based on standards, frameworks, legislation, regulations, and the expectations of internal and external stakeholders. This effort is documented in this Master's thesis, which uses a case study research strategy, employing interviews and document analysis as the primary methods. The research methods are supported by the literature review based on existing studies. Data sources include Kela's public documentation, experts from Kela, relevant legislation, and international standards and frameworks. The thesis resulted in a set of requirements to be used as the foundation for designing Kela's awareness program. Key findings emphasized requirements related to management support, resourcing, planning, content, implementation, and continuous improvement. The findings highlighted the importance of aligning the awareness program with the organizational strategy, ensuring sufficient time allocation, incorporating risk assessment in the planning phase, and employing diverse communication strategies.

Keywords: information security, awareness program, competence, development, requirements

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kyberrikollisuuden kehittyvät toimintatavat ja maailman turvallisuuspoliittisesti epävakaana jatkuva tilanne haastavat organisaatioita, erityisesti julkishallinnon organisaatioita, jatkuvaan turvallisuustoimintansa kehittämiseen sekä varautumiseen. Myös Kelassa suhtaudutaan turvallisuuden ja erityisesti tietoturvan kehittämiseen yhteiskunnallisen aseman edellyttämällä vakavuudella.

Kelassa on viimevuosina määrätietoisesti kehitetty kokonaisturvallisuutta. Keskeiseksi toimenpiteeksi voidaan katsoa turvallisuusyksikön perustaminen, jonka tehtävänä on johtaa, koordinoida ja kehittää Kela-tasoista turvallisuustoimintaa. Yksiköllä on keskeinen rooli turvallisuuden kehittämistyössä, jota toteutetaan laajasti Kelan tulosyksiköiden sekä toiminnallisten yksiköiden yhteistyönä. (Kela 2023b, s. 43)

Turvallisuuden kehittämiselle on Kelassa asetettu jo elokuussa 2021 Kela-tasoiset tavoitteet Turvallisuuden strategisten linjausten muodossa, joiden toimeenpanossa turvallisuusyksiköllä on ollut keskeinen rooli (Kela 2023b, s. 43). Eräinä linjausten toimeenpanoon liittyvänä konkreettisena toimenpiteenä ovat olleet Kelan tietoturvayksikön toteuttamat kehittämistehtävät niin hallinnollisen kuin teknisen tietoturvan osa-alueilla. Pro gradu -tutkielman kannalta merkityksellinen kehitystehtävä on ollut ISO/IEC 27001 -standardin mukaisen tietoturvan hallintajärjestelmän toteuttamisprojektin edistäminen. (Kela 2023b, s. 40)

Tietoturvallisuuden hallintajärjestelmä on kokonaisuus, joka kuvaa toimintaperiaatteet, menettelytavat, ohjeet sekä niihin liittyvät resurssit ja toiminnot, joita organisaatio hallinnoi kootusti suojatakseen tieto-omaisuuttaan. Sen avulla organisaation on mahdollista järjestelmällisesti hallita ja parantaa tietoturvallisuuttaan liiketoimintatavoitteiden saavuttamista varten. (Suomen standardoimisliitto SFS ry 2020, s. 16) Tietoturvallisuuden hallintajärjestelmän rakentamisessa on Kelassa noudatettu kansainvälistä ISO/IEC 27001 -standardia ja sen vaatimuksia. Projektin tehtävänä on vastata standardin vaatimuksiin hallintajärjestelmän rakenteen osalta sekä ottaa käyttöön standardissa mainittuja hallintakeinoja, mikäli niiden käyttöönotto Kelan kontekstissa on perusteltua. Ensivaiheessa hallintajärjestelmän soveltamisalana on Kelan tietoturvayksikkö ja sitä on

tarkoitus laajentaa myöhemmin Kelan tulosyksiköihin sekä toiminnallisiin yksiköihin.

Tässä tutkielmassa henkilöstön riittävän tietoisuuden saavuttamiseksi keskeisessä asemassa on standardissa (Suomen standardoimisliitto SFS ry 2022, s. 70) mainittu henkilöstön koulutusohjelman (jäljempänä tietoturvatietoisuusohjelma tai tietoisuusohjelma) suunnittelu ja toteuttaminen. Pro gradu -tutkielma muodostaa vaatimuskehikon itse tietoisuusohjelman kehittämiselle, jotta työtä Kelassa voidaan jatkaa perusteltuun suuntaan. Selvillä vaatimuksilla luodaan vahva perusta tietoturvatietoisuuden kehittämiselle Kelassa. Tämä pro gradu -tutkielma on laadittu Jyväskylän yliopiston kyberturvallisuuden maisteriohjelman opinnäytteenä. Aihe on rajaukseltaan sovitettu pro gradu -tutkielmalle soveltuvaksi. Tutkielman tutkimustehtävä on: Tietoturvatietoisuusohjelman kehittämiseen asetetut vaatimukset Kelan tietoturvayksikössä.

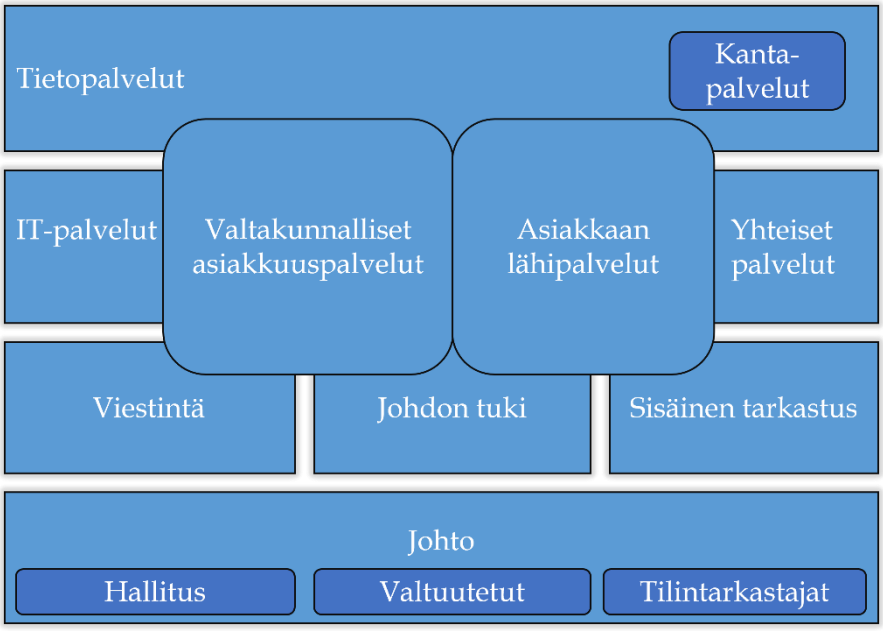
Tutkielma alkaa lyhyellä johdannolla sisältäen toimeksiantajan esittelyn. Tutkielma jatkuu aihepiiriin syventyvällä kirjallisuuskatsauksella, joka sisältää tutkielman teoreettisen viitekehyksen. Kirjallisuuskatsauksen jälkeen käydään läpi tutkimuskonsepti sisältäen valitun tutkimusstrategian ja -menetelmien esittelyt sekä itse tutkimuksen toteutuksen käytännössä. Tutkimusosiota seuraavat tutkimustulokset, joilla vastataan tutkimuskysymykseen. Tutkielman loppuosassa keskeiset löydökset tiivistetään diskurssissa johtopäätöksiksi. Johtopäätöksiä seuraa yhteenveto, jonka lopuksi esitetään joitakin tutkielmasta johdettuja kehitys- sekä jatkotutkimusehdotuksia.

2 TOIMEKSIANTAJA

Kuten tutkielman johdannostakin käy ilmi, pro gradu -tutkielma on toteutettu Kelan tietoturvayksikölle. Tässä luvussa pohjustetaan teoreettista viitekehystä esittelemällä toimeksiantajan organisaatio. Lisäksi luvussa kuvataan lyhyesti Kelan sekä tietoturvayksikön tehtäviä ja toimintaa pääpiirteittäin julkisten lähteiden avulla. Tavoitteena on muodostaa lukijalle yleiskuva Kelasta ja tietoturvayksiköstä sekä niiden toimintaympäristöstä, jotta teoreettista viitekehystä on mahdollista peilata näitä vasten.

Kela on itsenäinen julkisoikeudellinen laitos, joka toimii Suomen sosiaaliturvan toimeenpanijana eduskunnan valvonnan alaisuudessa. Sosiaaliturvan tarkoituksena on taata riittävä perustoimeentulo ja perusturva sekä Suomessa että ulkomailla asuville suomalaisille eri elämäntilanteissa. (Kela, 2023a) Sosiaaliturvaan kuuluvat niin perustoimeentulotuki, lapsiperheiden etuudet, asumistuki, opintotuki kuin työttömän perusturva. Etuusprosessiin kuuluu sekä käsittely että ratkaisu, jotka ovat hajautettu ympäri Suomen toimiviin vakuutuspiireihin. (Kela, 2023b, s. 6)

Eduskunta valitsee toimintakautensa ajaksi 12 valtuutettua, jotka valvovat Kelan toimintaa tilintarkastajien lisäksi. Kelan toimintaa johtaa ja kehittää kymmenjäseninen hallitus (Kela, 2023b, s. 6). Hallituksen ja johdon lisäksi Kelan organisaatio koostuu karkeasti seitsemästä eri vastuut omaavasta yksiköstä, joita ovat Asiakkaan lähipalvelut, Valtakunnalliset asiakkuuspalvelut, Tietopalvelut, IT-palvelut, Yhteiset palvelut, Viestintä sekä Johdon tuki (Kuvio 1). Yksiköiden tehtävät ja vastuut ovat määritelty Kelan työjärjestyksissä.



KUVIO 1 Kelan organisaatiorakenne (Kela 2023b, s. 6)

Kelan sosiaaliturvan toimeenpanoa koskevista tehtävistä on säädetty eri laeissa. Laissa Kansaneläkelaitoksesta (731/2001, 2 §) säädetyt tehtävät ovat:

- etuuksista ja palvelutoiminnastaan tiedottaminen,
- etuusjärjestelmien ja oman toimintansa kehittämistä palvelevan tutkimuksen harjoittaminen,
- tilastojen, arvioiden ja ennusteiden laatiminen sekä
- toimialaansa koskevan lainsäädännön kehittämistä koskevien ehdotusten tekeminen.

Sosiaaliturvan toimeenpanijana Kelalla on keskeinen asema yhteiskunnallisessa varautumisessa. Kela kuuluu suomalaisen yhteiskunnan eri toimijoiden muodostamaan kokonaisturvallisuuden verkostoon. Se osallistuu kaikkien muiden toimijoiden ja viranomaisten lailla verkoston toimintaan. (Yhteiskunnan turvallisuusstrategia 2017, s. 7) Kelalle asetettujen tehtävien sekä vastuiden näkökulmasta keskiössä ovat turvallisuus- ja varautumistoiminta sekä yhteiskunnan kriisinsietokyvyn varmistaminen.

Valtioneuvoston periaatepäätöksessä Yhteiskunnan turvallisuusstrategiasta (2017, s. 82) on määritelty yhteiskunnan elintärkeät toiminnot. Niistä väestön toimintakyvyn ja palveluiden ylläpitämisessä Kelalla on keskeinen rooli väestön viimesijaisen toimeentulon turvaajana. Käytännössä tämä tarkoittaa varautumista toimeentulotuen häiriöttömään maksatukseen kriisi- ja häiriötilanteissa sekä poikkeusoloissa erityisesti etuustietojärjestelmien toimintavarmuudesta huolehtimalla.

Kelalla on edellä mainitun lisäksi merkittävä rooli myös sosiaali- ja terveydenhuollon palvelujen turvaamisessa, sillä se ylläpitää kansallisia sote-

tietovarantoja. Niiden merkitys kasvaa kriisitilanteissa, kun paikalliset tietojärjestelmät eivät ole sote-toimijoiden käytettävissä. (Yhteiskunnan turvallisuusstrategia 2017, s. 84) Osana kansainvälisen ja EU-toiminnan strategisia tehtäviä Kela osallistuu myös laajamittaisen maahantulon hallintaan varautumissuunnitteluyhteistyöllä eri viranomaisten kanssa (Yhteiskunnan turvallisuusstrategia 2017, s. 49).

2.1 IT-palvelujen tulosyksikkö

IT-palvelujen tulosyksikkö vastaa yksin Kelan toiminnan edellyttämien IT-palvelujen tuottamisesta, kehittämisestä sekä ylläpidosta. Tulosyksikön tehtävänä on tuottaa lainsäädäntö- ja sopimusperusteisesti IT-palveluja myös Kelan sidosryhmien tarpeisiin. Yksikkö vastaa Kelan toiminnan edellyttämien IT-palvelujen jatkuvuudesta, toimintavarmuudesta sekä turvallisuudesta. IT-palvelujen erityisvastuualueena on myös Kelan tietoturvatyön johtaminen, ohjaaminen sekä kehittäminen. (Kela 2024a, s. 1)

IT-palvelujen tulosyksikön muodostavat kaksi toiminnallista kokonaisuutta: liiketoiminnan IT-palvelut sekä mahdollistavat palvelut. Toiminnallisilla kokonaisuuksilla on omat johtoryhmänsä ja niiden vastuulla on muun muassa toiminta-alueidensa palvelujen kehittäminen, elinkaarikustannusten hallinta, toiminnallisten tavoitteiden laatiminen strategisten tavoitteiden perusteella, henkilöiden allokointi sekä IT-johtoryhmän käsittelyyn menevien asioiden hyväksyntä. (Kela 2024a, s. 1)

Toiminnallisiin kokonaisuuksiin kuuluu kaiken kaikkiaan yhdeksän yksikköä: tuotanto-, teknologia-, tieto-, sote-, tietoturva-, innovaatio- ja kasvu, liiketoiminnan ohjaus, palvelutoiminnan IT- sekä yhteisten palvelujen IT-yksikkö. Yksiköt jakautuvat edelleen ryhmiin ja ryhmät tiimeihin. Kokonaisuudessaan Kelan IT-palveluissa työskentelee eri tehtävissä yhteensä yli 900 asiantuntijaa. (Kela 2024a, s. 1; Kela 2024c)

2.2 Tietoturvayksikkö

Kelan IT-palvelujen tulosyksiköstä käsin toimiva tietoturvayksikkö johtaa, ohjaa ja kehittää Kelan tietoturvatyötä. Tietoturvayksikkö tuottaa sekä Kelan keskitetyt tietoturvan hallinnan ja tilannekuvan muodostamisen palvelut. Tietoturvayksikkö vastaa Kelan toiminnan kehittämiseen liittyvistä tietoturvallisuuden asiantuntijapalveluista, tietoturvahäiriöiden hallinnasta, viranomaisyhteistyöstä sekä tietoturvan raportoinnista johdolle. Lisäksi tietoturvayksikön vastuulla on kehittää tietoturvan hallintajärjestelmää ja Kela-tasoista tietoturvariskienhallintaa sekä ohjata ja kehittää IT-jatkuvuus ja -valmiussuunnittelua. (Kela 2024a, s. 3)

Tietoturvayksikön muodostavat tietoturvaryhmä sekä tekninen tilannekuvakeskus. Yhteensä kummassakin ryhmässä työskentelee noin 50 tietoturvan

osa-alueiden sekä IT-valvonnan asiantuntijaa. Tietoturvaryhmän vastuulla ovat hallinnollisten tietoturvapalvelujen tuottaminen, joihin kuuluvat niin tieto- ja kyberturvallisuuden, kuin tietoturvakulttuurin kehittämistä, hankkeiden tietoturvatuen tuottamista, tietoturva-arkkitehtuurin kehittämistä, tietoturvatestausta sekä jatkuvuuden hallintaa. Teknisen tilannekuvakeskuksen tehtäviin kuuluvat operatiiviset palvelut, kuten tilannekuvan tuottaminen, tilannekuvan ja reagointikyvyn kehittäminen, tietoturvahäiriöiden hallinnan sekä kehittämisen koordinointi sekä toimiminen yhteyspisteenä kansallisiin tietoturvatoimijoihin. (Kela 2024b, s. 3–5)

3 TEOREETTINEN VIITEKEHYS

Tässä luvussa käydään tutkielman aihepiiriä läpi yleisestä näkökulmasta. Luku syventyy tietoturvatietoisuuden kehittämiseen organisaatioissa kirjallisuuskatsauksella, jonka lähteinä toimivat aihetta käsittelevä kirjallisuus sekä useat tutkimusartikkelit. Luvun tarkoituksena on esitellä lukijalle tutkielman keskeiset käsitteet ja muodostaa teoreettinen tietoperusta tietoturvatietoisuudesta ja sen kehittämisestä tietoisuusohjelman avulla.

3.1 Tietoturvatietoisuus nykypäivänä

Tietoisuudessa on kysymys siitä, mitä ihmiset tuntevat, ajattelevat ja tekevät. Tunteminen kattaa niin tunteelliset, hermostolliset kuin aistilliset kokemukset. Ajattelulla tarkoitetaan ihmisen älyllistä ja henkisestä toimintaa. Tekemisellä sen sijaan tarkoitetaan fyysistä ulottuvuutta, jossa työn tekeminenkin ilmenee. Tietoisuus voidaan tiivistää yhtälöön, jossa asiantuntemus yhdistettynä motivaatioon vaikuttaa ja näkyy siinä, miten ihminen käyttäytyy. (Peltier 2014, s. 100)

Tietoturvallisuudella tai tietoturvalla tarkoitetaan järjestelyitä, joilla pyritään varmistamaan tiedon saatavuus, eheys sekä luottamuksellisuus (Turvallisuuskomitea 2018, s. 15). Alexanderin ym. (2008, s. 97) mukaan on tärkeää tuoda esille, että tietoturvallisuudessa ei ole kyse ainoastaan luottamuksellisuuden ylläpitämisestä, vaan nykypäivän liiketoiminnassa korostuvat erityisesti myös tiedon saatavuuden sekä eheyden rooli. Saatavuus tarkoittaa, että tieto on hyödynnettävissä ja käytettävissä silloin, kun sitä tarvitaan. Eheydellä tarkoitetaan tiedon oikeellisuutta, jolloin tieto on yhtäpitävää alkuperäisen tiedon kanssa. Luottamuksellisuudella taas tarkoitetaan sitä, että tietoon on pääsy vain siihen oikeutetuilla henkilöillä, eikä kukaan sivullinen pääse käsiksi tietoon. (Turvallisuuskomitea 2018, s. 15)

Tietoturvallisuuden tehokas hallinta edellyttää organisaatioissa teknisiä sekä menetelmällisiä hallintakeinoja, joilla tietoon liittyviä riskejä hallitaan. Hallintakeinoilla tarkoitetaan toimenpiteitä, kuten prosesseja, periaatteita,

käytäntöjä ja laitteita, joilla pyritään vaikuttaman riskeihin (Suomen standardoimisliitto SFS ry 2020, s. 7). Hallintakeinoilla pyritään välttämään tietoturvapoikkeamien toteutuminen. Tietoturvapoikkeamat ovat ei-toivottuja tietoturvatapahtumia, jotka vaarantavat tietojen ja palvelujen tietoturvan sekä vaikuttavat organisaation toimintaan epäsuotuisasti (Turvallisuuskomitea 2018, s. 13). Ne voivat olla joko teknologialiitännäisiä tai niin sanottuja inhimillisiä virheitä, jolloin poikkeamaan ei liity teknologiaa (Carpenter 2019, s. 6). Yleisimpiä tietoturvaan liittyviä inhimillisiä virheitä ovat esimerkiksi tiedon lähettäminen väärälle vastaanottajalle tai sen tallentaminen ei turvalliseen sijaintiin, kuten pilvipalveluun, jossa ei ole rajattuja käyttöoikeuksia (Khando ym. 2021, s. 2).

ISO/IEC 27000 -standardissa yhdeksi tietoturvallisuuden hallintajärjestelmän onnistunutta toteutumista edistäväksi perusperiaatteeksi on mainittu tietoisuus (Suomen standardoimisliitto SFS ry 2020, s. 16). Tämän tutkielman kontekstissa tietoturvatietoisuudella tarkoitetaan ymmärrystä siitä, että uhkia on olemassa ja niitä hallitaan olemassa olevilla hallintakeinoilla. Tietoturvatietoisuus sisältää käsityksen siitä, että organisaatio ei ole automaattisesti immuuni näitä uhkia vastaan. (Peltier 2014, s. 96) Hallintakeinojen tehokkuus riippuu organisaation työntekijöistä, jotka toteuttavat hallintakeinoja organisaation sisällä. Mikäli henkilöstö jättää huomioimatta organisaation turvallisuuteen liittyvät politiikat, periaatteet ja menettelyohjeet, on hallintakeinojen toteuttamisessa tällöin puutteita. Hallintakeinojen tehokas toteuttaminen edellyttää positiivisen turvallisuuden ilmapiirin rakentamista, jossa jokainen ymmärtää, mitä heiltä odotetaan, ja sitoutuu turvallisiin toimintatapoihin. (Kruger & Kearney 2006, s. 289)

On usein sanottu, että ihminen on organisaatiossa suurin uhka tai sen turvallisuuden heikoin lenkki. Tämä perustuu ajatukseen siitä, että ihminen on erehtyväinen. Ihminen myös tekee virheitä tahattomasti. Erityisen alttiina virheille ihminen on tuntiessaan kiirettä, painetta ja stressiä. Tästä voi seurata kyvyttömyyttä keskittymistä vaativiin tehtäviin sekä rationaaliseen ajatteluun. Lisäksi ihminen on taipuvainen tekemään itsenäisiä kontekstilähtöisiä riskiarvioita, joiden perusteella yleisten normien ja sääntöjen rikkominen on joskus mahdollista. Moni ihminen tulkitsee esimerkiksi nopeusrajoitukset suosituksina. Nopeusrajoitusten noudattamiseen vaikuttaa subjektiivinen käsitys ja tulkinta vallitsevista liikenneolosuhteista. Auton kuljettaja saattaa kuvitella hallitsevansa riskin, vaikka rikkookin voimassa olevaa nopeusrajoitusta. (Carpenter 2019, s. 15) Esimerkki nopeusrajoituksista pätee myös tavalliseen työelämään. Organisaation työntekijät saattavat tehdä itsenäisiä riskipäätöksiä ja toimia esimerkiksi tietoturvaohjeiden vastaisesti. Rikolliset tiedostavat nämä kaikki edellä mainitut taipumukset ja pyrkivät hyödyntämään inhimillisiä heikkouksia saavuttaakseen tavoittelemansa hyödyn.

Euroopan unionin kyberturvallisuusvirasto ENISA:n (The European Union Agency for Cybersecurity, 2023a, s. 72) mukaan tietojenkalastelu on edelleen yksi käytetyimmistä hyökkäyskeinoista ja suurin osa tietomurroista perustuu ihmisen toimintaan, kuten käyttäjän tekemään virheeseen. Merkittävä osa tietoturvapoikkeamista on seurausta ihmisten tietämättömyydestä ja kyvyttömyydestä tunnistaa tilanteita, joissa he itse vaarantavat toiminnallaan tietoturvallisuuden

tai heitä hyödynnetään osana kyberhyökkäystä. Rikollisten yleisesti hyödyntämä keino tietojen kalasteluun on sosiaalinen manipulointi. Sosiaalinen manipulointi on toimintaa, jonka tavoitteena on hankkia luottamuksellista tietoa tekeytymällä tietoon oikeutetuksi tahoksi hyväksi käyttäen tiedon käyttöön oikeutettuja henkilöitä (Turvallisuuskomitea 2018, s. 19).

Työntekijät voivat olla organisaation tietoturvallisuuden vahvin lenkki, jos kaikki heistä ymmärtävät, mitä hyötyä tiedon turvaamisesta on. Lisäksi heidän on ymmärrettävä, mitkä ovat heidän roolinsa sekä vastuunsa organisaation tietojen turvaamisessa ja toimittava myös sen mukaisesti joka päivä. (Thomson & von Solms 2006, s. 14) Pelkkiin teknisiin seikkoihin keskittyminen on riittämätöntä ja inhimillinen tekijä on kriittistä ottaa mukaan tietoturvallisuuden hallinnassa sekä kehittämisessä. Resursseja tulisi keskittää teknologisten valintojen lisäksi myös tietoturvatietoisuuden kehittämiseen, jotta kyberrikollisuuden torjunta on edes mahdollista. (Grassegger & Nedbal 2021, s. 65; Carpenter 2019, s. 4; Li ym. 2019, s. 21)

Peltierin (2014, s. 94) mukaan tietoturvatietoisuudella on keskeinen asema osana tietoturvallisuuden hallintakeinojen valikoimaa, ja sen tulisi olla johdettuna keskeiseksi osaksi organisaation tietoturvallisuuden hallintakeinojen kehittämistä. Organisaatiot, jotka eivät kehitä henkilöstönsä turvallisuustietoisuutta, kärsivät todennäköisemmin tietoturvapoikkeamista (Grassegger & Nedbal 2021, s. 65; Alexander ym. 2008, s. 145). Tietoturvatietoisuus sisältää useita erilaisia lähestymistapoja sekä toimenpiteitä, joiden tavoitteena on saada aikaan joko laajamittaisia tai tarkoin valittuja kohdennettuja muutoksia turvallisuuskäyttäytymiseen, sekä parantaa kykyä tunnistaa ja tiedostaa uhkia eri organisaation tasoilla (Peltier 2014, s. 94).

Tietoisuuden kehittämisellä pyritään vaikuttamaan henkilöstön käyttäytymiseen ja muokkaamaan sitä toivottuun suuntaan. Tietynlainen toivottu käyttäytyminen tai toiminta edellyttää henkilöiden samanaikaista motivaatiota sekä kykyä toimia toivotulla tavalla. Puutteet sekä motivaatiossa että osaamisessa ovat esteenä toivotulle käyttäytymiselle. (Carpenter 2019, s. 117–118) Toivottu käyttäytyminen edellyttää motivaation sekä osaamisen lisäksi myös jonkinlaisen ajurin. Ajuri on yleensä ulkopuolelta saatu signaali, kuten viesti, puhelu, keskustelu, sosiaalinen paine tai ympäristöstä tehdyt havainnot, mutta se voi olla myös sisäisen motivaation ja kiinnostuksen synnyttämä. Tietoisuusohjelmassa ajureiden toteuttaminen ja ylläpito edellyttää suunnittelua. Suunnittelussa tärkeä vaihe on listata kaikki mahdolliset asiat, jotka voisivat toimia ajurina ja valita niistä sellaiset, jotka olisivat realistisia toteuttaa. (Carpenter 2019, s. 119)

Tietoisuuden kehittämisessä on huomioitava inhimillisiä tekijöitä, jotka muodostavat haasteita käyttäytymisen muokkaamiseen. Ihmisellä on tutkitusti taipumusta omaksua helpommin tietoa, joka tukee jo valmiiksi omaksuttuja uskomuksia. Toisaalta ihmisellä on taipumusta vähätellä tietoa, joka on ristiriidassa omaksuttujen uskomusten kanssa. Ihminen myös usein keskittyy ja antaa enemmän painoarvoa tuoreessa muistissa oleville uhkakuville. Esimerkiksi uutisissa kuluvalla ajanhetkellä näkyvästi olevat tapahtumat saavat paljon painoarvoa ihmismielessä, vaikka todellisuudessa niiden käsittelemä uhkakuva olisi

merkitykseltään pienempi. Lisäksi ihmiselle on luonnollista ajatella harhaanjohtavasti, että uhkakuvien toteutuminen muille kuin itselle on todennäköisempää. (Tsohou ym. 2015, s. 132)

Ihmisten lisäksi myös jatkuvassa muutoksessa oleva teknologia on vaikea kokonaisuus hallita. Verkottunut maailma erilaisine langattomine yhteyksineen parantaa tiedon liikkumista. Tämä lisää jatkuvasti myös uudenlaisia hyökkäysrajapintoja sekä digitaaliseen maailmaan liittyviä riskejä, joita rikolliset voivat käyttää hyväkseen. Tietoisuuden kehittäminen on kuitenkin teknisiin hallintakeinoihin verrattuna yleisesti edullisempaa toteuttaa. Jopa pieni muutos käyttäytymisessä voi olla ratkaisevammassa asemassa, kuin suuret investoinnit tietoturvateknologiaan. (Alexander ym. 2008, s. 149)

Tietoisuuden kehittäminen sisältää monia eri lähestymistapoja. Sillä ei tarkoiteta vain kouluttamista, joka on yksi monista keinoista kehittää tietoisuutta. Kouluttaminen on yksin riittämätöntä, sillä se keskittyy tarkoin valittujen taitojen opettamiseen siinä missä tietoisuuden kehittäminen tähtää kokonaisvaltaisempaan muutokseen ihmisten käyttäytymisessä. (Alexander ym. 2008, s. 146)

Tietoturvatietoisuuden kehittämisessä on kyse paitsi asenteiden muuttamisesta myös osaamisen lisäämisestä. Tietoturvallisuuden hallinnan edellytyksenä on tietojenkäsittelyn erityisosaamisen lisäksi yleinen tietoturvatietoisuus, joka pitää sisällään koko henkilöstölle kuuluvan perustason tietoturvaosaamisen. Mikään tietoturvallisuuden hallintajärjestelmä ei suojaa tietoa, ellei sen rooleissa toimivien henkilöiden tietoturvatietoisuus ole riittävää. Toisaalta henkilöiden tietoturvatietoisuus on yksi tavoiteltavista asioista, joita hallintajärjestelmällä pyritään saavuttamaan. Henkilöiden on ymmärrettävä, kuinka hallintajärjestelmällä suojataan tieto-omaisuutta ja mikä on heidän roolinsa siinä. Tässä asiassa ohjauksen on tultava sen merkityksen korostamiseksi suoraan ylimmältä johdolta esimerkiksi tietoturvapolitiikan muodossa. (Alexander ym. 2008, s. 96–97; Rocha Flores & Ekstedt 2016, s. 32)

Tietoturvatietoisuudella voidaan nähdä useita selkeitä etuja nykypäivän organisaatioille. Ei ole liioittelua sanoa, että riittävä tietoturvatietoisuuden taso henkilöstön keskuudessa on yksi perusedellytyksistä toiminnan jatkuvuuden kannalta. Hyvän yleisen tietoturvatietoisuuden saavuttaminen on välttämätöntä, jotta organisaatio voi suojautua tietoturvauhkia vastaan. Stewartin ja Jürjensin (2017, s. 497) mukaan korkea tietoturvatietoisuuden taso myös parantaa sekä lisää organisaation tuottavuutta ja innovaatiokyvykkyyttä. Tietoturvatietoisuus on täten eittämättä nykypäivänä yksi liikemaailman kilpailueduista.

3.2 Tietoisuuden kehittämisen kulttuurisidonnaisuus

Tietoturvallisuuden on oltava osa organisaation kulttuuria. Kulttuuri tarkoittaa uskomusten, käyttäytymisen ja arvojen esiintymistä jossakin ihmisryhmässä. Kulttuurin olemassaolo perustuu ihmisten sosiaalisuuteen ja siihen, että ihmisryhmässä ilmenevät uskomukset, käyttäytymismallit sekä arvot vahvistavat toinen toisiaan. Turvallisuuskulttuuri on sitä, että turvallisuutta koskevat asenteet,

käyttäytymismallit sekä arvomaailma sisältyvät ihmisryhmää koskeviin sosiaalisiin odotuksiin. (Carpenter 2019, s. 143)

Tietoturvakulttuurissa on kysymys moniulotteisesta kokonaisuudesta, joka koostuu strategisista, teknisistä, organisatorisista, inhimillisistä ja ympäristötekijöistä (AlHogail 2015, s. 573). Se toimii ohjaavana ja rajoja asettavana tekijänä, jotta organisaation henkilöstö ei toimintatavoillaan aiheuttaisi vaaraa organisaation tieto-omaisuudelle. Tietoturvakulttuuri tuo tietoturvallisuuden osaksi henkilöstön arkipäiväistä toimintaa erilaisin sosiokulttuurisin toimenpitein. Nämä toimenpiteet tukevat olemassa olevia teknisiä hallintakeinoja. (AlHogail 2015, s. 567)

Kulttuuri ja ympäristö vaikuttavat ihmisten riskikäsityksiin merkittävästi. On tutkittu, että samaan ryhmään kuuluvat ihmiset näkevät ja ymmärtävät riskejä samalla tavalla. Nämä käsitykset myös eroavat toiseen ryhmään kuuluvien ihmisten käsityksistä. (Tsohou ym. 2015, s. 134) Samaan sosiaaliseen ihmisryhmään kuuluvien vertaisten käyttäytymisellä on tutkittu olevan selvä vaikutus ihmisten tietoturvakäyttäytymiseen (Li ym. 2019, s. 20). Khandon (ym. 2021, s. 17) mukaan yksilötasolla kulttuuriset vaikuttimet, kuten sosiokulttuuriset tekijät, kulttuuriset oletukset ja uskomukset, äidinkieli ja uskonto vaikuttavat nekin tietoturvatietoisuuteen. Kulttuurilla on täten merkittävä rooli tietoturvatietoisuuden kehittämisen suunnittelutyössä (Riahi & Islam 2024, s. 20).

Peltierin (2014, s. 108) mukaan myös kulttuurisidonnaiset haasteet tietoturvatietoisuuden kehittämisessä ovat todennäköisiä ja niihin on varauduttava. Toimenpiteet saattavat horjuttaa organisaatiossa vallitsevaa kulttuuria, joka väistämättä aiheuttaa muutosvastarintaa. Organisaation kulttuurin muokkaaminen voi olla vaikeaa esimerkiksi organisaation kulttuurissa vallitsevien ennakkoluulojen tai gravitaatiovaikutuksen vuoksi. Gravitaatiovaikutuksella tarkoitetaan sitä, että turvallisuustyötä tekevien henkilöiden osuus on tavanomaisesti pieni suhteutettuna koko organisaation henkilömäärään. Muutosvastarintaan kuuluvat myös ennakkoluulot, jotka vaikuttavat välillisesti henkilöstön tietoturvatietoisuuteen ja valmiuteen noudattaa tietoturvallisia toimintatapoja sekä käytänteitä. (Carpenter 2019, s. 145–146; Tsohou ym. 2015, s. 136)

Edellä mainitun gravitaatiovaikutuksen kumoaminen edellyttää tehostinta. Sellaisena toimii esimerkiksi ympäri organisaation kattavana verkostona kulttuuria välittävät avainhenkilöt. Nämä henkilöt omaavat jo oletusarvoisesti positiivisen asenteen turvallisuutta ja sen kehittämistä kohtaan. (Carpenter 2019, s. 157) Avainhenkilöinä kannattaa käyttää erityisesti johtajia sekä organisaatiossa vallitsevan kulttuurin mukaisia työyhteisön epävirallisia johtajia. Epävirallisilla johtajilla saattaa olla enemmän vaikutusvaltaa ja juuri heidän avullaan on mahdollista muuttaa organisaatiossa vallitsevia asenteita. (Carpenter 2019, s. 194; Peltier 2014, s. 109)

Yksittäisten ihmisten asenteilla voi olla suuri vaikutus tietoturvallisuuteen. On tutkittu, että kulttuurilla voidaan vaikuttaa näihin asenteisiin. (Rocha Flores & Ekstedt 2016, s. 39–40) Vaikka kulttuurin muokkaamiseen liittyy haasteita, on hyvällä tietoturvakulttuurilla useita etuja. Hyvä tietoturvakulttuuri luo perustan organisaation tietoturvatoiminnalle. Se lisää vastuullisuutta tietoturva-asioissa ja

motivoi sekä kannustaa työntekijöitä muuttamaan käyttäytymistään tietoturvallisemmaksi. (AlHogail 2015, s. 574)

3.3 Tietoisuusohjelma suunnitelmallisena lähestymistapana

Ratkaisevassa asemassa tietoturvatietoisuuden kehittämisessä on tutkielman johdannossakin mainittu tietoisuusohjelma, jolla kehitetään organisaation henkilöstön tietoturvatietoisuutta ja turvallisuuskulttuuria. Peltierin (2005, s. 40) mukaan se tarjoaa vastaukset henkilöstölle siitä, mitä heiltä odotetaan ja mistä he saavat tarvittaessa apua tietoturvaan liittyvissä kysymyksissä.

Tietoisuusohjelma sisältää toimintoja, joilla pyritään tekemään henkilöstö tietoiseksi tietoturvasta ja siihen liittyvistä organisaation käytännöistä. Tietoturvatietoisuusohjelman tavoitteena on varmistaa henkilöstön tietoisuus organisaation tietojen turvaamiseen liittyvistä politiikoista, ohjeista ja määräyksistä (Khando ym. 2021, s. 2). Tietoisuusohjelman tarkoituksena on saattaa henkilöstö myös tietoiseksi mahdollisista uhkista ja siitä, mitä heidän kuuluu tehdä, jotta näiden uhkien toteutuminen organisaatiossa vältetään (Peltier 2005, s. 49). Tsohoun (ym. 2015, s. 129) mukaan käyttäytymiseen voidaan vaikuttaa parhaiten, kun henkilöstö ymmärtää riskit ja oman toimintansa vaikutuksen niihin.

Tietoisuusohjelma on moniulotteinen kokonaisuus, jolla pyritään muuttamaan käsityksiä sekä muokkaamaan organisaation kulttuuria. Sen viestin on oltava kiinnostava sekä samaistuttava. Sen on tuotava esille konkreettisia esimerkkejä, mitä seurauksia ohjeiden laiminlyönnistä voi organisaatiolle olla. (Alexander ym. 2008, s. 97) Tietoisuusohjelmalla pyritään vastaamaan suunnitelmallisesti myös siihen haasteeseen, että tietoisuus on dynaaminen ja jatkuvasti muuttuva tila, jota haastaa muuttuva riskiympäristö. Tietoisuusohjelma pitää sisällään jatkuvan mittaamisen ja sitä johdetaan tietoon perustuen. Kruger ja Kearney (2006, s. 290) mainitsevat tälle keskeiseksi perusteeksi sen, että tietoisuuden kehittämisellä voidaan vastata riskiympäristön muutoksiin. Tällöin tietoisuusohjelma noudattaa jatkuvan parantamisen mallia. Jatkuvan parantamisen malli on kuvattu tarkemmin luvussa 3.7.

Khandon (ym. 2021, s. 7) mukaan toimivaa tietoisuusohjelman sisältöä ei voi rakentaa vain teknisistä lähtökohdista ja teknisiin vaatimuksiin perustuen. Mukaan täytyy ottaa myös psykologisia näkökulmia. Teoreettisten mallien hyödyntäminen ihmismielen ymmärtämiseksi tietoisuusohjelman sisällön suunnittelussa on osoittautunut hyödylliseksi lähestymistavaksi useissa tapauksissa (Khando ym. 2021, s. 8).

3.4 Johdon sitoutumisen merkitys

Organisaation johtaminen, sen sitouttaminen tietoisuusohjelmaan sekä organisaation johdon ilmaisema tuki tietoisuuden kehittämiselle ovat kaikista kriittisimpiä tekijöitä tietoisuusohjelman kannalta (Stewart & Jürjens 2017, s. 516). Ilman johdon tukea ei ole mahdollista toteuttaa tietoisuusohjelmaa. Riahin ja Islamin (2024, s. 20) mukaan johdon tuen puuttuessa vastuuta tietoturvasta ei tunneta, eikä se jakaudu organisaatioon.

Johdon sitoutumisella varmistetaan tietoisuusohjelman ydinviestien olevan johdonmukaisia organisaation arvojen ja tavoitteiden kanssa. Ylimmän johdon sitoutuminen takaa todennäköisesti myös tietoturvatietoisuusohjelman edellyttämät asianmukaiset resurssit sekä budjetin. (Alexander ym. 2008, s. 146; Kolb & Abdullah 2009, s. 105)

Ylimmällä johdolla on pääsy organisaation kaikista arkaluonteisimpaan tietoon. He myös tiedostaen tai tiedostamattaan näyttävät toiminnallaan esimerkkiä koko organisaatiolle. Johdon aktiivisen osallistumisen tietoisuuden kehittämiseen on havaittu edistävän tietoisuuden kasvua. (Alexander ym. 2008, s. 146; Khando ym. 2021, s. 11) Puhakaisen ja Siposen (2010, s. 774) mukaan ylimmän johdon tuki tietoturvatietoisuudelle on oltava näkyvää. Jatkuvaa näkyvyyttä voidaan toteuttaa jatkuvalla viestinnällä esimerkiksi intranetin välityksellä.

Mikäli johto ei sitoudu tietoisuusohjelmaan, sitä ei Alexanderin (ym. 2008, s. 146) mukaan todennäköisesti viestitä henkilöstölle riittävän hyvin, eikä henkilöstölle varata tarpeeksi aikaa tietoisuutta kehittävien toimintojen suorittamiseen. Johdon suhtautuminen turvallisuuteen on suora viesti henkilöstölle siitä, kuinka tärkeänä turvallisuutta organisaatiossa pidetään. Johdon on ymmärrettävä, että henkilöstön ei voi olettaa toimivan tietyllä tavalla, elleivät he itsekään toimi näiden sääntöjen mukaisesti. Ainoastaan esimerkillä johtaminen voi muuttaa kulttuuria. (Alexander ym. 2008, s. 97)

Edellä mainituiden seikkojen vuoksi voidaankin todeta, että tietoisuusohjelman menestyminen riippuu viimekädessä ylimmästä johdosta. Voidaan myös päätellä, että organisaation johto on kaikista tietoisuusohjelman kohderyhmistä kriittisin. Johdon sitouttamiseksi tietoisuusohjelmaan on tehtävä huolellista työtä. Peltierin (2014, s. 127) mukaan vuoropuhelussa johdon kanssa auttaa, kun käyttää johdon ymmärtämää terminologiaa. Esimerkiksi kustannus-hyötyanalyysi on hyvä keino perustella tietoisuusohjelman tarpeellisuutta johdolle. Analyysissä odotettavissa olevat henkilöstö- sekä muut kustannusarviot suhteutetaan saavutettaviin hyötyihin.

Hyötynäkökulmaa voidaan nostaa esille erityisesti tieto-omaisuuden suojaamisen kautta ja nostaa esille esimerkkejä, mitä tietoturvariskejä voidaan välttää tietoisuutta kehittämällä. Tietoisuusohjelman perusteleminen tieto-omaisuuden suojaamisella oikeuttaa tietoisuusohjelman toteuttamista liiketoiminnallisesta näkökulmasta. Tieto-omaisuuden turvaamisesta tai sen tekemättä jättämisestä koituvat seuraukset tuovat organisaatiossa esille konkreettisesti sen, mitä vaikutuksia tietoisuusohjelmalla voi olla sen liiketoimintaan. Johdon kanssa

keskustelussa auttavat myös tilastot tietoturvapoikkeamista ja häiriöistä, olivat ne omasta tai jostakin toisesta organisaatiosta. (Peltier 2014, s. 127; ENISA 2023b, s. 4)

3.5 Tiimistä toimintasuunnitelmaksi

Tietoisuusohjelma toteutetaan organisaatioissa tavanomaisesti projektina, jolla on johdon hyväksymät tavoitteet. Tavoitteita voivat olla esimerkiksi lain- sekä standardien vaatimustenmukaisuus tai henkilöstön käyttäytymisen ja turvallisuuskulttuurin muokkaaminen. Kun ohjelmalla on selvät tavoitteet, sen toteutus on tehokasta ja edistyminen mitattavissa. Tietoisuusohjelman suunnittelu alkaakin tavoitteiden määrittelemisestä. Organisaatiolle on oltava selvää, miksi tietoisuusohjelma tarvitaan ja mitä sillä tavoitellaan ennen konkreettisten toimenpiteiden suunnittelua. Tietoisuusohjelman tavoitteiden tulisi olla selvästi yksilöityjä, mitattavissa sekä saavutettavissa olevia ja aikaan sidottuja. Yleisiä esimerkkejä tavoitteista olevat tietoturvakulttuurin kehittäminen ja tietoturvapoikkeamiin sekä -häiriöihin varautuminen. (Alexander ym. 2008, s. 146–147; Carpenter 2019, s. 20; ENISA 2023b, s. 3)

Organisaation tulisi muodostaa pätevä asiantuntijatiimi, joka vastaa tietoisuusohjelman kehittämisestä sekä sen toteuttamisesta (Stewart & Jürjens 2017, s. 513). Riippuen organisaatiosta, tiimi voi toimia oman toimensa ohella, osa-aikaisena tai kokopäiväisenä. Tiimissä tulisi olla edustettuna asiantuntijuutta eri aloilta ja organisaatiohaaroista myös turvallisuuden asiantuntijuuden ulkopuolelta. Vaikka turvallisuus on keskiössä, monipuolinen asiantuntijuus on perusteltua siksi, että tietoisuuden kehittämisessä on kysymys kompleksisesta kokonaisuudesta, joka poikki leikkaa organisaation eri toimintoja. (Peltier 2014, s. 101–102; Kolb & Abdullah 2009, s. 105)

Kun tiimin edustajia valitaan ympäri organisaatiota, on mahdollista varmistaa se, että tietoisuuden kehittämistä tehdään koko organisaation lähtökohdista ja suunnittelu sidotaan organisaation tavoitteisiin. Tiimin kokoonpano riippuu organisaation ominaispiirteistä, mutta siihen tulisi harkita mukaan asiantuntijuutta esimerkiksi

- tietojärjestelmäturvallisuudesta,
- sovelluskehityksestä,
- fyysisestä turvallisuudesta,
- varautumisesta,
- viestinnästä,
- kouluttamisesta,
- erityistoimintojen johtamisesta,
- laintulkinnasta,
- henkilöstöhallinnosta sekä
- loppukäyttäjiltä.

Tietojärjestelmäturvallisuudesta vastaavat asiantuntijat tuntevat uhkaympäristön tilannekuvan parhaiten. Nämä henkilöt voivat tarjota operatiivista tietoa tietoisuusohjelman toteuttamisen tueksi. Viestintäosasto tuntee usein soveltuvimmat keinot organisaation eri kohderyhmien tavoittamiseen. Henkilöstöhallinto vastaa usein toimenpiteiden implementoinnista työntekijöiden rekrytointiprosessin aikana. Viimeisenä linkkinä toimivat kouluttajat. Asiantuntevien kouluttajien mukanaololla varmistetaan, että koulutustapahtumat toteutetaan riittävällä ammattitaidolla. (ENISA 2023b, s. 5–6)

Lyhyesti sanottuna tiimin on kyettävä muuntamaan koko organisaatiota koskevat tavoitteet tietoisuuden kehittämisen toimintasuunnitelmaksi, jossa pohdittaisiin ainakin,

- mitkä ovat tietoisuuden kehittämisen tärkeimmät kohderyhmät,
- miten heidän käyttäytymistään tulisi muuttaa nykyisestä ja
- mitkä ovat minimivaatimukset kohderyhmien osaamiselle?

Toimintasuunnitelman tulisi kattaa myös tietoisuusohjelman toteuttaminen organisaatioon sekä sen kustannusarviot eli toiminnalle vaadittu budjetti. Myös sopiva ajankohta projektin toteuttamiselle on suunniteltava, sillä ajankohta voi vaikuttaa olennaisesti projektin menestymiseen. Viimeisenä asiana tiimin tulisi suunnitella, miten onnistumista mitataan. (Peltier 2014, s. 102)

Vaikka tietoisuusohjelma noudattaa koko organisaation tavoitteita kattaen koko organisaation henkilöstön, henkilöstöryhmissä on paljon erilaisia koulutustarpeita. Kohderyhmien erityispiireet on otettava tietoisuusohjelmassa huomioon. Lähtökohtana on se, että jokainen organisaation tietoa käsittelevä ymmärtää, mitä voi tehdä tietoturvan parantamiseksi päivittäisessä työssään. Tietoisuusohjelma, jossa koko henkilöstön tietoisuutta pyritään lisäämään, ei kuitenkaan yksin täytä kaikkien kohderyhmien tarpeita. Esimerkiksi IT-asiantuntijat tarvitsevat yksityiskohtaista teknistä tietoturvakoulutusta. Sen sijaan johtajien tiedontarve keskittyy suurpiirteisempään tietoon ja kokonaisuuksien ymmärtämiseen. (Peltier 2014, s. 94)

Tietoisuusohjelman suunnittelu alkaa usein kohderyhmien tunnistamisesta. Tähän ei ole olemassa valmista ratkaisua, vaan tunnistaminen riippuu täysin organisaation ominaispiirteistä. Usein tunnistettavia kohderyhmiä ovat loppukäyttäjät, organisaation tietotekniikasta sekä teknisestä tietoturvasta vastaavat tahot, tiedon omistajat sekä kaikki organisaation johtotehtävissä työskentelevät henkilöt. Loppukäyttäjillä tarkoitetaan usein kaikkia organisaatiossa ja sen tehtävissä työskenteleviä henkilöitä. (Peltier 2014, s. 103)

Sama tietoisuusohjelma ei toimi jokaisessa organisaation osassa tai liiketoimintayksikössä. Tietoisuusohjelmalla on oltava tästä syystä mukautumiskykyä. kohderyhmien on saatava mahdollisuus vaikuttaa tietoisuusohjelman sisältöön, jotta heidän tarpeensa tulee huomioiduksi suunnittelussa. (Peltier 2005, s. 42) Tietotekniikasta vastaavien sisällä tietotarpeita on monenlaisia ja tällä osa-alueella saattaa olla tarvetta todella yksityiskohtaiselle, jopa koodirivien tasolle

menevälle tiedolle. Tiedon omistajat ovat myös tärkeä kohderyhmä juuri siksi, että he usein ensisijaisesti vastaavat omistamansa tiedon turvallisuusjärjestelyiden toteutumisesta. He päättävät käytännössä tiedon luokituksesta sekä siihen liittyvistä käyttöoikeuksista organisaation sisällä. Näillä tavallisesti päällikkö- tai johtotason tehtävissä toimivilla henkilöillä on muuta henkilöstöä laajempi pääsy salassa pidettäviin tietoihin. Tieto voi vaarantua tahattomasti, jos johdon tietoturvatietoisuus ei ole riittävällä tasolla. (Peltier 2014, s. 103)

Kohderyhmät voidaan tarkkojen roolien lisäksi määritellä myös ENISA:n esimerkin (Taulukko 1) mukaisesti karkeammalla ryhmittelyllä, joka perustuu esimerkiksi rooleihin liittyviin riskialttiimpiin vastuisiin, kuten päätöksentekoon tai taloudenhoitoon.

TAULUKKO 1 Kohderyhmien ryhmittelyesimerkki (ENISA 2023b, s. 6)

	Kohderyhmä	**Ryhmittely**
1	Työntekijät	Tavallinen työntekijä
2	Palveluntuottajat	
3	HR-asiantuntijat	
4	Viestintäasiantuntijat	
5	Juristit	
6	Talous-/hankinta-asiantuntijat	Johtajat, päättäjät ja budjetin suunnittelu
7	Johtajat ja yksikön päälliköt	
8	Tuoteomistajat ja palvelupäälliköt	
9	Tietoturva-asiantuntijat	Tietoturvan hallintakeinojen suunnittelu sekä toteuttaminen
10	IT-asiantuntijat	

Kohderyhmien määrittely voi pohjautua myös lähtökohtaiseen taitotasoon tai organisaation toimintoihin. Määrittely riippuu täysin organisaation koosta, toimialasta ja muista erityispiirteistä. (Peltier 2014, s. 104) Kohderyhmiä määriteltäessä on arvioitava ja tunnistettava kunkin kohderyhmän henkilömäärä organisaatiossa. Henkilömäärällä on suuri vaikutus tietoisuuden kehittämistoimintojen valintaan (Peltier 2014, s. 106). Kohderyhmien määrittelyssä olisi tunnistettava myös kohderyhmien erilaiset kulttuurilliset taustat sekä mahdolliset ennakkoluulot tietoturvallisuutta kohtaan (Tsohou ym. 2015, s. 136).

Seuraavana asiana tietoisuusohjelman suunnittelussa on vaadittujen taitojen tai pätevyyksien tunnistaminen. Pätevyydet riippuvat muutamasta tekijästä, joita ovat henkilöstön työnkuvaan sisältyvän tietojen käsittelyn luonne sekä tilat ja ympäristö, joissa tietoa käsitellään. Lisäksi pätevyyksiin vaikuttaa työyhteisössä vallitseva kulttuuri ja ylimmän johdon sitoutuminen tietoisuuden kehittämiseen. (Peltier 2014, s. 106)

Vaikka suurin osa organisaation henkilöstöstä käyttääkin samoja perustason työvälineitä ja sovelluksia, vaihtelevat niillä suoritettavat työtehtävät hyvin laajalla skaalalla tehtävänkuvan mukaan.

Peltierin (2014, s. 107) mukaan henkilöstön keskeisiin taitoihin ja pätevyyksiin kuuluvat niin

- fyysinen turvallisuus,
- turvallinen salasanojen ja käyttäjätunnusten hallinta,
- tietojen kalastelun tunnistaminen,
- tietosuojataidot, tietojen luokittelu ja käsittely,
- varautuminen kuin
- tietoturvahäiriöiden hallinta mukaan lukien
    - häiriöiden ennalta ehkäisyn,
    - tunnistamisen,
    - ilmoittamisen sekä
    - reagoimisen.

Tietoturvan saralla osaamismalleja sekä -kehyksiä on olemassa useita. Näissä tavallisesti korostuvat poikkeamien ja riskienhallintaan liittyvä osaaminen. Teknisen osaamisen osa-alueisiin keskitytään sen sijaan tavallisesti vähemmän. (Bendler & Felderer 2023, s. 25) Tässä tutkielmassa käsitellään viitekehyksiä tarkemmin luvussa 5.3.

ENISA (2023b, s. 14) käyttää pätevyydestä esimerkkiä, jossa on kaksi tasoa: ensimmäisellä tasolla henkilö on tietoinen ja toisella tasolla henkilö on koulutettu aiheesta. Vaadittu vähimmäispätevyystaso sekä toimenpiteet sen saavuttamiseksi voidaan määrittää osaamisaiheittain jokaiselle tunnistetulle kohderyhmälle. Tällöin esimerkiksi organisaation kaikkien työntekijöiden tulee olla tietoisia haavoittuvuuksista, mutta IT-asiantuntijoiden on oltava niiden osalta koulutettuja. Ensimmäisen tason saavuttamiseen voivat riittää intratiedotteet. Seuraavan tason saavuttaminen tarkoittaa käytännössä kurssien sekä esimerkiksi sertifikaattien suorittamista.

Tietoisuusohjelman kohdentaminen edellyttää priorisointia: kaikkea ei ole mahdollista saada heti valmiiksi. Kun suunnitellaan, mihin organisaation toimintoihin tietoisuusohjelmalla tulisi aluksi keskittyä, olisi tunnistettava toiminta-alueita, joissa ilmenee selkeitä tietoturvapuutteita tai -heikkouksia. Organisaatiossa vallitsevaa nykytilaa voidaan analysoida esimerkiksi kyselyin, havainnoimalla, erilaisin mittarein tai haastatteluilla ja nykytila-analyysin perustana voidaan käyttää kansainvälisiä standardeja sekä viitekehyksiä. (Peltier 2014, s. 116; Carpenter 2019, s. 149)

Nykytila-analyysina toimiva kysely voi kartoittaa, kuinka tietoisia henkilöstö on organisaation tietoturvallisuuteen liittyvistä periaatteista sekä toimintatavoista (Kolb & Abdullah 2009, s. 106). Krugerin ja Kearneyn (2006, s. 293) mukaan kyselyn avulla voidaan mitata kolmea ulottuvuutta: henkilöstön käyttäytymistä, asennetta sekä osaamista, jos kysymykset muotoillaan tarkoitukseen soveltuvalla tavalla.

Nykytila-analyysissä on kerättävä myös sosiaalidemografista dataa, jotta muun datan segmentointi ja jaottelu on mahdollista. Esimerkiksi henkilön organisaatioyksikkö sekä työsuhteen pituus ovat kulttuurin kehittämisen kannalta

merkityksellisiä, jotta on mahdollista havaita vaihtelua eri henkilöstöryhmien välillä sekä kehityskohtia. On tärkeää kerätä tietoa asenteista ja mielipiteistä sen lisäksi, mitä henkilöstö osaa tai tietää. Puutteiden tunnistaminen oikeuttaa tietoisuusohjelman toimeenpanoa, mutta analyysi indikoi myös suoraan, missä päin organisaatiota kehittämisen tarve on kriittisin. (Peltier 2014, s. 116; Carpenter 2019, s. 153)

Tietoisuusohjelman toteuttaminen organisaatiossa ei takaa automaattisesti sitä, että henkilöstö ymmärtäisi roolinsa sekä velvollisuutensa organisaation tieto-omaisuuden turvaamisessa. Tämän vuoksi tietoisuusohjelman suunnittelussa on otettava kantaa siihen, kuinka sen toteutumista ja tehokkuutta mitataan. (Kruger & Kearney 2006, s. 295; Kolb & Abdullah 2009, s. 106) Peltierin (2005, s. 40) mukaan tietoisuusohjelmissa epäonnistutaan usein juuri heikon seurannan vuoksi. Organisaatiolle on hyödyllistä ymmärtää, kuinka tehokas ohjelma on toteutuessaan, ja saadaanko sillä aikaan toivottuja muutoksia henkilöstössä.

Carpenterin (2019, s. 171) mukaan jo nykytila-analyysi kannattaa suunnitella siten, että se kestää aikaa ja toimii yhtenä tavoitteiden toteutumisen seurannan mittarina. Tällöin sillä on mahdollisesta esimerkiksi vuosittain mitata tietoisuusohjelman tuloksia ja seurata tietoisuuden kehittymistä. Aikaa kestävä kysely edellyttää kattavan kysymyslistan luomista, jotta kysymysten esittäminen ei ole toisteista ja henkilöstön ei ole mahdollista opetella ulkoa kysymyksiä ja niiden vastauksia (Kruger & Kearney 2006, s. 294). Kysymysten laatiminen kannattaa Krugerin ja Kearneyn (2006, s. 294) mukaan tehdä huolellisesti, jotta sen tuloksena saatu tieto vastaa organisaation tarpeisiin.

Käytännössä mittaamisen perustaksi tulee määritellä, mitä muutoksia tietoisuusohjelmalla tavoitellaan ja miten tavoitteiden toteutuminen on mahdollista havaita. Kysymykseen monia vastauksia ja täten tulosten saavuttamisen mittaamiseen myös monia tapoja. Indikaattoreita tietoturvatietoisuuden kehittymisestä voivat olla esimerkiksi

- tietoturvapoikkeamista tai häiriöstä raportoinnin lisääntyminen,
- tietoturvaa koskevien kehitysehdotusten lisääntyminen,
- häiriöiden väheneminen,
- tietoturvabudjetin kasvaminen tai
- hyväksyvämpi asenne tietoturvaa kohtaan. (Peltier 2014, s. 108)

Keskeisimpänä näkökulmana tietoisuuden mittaamisessa voidaan pitää henkilöstön käyttäytymistä, koska tietoisuuden kehittämisellä pyritään vaikuttamaan ihmisten käyttäytymiseen. Tätä varten organisaatiolla tulee olla oikeat työkalut henkilöstön toiminnan seurantaan sekä havaitsemiseen. Työkalujen avulla organisaatiolla tulisi olla näkymä henkilöstön toiminnan seurauksena tapahtuviin tietoturvapoikkeamiin, kuten haittaohjelmistojen lataamiseen sekä haitallisilla verkkosivuilla vierailuun. (Stewart & Jürjens 2017, s. 515)

Tietoturvatietoisuuden nykytilan määrittelyssä voidaan hyödyntää osaamisen kypsyystasoajattelua, johon on olemassa valmiita malliesimerkkejä. Thomsonin ja von Solmsin (2006, s. 14) tietoturvaosaamisen neliportaisen

kypsyystasomallin mukaan tietoisuutta on kehitettävä edelleen koulutuksen ja harjoittelun keinoin. Vasta riittävällä kokemuksella voidaan saavuttaa korkein taso, jossa ihminen toimii tiedostamattaan tietoturvallisesti. Alemmilla osaamisen tasoilla puutteellinen kokemus saa aikaan sen, että tietoturvallinen toiminta vaatii tietoista ajattelua. Mikäli osaamisen kypsyystaso on heikko, ihminen on altis toimimaan tiedostamattaan väärin.

Oli nykytila-analyysissä käytetty menetelmä mikä tahansa, sen tulosten raportoinnissa on tuotava esille lähtötaso sekä ohjelmalle asetetut tavoitteet. Tällä tavoin on mahdollista luoda voimakas viesti kulttuurin kehittämisestä ja osoittaa, että toimenpiteet ovat seurausta tietoon perustuvalle päätöksenteolle. (Carpenter 2019, s. 171)

3.6 Tietoisuusohjelman sisältö

Tietoisuusohjelman konkreettinen sisältö eli toimenpiteet, joita tietoisuuden kehittämiseksi tehdään, riippuvat organisaation tavoitteista, kohderyhmistä, käytettävissä olevasta ajasta, resursseista sekä budjetista. Lähtökohtaisesti sisällön suunnittelu perustuu organisaation omiin tarpeisiin ja vasta sen jälkeen tulevat muut sisältöä määrittävät tekijät. (Peltier 2014, s. 110–111; ENISA 2023b, s. 7) Keskeisenä tavoitteena on, että toimenpiteillä aikaansaatu tietoisuuden tason parantuminen edistää toivottua käyttäytymistä, kuten tehokasta reagointia tietoturvauhkiin (AlHogail 2015, s. 574). Tietoturvatietoisuusohjelman sisällön tulisi rohkaista organisaation henkilöstöä ilmoittamaan havaitsemistaan tietoturvapoikkeamista ja osallistaa henkilöstöä tietoturvallisuuden kehittämiseen (Puhakainen & Siponen 2010, s. 774).

Tietoisuusohjelman on oltava sisäänrakennettu organisaatioon kulttuuriin, jotta henkilöstön osaaminen pysyy ajan tasalla. Avainasemassa on monipuolinen ja monikanavainen viestintä, jossa korostuu merkityksellisyys, ajankohtaisuus sekä johdonmukaisuus. Kertaluonteinen koulutustapahtuma ei ole sisällöksi riittävää, vaan organisaatiossa tulisi luoda prosessi jatkuvalle tietoturvaviestinnälle. (Kruger & Kearney 2006, s. 290; Puhakainen & Siponen 2010, s. 774)

Henkilöstön ajattelussa ja mieltymyksissä vallitsee monimuotoisuus, joka tulisi huomioida tietoisuusohjelmassa. Ei ole yhtä tapaa toteuttaa tietoisuusohjelman sisältöä, joka sopisi kaikille. Hienovarainenkin vaihtelu sisällössä voi olla ratkaiseva käännekohta tietoisuusohjelman menestymisen kannalta. Carpenter (2019, s. 178–179) vertaa ohjelman sisältöä hypermarketin tuotteiden osastointiin. Hypermarketin suurin osasto sisältää kaikille asiakkaille tarkoitettuja perustuotteita. Suurimman osaston lisäksi hypermarketista löytyy pienempiä osastoja erityiskohderyhmien erityistarpeisiin.

Tietoisuusohjelman suunnittelussa on otettava huomioon myös yksilölliset oppimistyylit. Oppimistyyleillä tarkoitetaan toisistaan poikkeavia taipumuksia omaksua uutta tietoa. Toiset esimerkiksi oppivat paremmin näkemällä ja toiset kuulemalla. Tällöin he ovat oppimistyyliltään joko visuaalisia tai auditiivisia. (Peltier 2005, s. 44)

Tietoisuusohjelmaa suunniteltaessa on ymmärrettävä kohderyhmien päivittäistä elämää, käyttäytymistä ja vuorovaikutusta, jotta valitut tietoisuusstrategiat ja -toimenpiteet kohtaavat näiden näkökulmien kanssa (Carpenter 2019, s. 239). Tähän tarkoitukseen voidaan käyttää esimerkiksi roolikohtaisten asiakaspolkujen muodostamista. Asiakaspoluista voidaan tunnistaa mahdollisuuksia hetkiin, jolloin on todennäköisempää herättää tietyssä roolissa toimivan henkilön kiinnostus. Asiakaspolun muodostamisessa on huomioitava

- tyypillinen työpäivä,
- vallitsevat työolosuhteet,
- olosuhteiden muutokset lomakausina tai kiireellisinä aikoina,
- työssä kohdatut turvallisuusasiat,
- motivaatioon vaikuttavat tekijät,
- tavoitteet ja
- mahdolliset häiriötekijät. (Carpenter 2019, s. 242)

Kohderyhmien osalta merkitsevät niin kohderyhmien osaamistaso kuin henkilömäärätkin. Kohderyhmät tulisi jakaa osaamisen mukaan, jotta aiempi osaaminen voidaan ottaa huomioon (Puhakainen & Siponen 2010, s. 774). Ajallisesti ohjelman sisältö olisi suunniteltava niin, ettei se osu päällekkäin muiden henkilöstön aikaa ja huomiota vaativien tapahtumien kanssa. Tällaisia voivat olla esimerkiksi merkittävän projektin, toimintamallin tai muutoksen toteuttaminen organisaatioon. (Peltier 2014, s. 110)

Tietoisuusohjelman toteuttaminen vaatii todennäköisesti ulkoisia resursseja. Ennen ulkoisten resurssien hankkimista on kartoitettava, mitä organisaation sisäisiä resursseja on käytettävissä. Mitä suurempi organisaatio on kyseessä, sitä todennäköisempää on, että henkilöstöstä löytyy asiantuntevia henkilöitä, jotka kykenevät auttamaan tietoisuusohjelman toteuttamisessa. Organisaation sisältä hyödyllisiä resursseja voi löytyä niin järjestelmä- ja sovelluskehityksestä, laintulkinnasta, kouluttamisesta kuin viestinnästä. Ulkoisia resursseja sen sijaan voivat olla turvallisuusalan järjestöt, yksityiset turvallisuuspalveluyritykset ja niiden asiakkaat, konsultit, yliopistot sekä erilaiset julkaisut ja digitaaliset tietolähteet. (Peltier 2014, s. 115–116)

Asiantuntija- tai muiden resurssien käytettävyys vaikuttaa siihen, miten paljon tietoisuusohjelmassa voi olla toimintoja, jotka vaativat asiantuntijoiden osallistumista tai manuaalista työtä. Mikäli resursseja ei ole paljon käytettävissä, on organisaation tukeuduttava itseopiskelumateriaaleihin. On huomioitava, että toisille kohderyhmille mahdollisuus vuorovaikutukseen toimii parhaiten. Esimerkiksi koulutustilaisuudet kasvokkain voivat monesti olla paras tapa lähestyä ylintä johtoa. Myös budjetti vaikuttaa tietoisuusohjelman sisältöön. Turvallisuuden ohella muutkin organisaation toiminnot ja hankkeet kilpailevat käytössä olevasta budjetista. (Peltier 2014, s. 110–111)

Tekoäly, koneoppiminen ja tietojen yhdistäminen mahdollistavat organisaatioille työkaluja, jotka tarjoavat monipuolisen ymmärryksen henkilöstön käyttäytymisestä ja oppimistavoista. Kehittyneet järjestelmät edellyttävät

jatkossa yhä vähemmän manuaalista työtä. Algoritmeihin perustuva suunnittelu voi mahdollistaa organisaatiolle äärettömän määrän tietoisuusohjelmia. Käytännössä tämä tarkoittaa, että tietoisuusohjelma on mahdollista räätälöidä jokaiselle henkilölle täysin yksilöllisistä lähtökohdista. (Carpenter 2019, s. 279–280)

Tietoisuusohjelman sisällön tulee olla johdonmukaista organisaation vaatimuksiin sekä henkilöstön tavoitteisiin nähden. Toimenpiteistä on viestittävä ajoissa ja tietoisuusohjelma on pystyttävä perustelemaan kaikille sen kohderyhmille. Henkilöstölle on tehtävä selväksi, miksi tietoisuusohjelmaa tarvitaan ja miksi juuri tietyt toimenpiteet on valittu toteutettaviksi, jotta he voivat sitoutua tietoisuusohjelmaan. (Peltier 2014, s. 111) Suunniteltaessa toimenpiteitä kohderyhmäkohtaisesti on Alexanderin (ym. 2008, s. 146) mukaan pohdittava,

- mitä ja miksi henkilöiden tarvitsee tietää,
- mikä on heidän nykyinen osaamisensa,
- miten heidän tulisi ajatella ja käyttäytyä?

Peltierin (2014. s. 111–113) mukaan tietoisuusohjelman pitää käytännössä sisällään politiikan, uhkaskenaariot, palkitsemis- ja seuraamuskäytännöt, lainsäädännölliset velvollisuudet ja vastuut sekä turvallisuusmenettelyt. Tietoisuusohjelman laaja sisältö viesteineen on priorisoitava. Tämä edellyttää muun muassa riskien arviointia, jonka perusteella voidaan muodostaa prioriteettiluettelo tietoisuusohjelmaan valittavista merkityksellisistä aiheista. Arvioinnin ei tarvitse olla perusteellinen tai muodollinen, mutta sen avulla on mahdollisuus tarkastella organisaation toiminnan syy-seuraussuhteita sekä havaita mahdollisia keskeisiä riskejä nykytoiminnassa. (Peltier 2005, s. 45; Peltier 2014, s. 127)

Politiikoissa on tärkeää tuoda esille työntekijöitä koskevat vastuut sekä sääntöjen rikkomisen seuraamukset, jotta aiheen vakavuus ymmärretään läpi organisaation. Henkilöstön tulee tietää heidän tehtäviinsä liittyvät todennäköiset hyökkäysrajapinnat sekä menetelmät, joilla esimerkiksi järjestelmiin pyritään tunkeutumaan. On tärkeää ymmärtää, kuinka hyökkäyksen kohteeksi jouduttaessa toimitaan ja kuinka uhkatilanteen käsittely eskaloidaan eteenpäin. Myös esimerkkejä toteutuneista kyberhyökkäyksistä on perinteisesti käytetty osana tietoisuusohjelmaa. Uhkaskenaarioista tosimaailman varoittavien esimerkkien käyttämisellä voi olla positiivisia vaikutuksia, jos niiden käyttämisen tavoitteet, ydinviestit sekä kohderyhmät suunnitellaan huolellisesti. (Peltier 2014. s. 111–112) Henkilöstön on todettu oppivan tehokkaasti tietoturvatapahtumista, olivatpa ne sitten toteutuneita tai harjoiteltuja skenaarioita. Tämä korostaa uhkaskenaarioiden käyttämisen tärkeyttä osana tietoisuusohjelmaa. (Riahi & Islam 2024, s. 20)

Singhin (ym. 2014, s. 661) mukaan organisaatioissa on syytä ryhtyä toimenpiteisiin, mikäli tietoturvapolitiikkoja tai -periaatteita ei noudateta. Tällä tavoin annetaan työntekijöille selkeä viesti siitä, että tietoturvaan suhtaudutaan vakavasti. Organisaatioissa on monesti käytössä seuraamuskäytäntö, jonka mukaan haitallisesta toiminnasta on seuraamuksia. Seuraamukset voivat syyn perusteella vaihdella sanallisesta varoituksesta pakolliseen lisäkoulutukseen,

käyttöoikeuksien vähentämiseen, tehtävänkuvan vaihtamiseen tai irtisanomiseen. Siinä missä vahingollisesta toiminnasta on oltava seuraamuksia, on esimerkillisestä toiminnasta tärkeää antaa tunnustusta palkitsemalla. Palkitsemisella voidaan hälventää turvallisuuteen liittyviä negatiivisia asenteita ja ennakkoluuloja. Palkiseminen auttaa henkilöstöä ymmärtämään, että yksittäisillä henkilöillä ja heidän toiminnallaan on positiivisessakin mielessä merkitystä. Palkitseminen osoittaa, että yksittäisiä tietoturvaa parantavia tekoja arvostetaan. (Peltier 2014, s. 112)

Tietoisuusohjelman sisällöstä konkreettisin jokapäiväiseen työhön vaikuttava asia on turvallisuusmenettelyiden tai turvallisten toimintamallien kuvaaminen. Käytännössä tällä tarkoitetaan henkilöstölle suunnattuja turvallisuutta koskevia turvallisuusohjeita ja periaatteita. Yleisiä aiheita ovat esimerkiksi salasanojen käsittely, tietojen luokittelu ja lokienhallinta. Ohjeiden ja periaatteiden sisältö sekä tarkkuustaso voi vaihdella paljonkin riippuen siitä, mille kohderyhmälle ohje on suunnattu. (Peltier 2014, s. 113–114)

Tietoisuusohjelmassa ohjeiden ja periaatteiden toimeenpanemiseen käytettävillä tekniikoilla ja oppimismenetelmillä on suuri merkitys. Digitalisoituneessa maailmassa nämä tekniikat sekä oppimismenetelmät kehittyvät ja monipuolistuvat jatkuvasti, vaikka perinteisillä tekniikoilla on edelleen paikkansa. Esimerkkejä tekniikoista ja menetelmistä ovat

- luokkahuonekoulutukset,
- teemapäivät,
- road show't,
- tapahtumat,
- verkkokoulutukset,
- erilaiset esitykset, kuten
    - tietoiskut,
    - infotilaisuudet,
    - vierasluennot,
    - paneelit ja
    - webinaarit.

Lisäksi tärkeänä käytännön tekemistä tukevana menetelmänä toimivat erilaiset harjoitukset. Tavallisia tiedon välittämisen tekniikoita ovat myös videotallenteet, julisteet, lehtiöt tai kirjaset sekä intran ilmoitukset ja uutisjulkaisut. Intrasivuilla erilaisten tiedon esitystapojen valikoima on käytännössä rajaton. (Peltier 2014, s.117–126) Carpenterin (2019, s. 61) mukaan hyvin suunniteltu visuaalisia ulottuvuuksia sisältävä viestintä on aina yksinkertaista kirjallista viestintää tehokkaampaa. Tämän lisäksi on olemassa myös selvä tarve oppimistehtäville, joissa henkilöt voivat käytännössä havaita, mitä vaikutuksia heidän toiminnallaan on organisaation turvallisuuteen, heille itselleen ja muille. (Puhakainen & Siponen 2010, s. 774)

Käytettävien menetelmien valinnassa on huomioitava kohderyhmän monimuotoisuus sekä välitettävän viestin painoarvo. Erilaisissa menetelmissä on sekä

hyviä ja huonoja puolia. Esimerkiksi koulutusvideot ovat käytettävyydeltään parempi vaihtoehto kuin luokkahuonekoulutukset. Toisaalta niiden heikkoutena on kouluttajan ja koulutettavan välisen vuorovaikutuksen puuttuminen. Verkkokursseissa saattaa olla koulutusalustasta riippuen mahdollisuus hyödyntää parhaita ominaisuuksia sekä video- että luokkahuonekoulutuksesta. Lisäksi verkkokurssien etuna on tarkallekin tasolle mahdollistettu seuranta. Julisteiden ja esitteiden osalta ei voida olla varmoja, saavuttaako tieto koskaan kohderyhmäänsä. Näillä keinoilla voidaan kuitenkin loistavasti vahvistaa esimerkiksi tietoturvakurssin sanomaa. (Alexander ym. 2008, s. 148)

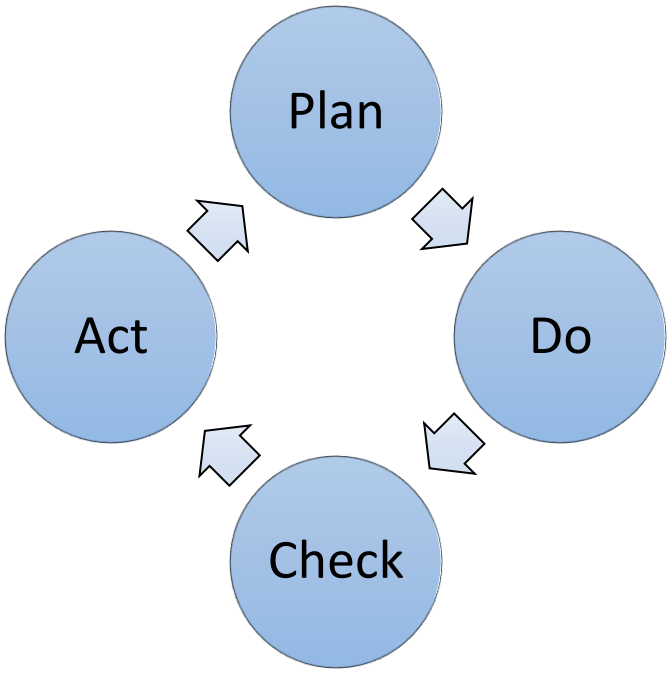
Yhtenä erinomaisena keinona viestin välittämiseen voi toimia myös ääni tai musiikki. Tutun kappaleen sävel tuo kuulijan mieleen sanat, vaikka niitä ei olisi tarkoituksellisesti opetellutkaan. (Carpenter 2019, s. 63) Musiikkia sekä ääniä käytetään esimerkiksi radio- ja tv-mainontaa tehostavana keinona. Markkinoinnin teoriassa yksi keskeisistä periaatteista on tehdä kaikki mahdollinen, jotta välitettävä viesti tavoittaisi kohdeyleisönsä. Tämän toteuttamiseksi käytetään niin sanottua monikanavaista viestintää. Monikanavaisessa viestinnässä markkinointi ei nojaa pelkästään yhteen viestintäkanavaan. (Carpenter 2019, s. 74) Tietoisuusohjelman viestintä on muotoiltava huolellisesti ja tarkoituksenmukaisesti siten, että se ei herätä negatiivisia tai kielteisiä tunteita kohderyhmissä. Muotoilu on kriittistä sen kannalta, kuinka esimerkiksi tietoisuuskampanja otetaan organisaatiossa vastaan. (Carpenter 2019, s. 114)

Jotta tietoisuusohjelma saadaan jalkautettua organisaatioon, yksi ensimmäisistä tehtävistä on johdon ja organisaation henkilöstön vakuuttaminen sen tarpeellisuudesta. Tietoturvallisuudessa on tavoiteltava tilaa, jolloin se hyväksytään osaksi organisaatiota ja sen normaalia kulttuuria. Tämä tavoitteen saavuttamiseksi on olemassa keinoja, kuten tietoisuusohjelman linkittäminen organisaatiotason tavoitteisiin, keskittyminen tärkeään tieto-omaisuuteen, riskianalyysin tekeminen, oman toiminnan vertaileminen muiden toimintaan sekä ohjelman hyötyjen esille tuominen. On todennäköistä, että toiset organisaatiot kamppailevat vastaavien haasteiden kanssa. On siksi hyvä tarkastella muiden toimintaa ja jakaa tietoa. Toisten toiminnasta on esimerkin avulla mahdollista saada nopeastikin toimivia ratkaisuja kohdattuihin haasteisiin. (Peltier 2014, s. 126–127)

3.7 Tietoisuusohjelman jatkuva parantaminen

Tietoisuusohjelman sitominen organisaatiotason tavoitteisiin on lähtökohtaisesti paras tapa perustella tietoisuusohjelman tarpeellisuus. On kuitenkin tavallista, että tavoitteet muuttuvat, jolloin myös tietoisuusohjelmaa on tarkasteltava niiden näkökulmasta uudelleen, sekä päivitettävä uusien tavoitteiden mukaisesti. (Peltier 2014, s. 126) Tietoisuusohjelmaan on sovellettava jatkuvan parantamisen ajattelua, sillä organisaatio on muun muassa toimintaympäristöstä tulevien muutospaineineiden vuoksi jatkuvan muutoksen alla. Jatkuvalla parantamisella tarkoitetaan toistuvaa toimintaa, jolla parannetaan suorituskykyä (Suomen standardoimisliitto SFS ry 2020, s. 7). Demingin laatuympyrää noudattavan jatkuvan

parantamisen PDCA-mallin (Kuvio 2) hyödyntäminen tietoisuuden kehittämisessä onkin empiiristen tutkimusten mukaan osoittautunut tehokkaaksi lähestymistavaksi. Tietoisuusohjelma ei ole koskaan valmis, vaan sen on mukauduttava organisaatiossa ja sen toimintaympäristössä tapahtuviin muutoksiin. (Carpenter 2019, s. 259; Khando ym. 2021, s. 17–18)



KUVIO 2 Jatkuvan parantamisen PDCA-malli

Mikäli organisaatiossa on sisäisiä auditointeja toteuttava elin, kannattaa tätä hyödyntää jatkuvan parantamisen mallin toteuttamisessa. Yhteistyö jo organisaatiossa valmiiksi olevien resurssien kanssa juurruttaa tietoisuusohjelman kehittämisen organisaation alkuperäisiin toimintoihin. Mahdolliset muutokset ja parannukset kannattaa pilkkoa pienemiin osatavoitteisiin, jolloin muutos ei tunnu kohtuuttoman suurelta askeleelta. Esimerkiksi pienempien kokonaisuuksien kouluttaminen on myös usein tehokkaampaa, joustavampaa ja vie vähemmän aikaa sekä muita resursseja. (Peltier 2014, s. 128)

4 TUTKIMUSKONSEPTI, -STRATEGIA JA-MENETELMÄT

Tutkimuskohde on pro gradu -tutkielmassa selkeästi rajattu ja perustuu opinnäytetyön toimeksiantajan kehittämistavoitteisiin. Pääosin tästä syystä sen tutkimusstrategiaksi on valittu tapaustutkimus (eng. case study research). Ojasalon ym. (2014, s. 53) mukaan tapaustutkimuksessa tutkimuskohde valitaan työelämän kehittämistyössä havaitun käytännön tarpeen ja kehittämistyölle asetettujen tavoitteiden ohjaamana. Juuri tästä tutkielmassa on kysymys. Tutkielman tutkimuskysymys on:

> Mitä hyvien käytänteiden mukaisia, laissa säädettyjä sekä sidosryhmiltä tulevia vaatimuksia Kelan tietoturvayksikön tietoisuusohjelmaan kohdistuu yksikön tehtävät ja vastuut huomioiden?

Yinin (2018, s. 15) mukaan tapaustutkimus on empiirinen lähestymistapa tutkimukseen, joka tutkii valittua ilmiötä syvällisesti, nykyhetkessä ja sen todellisessa ympäristössä. Tapaustutkimuksessa ei tällöin rakenneta keinotekoista tutkimustilannetta (Vilkka 2015, s. 156). Tämä kuvastaa hyvin pro gradun tutkimustehtävän tavoitteita ja puoltaa edelleen tapaustutkimuksen valintaa tutkimusstrategiaksi. Myös tutkimuksen kartoittava lähestymistapa puoltaa tutkimusstrategian valintaa, sillä tämän tarkoituksen omaavassa tutkimuksessa tapaustutkimus on sopiva valinta tutkimusstrategiaksi (Hirsjärvi ym. 2009, s. 138). Pro gradussa painottuu tapaustutkimukselle tunnusomaisesti tavanmukaisen tutkimuksen tavoite eli tiedon tuottaminen valitusta kohteesta (Ojasalo ym. 2014, s. 37). Tapaustutkimuksen pyrkimyksenä on ymmärtää tosimaailman tapausta pureutumalla kysymyksiin: kuinka, miten ja miksi jokin tapahtuu? (Yin 2018, s. 15; Ojasalo ym. 2014, s. 52)

Tapaustutkimusta on usein käytetty tutkimusstrategiana liiketaloustieteissä. Se soveltuu tilanteisiin, joissa on tavoitteena saada aikaan kehittämisehdotuksia tai -ideoita. Tutkimuksen kohteeksi eli tapaukseksi soveltuu esimerkiksi organisaation osa tai prosessi, jolloin tarkoituksena on tutkia

perusteellisesti jonkin organisaation tai sen osan tilannetta, tuottaa ratkaisu tunnistettuun ongelmaan tai luoda kehittämisehdotuksia. (Ojasalo ym. 2014, s. 37 & 52)

Tapaustutkimuksen ominaispiirteitä ovat aiheen tarkka rajaus sekä teoreettinen kattavuus (Vilkka 2015, s. 154). Kirjallisuuteen ja teoriaan perehtymisen tarkoituksena on löytää olemassa olevasta se, mikä on merkityksellistä tutkimustehtävän kannalta. Pro gradun teoreettinen kattavuus on laaja, sillä tapaustutkimuksessa tutkijan on perehdyttävä aiheeseen, jotta kehittämistehtävän voi tarkemmin määritellä ja aiheesta osaa kysyä tutkimustavoitteiden saavuttamisen kannalta olennaisia asioita. Tapaustutkimus hyötyy aiemmasta tapaukseen liittyvästä teoriasta, sillä aiemmin kehitetyt teoreettiset mallit voivat ohjata tutkittavan ilmiön kehittämistä. (Ojasalo ym. 2014, s. 54; Yin 2018, s. 15)

Tapaustutkimukseen soveltuvat niin määrälliset kuin laadulliset menetelmät, mutta useimmiten siihen yhdistetään laadullisia menetelmiä, kuten havainnointia sekä haastatteluiden tekemistä. Tutkimuksessa huomioidaan paikalliset, ajalliset ja sosiaaliset tilanteet ja yhteydet tarkoituksena tuottaa uutta tietoa kehittämisen tueksi. Tutkimusaineisto rajataan tarkasti tutkimuksen teoreettista kattavuutta silmällä pitäen ja siihen voivat tavallisesti kuulua esimerkiksi organisaation vuosikertomukset tai työntekijät. (Ojasalo ym. 2014, s. 53 & 55; Vilkka 2015, s. 153–155)

Pro gradu -tutkielma muodostaa tapaustutkimukselle ominaisesti tutkimuskohteesta kokonaisvaltainen sekä perusteellinen kuvan useita eri tiedonhankintamenetelmiä käyttäen (Ojasalo ym. 2014, s. 37). Pro gradussa valitut keskeiset tiedonkeruumenetelmät ovat asiantuntijoiden puolistrukturoidut teemahaastattelut sekä teoreettiseen viitekehykseen ja muuhun lähdemateriaaliin nojaava dokumenttianalyysi. Dokumenttianalyysissa tarkempi lähestymistapa on aineistolähtöinen sisällönanalyysi. Menetelmien valinnassa on tavoiteltu laadullisen tutkimuksen uskottavuutta, sekä luotettavuutta lisäävää triangulaatiota eli tutkimuskohteen tutkimista useista eri näkökulmista (Ojasalo ym. 2014, s. 105).

4.1 Haastattelut

Tapaustutkimuksessa tutkimuskohteen asiantuntijoiden tai muiden tutkimuskohteeseen liittyvien avainhenkilöiden tunnistaminen sekä haastatteleminen ovat usein tutkimustavoitteiden saavuttamisen kannalta ratkaisevassa asemassa. Heiltä on mahdollista saada sisäpiirin tietoa tutkimuskohteesta sekä heidän avullaan voidaan tunnistaa muita potentiaalisia haastateltavia henkilöitä. (Yin 2018, s. 119) Haastattelun yleisiä vahvuuksia ovat tiedonkeruun nopeus sekä sen avulla saavutetun tiedon syvällisyys (Ojasalo ym. 2014, s. 106). Haastattelun avulla on mahdollista saada selville tutkimustavoitteiden kannalta merkityksellisiä asioita, joita ei muilla tiedonkeruumenetelmillä saataisi lainkaan selville. Menetelmän etuna pidetään myös sen joustavuutta, sillä haastatteluaiheiden järjestystä on mahdollista säädellä. Ihmiselle annetaan haastattelussa tutkimuksen

subjektina mahdollisuus tuoda esille itseään koskevia asioita mahdollisimman vapaasti. (Hirsjärvi ym. 2009, s. 205)

Vaikka haastatteluun liittyy menetelmänä kiistämättömiä etuja, vaatii haastatteluiden valmistelu sekä toteuttaminen paljon työtä. Ensinnäkin tutkijan on perehdyttävä hyvin tutkimuskohteeseen ja sen kontekstiin ennen haastatteluiden laatimisen aloittamista. Vilkan (2015, s. 130) mukaan tutkijan tulisi tuntea tutkittava kohderyhmä, sen toimintaympäristö ja kulttuuri, jotta ihmisten kulttuurisidonnaisten ja tilannekohtaisten kokemusten ja käsitysten ymmärtäminen sekä tulkitseminen olisi mahdollista. Tutkijan tulisi muun muassa tuntea, millaisten kulttuuristen merkitysrakenteiden ja aineellisten elinolosuhteiden mukaan tutkittava toimii ja tuottaa merkityksiä.

Pro gradun yhtenä tutkimusmenetelmänä käytettiin puolistrukturoitua haastattelua eli teemahaastattelua sekä ryhmä- että yksilöhaastatteluna. Vilkan (2015, s. 124) mukaan teemahaastattelu on strukturoidun lomakehaastattelun ja avoimen haastattelun välimuoto, ja se on yleisimmin käytetty haastattelun muoto laadullisessa tutkimuksessa. Tutkielmassa noudatettiin teemahaastatteluiden ominaispiirteitä. Haastattelussa tarkoituksena oli kerätä tietoa organisaation henkilöstöltä, joka toimii keskeisenä tutkimuksen tiedonkeruun lähteenä. Yinin (2018, s. 118) mukaan tapaustutkimuksessa haastattelut muistuttavat enemmän ohjattua keskustelua, kuin strukturoitua haastattelua. Teemahaastattelu oli tästä syystä looginen valinta haastattelumenetelmäksi.

Haastateltavat valittiin tutkimuksessa suostumuksen perusteella, joka pyydettiin antamaan erikseen laaditun kyselyn perusteella (Liite 1). Lomakkeella pyydettiin suostumusta haastatteluun, nimen julkaisuun pro gradu -tutkielmassa sekä ehdotuksia haastateltaviksi henkilöiksi. Linkki kyselylomakkeeseen lähetettiin sähköpostitse tietoturvayksikön asiantuntijoille, tietoturvan johtotiimille sekä organisaatiosta tunnistetuille tietoisuustyön näkökulmasta keskeisille sidosryhmille. Suostumuksen haastatteluun antoi yhteensä 15 henkilöä, joista haastateltaviksi valittiin 12 henkilöä. Haastattelujoukosta johdon näkökulmaa edusti tietoturvapäällikkö sekä kaksi tiimipäällikköä ja yksikön henkilöstön näkökulmaa edustivat eri rooleissa työskentelevät haastateltavaksi valikoituneet asiantuntijat. Sidosryhmien näkökulmaa edustivat turvallisuuden, tietoturvan sekä tietosuojan keskeiset yhteyshenkilöt muualta Kelan organisaatiosta. Osa haastateltavista ei antanut lupaa julkaista nimeään tutkielmassa, joten heidän nimiään ei tästä syystä mainita tutkielman lähdeluettelossa.

Vain tietoturvapäällikön haastattelu toteutettiin yksilöhaastatteluna. Lopuista haastatteluun suostuneista muodostettiin haastatteluryhmät: asiantuntijoiden ryhmähaastattelu 1 ja 2, sidosryhmien haastattelu sekä teknisen tilannekuvakeskuksen haastattelu. Ryhmähaastattelun käyttäminen oli perusteltua, sillä se on monissa tapauksissa yksilöhaastatteluita tehokkaampi tiedonkeruutapa. Tehokkuus perustuu siihen, että menetelmällä saatiin kerättyä tietoa usealta henkilöltä samanaikaisesti. Eduksi voitiin katsoa myös haastattelutilanteessa esiintyvä haastateltavien ryhmädynamiikka, joka usein vie käsiteltäviä aiheita uusille tasoille haastateltavien tukiessa toisiaan ja täydentäessä vastauksiaan. (Hirsjärvi ym. 2009, s. 210–211; Ojasalo ym. 2014, s. 111)

Vilkan (2015, s. 125) mukaan ryhmähaastattelu on mielekäs keino tiedonkeräämiseen työelämän tutkimuksellisissa kehittämishankkeissa, joissa tavoitteena on yhteisen kielen, käsitteiden, toimintatapojen ja ymmärtäminen. Ryhmille lähetettiin haastattelukutsut sähköpostitse. Ryhmiin valittiin henkilöitä heidän roolinsa sekä työkalenterissa samaan aikaan vapaana olevien ajankohtien perusteella. 4 haastattelua toteutettiin Kelan videoneuvottelusovelluksen kautta etähaastatteluna ja toinen asiantuntijoiden ryhmähaastatteluista toteutettiin fyysisesti samassa tilassa haastateltavien kanssa. Kaikkiin haastatteluihin varattiin aikaa vähintään tunti.

Teemahaastatteluissa noudatettiin teemahaastattelurunkoa (Liite 2), joka pohjautui aiemmin muodostetusta teoreettisesta viitekehyksestä nostettuihin tutkimustavoitteen kannalta keskeisiin teemoihin (Luku 5.1). Vaikka teemojen tai aiheiden käsittelyjärjestyksellä ei ole puolistrukturoidussa teemahaastattelussa merkitystä, noudatettiin haastatteluissa teemojen loogista järjestystä. Kysymysten tarkka järjestys ja muoto puuttuivat. Haastatteluissa esitettiin myös ennakkoon kirjaamattomia kysymyksiä, mikäli ne koettiin tarpeelliseksi. Haastatteluissa kysymykset pyrittiin esittämään niin, että niihin oli vastattava kuvailevasti ja kertomuksenomaisesti kyllä- ja ei-vastausten sijaan. (Hirsjärvi ym. 2009, s. 208; Ojasalo ym. 2014, s. 108; Vilkka 2015, s. 128 & 135)

Haastattelut äänitettiin, sillä Ojasalon ym. (2014, s. 110) mukaan haastattelijan on tällöin mahdollista tarkkailla haastateltavaa paremmin haastattelutilanteessa. Kelan videoneuvottelusovellus mahdollisti haastattelun tallentamisen videotallenteeksi. Yksi fyysisesti samassa tilassa toteutettu haastattelu tallennettiin puhelimen ääninauhurilla. Äänittämisen suurin etu oli se, että se mahdollisti hyvin tarkalle tasolle menevän litteroinnin vielä haastattelun jälkeenkin. Ojasalon (ym. 2014, s. 107) mukaan äänitteiden kuunteleminen jälkeenpäin auttaa tutkijaa ymmärtämään haastateltavan vastauksia useammista näkökulmista.

Haastattelujen jälkeen toteutettiin haastatteluiden litterointi eli haastatteluaineiston puhtaaksi kirjoittaminen äänitallenteiden perusteella. Puhtaaksi kirjoittamisessa haastateltavien haastattelutavoitteen kannalta olennaiset puheenvuorot kirjoitettiin sanatarkasti ylös teemojen mukaisessa järjestyksessä. Puheenvuoroista jätettiin kirjaamatta sellaiset tiedot, jotka olisi jätettävä pois julkisesta aineistosta.

4.2 Dokumenttianalyysi

Laadullisessa tutkimustyössä käytetään usein tiedonkeruumenetelmänä tutkimuskohteen tutkimista sen itse tuottaman tai siitä tuotetun dokumentaation avulla (Hirsjärvi ym. 2009, s. 217). Yinin (2018, s. 114) mukaan dokumentoituun tietoon tutkimuslähteenä liittyy paljon etuja, kuten aineiston sisältämän tiedon yksityiskohtaisuus, laajuus sekä mahdollisuus toistuvaan aineiston läpikäymiseen. Tästä syystä dokumenttianalyysi soveltui erinomaisesti myös tämän tutkielman tiedonkeruumenetelmäksi. Dokumenttianalyysillä pyrittiin tekemään päätelmiä kirjallisessa muodossa olevasta aineistosta. Ojasalon (ym. 2014, s. 136)

mukaan dokumenttianalyysin tavoitteena on tuottaa selkeä kuvaus tutkittavasta kohteesta analysoidun aineiston perusteella. Tarkastelun kohteena olivat monenlaiset aineistot, kuten kirjallisuus, standardit, lainsäädäntö, Kelan julkiset www-sivut, tutkimusartikkelit, politiikat, vuosikertomukset, raportit sekä myös litteroidut haastatteluaineistot. Tutkielman kannalta keskeisimpänä aineistona toimii teoreettisen viitekehyksen muodostava kirjallisuuteen sekä tutkimusartikkeleihin pohjautuva kirjallisuuskatsaus, jossa on kuvattu tutkimuksen keskeisiä käsitteitä.

Teoreettisen viitekehyksen lähteet haettiin Laurea-ammattikorkeakoulun Finna -tiedonhakupalvelua sekä Jyväskylän Yliopiston kirjaston JYKDOK -tiedonhakupalvelusta, josta on pääsy useisiin eri tietokantoihin. Tietokannoista haettiin sekä niin fyysisenä painoksena kuin verkossa saatavilla olevia kirjallisia teoksia, että vertaisarvioituja tutkimusartikkeleita. Hakuehtoina lähteiden hakemiseen toimivat suomenkieliset termit: tietoturvallisuus, tietoturva, turvallisuusosaaminen sekä englanninkieliset termit information, security, information security, information security awareness, awareness, program, awareness program, cyber awareness, competence, learning, requirements.

Ojasalon ym. (2009, s. 136) mukaan lähdeaineistoksi lukeutuvat kaikki tutkittavasta ilmiöstä kirjoitettu, puhuttu tai kuvattu materiaali. Jossain määrin jopa rajaton tietolähteiden määrä saattaa toimia tutkimustyön varjopuolena ja tutkija saattaa hukkua tietoon, mikäli aineiston rajausta ei tehdä huolellisesti (Yin 2018, s. 117). Tästä syystä tutkielmassa pyrittiin keskittymään vain sen kannalta kaikista olennaisimpaan tietoon, jotta tiedonhakuun ei kuluisi kohtuuttomasti aikaa. Kelaan liittyvästä ja Kelan sisäisestä dokumentaatiosta käytettiinkin aineistona vain keskeisimpiä tutkimuskysymyksen kannalta relevantteja kirjallisia ja julkiseksi luokiteltuja dokumentteja, lainsäädäntöä sekä viitekehyksiä. Kelan dokumentaatiosta keskeisimpinä lähteinä toimivat Kelan strategia, tietoturva- ja tietosuojapolitiikka ja Kelan turvallisuuden strategiset linjaukset.

Pro gradun dokumenttianalyysin lähestymistapana on käytetty aineistolähtöistä sisällönanalyysiä, jolla kuvataan sanallisesti dokumenttien sisältöä ja pyritään löytämään tutkimusaineistosta merkityssuhteita sekä -kokonaisuuksia. Tavoitteena on tunnistaa aineistosta esimerkiksi jonkinlainen tutkimusaineiston ohjaama logiikka tai tyypillinen kertomus eli narratiivi. (Ojasalo ym. 2014, s. 137; Vilkka 2015, s. 163) Aineistolähtöisen sisällönanalyysin työvaiheissa on noudatettua Ojasalon ym. (2014, s. 139) esittämää mallia, jossa analyysin työvaiheita ovat aineiston pelkistäminen, ryhmittely ja abstrahointi, jolla tarkoitetaan yleiskäsitteiden muodostamista. Analyysin tulokset esitellään seuraavassa luvussa.

5 TUTKIMUSTULOKSET JA TULOSTEN ANALYYSI

Tässä luvussa esitetään tutkimuksen tulokset vastaten päätutkimuskysymykseen: Mitä hyvien käytänteiden mukaisia, laissa säädettyjä sekä sidosryhmiltä tulevia vaatimuksia Kelan tietoturvayksikön tietoisuusohjelmaan kohdistuu yksikön toimintaympäristö, tehtävät ja vastuut huomioiden?

Tutkimustulokset sisältävät aihealueittain sekä haastatteluiden että dokumenttianalyysin tuotokset. Tietoisuusohjelman vaatimuksia tarkastellaan tulosten ja niiden analyysin muodossa ensin hyvien käytäntöjen, seuraavaksi Kelaa velvoittavan lainsäädännön ja määräysten sekä lopuksi sisältä ja sidosryhmiltä tulevien vaatimusten näkökulmasta.

Vaatimukset on tämän luvun pohjalta koottu tutkielman liitteeksi taulukkoon (Liite 3). Taulukoinnissa vaatimusten lähteitä ei ole eritelty, sillä tutkimusteoriaan, lainsäädäntöön ja määräyksiin, viitekehyksiin ja standardeihin sekä sisäisiin että sidosryhmien odotuksiin perustuvat vaatimukset ovat tutkimustuloksissa esitetty toisiinsa nähden tasavertaisina.

5.1 Aiempi tutkimus

Tietoturvakulttuurin kehittäminen edellyttää suunnittelua. Aiheeseen liittyvän tutkimustiedon ja kirjallisuuden pohjalta voidaan todeta, että organisaation tulisi harkita suunnitelmallisena lähestymistapana tietoisuusohjelman toteuttamista. Kaiken lähtökohtana on ylimmän johdon vankkumaton tuki tietoturvallisuuden ja siihen liittyvän tietoisuuden kehittämiselle, jotta ohjelman resursointi ja organisaation tavoitteiden mukaisuus voidaan taata.

Tietoisuusohjelma on sisältöineen laaja kokonaisuus, joka edellyttää organisaation nykytilaan, toimintaympäristöön sekä ominaispiirteisiin pohjautuvaa tarkkaa priorisointia. Tietoisuusohjelman läpivienti sisältää teoreettisen viitekehyksen perusteella kuusi eri vaihetta, joissa on huomioitava joitakin keskeisimpiä osatekijöitä. Vaiheet ja osatekijät on tiivistetty kirjallisuuskatsauksesta

toteutetun aineistolähtöisen sisällönanalyysin keinoin seuraavaan taulukkoon (Taulukko 2):

TAULUKKO 2 Tietoturvatietoisuuden kehittämisen vaiheet ja osatekijät

1 Johdon tuki	Strategiaa noudattavat tavoitteet
	Näkyvä ja jatkuva viestintä
	Esimerkillä johtaminen
2 Projektin ja tiimin perustaminen	Monipuolinen asiantuntijuus
	Edustajat eri puolilta organisaatiota
	Raportointi ylimmälle johdolle
3 Toimintasuunnitelman laatiminen	Tavoitteiden määrittely
	Käytettävissä oleva budjetti
	Sisäiset ja ulkoiset resurssit
	Nykytilan analyysi
	Kohderyhmien tunnistaminen
	Asiakaspolkujen laatiminen
	Vaadittavan pätevyystason määrittely
4 Sisältö	Politiikat ja periaatteet
	Uhkaskenaarioiden laatiminen
	Velvollisuudet ja vaatimukset
	Seuraamus- ja palkitsemiskäytäntö
	Käytännön toimintamallit
5 Toteuttaminen	Jatkuva monikanavainen viestintä
	Käytännönläheiset oppimistehtävät
	Yksilöllisten oppimistyylien huomiointi
6 Jatkuva parantaminen	PDCA-syklin noudattaminen
	Sisäiset auditoinnit
	Muuttuvien tavoitteiden huomiointi

5.2 Standardit

Tässä luvussa esitellään dokumenttianalyysin keskeisiä havaintoja tutkielman aiheen kannalta merkityksellisimmistä standardeista ja viitekehyksistä. Kansainvälisen standardoimisjärjestö ISO:n (International Organization for Standardization) standardeista katselmoitavana oli ISO/IEC 27000 -sarjan standardit. Kyseiset standardit ovat lisenssin alaisia, joten niiden osalta käytetään tässä tutkielmassa referointia suorien lainausten sijaan.

ISO/IEC 27001 -standardissa tietoturvallisuuden hallintajärjestelmän vaatimuksista (Suomen standardoimisliitto SFS ry 2023, s. 12) hallintajärjestelmän rakenteeseen liittyy keskeisinä tukitoimintoina henkilöstön pätevyys, tietoisuus sekä viestintä. Näihin liittyvissä vaatimuksissa organisaation ohjauksessa työskentelevien henkilöiden on oltava tietoisia sen tietoturvapolitiikasta ja ymmärrettävä, miten he voivat omalla toiminnallaan vaikuttaa tietoturvan tasoon sekä

mitä seurauksia tietoturvan hallintajärjestelmää koskevien vaatimusten noudattamatta jättämisellä voi olla. Lisäksi organisaation on

- määriteltävä tietoturvarooleissa vaadittava pätevyyden taso,
- varmistettava kyseisten henkilöiden riittävä pätevyys,
- kehitettävä pätevyyttä tarpeen mukaan ja
- arvioitava kehitystoimenpiteitä sekä
- säilytettävä näyttöä henkilöiden pätevyydestä.

Organisaation olisi myös määriteltävä, millaista viestintää tietoturvallisuuden hallintajärjestelmän kannalta tarvitaan sekä suunniteltava, kuinka tämä viestintä toteutetaan (Suomen standardoimisliitto SFS ry 2023, s. 12).

Henkilöstön osaamiseen liittyy myös standardin hallintakeino 6.3: Tietoturvatietoisuus, -opastus ja -koulutus. Tämän mukaan organisaation ja sen sidosryhmien henkilöstön on saatava tietoturvakoulutusta ja heidän tietojaan tietoturvaa koskevien periaatteiden ja menettelyjen muutoksista on päivitettävä säännöllisesti tehtävien edellyttämässä laajuudessa (Suomen standardoimisliitto SFS ry 2023, s. 20).

Hallintakeinoa tarkemmin käsittelevässä ISO/IEC 27002 -standardissa opastetaan organisaatiota tietoisuusohjelman toteuttamiseen. Tietoisuusohjelman tavoitteena on sen mukaan tuoda esille henkilöstön vastuut tietoturvasta sekä keinot näiden toteuttamiseksi. Standardi korostaa, että henkilöstön on tärkeää ymmärtää tietoturvan tarkoitus ja heidän käytöksestään johtuvat niin hyvät kuin huonotkin vaikutukset. (Suomen standardoimisliitto SFS ry 2022, s. 72)

Tietoisuusohjelmalla varmistettaisiin toimenpiteiden säännöllisyys sekä kattavuus kohderyhmittäin. Ohjelma sisältää erilaisia fyysisten ja virtuaalisten kanavian kautta toteutettuja tietoisuutta parantavia toimenpiteitä, jotka kattavat yleisiä näkökohtia

- vaatimustenmukaisuudesta,
- johdon sitoutumisesta,
- henkilökohtaisesta vastuusta,
- yleisistä tietoturvamenettelyistä,
- hallintakeinoista sekä
- yhteydenotto ja neuvontakanavista. (Suomen standardoimisliitto SFS ry 2022, s. 71)

Toimenpiteitä ei tarvitse toteuttaa erillisinä, vaan ne voidaan integroida esimerkiksi yleiseen tietojenhallinnan, tietotekniikan tai turvallisuuden koulutukseen. (Suomen standardoimisliitto SFS ry 2022, s. 72)

Opastuksesta ja koulutuksesta hallintakeinossa esitetään, että IT-asiantuntijaryhmille, joiden tehtävät edellyttävät erityistä tietoturvaosaamista, olisi laadittava ja toteutettava oma koulutussuunnitelmansa. Suunnitelmalla varmistettaisiin riittävä osaaminen organisaation teknisen ympäristön riittävän turvallisuustason konfigurointiin sekä ylläpitämiseen. ISO/IEC 27002 -standardi ei rajaa

keinoja, joita organisaatio voi käyttää riittävän osaamisen saavuttamiseen, vaan se kattaa kaikki keinot luokkahuonekoulutuksesta osaavien konsulttien palkkaamiseen. Organisaation vastuun lisäksi standardissa korostetaan myös henkilöstön vastuuta ylläpitää omaa osaamistaan esimerkiksi lukemalla ajankohtaista tietoa tai käymällä asiantuntijatapahtumissa. (Suomen standardoimisliitto SFS ry 2022, s. 71–72)

Koulutuksen tai muun tietoisuutta lisäävän toiminnan jälkeen sen vaikutusta, eli henkilöstön ymmärrystä koulutetusta aiheesta on arvioitava, jotta savutettu ymmärrys voidaan todentaa. Hallintakeinon tarkoituksena on varmistaa henkilöstön tietoisuus tietoturvavastuistaan sekä varmistaa, että henkilöstö myös täyttää nämä vastuut. (Suomen standardoimisliitto SFS ry 2022, s. 70–71)

5.3 Viitekehykset

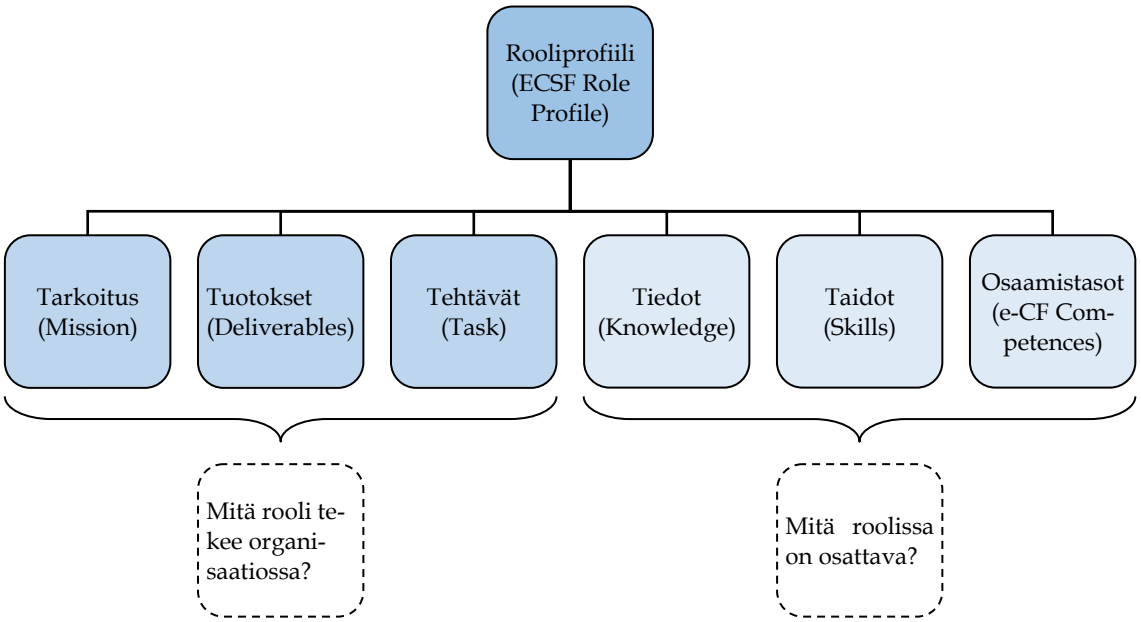
Kuten aiemmin kirjallisuuskatsauksessa on tullut ilmi, tietoturvaosaamiseen liittyviä viitekehyksiä on olemassa useita erilaisia. Tämän tutkielman kontekstissa käsitellään lyhyesti kaksi aiheeseen vahvasti nivoutuvaa kansainvälisesti laajasti tunnettua viitekehystä: Yhdysvaltojen kansallisen standardisointi ja teknologiainstituutin NIST:in (National Institute of Standards and Technology) julkaisema NICE-viitekehys (Workforce Framework for Cybersecurity sekä eurooppalainen ENISA:n julkaisema kyberturvallisuusosaamisen ECSF-viitekehys (European Cybersecurity Skills Framework).

ECSF-viitekehys on tarkoitettu Euroopan Unionin alueella sijaitseville organisaatioille, koulutusalan toimijoille, ammattilaisille sekä yhdistyksille ja kaikille kyberturvallisuuden osaamisen kehittämisestä kiinnostuneille tahoille. Sen tavoitteena on ollut vastata kyberturvallisuuteen liittyvään työvoiman sekä osaamisen puutteeseen. Viitekehys tarjoaa käytännöllisen apuvälineen kyberturvallisuuteen liittyvien roolien sekä näiltä vaadittavan osaamisen tunnistamiseen kuvaamalla 12 keskeisintä kyberturvallisuuteen liittyvää rooliprofiilia. (ENISA 2022, s. 5)

ECSF-viitekehyksessä kuvatut roolit ovat:

- Chief Information Security Officer (CISO),
- Cyber Incident Responder,
- Cyber Legal, Policy and Compliance Officer,
- Cyber Threat Intelligence Specialist,
- Cybersecurity Architect,
- Cybersecurity Auditor,
- Cybersecurity Implementer,
- Cybersecurity Researcher,
- Cybersecurity Risk Manager,
- Digital Forensics Investigator ja
- Penetration tester. (ENISA 2022, s. 6)

Kullekin roolille on oma roolikorttinsa, joka koostuu muun muassa roolin yleiskuvauksesta, tarkoituksesta, ydintehtävistä sekä roolille merkityksellisistä tiedoista ja taidoista. Viitekehys on yhteensopiva eurooppalaisen viisiportaisen e-CF viitekehyksen (e-Competence Framework) kanssa, joka on tarkoitettu kuvaamaan ICT (Information and Communication Technology) -organisaation eri asiantuntijarooleihin ja niiden mukaisiin tehtäviin tarvittavaa osaamista, tietoja sekä taitoja. (ENISA 2022, s. 9 & 26) ECSF-viitekehyksen roolikorteissa on suorat viittaukset e-CF-viitekehyksen osaamistasoihin. Roolikorttia on havainnollistettu rooliprofiililla (Kuvio 3).

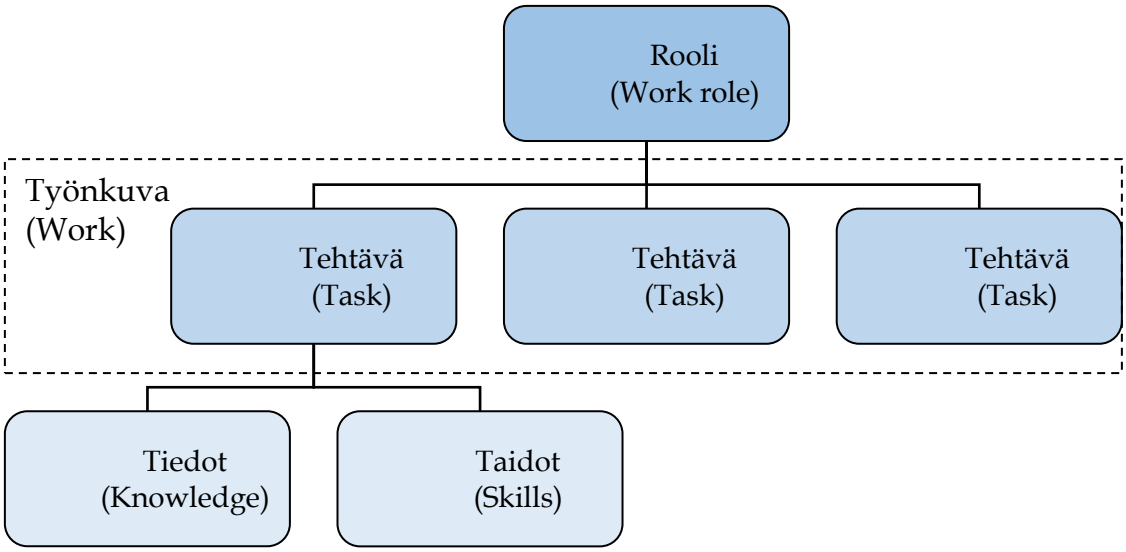


KUVIO 3 ECSF-rooliprofiilin osa-alueet (ENISA 2022, s. 24)

Organisaatiot voivat hyödyntää näitä roolikortteja joko suoraan tai mukautettuna. Organisaation tulee ensin tunnistaa tarvitsemansa asiantuntijaroolit sekä rooleilta vaadittava osaaminen perustuen organisaation kyberturvallisuuden tilaan, strategiaan sekä tavoitteisiin. Viitekehyksen rooleja voidaan täten hyödyntää joko suoraan rekrytoinneissa tai osaamisen kehittämisessä. (ENISA 2022, s. 15) ENISA:n (2022, s. 11) mukaan yhteinen terminologia sekä EU:n lainsäädännön huomioiminen kriittisten kyberturvallisuuteen liittyvien osaamistarpeiden tunnistamisessa ovat keskeisiä hyötyjä, joita viitekehys voi tarjota sen käyttäjille.

Yhdysvaltalainen NICE-viitekehys on suunnattu kaikenlaisille organisaatioille riippumatta siitä, onko organisaatio voittoa tavoittelematon, julkisen sektorin toimija tai yksityisen sektorin toimija. NICE-viitekehyksen käsitteellinen lähestymistapa mahdollistaa sen sovittamisen organisaation omaan ainutlaatuiseen toimintaympäristöön. Viitekehys muodostaa aihepiiristä organisaatioiden välistä yhteistä käsitteistöä, jotta yhteistyö aiheen ympärillä olisi vaivattomampaa. (NIST 2020, s. 2–3)

Viitekehyksen tarkoitus on auttaa organisaatioita kuvaamaan ne rakennuspalikat, joista organisaation sekä sen sidosryhmien kyberturvallisuusosaaminen koostuu. Viitekehyksen rakennuspalikoita ovat tiedot ja taidot, joita oppijalla eli henkilöllä voi olla. Viitekehyksessä henkilö voi kuvastaa esimerkiksi opiskelijoita tai työnhakijoita, eikä rajoitu pelkästään organisaation työntekijöihin. Rakennuspalikoita ovat myös tehtävät, jotka sisältyvät organisaation kyberturvallisuuden tavoitteiden saavuttamiseksi toteutettavaan työhön. Tehtävien sisältö määrittää henkilöltä työhön vaadittavat tiedot sekä taidot. (NIST 2020, s. 1–3)



KUVIO 4 Työroolin jakautuminen NICE-viitekehyksessä (NIST 2020, s. 11)

Viitekehyksen mukaan tehtävät puolestaan muodostavat pätevyydet erilaisille kyberturvallisuuden rooleille tai tehtävänkuville (Kuvio 4). Tarkat noin 50 roolikuvausta löytyvät taulukosta ja jakautuvat seitsemälle eri osa-alueelle, joita ovat

- valvonta ja johtaminen (oversight and governance),
- suunnittelu ja kehittäminen (design and development),
- implementointi ja toiminta (implementation and operation),
- suojaaminen ja puolustus (protection and defence),
- tutkinta (investigation),
- kybertiedustelu (cyberspace intelligence) ja
- kybervaikuttaminen (cyberspace effects).
  (NIST 2024)

Viitekehyksellä on useita kuvattuja käyttötapauksia. Käyttötapauksista tämän tutkielman kontekstissa keskeisin on valmiiksi kuvattujen työroolikuvausten ja pätevyyksien hyödyntäminen referenssinä organisaation eri roolien riittävän kyberturvallisuusosaamisen tavoittelemisessa. (NIST 2020, s. 6–7)

Kummastakaan esitellystä viitekehyksestä ei ole suoraan nostettavissa vaatimuksia tietoturvatietoisuusohjelmalle Kelan tietoturvayksikössä. Viitekehysten sisältämiä rooli-, tehtävä- sekä osaamiskuvauksia voi kuitenkin käyttää apuna soveltuvin osin tietoturvaroolien suunnitteluun sekä tietoturvarooleissa työskentelevien asiantuntijoiden osaamistarpeiden tunnistamiseen.

5.4 Lainsäädäntö sekä määräykset

Kelan tietoturvaa ohjaava lainsäädäntö kattaa lukuisia lakeja. Tässä luvussa dokumenttianalyysin tuloksia tarkastellaan kuitenkin vain tieturvatietoisuuden kehittämistä koskevien asetusten, lakien sekä määräysten perusteella. Näitä ovat

- Euroopan unionin yleinen tietosuoja-asetus 2016/679,
- Euroopan parlamentin ja neuvoston (NIS 2) direktiivi 2022/2555,
- laki julkisen hallinnon tiedonhallinnasta 906/2019,
- laki sosiaali- ja terveyshuollon asiakastietojen käsittelystä 703/2023 sekä
- Terveyden ja hyvinvoinnin laitoksen määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista 3/2024.

Euroopan unionin yleisen tietosuoja-asetuksen (2016) artiklojen 29 ja 32 mukaan Kelan tulee laatia henkilötietojen käsittelyä koskevat ohjeet ja varmistaa, että tietoja käsitellään näiden ohjeiden mukaisesti. Lokakuussa 2024 sovellettavaksi tulleessa NIS 2 -direktiivissä (2022) 21 artiklan kohdassa 1 edellytetään, että:

> Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat toteuttavat asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet hallitakseen riskejä, joita niiden toiminnoissaan tai palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen kohdistuu, ja estääkseen tai minimoidakseen poikkeamien vaikutuksen palvelujensa vastaanottajiin ja muihin palveluihin.

Kela voidaan ymmärtää direktiivin tarkoittamana kansallisesti tärkeänä toimijana. Tietoisuuden kehittämisen näkökulmasta edellytetyt asianmukaiset organisatoriset toimenpiteet sisältävät muun muassa perustason kyberturvallisuushygieniakäytäntöjen ylläpitämisen sekä kyberturvallisuuskoulutuksen järjestämisen (NIS 2 -direktiivi 2022).

Laissa julkisen hallinnon tiedonhallinnasta (906/2019) 4 §:n 2 momentin kohdan 3 mukaan Kelan on perehdytyksen, koulutusten sekä viestinnän avulla varmistettava, että Kelan lukuun toimivilla henkilöillä on riittävä tuntemus voimassa olevista tietoturvaa koskevista säädöksistä, määräyksistä ja ohjeista. Henkilöillä tulee olla selvillä tiedon suojaamista sekä asiakirjojen turvallista käsittelyä koskevat periaatteet sekä toimenpiteet. Kelan on valvottava ohjeiden ja määräysten noudattamista.

Laissa sosiaali- ja terveyshuollon asiakastietojen käsittelyssä (703/2023) säädetään tietoturvasuunnitelman laatimisesta myös Kelaa koskien. Lain

mukaan Kelan on laadittava tietoturvaa, tietosuojaa sekä tietojärjestelmien käyttöä koskeva tietoturvasuunnitelma. Terveyden ja hyvinvoinnin laitos on antanut lakiin sosiaali- ja terveyshuollon asiakastietojen käsittelystä (703/2023) perustuvan määräyksen, joka kuvaa ja määrittää tietoturvasuunnitelman tarkoitusta sekä sisältöä tarkemmin:

> Tietoturvasuunnitelma on käytännön työväline, jolla hahmotetaan tietoturvallisuuden kokonaiskuvaa ja toteutetaan asiakastietojen käsittely hyvien käytäntöjen mukaisesti. Tietoturvasuunnitelmassa kuvatut selvitykset ja käytännöt voidaan yhdistää muihin tietoturvallisuuden omavalvonnan kohteen tietosuojaa ja tietoturvallisuutta ohjaaviin menettelyohjeisiin, laatukäsikirjoihin tai tietoturvapolitiikkoihin. (Terveyden ja hyvinvoinnin laitos 2024, s. 8)

Omavalvonnan kohteilla tarkoitetaan niitä toimijoita, joita määräys koskee. Tutkielman kontekstissa omavalvonnan kohteella tarkoitetaan Kelaa. Terveyden ja hyvinvoinnin laitos (2024, s. 7) suosittelee määräyksessä käyttämään ISO/IEC 27000 -sarjan standardeja tietoturvasuunnitelman laatimisessa. Suositus koskee etenkin isoja organisaatioita, jollaisena Kelakin voidaan käsittää. Kela on velvollinen toimimaan laatimansa suunnitelman mukaisesti ja säännöllisesti ylläpitämään ja katselmoimaan suunnitelmaa sekä seuraamaan aktiivisesti sen toteutumista. (Terveyden ja hyvinvoinnin laitos 2024, s. 3)

Tietoisuuden kehittämisen näkökulmasta suunnitelman sisällöstä on löydyttävä tieto muun muassa keskeisistä tietoturvallisuusohjeista sisältäen etä- ja hybridityön ohjeistukset, tietoturvapoikkeamista raportoinnin ohjeet sekä häiriötilanteista toipumisen ohjeet. Ohjeiden tulee ohjata tietoa käsitteleviä henkilöitä tiedon asiakastiedon turvalliseen käsittelyyn sekä tietoturvallisiin työtapoihin. Niiden katselmoinnista sekä päivittämisestä on huolehdittava asianmukaisesti. (Terveyden ja hyvinvoinnin laitos 2024, s. 9–12) Ohjeiden kuvaamisesta tietoturvasuunnitelmassa on määrätty tarkemmin seuraavalla tavalla:

> Tietoturvasuunnitelmassa on kuvattava, miten varmistetaan, että tietojärjestelmien käyttäjien saatavilla on tarpeelliset ja ajantasaiset organisaation toimintaohjeet (toimintamallit) ja tietojärjestelmien käyttöohjeet. Nämä ohjeet tulee olla vähintään sillä kielellä, jonka osaaminen on vähimmäisvaatimus kyseisessä työtehtävässä toimimiselle. Ohjeiden tulee olla helposti henkilökunnan saatavilla ja niiden sijainti on oltava kaikkien tiedossa. (Terveyden ja hyvinvoinnin laiton 2024, s. 12)

Terveyden ja hyvinvoinnin laitos (2024, s. 11) on myös ottanut määräyksessään kantaa henkilöstön kouluttamiseen, osaamisen kehittämiseen sekä ylläpitoon. Tietoturvasuunnitelmalla varmistetaan, että henkilöstö hallitsee tietojärjestelmien turvallisen käytön, ottaa huomioon tiedon luokitukseen liittyvät vaatimukset sekä ymmärtää tietoturvaa koskevat seuraamuskäytännöt.

Kelalta edellytetään koulutussuunnitelman tai vastaavan dokumentin ylläpitämistä, jossa kuvataan henkilökunnan tietoturvaperehdyttämisen, -kouluttamisen ja -osaamisen kehittämisen toimintamalli. Toimintamalli kattaa erilaiset rooleissa vaadittavan koulutuksen sisällön sekä toteuttamistavat. Osaaminen tulisi todentaa merkinnällä koulutuksiin osallistumisesta tai muin mahdollisin

keinoin. (Terveyden ja hyvinvoinnin laitos 2024, s. 12) Koulutusten toteuttamisesta sekä kuvaamista osana tietoturvasuunnitelmaa on määräyksessä kuvattu seuraavalla tavalla:

> Tietoturvasuunnitelmassa on kuvattava, kuinka koulutukset on järjestetty tietojärjestelmiä käyttäville henkilöille eli kuinka käytännössä varmistetaan järjestelmien käytön vaatima koulutus ja osaaminen. Tietojärjestelmiä käyttävillä henkilöillä on oltava koulutusta sekä asiakastietojen käsittelyyn että tietosuoja- ja tietoturva-asioihin. (Terveyden ja hyvinvoinnin laitos 2024, s. 11)

Suunnitelmassa kuvatun koulutuksen on oltava säännöllistä. Koulutuksen olisi myös oltava niin laadullisesti kuin määrällisesti riittävää ja tarkoituksenmukaista koulutettavan henkilön työtehtäviin sisältyvän tietojenkäsittelyn näkökulmasta. (Terveyden ja hyvinvoinnin laitos 2024, s. 11)

5.5 Sisäiset ja sidosryhmien vaatimukset

Tietoturvayksikölle Kelan sisäisen tietoturvatietoisuusohjelmaa koskevan dokumentoidun vaatimuskehikon muodostavat Kelan strategia, strategiset linjaukset, politiikat, periaatteet ja työjärjestys. Näiden ohella tärkeässä asemassa ovat henkilöstöltä, johdolta sekä sidosryhmiltä tulevat odotukset tietoisuuden kehittämistä kohtaan. Tässä luvussa käsitellään vaatimuksia, jotka on johdettu sisäisen dokumentaation sekä haastatteluiden perusteella.

Vaatimuksia käsitellään luvussa 5.1 esitettyjen tietoisuuden kehittämisen tärkeiden vaiheiden ja osatekijöiden kautta. Osatekijöistä ensimmäisenä oleva johdon tuki koetaan asiantuntijahaastattelun perusteella perusedellytyksenä tietoturvatietoisuusohjelman toteuttamiselle:

> Johdon tuki on oltava, jotta millään organisaation laajuisella ohjelmalla on edellytykset onnistua. (Allonen ym. 2024)

Haastatteluiden perusteella ylimmän johdon tuen merkitys ymmärretään tietoturvayksikössä sekä sen sidosryhmissä laajasti. Ylemmältä johdolta odotetaan näkyvyyttä tietoturva-asioissa sekä viestiä siitä, että he arvostavat tietoturvayksikön työpanosta. Tältä osin johdon tuki on koettu tietoturvajohdon näkökulmasta riittäväksi. (Arkko 2024; Haastateltava 1 ym. 2024) Riittäväksi johdon tuki on koettu myös asiantuntijatasolta. Tietoturvayksikön asiantuntijat odottavat, että tietoisuuden kehittämiselle annetaan selkeät tavoitteet, resursseja sekä työaikaa. Tavoitteet tulisi tarkistaa riittävin väliajoin. Asiantuntijat eivät kaipaa kädestä pitäen ohjausta, vaan jonkinlaisia suuntaviivoja, jotka perustuvat tunnistettuihin tulevaisuuden kannalta relevantteihin osaamistarpeisiin. Osaamisalueet olisi täten hyvä tunnistaa sekä priorisoida, jotta osaamistarpeiden kytkeminen liiketoimintahyötyihin toteutuu. (Knuutila & Lehikoinen 2024)

Tiimipäälliköiden näkemyksen mukaan heillä on keskeinen asema tietoisuuden kehittämiseen liittyvien tehtävien asiantuntijatasolla toteutumisen varmistamisessa (Haastateltava 1 ym. 2024). Täten johdon tuen tulisi kanavoitua arkeen esihenkilöiden kautta aina toimihenkilöille asti. Erityisesti tietoturvatietoisuuden kehittämiseen ja sen suunnitteluun osallistuvien sidosryhmien keskuudessa koetaan tärkeäksi, että johto osoittaa aktiivisuuttaan ja on oma-aloitteisesti esillä. Ylimmän johdon lisäksi myös keskijohdon viestinnällinen näkyvyys on tärkeässä asemassa, jotta aiemmin mainittu kanavoituminen aina toimihenkilölle asti toteutuu. Tietoturvayksikön johdolta sidosryhmät odottavat avointa sekä aktiivista viestintää ja tiedonjakamista sidosryhmilleen ainakin niissä foorumeissa, joissa sidosryhmien edustajat ovat läsnä. (Koskinen ym. 2024)

Kelan strategiassa (2023c, s. 6) eräänä turvallisuuteen liittyvänä tavoitteena on kuvattu, että Kelan palvelut toimivat turvallisesti. Kelan strategiasta johdetuissa turvallisuuden strategisissa linjauksissa (Kela 2021, s. 5) linjataan, että turvallisuusviestinnän kehittäminen on osa Kelan turvallisuuskulttuurin rakentamista. Turvallisuus nähdään linjauksissa myös keskeisenä osana jokaisen kelalaisen osaamista ja arkea. Linjausten toimeenpanemisen keinona mainitaan osaamisen kehittäminen:

> Kasvatamme ja ylläpidämme kelalaisten turvallisuustaitoja säännöllisellä osaamisen kehittämisellä ja viestinnällä. (Kela 2021, s. 5)

Kuten edellä mainittu, tietoturvatietoisuusohjelmalle kohdistetaan vaatimuksia jo strategisista tavoitteista sekä linjauksista alkaen. Myös asiantuntijatasolla linkitys strategiaan on havaittu ja nähdään keskeisenä edellytyksenä tietoisuusohjelman toteuttamiselle. Strategia pitäisi tuoda henkilöstön näkökulmasta lähelle arkea ja osaksi päivittäistä tekemistä. Johdon suunnalta kaivataan viestintää siitä, kuinka tietoturvatekeminen liittyy Kelan strategiaan ja miten tietoturva on huomioitu strategisissa tavoitteissa. (Allonen ym. 2024)

Tietoisuuden kehittämiseen tarvittavien asiantuntijaresurssien mahdollistamiseksi on haastatteluiden perusteella loogisinta muodostaa virtuaalitiimi. Virtuaalitiimiin olisi mahdollista koota osaamista ylitse yksikkörajojen. Virtuaalitiimiin kutsuttavilla asiantuntijoilla tulisi kuitenkin olla riittävä motivaatio tietoturvatietoisuuden kasvattamiseen ja valmiiksi paloa näiden asioiden kehittämiseen. (Arkko 2024)

Motivaation lisäksi on kiinnitettävä huomiota tarvittavan osaamiseen:

> Viestinnällinen osaaminen on kriittisessä asemassa, sillä tietoturvaviestintä vaatii enemmän harkintaa kuin muu viestintä. (Haastateltava 1 ym. 2024)

Tietoturvaviestinnän asiantuntijaosaaminen koetaan tietoisuuden kehittämisen kannalta tärkeimpänä. Tämän lisäksi tietoisuuden kehittämistiimissä tulisi olla myös liiketoimintaymmärrystä, joka auttaisi tulkitsemaan tietoturvayksikön asiakkaiden odotuksia. Myös riskienhallintaosaaminen koetaan kriittisenä, jotta riskinotto henkilötasolla ei perustuisi puutteellisiin subjektiivisiin riskikäsityksiin. Tietoturvayksikön sisällä odotetaan, että eri vastuualueiden syväosaajat

tunnistetaan ja syväosaajat tukevat muita asiantuntijoita omilla vahvuuksillaan. Myös sidosryhmien puolelta on odotuksia selkeälle vastuunjaolle, jotta tietoturvatyössä olisi selkeää, keneltä saa tarvittaessa lisätietoja aiheesta, josta lisätietoa tarvitsee. (Allonen ym. 2024; Koskinen ym. 2024)

Asiantuntijat odottavat, että myös tietoturvaosaamisen kehittämiseen on nimettynä vastuutaho, jolla on kyky kansantajuistaa tietoturva-aiheita, tunnistaa osaamistarpeita sekä jatkojalostaa asiantuntijoiden ammattitaitoa tietoturvatietoisuuden kehittämisessä hyödynnettävään muotoon. Lisäksi asiantuntijoiden mielestä on tärkeää välttää myös tilannetta, jossa yksi vastuualue on täysin yhden henkilön varassa. (Allonen ym. 2024; Knuutila & Lehikoinen 2024) Sidosryhmien puolelta odotuksena on edellä mainittujen lisäksi, että tietoisuuden kehittämisessä olisi mukana myös sekä psykologista että kielenhuollon osaamista. Myös haastatellut sidosryhmät korostivat liiketoimintaosaamisen sekä viestintäosaamisen mukanaolon merkitystä. (Koskinen ym. 2024)

Haastatteluissa asiantuntijoiden kanssa nousi toistuvasti esille se, että tietoisuuden kehittämiseen tulisi budjetoida jokaisen työaikaa. (Knuutila & Lehikoinen 2024; Allonen ym. 2024) Myös tietoturvapäällikön näkemys ajankäytön mahdollistamisesta oli linjassa asiantuntijoiden näkemysten kanssa:

> On saatava henkilöstölle fokusta eli käytännössä aikaa suorittaa tietoisuutta kehittäviä toiminteita työn lomassa. Toiminteet on myös mukautettava käytettävissä olevaan aikaan. (Arkko 2024)

Tavoitteet ajankäytölle tulisi myös asiantuntijoiden mielestä olla selkeät ja johdettu strategisista tavoitteista. Sidosryhmien edustajien mukaan tietoturvayksikössä olisi tunnistettava ne keskeiset tavoitteet, joiden saavuttamista tietoisuuden kehittämisellä voidaan tukea. (Allonen ym. 2024; Koskinen ym. 2024)

Keskeisenä tavoitteena nähdään, että tietoturvariskien käsittelyyn riittävät tiedot, taidot sekä ymmärrys saavutettaisiin. Esimerkiksi uudet ilmiöt, kuten tekoäly, nosti haastatteluissa päätään yhtenä esimerkkinä osaamisesta, johon tulisi kiinnittää huomiota. Perimmäisenä ajatuksena taustalla on, että kussakin tietoturvaroolissa toimiva henkilö toimii oikein. Myös henkilöstön hyvä käsitys siitä, mitä tietoturvayksikössä tehdään, on tavoittelemisen arvioista niin yksikön sidosryhmien kuin asiantuntijoiden mielestä. (Allonen ym. 2024; Koskinen ym. 2024)

Tietoisuusohjelman keskeisenä teemana käsiteltiin suunnittelun perustumista nykytilan kartoittamiseen. Haastatteluiden perusteella nykytilan selvittäminen nähdään tarpeellisena, jotta kehittämistoimenpiteitä osataan kohdistaa oikein (Arkko 2024). Sekä sidosryhmien että asiantuntijoiden mielestä tietoisuusohjelman nykytilaa voidaan arvioida riskien kautta. Suunnittelu tulisi kytkeä riskien arviointiin, sillä monissa tapauksissa riskien käsittely edellyttää tietoisuuden kehittämistä. Riskien arviointiin kytkettynä nykytilan analyysi helpottaa kehittämistoimenpiteiden priorisointia. Riskien arviointiin perustuva suunnittelu vaatii erilaisia näkökulmia ja eri roolien mukaan ottamista. (Koskinen ym. 2024; Allonen ym. 2024)

Hankittu tietoturvaosaaminen riippuu pitkälti siitä, mitä osaamistarpeita Kelassa on havaittu ja mitä osaamista on ollut rekrytointien kautta saatavilla. Rekrytoinnit ovat nopea tapa saada osaamista organisaatioon. Niissä keskitytään osaamisen näkökulmasta lähitulevaisuuden osaamistarpeisiin ja organisaation strategiseen suuntaan. (Arkko 2024) Asiantuntijoiden mielestä rekrytoinneissa on korostettu myös valmiuksia ammatilliseen kehittymiseen (Allonen ym. 2024).

Tietoturvaosaamista koskevan viitekehysten hyödyntämisen tarve tunnistetaan erityisesti teknisen tilannekuvakeskuksen puolella sekä sidosryhmien toimesta. Myös tietoturvaryhmän asiantuntijoiden keskuudessa jonkin yleisesti tunnustetun viitekehyksen käyttäminen ainakin Kelaan soveltuvin osin nähdään hyödyllisenä. Ensisijaisesti keskeinen osaaminen tulisi kuitenkin olla johdettu suoraan Kelan strategisista tavoitteista. (Allonen ym. 2024; Koskinen ym. 2024)

Sidosryhmien haastattelun perusteella pätevyysprofiilit, joiden kautta osaamisen hallinta on sisäänrakennettu Kelan HR-järjestelmiin ei välttämättä palvele tietoturvatietoisuusohjelman tarkoitusta. Sidosryhmien edustajat odottavat suunnittelulta, että osaamisen tavoitetaso määritellään ja osaamisen kehittämiselle luodaan edellytyksiä työsuhteen aikana:

> Olisi suunniteltava, miten määritellään yksilön tai kohderyhmän osaamisen tavoitetaso ja miten työsuhteen aikana luodaan edellytyksiä osaamisen kehittämiseen ja siten tietoturvatietoisuuden lisääntymiseen koko organisaatiossa. (Koskinen ym. 2024)

Tiimipäälliköt tunnistavat osaamistarpeita parhaiten kahdenvälisissä keskusteluissa asiantuntijoiden kanssa. Osaamistarpeet saattavat olla todella syvällisiä ja rajattuja esimerkiksi liittyen johonkin tiettyyn teknologiaan. (Haastateltava 1 ym. 2024) Tietoisuuden tasosta kertoo myös se, kuinka paljon tietoturvapäällikölle osoitetaan kysymyksiä tietoturvaa koskevista päätöksistä ja linjauksista. Asiantuntijoiden osaamistarpeita nousee arjessa säännöllisesti esille, ja tarpeet voivat liittyä esimerkiksi työssä tarvittaviin ohjelmistoihin ja työkaluihin. (Arkko 2024)

Tietoturvaryhmässä asiantuntijaosaamista on tunnistettu tiimitasolla työpajassa. Työpajan toteuttaminen voisi olla hyödyllistä myös teknisessä tilannekuvakeskuksessa. On tärkeää, että työpajassa tunnistettujen osaamistarpeiden saavuttamiseksi tehdään myös toimenpiteitä. Asiantuntijat odottavat, että johto ja esihenkilöt priorisoisivat tähän liittyvän sisäisen kehittämistyön riittävän korkealle. Asioiden nostaminen esille satunnaisesti ei riitä, vaan tietoisuuden kehittämisen tulisi olla kiinteä osa jokaista työviikkoa. Asiantuntijat odottavat systemaattista lähestymistapaa osaamisen kehittämiseen, jossa tieto tehdyistä toimenpiteistä kirjataan ylös ja osaamisen kehittymistä seurataan. (Allonen ym. 2024; Knuutila & Lehikoinen 2024)

Tutkimustiedon (luku 5.1) mukaan politiikat ja periaatteet muodostavat osan tietoisuusohjelman sisällöstä. Haastatteluiden perusteella politiikalta ja periaatteilta odotetaan asiantuntijoiden keskuudessa sitä, että niissä Kelan toiminnan tavoitteet kytketään tietoturvatavoitteisiin. Politiikalla ja periaatteilla on oltava niiden edellyttämä painoarvo, jolloin niitä myös noudatetaan läpi

organisaation. Sidosryhmien mukaan politiikka ja periaatteet luovat kehyksen tietoturvalle ja varmistavat tarvittavat edellytykset, kuten resurssit. Ne myös tuovat yhteisiä tavoitteita ja yhtenäisyyttä organisaatiotasolla. (Allonen ym. 2024; Knuutila & Lehikoinen 2024; Koskinen ym. 2024)

Kelassa on yksi tietoturva- ja tietosuojapolitiikka sekä useita tätä tarkentavia periaatteita määriteltynä sekä dokumentoituna osaksi hallintajärjestelmää. Tietoturvan periaatteiden kokoaminen hallintajärjestelmän alle koetaan sekä tietoturvayksikössä että sen sidosryhmien keskuudessa järkevimpänä toimintatapana. Parhaimmillaan hallintajärjestelmä tuo näkyviin eri organisaation osien väliset yhteydet tietoturvatyössä. (Arkko 2024; Koskinen ym. 2024) Kelan tietoturva- ja tietosuojapolitiikassa (Kela 2023d, s. 4) tietoisuutta koskevaksi tavoitteeksi on kirjattu:

> 7. Edistämme hyvää turvallisuuskulttuuria varmistamalla henkilöstön riittävän tietoisuuden ja osaamisen. Tiedotamme ja muistutamme henkilöstöllemme, että vastuu tietoturvasta ja tietosuojasta huolehtimisesta kuuluu jokaiselle.

Välillisesti tietoisuuden kehittämistä koskee myös seuraava politiikkaan (Kela 2023d, s. 4) kirjattu tavoite:

> 8. Hallitsemme ja jatkuvasti parannamme tietoturvaa ja tietosuojaa noudattaen ISO/IEC 27701 -standardia, joka sisältää ISO/IEC 27001 -standardin tietoturvavaatimukset ja lisävaatimukset tietosuojalle.

Kirjatun tavoitteen vuoksi luvussa 5.2 käsitellyt vaatimukset voidaan ymmärtää myös Kelan sisäisiksi vaatimuksiksi tietoturvatietoisuusohjelmaa kohtaan. Tavoitteiden lisäksi politiikkaan (Kela 2023d, s. 5–6) on kirjattuna periaatteita sekä yleiset tietoturvan toteuttamisen vastuut. Periaatteista tietoturvatietoisuuteen liittyy olennaisesti periaate:

> Turvallisuustietoisuutta kehitetään jatkuvasti Kelassa. Työyhteisöviestintä, sekä henkilöstön ohjeistaminen ja kouluttaminen ovat osa jokapäiväistä toimintaa.

Periaatteen mukaan tietoturvatietoisuuden kehittämisen on oltava jatkuvaa toimintaa. Työyhteisöviestinnän, ohjeiden ja kouluttamisen tulisi näkyä kelalaisten arjessa. Vastuissa tietoturvatietoisuuden osalta korostetaan esihenkilön roolia. Esihenkilön vastuulla varmistaa, että tietoturvaosaaminen on riittävää, vaikka toimihenkilöllä onkin ensisijainen vastuu työtehtäviinsä liittyvän tietoturvaosaamisen kehittämisestä. (Kela 2023d, s. 6)

Politiikassa mainittujen vastuiden lisäksi eri rooleja koskevia vastuita tuodaan ilmi periaatteiden kautta. Vastuiden vieminen käytäntöön vaatii tietoturvapäällikön sekä tiimipäälliköiden mukaan toistoja ja käytännön tekemistä, jossa tietoturvan hallintajärjestelmän periaatteita pääsee hyödyntämään (Arkko 2024; Haastateltava 1 ym. 2024).

Asiantuntijoiden mukaan periaatteet voi esimerkiksi pilkkoa roolikohtaisiksi koulutuksiksi, joiden avulla eri tietoturvarooleissa toimivien henkilöiden tietoisuutta roolikohtaisista vastuista ja velvollisuuksista voisi kehittää (Allonen

ym. 2024). Lisäksi asiantuntijat pitävät tärkeänä periaatteita koskevaa dokumenttienhallintaa, joka ei voi olla puutteellista (Knuutila & Lehikoinen 2024).

Tietoturvan asiantuntijatyö sisältää paljon periaatteiden sekä muun dokumentoidun tiedon omaksumista. Tietoisuuden kehittämisessä olennainen käytännönläheinen oppiminen toteutuu pitkälti työtehtäviin liittyvänä tiedonhankintana. Käytännönläheistä oppimista voidaan lisätä myös erillisen harjoittelun kautta. Haastatteluiden perusteella harjoituksiin osallistuminen on tietoturvan asiantuntijatehtävissä välttämätöntä. Harjoittelu koetaan keskeisenä osana sidosryhmäyhteistyötä sekä yksikön että sen sidosryhmien toimesta. Lisäksi harjoituksia tulisi toteuttaa niin sanottuina pöytälaatikkoharjoituksina yksikön tai eri tiimien sisäisinä harjoituksina. Myös teknisiä harjoitteluympäristöjä tulisi olla asiantuntijoiden saatavilla. (Knuutila & Lehikoinen 2024; Arkko 2024; Koskinen ym. 2024)

Monien harjoitustenkin taustalla vaikuttavat uhkaskenaariot voisivat toimia tietoisuuden ajureina, ja niitä tulisi hyödyntää myös hallinnollisen tietoturvan puolella (Arkko 2024; Allonen ym. 2024). Skenaariotyö pitäisi asiantuntijoiden mukaan joukkoistaa sen sijaan, että siihen liittyvä tiedonhankinta olisi yksittäisen asiantuntijan vastuulla:

> Uhkaskenaarioiden prioriteettijärjestys voisi tuoda asiantuntijatyöhön systemaattisuutta. Yhteisesti ylläpidettävä uhkaskenaariolistaus vähentää yksittäisen asiantuntijan tiedonhankintataakkaa. (Allonen ym. 2024)

Haastatteluiden perusteella palkitsemiskäytänteet koetaan päivittäisen työn kannalta seuraamuskäytäntöjä merkityksellisempinä. Kerran vuodessa palkitseminen ei olisi riittävää, vaan palkitsemista pitäisi tapahtua säännöllisemmin, esimerkiksi kuukausittain. Jo pelkästään palkitsemiseen liittyvällä säännöllisellä viestinnällä olisi asiantuntijoiden mielestä positiivinen vaikutus turvallisuuskulttuuriin. Palkitsemiskäytäntöjen tulisi olla myös monipuolisia, sillä henkilöt motivoituvat eri asioista. (Allonen ym. 2024) Tiimipäälliköiden vastauksista nousi keskeinen havainto palkitsemiskäytäntöjen haasteesta:

> Palkitsemiskäytännöt ovat haastavia, sillä hyvin toteutettu tietoturva on melko näkymätön osa kokonaisuutta. (Haastateltava 1 ym. 2024)

Useiden haastateltavien mukaan palkitseminen on myös arjen työssä tapahtuvaa kiittämistä hyvin tehdystä työstä. Palkitseminen tulisi suunnitella niin, että se ohjaa kohti tavoitteita. Ilmapiiri olisi tavoitetilassa sellainen, että minkä tahansa tietoturvaan liittyvän asian esille nostaminen on kannustettavaa. Tahattomista virheistä ei koskaan pitäisi rangaista. Sekä yksikön sisäisessä että sidosryhmien kanssa tapahtuvassa viestinnässä pitää pyrkiä noudattamaan positiivista asiakaspalveluotetta. (Haastateltava 1 ym. 2024; Koskinen ym. 2024)

Viestinnän suunnittelussa yksi keskeisimmistä näkökulmista on se, että viestinnän tulisi saavuttaa kohderyhmänsä ilman erillistä tiedonhakemista (Koskinen ym. 2024). Kaikkien haastatteluiden perusteella viestintä teknisen

tilannekuvakeskuksen puolella kannattaa keskittää pikaviestintävälineisiin. Tietoturvaryhmän puolella tiedonjakoon sen sijaan toimivat parhaiten viikkopalaverit sekä sähköpostin jakelulista. Viestintä- ja työvälineinä toimiviin ohjelmistoihin liittyviä mahdollisuuksia kannattaa haastateltavien hyödyntää tulevaisuudessa yhä enemmän. (Haastateltava 1 ym. 2024; Arkko 2024; Knuutila & Lehikoinen 2024) Edellä mainittujen lisäksi tiedonjakamiseen tulisi käyttää tallennettavia infotilaisuuksia, joihin on mahdollista palata vielä tilaisuuden jälkeenkin. Erityisesti vuorovaikutukselliset tilaisuudet ovat asiantuntijanäkökulmasta tervetulleita. Vuorovaikutuksellisuus ja aiheeseen palaaminen pitäisi varmistaa myös niille, jotka katselevat tilaisuutta tallenteelta. (Allonen ym. 2024)

Vaihtelevat oppimistyylit tulisi ottaa tietoisuusohjelmassa huomioon. Oppimistyylit pitäisi kirjata ylös henkilökohtaisissa oppimissuunnitelmissa ja kehityskeskusteluissa (Arkko 2024; Knuutila & Lehikoinen 2024). Erilaisten oppimistyylien huomioimiseksi olisi tarjottava viestintää eri muodoissa. Esimerkiksi videomuotoinen materiaali voisi olla keskeinen osa viestintää. (Haastateltava 1 ym. 2024; Koskinen ym. 2024)

Haastatteluiden perusteella jatkuva oppiminen voidaan varmistaa sillä, että osaamisen kehittämistä tehdään riittävän usein. Esihenkilöiden olisi varmistettava osaamisen kehittämiselle aikaa jatkuvasti koko työsuhteen elinkaaren aikana. (Koskinen ym. 2024; Allonen ym. 2024) Tiimipäälliköiden mielestä avainasemassa on erilaisten persoonien ja kyvykkyyksien huomioiminen. Osalla asiantuntijoista ohjauksen ja tuen tarve ilmenee lyhyemmissä sykleissä kuin toisilla. (Haastateltava 1 ym. 2024)

Edellytyksenä jatkuvalle oppimiselle koetaan myös asiantuntijoiden oma motivaatio. Jokaisen tulee ymmärtää, että oman osaamisen jatkuva kehittäminen on työn tavoitteiden saavuttamisen kannalta tärkeää. Esihenkilöiden tulee huolehtia, että työn kuorma pysyy kohtuullisena ja mielekkäänä siten, että motivaatio osaamisen kehittämiseen säilyy. (Koskinen ym. 2024; Knuutila & Lehikoinen 2024; Haastateltava 1 ym. 2024)

Seuranta ja mittaaminen on haastateltavien mielestä keskeinen osa tietoisuusohjelman jatkuvaa parantamista, sillä toimenpiteiden vaikuttavuutta voidaan seurata mittaamalla (Koskinen ym. 2024). Mittarit on sidottava tietoisuusohjelman tavoitteisiin. Asiantuntijatyössä keskeisenä mittarina nähdään haastatteluiden perusteella koulutukset, asiantuntijaseminaarit ja infotilaisuudet:

> Mittarina tulisi käyttää koulutuksiin ja seminaareihin osallistumisia sekä konkreettisia hyötyjä, joita niihin osallistuminen on tuonut tietoturvayksikön toimintaan. Myös palautetta koulutus-, info- tai seminaaritilaisuuksista kannattaa käyttää mittarina. Palautetta voisi kerätä esimerkiksi lyhyen kyselyn muodossa. (Arkko 2024; Allonen ym. 2024;)

Yksittäisen koulutuksessa käyvän tai seminaariin osallistuvan asiantuntijan odotetaan jakavan tietoa tilaisuudesta organisaatiossa muille asiantuntijoille. Tämä toimintamalli auttaa tietoisuuden levittämisessä laajemmalle joukolle sekä parhaimmillaan syventää myös tiedon jakajan omaa oppimista. (Allonen ym. 2024)

Työpaja- tai infomuotoisina pidettävien tilaisuuksien osalta asiantuntijat painottavat selkeiden yhteisten sääntöjen merkitystä, jotta tieto tavoittaa kaikki osallistujat:

> Yhteisten tilaisuuksien aikana, joissa keskustellaan, suunnitellaan tai esitetään jotakin, ei saisi koskaan tehdä mitään päällekkäistä, joka häiritsee keskittymistä itse asiaan. (Allonen ym. 2024)

Jatkuvan parantamisen näkökulmasta keskeistä on huomioida muutokset strategisella tasolla ja niiden vaikutukset tietoisuusohjelmaan. Myös tietoisuusohjelman kehittäminen voidaan nähdä eräänlaisena muutoksena. Sidosryhmien edustajien haastattelussa nousi esille muutoksia koskeva keskeinen vaatimus:

> Kaikissa muutoksissa olisi huomioitava henkilöt, joiden elämään muutokset tulevat jollain tavalla vaikuttamaan. (Koskinen ym. 2024).

Asiantuntijoiden mielestä heitä voisi osallistaa tietoisuusohjelmaan liittyvien muutosten suunnittelussa esimerkiksi tätä koskevan kyselyn avulla (Allonen ym. 2024). Tietoturvapäällikön mukaan strategisten tavoitteiden muutokset huomioidaan osana normaalia kehittämistä ja tietoisuuteen liittyvät tavoitteet määritellään uudelleen strategisten muutosten yhteydessä. Tarvittavat resurssit tietoisuuden kehittämiseen myös muutoksissa tulisi varmistaa muutosjohtamisen avulla, joka ottaa huomioon erityisesti tulevaisuuden keskeiset osaamistarpeet. (Arkko 2024; Koskinen ym. 2024; Allonen ym. 2024)

6 JOHTOPÄÄTÖKSET

Tutkielman teoreettisen viitekehyksen pohjalta voidaan todeta, että tietoturvatietoisuuden kehittämistä on tutkittu runsaasti ja se tunnistetaan keskeisenä osana tietoturvallisuuden hallintaa organisaatioissa. Kansallinen osuus tehdystä tutkimuksesta on pientä, joten suurin osa tutkielman teoreettisen viitekehyksen tiedonhausta painottui näin ollen kansainvälisiin tutkimusartikkeleihin. Erityisesti englanninkielisessä lähdemateriaalissa termien kouluttaminen ja tietoisuus käyttö sekä merkitykset vaihtelevat jonkin verran. Valtaosassa lähteistä koulutus on katsottu olevan yksi tietoisuuden kasvattamisen keinoista. Myös tämä kyseinen tapa termien määrittelyssä ja niiden välisen suhteen kuvaamisessa on vakiintunut Kelan organisaatiokulttuurissa.

Tietoturvallisuus ja siihen liittyvän tietoisuuden kehittämiseen tunnistettiin runsaasti vaatimuksia dokumenttianalyysillä tutkimusteoriasta, Kelaa velvoittavasta lainsäädännöstä ja määräyksistä, viitekehyksistä, organisaation strategisen tason dokumentaation pohjalta sekä tietoturvayksikön henkilöstön ja sidosryhmien haastatteluista. Velvoittavan lainsäädännön ja määräysten osalta vaatimukset kuvataan hyvin ylätasolla. Kela pyrkii noudattamaan kansainvälistä ISO/IEC 27001 -standardia, joka varmistaa käytännössä näiden vaatimusten toteutumisen. Myös sisäisen ohjaavan dokumentaation ja sisäisten vaatimusten osalta voidaan todeta Kelan huomioivan toiminnassaan lainsäädännöstä sekä määräyksistä tulevat vaatimukset tietoturvatietoisuuden kehittämisestä. Tietoturvatietoisuusohjelmaa suunniteltaessa ja toteutettaessa näihin vaatimuksiin on kuitenkin syytä kiinnittää erityistä huomiota.

Haastatteluihin saatiin suhteellisen vähän suostumuksia haastatteluun osallistumiseksi, vaikka haastateltavien määrä oli riittävä tiedon saturaatiopisteen saavuttamisen kannalta. Haastattelutuloksista on johdettavissa monia yhtymäkohtia aiempaan tutkimukseen. Johdon tuen sekä johdon aktiivisen, avoimen ja näkyvän viestinnän voidaan todeta olevan yksi perustavanlaatuinen vaatimus tietoisuusohjelman toteuttamiselle. Tulosten perusteella johdon merkitys on yhtä kriittinen organisaatiotasosta riippumatta: Vaikka ylin johto viestisi aktiivisesti, ei viesti välity henkilöstölle ilman keski- ja lähijohdon aktiivista osallistumista.

Tutkimustuloksista koottuun taulukkoon (Liite 3) nousi useita vaatimuksia johdon toteuttamaan viestintään sekä esimerkillä johtamiseen liittyen.

Haastattelutulosten sekä teoreettisen viitekehyksen perusteella tietoisuusohjelmalle keskeistä on sen kytkeminen strategisiin tavoitteisiin. Tulokset tukevat havaintoja aiemmasta tutkimuksesta myös siinä, että riskienhallintaan pohjautuva suunnittelu varmistaa tietoisuusohjelman tavoitteiden priorisoinnin riittävälle tasolle sekä tietoisuuden kehittämistoimenpiteiden kohdentamisen kriittisiin kohteisiin. Tietoturvaosaamisen lisäksi tuloksissa korostuu liiketoimintaosaamisen merkitys tietoisuusohjelman resursoinnissa, suunnittelussa ja toteuttamisessa. Tämä on merkittävä havainto, joka poikkeaa aiemmasta tutkimuksesta. Tuloksissa esille nousi myös psykologisen osaamisen, joka sen sijaan tukee havaintoja aiemmasta tutkimustiedosta. Sekä liiketoiminta- sekä psykologinen osaaminen on nostettu taulukoinnissa (Liite 3) tietoisuusohjelman resursointia koskeviksi osaamisvaatimuksiksi.

Asiantuntija- tai muiden resurssien käytettävyys vaikuttaa siihen, miten paljon tietoisuusohjelmassa voi olla toimintoja, jotka vaativat asiantuntijoiden osallistumista tai manuaalista työtä. Mikäli resursseja ei ole paljon käytettävissä, on organisaation tukeuduttava työnsä lomassa itseopiskelumateriaaleihin. Ajankäytön mahdollistaminen oli yksi haastatteluissa eniten esille nousseista vaatimuksista. Tässä asiassa esihenkilön rooli on tunnistettu keskeiseksi. Esihenkilöille on yksilöity tietoisuuden kehittämiseen liittyviä vastuita jo politiikan tasolla. Myös tietoturvayksikössä ymmärretään, että lähiesihenkilö voi viimekädessä mahdollistaa asiantuntijan ajankäytön tietoisuusohjelmalle. Vaikka asiantuntijan henkilökohtaista vastuuta ja itseohjautuvuutta osaamisensa kehittämisessä ei voi vähätellä, korostuu esihenkilön mahdollistava sekä huolehtiva rooli tulosten taulukoinnissa (Liite 3).

Aiempi tutkimus sekä tulokset puoltavat yksimielisesti osaamisviitekehyksen hyödyntämistä. Viitekehysten käyttäminen on täten nostettu myös tulosten taulukoinnissa (Liite 3) omaksi vaatimuksekseen. Tutkielmassa kahdesta esitellystä viitekehyksestä loogisempi valinta Kelalle on ENISA:n EU-lainsäädännön huomioiva ECSF-viitekehys. Myös NIST:in NICE-viitekehystä voi suositella hyödynnettävän Kelalle soveltuvin osin. Vaikka viitekehyksistä ei ole johdettavissa suoria vaatimuksia Kelalle, niiden avulla voidaan saavuttaa haastatteluissa peräänkuulutettua systemaattisuutta asiantuntijaroolien sekä rooleissa vaadittavan osaamisen määrittelyyn.

Haastattelutulokset ovat yhdenmukaisia aiemman tutkimuksen kanssa siinä, että tietoisuusohjelmassa politiikoilla ja periaatteilla on oltava painoarvoa ja niitä on noudatettava läpi organisaation. Teoreettisen viitekehyksen perusteella politiikka ilmentää johdon tukea tietoturvallisuudelle ja periaatteiden on oltava samaistuttavia. Niiden toimeenpaneminen riippuu usein vallitsevasta turvallisuuskulttuurista ja siitä, kuinka vakavasti sekä myönteisesti organisaatiossa suhtaudutaan turvallisuusasioihin. Tärkeä tulosten taulukointiin (Liite 3) nostettu vaatimus politiikkoihin ja periaatteisiin liittyen on, että niissä kytketään Kelan strategiset tavoitteet tietoturvan tavoitteisiin ja kuvataan strategian toteuttamista arjessa.

Tutkielman perusteella henkilöstömäärällä on suuri vaikutus tietoisuuden kehittämistoimintojen valintaan. Rajaus tietoturvayksikköön mahdollistaa yksilöllisiin tarpeisiin vastaamien niin oppimistyylien kuin tarvittavan osaamisen osalta. Aiemman tutkimustiedon perusteella henkilöstön monimuotoiset tarpeet huomioidakseen tietoisuusohjelman sisällön on oltava monipuolista sekä vaihtelevaa. Myös tulosten perusteella tietoisuusohjelman toteuttamiselta odotetaan vaihtelua, jotta esimerkiksi asiantuntijoiden henkilökohtaiset oppimistyylit tulevat huomioiduksi.

Erityisesti tarve videomuodossa olevalle viestinnälle nousi haastatteluissa useasti esille. Tästä syystä esimerkiksi infotilaisuuksia koskevat vaatimukset näkyvät omana osionaan tutkimustulosten pohjalta kootussa taulukossa (Liite 3). Haastattelut puolsivat sitä aiemman tutkimustiedon pohjalta noussutta näkökulmaa, että hyvin suunniteltu visuaalisia ulottuvuuksia sisältävä viestintä on aina yksinkertaista kirjallista viestintää tehokkaampaa. Yhtymäkohta teoriaan löytyi myös siitä, että viestivä taho vastaa aina viestinnän tehokkuudesta eli siitä, kuinka hyvin viestintä saavuttaa kohderyhmänsä.

Palkisemisen merkitystä turvallisuuskulttuurin kehittämisessä ei voi aliarvioida, koska juuri sillä voidaan muuttaa turvallisuuteen suhtautuvaa ilmapiiriä positiivisempaan suuntaan. Palkitsemisen merkitys korostuu myös tulosten taulukoinnissa (Liite 3), jossa palkitsemista kohtaan on nostettu useita vaatimuksia. Palkitsemiskäytänteiden ei haastattelutulosten perusteella tarvitse olla raskaita. Aineellisen palkitsemisen sijaan sanallinen palkitseminen työarjessa voi riittää. Tärkeää on, että palkitsemiskäytänteistä viestitään avoimesti organisaatiossa.

Tietoisuusohjelman sisällöltä edellytetään haastatteluiden sekä teoreettisen viitekehyksen mukaan perusteluita, jotta henkilöstö ymmärtää asian tärkeyden. Sisällön suunnittelussa olisi myös kuultava henkilöstöä. Haastatteluiden perusteella esimerkiksi tietoturvayksikön asiantuntijat kokevat heille suunnatut kyselyt soveltuvimpana keinona vaikuttaa tietoisuusohjelmaan.

Henkilöstön on aiempaan tutkimukseen viitaten todettu oppivan tehokkaasti tietoturvatapahtumista, olivatpa ne sitten toteutuneita tai harjoiteltuja skenaarioita. Tämä korostaa uhkaskenaarioiden käyttämisen merkitystä osana tietoisuusohjelmaa. Uhkaskenaariot ja niihin perustuvien harjoitusten järjestäminen on tulosten perusteella erittäin olennainen osa osaamisen kehittämistä, sillä tietoturvaan liittyvissä asiantuntijarooleissa juuri harjoitusten ideologia sekä työssä oppiminen ovat keskiössä. Tulosten taulukoinnissa (Liite 3) uhkaskenaarioita koskevat vaatimukset liittyvät oleellisesti harjoittelua koskeviin vaatimuksiin, sillä harjoittelun on perustuttava laadittuihin uhkaskenaarioihin.

Haastatteluissa myös koulutuksiin ja seminaareihin osallistuminen nousivat esille tietoisuusohjelman toteuttamisen keinoina. Koulutuksiin osallistuminen koettiin myös hyväksi mittariksi tietoisuusohjelman seurannalle. Teoreettisen viitekehyksen perusteella seurantaan tulisi käyttää myös kyselyitä, sillä niiden avulla on mahdollista mitata monipuolisesti käyttäytymistä, asennetta sekä osaamista. Mittareiden olemassaoloon nojaava seuranta on edellytys tietoisuusohjelman jatkuvalle parantamiselle, jossa ennen kaikkea on huomioitava kohderyhmien jatkuva osallistuminen suunnitteluun ja sen mahdollistaminen.

7 YHTEENVETO

Tulosten ja johtopäätösten perusteella voidaan todeta, että tietoturvatietoisuusohjelmaa Kelan tietoturvayksikössä koskien saatiin tutkielman avulla muodostettua varsin kattava, eri tahoja ja näkökulmia huomioiva tutkimusteoreettisesti uskottava vaatimuskehikko. Näin ollen tutkielma vastasi myös tutkimuskysymykseen:

> Mitä hyvien käytänteiden mukaisia, laissa säädettyjä sekä sidosryhmiltä tulevia vaatimuksia Kelan tietoturvayksikön tietoisuusohjelmaan kohdistuu yksikön toimintaympäristö, tehtävät ja vastuut huomioiden?

Tapaustutkimukselle tyypillisesti tutkielman rajaus oli hyvin suppea ja keskittyy Kelan tietoturvayksikköön huomioiden sen toimintaympäristön sekä ominaispiirteet. Tästä syystä tulokset eivät ole tutkimusteoriaan sekä viitekehyksiin liittyvää tietoa lukuun ottamatta suoraan sovellettavissa muihin organisaatioihin. Tapaustutkimuksen voidaan todeta olleen toimiva valinta tutkimusstrategiaksi tutkimustehtävän näkökulmasta, sillä tavoitteena ei ollut tulosten yleistettävyys, vaan hyödyllisyys toimeksiantajan sisäisen kehittämisen kannalta.

Kelan organisaatiossa tapahtuvat muutokset, Kelaa koskevan lainsäädännön sekä määräysten kehittyminen ja viitekehysten päivittyminen vaikuttavat väistämättä ajan saatossa tutkimustuloksiin ja niiden sovellettavuuteen myös Kelan tietoturvayksikössä. Sen sijaan tutkielman tutkimuskonseptia ja menetelmiä on mahdollista hyödyntää muissakin organisaatioissa. Tutkimuskonseptin hyödyntämistä Kelassa voi suositella myös tulevaisuudessa. Täten mahdolliset muutokset tulevat huomioiduksi ja vaatimuskehikko tietoturvatietoisuusohjelman vaatimuksista pysyy ajantasaisena.

Tutkimustiedon perusteella muodostetut tietoturvatietoisuuden kehittämisen vaiheet ja keskeiset osatekijät (luku 5.1) ovat yleistettävissä mihin tahansa organisaatioon. Vaiheet ovat hyvä lähtökohta erityisesti organisaatioille, joissa suunnitelmallinen tietoisuusohjelman kehittäminen on alkuvaiheessa. Myös standardeihin perustuva suunnittelu varmistaa organisaatioita saavuttamaan

yleisesti hyväksyttävän tason. Kelassa standardeista onkin jo valittu sovellettavaksi ISO/IEC 27001, jonka vaatimuksia tulisi soveltaa kaikessa tekemisessä.

Ohjeita sekä malleja tietoturvaroolien ja niissä vaadittavan osaamisen määrittelyyn löytyy kattavasti tietoturvallisuuden osaamisviitekehyksistä. Viitekehyksiä on tutkielman tulosten valossa järkevää hyödyntää erityisesti sellaisten organisaatioiden tietoturvatietoisuuden kehittämisessä, jossa tietoturvan asiantuntijaresurssit tulevat organisaation sisältä.

Tutkielman pohjalta luonnollisena jatkokehitysehdotuksena Kelan tietoturvayksikölle on suunnitella ja toteuttaa tietoturvatietoisuusohjelma, joka vastaa tässä tutkielmassa esitettyihin vaatimuksiin. Tämän lisäksi erityisesti rooleihin liittyvänä kehitysehdotuksena on tutkielmassa esiteltyjen osaamisviitekehysten vertaaminen sekä roolien että osaamisprofiilien osalta Kelan tietoturvayksikön eri rooleihin sekä rooleissa toimivien henkilöiden osaamiseen.

On todennäköistä, että toiset Kelan kaltaiset organisaatiot työskentelevät vastaavien kysymysten parissa. Siksi on hyvä tarkastella myös muiden toimintaa ja jakaa tietoa etenkin julkisen hallinnon organisaatioiden kesken. Myös aiempi tutkimus osoittaa, että toisten toiminnasta on esimerkin avulla mahdollista saada nopeastikin toimivia ratkaisuja kohdattuihin haasteisiin.

Teoreettisessa viitekehyksessä sivuttiin tekoälyä ja sen hyödyntämistä. Tekoälyn käyttäminen on tutkielman kirjoittamisen aikaan yleistynyt valtavasti, mutta aihepiiriin liittyvää kattavaa tutkimustietoa ei siitä vielä löydy. Jatkotutkimusehdotuksena on tutkia tekoälyn hyödyntämistä tietoturvatietoisuusohjelman suunnittelussa ja toteuttamisessa.

LÄHTEET

Alexander, D., Finch, A., Sutton, D., & Taylor, A. (2008). *Information Security Management Principles*. British Informatics Society Limited.

Allonen, N., Seppänen, P., haastateltava 3 & haastateltava 4. (2024.) Asiantuntijoiden etähaastattelu 23.10.2024. Helsinki.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in human behavior, 49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Arkko, K. (2024.) Tietoturvapäällikön etähaastattelu 2.10.2024. Helsinki.

Bendler, D., & Felderer, M. (2023). Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model. *ACM transactions on computing education, 23*(2), 1–33. https://doi.org/10.1145/3573205

Carpenter, P. (2019). *Transformational Security Awareness*. Wiley Data and Cybersecurity.

ENISA. (2022). *User Manual for European Cybersecurity Skills Framework (ECSF).* Luettu 1.9.2024. https://data.europa.eu/doi/10.2824/95989.

ENISA. (2023a). *ENISA Threat Landscape 2023.* Luettu 13.12.2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ENISA. (2023b). *AR-IN-A-BOX, Your guide to designing a cyber-awareness programme, European Union Agency for Cybersecurity*. https://data.europa.eu/doi/10.2824/241036

Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia computer science, 181*, 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). *Tutki ja kirjoita*. 15. uud. painos, Tammi, Helsinki.

Kela (2021). *Turvallisuuden strategiset linjaukset.* https://www.kela.fi/documents/20124/410405/kelafi-kelan-turvallisuuden-strategiset-linjaukset.pdf

Kela (2023a). *Tietoa Kelasta*. Luettu 16.11.2023. https://www.kela.fi/tietoa-kelasta.

Kela (2023b). *Kelan toimintakertomus 2022*. https://www.kela.fi/documents/20124/410408/Kela-toimintakertomus-2022.pdf/242271ae-e622-aa8b-5a9f-15e1d45d205d?t=1682421803394.

Kela (2023c). *Kelan strategia 2023*. Luettu 27.9.2024. https://www.kela.fi/documents/20124/410405/Kelan-strategia-2023.pdf/ccbe2e2e-0b47-0e7a-c4b2-84982e3854ed?t=1687775657368.

Kela (2023d). *Kelan tietoturva- ja tietosuojapolitiikka.* PDF-dokumentti. Luettu 29.10.2024.

Kela (2024a). *IT-palvelujen tulosyksikön työjärjestys 1.1.2024*. PDF-dokumentti. Luettu 13.5.2024.

Kela (2024b). *Tietoturvayksikön esittely*. PowerPoint -esitys. Luettu 13.5.2024.

Kela (2024c). *Kelan IT-palvelut numeroina*. PowerPoint-esitys. Luettu 13.5.2024.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security, 106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Knuutila, V. & Lehikoinen, S. (2024.) Tietoturva-arkkitehtien ryhmähaastattelu 22.10.2024. Kelan Tapiolan toimitila, Espoo.

Koskinen, M., Nieminen P., & haastateltava 3. (2024.) Sidosryhmien etähaastattelu 16.10.2024. Helsinki.

Kolb, N., & Abdullah, F. (2009). Developing an Information Security Awareness Program for a Non-Profit Organization. *International management review, 5*(2), 103.

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers & security, 25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Laki julkisen hallinnon tiedonhallinnasta (906/2019). Luettu 14.5.2024. https://www.finlex.fi/fi/laki/alkup/2019/20190906

Laki Kansaneläkelaitoksesta (731/2001). Luettu 16.11.2023. https://www.finlex.fi/fi/laki/ajantasa/2001/20010731

Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023). Luettu 14.5.2024. https://www.finlex.fi/fi/laki/alkup/2023/20230703

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International journal of information management, 45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

NIS 2 -direktiivi (2022). *Euroopan parlamentin ja neuvoston direktiivi 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta*. http://data.europa.eu/eli/dir/2022/2555/oj

NIST. (2020). NIST Special Publication 800–181. Revision 1. *Workforce Framework for Cybersecurity (NICE Framework).* Viitattu 8.9.2024. https://doi.org/10.6028/NIST.SP.800-181r1

NIST. (2024). NICE Framework Components. Excel-tiedosto. Haettu 8.9.2024. https://www.nist.gov/document/nice-framework-components-v100

Ojasalo, K., Moilanen, T., & Ritalahti, J. (2014). *Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan*. 3. uud. painos, Sanoma Pro, Helsinki.

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information systems security*, 14(2), 37–49. https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6

Peltier, T. R. (2014). *Information security fundamentals*. CRC Press.

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS quarterly, 34*(4), 757–778. https://doi.org/10.2307/25750704

Riahi, E., & Islam, M. S. (2024). Employees' information security awareness (ISA) in public organisations: Insights from cross-cultural studies in Sweden, France, and Tunisia. *Behaviour & information technology,* 1–23. https://doi.org/10.1080/0144929X.2024.2311734

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers & security, 59, 26–44. https://doi.org/10.1016/j.cose.2016.01.004

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of 'organizational information security management'. *Journal of enterprise information management, 27*(5), 644–667. https://doi.org/10.1108/JEIM-07-2013-0052

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and computer security, 25*(5), 494–534. https://doi.org/10.1108/ICS-07-2016-0054

Suomen standardoimisliitto SFS ry (2020). ISO/IEC 27000:2020. *Informaatioteknologia. Turvallisuustekniikat. Turvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto*. 2. painos. Haettu SFS-online palvelusta 13.5.2024.

Suomen standardoimisliitto SFS ry (2022). ISO/IEC 27002:2022. *Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot.* 2. painos. Haettu SFS-online palvelusta 23.11.2023.

Suomen standardoimisliitto SFS ry (2023). ISO/IEC 27001:2023. *Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Turvallisuuden hallintajärjestelmät. Vaatimukset.* 2. painos. Haettu SFS-online palvelusta 23.11.2023.

Terveyden ja hyvinvoinnin laitos (2024). *Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista 3/2024.* Luettu 14.5.2024. https://thl.fi/documents/155392151/190361269/THL_Maarays_3_2024_Tietoturvasuunnitelmaan_sisallytettavista_sevityksista_ja_vaatimuksista.pdf/9123733d-c1ae-09f5-e05d-

a33894441c6c/THL_Maarays_3_2024_Tietoturvasuunnitelmaan_sisallytettavista_sevityksista_ja_vaatimuksista.pdf?t=1708438054468

Thomson, K., & von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer fraud & security, 2006*(5), 11–15. https://doi.org/10.1016/S1361-3723(06)70356-6

Haastateltava 1 & haastateltava 2. (2024.) Tiimipäälliköiden etähaastattelu 17.10.2024. Helsinki.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & security, 52*, 128–141. https://doi.org/10.1016/j.cose.2015.04.006

Turvallisuuskomitea (2018). *Kyberturvallisuuden sanasto*. Haettu 8.12.2023. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

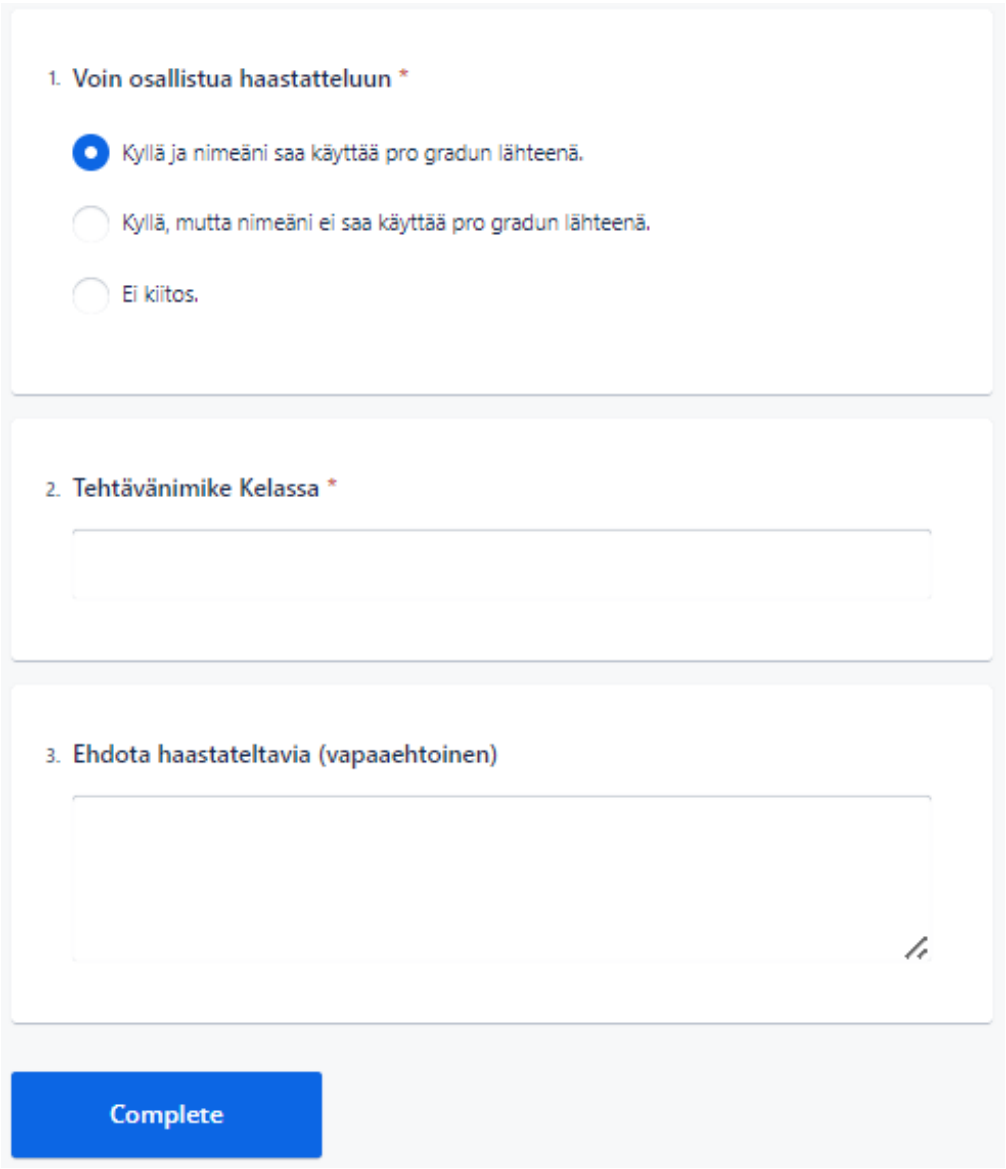
Vilkka, H. (2015). *Tutki ja kehitä*. 4. uud. painos, PS-kustannus, Jyväskylä.

Yhteiskunnan turvallisuusstrategia (2017). *Valtioneuvoston periaatepäätös 2.11.2017*. Turvallisuuskomitea. Luettu 22.11.2023. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf.

Yin, R. K. (2018). *Case study research and applications: Design and methods*. 6. painos. SAGE, Thousand Oaks.

Yleinen tietosuoja-asetus. (2016). *Euroopan parlamentin ja neuvoston asetus 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.* http://data.europa.eu/eli/reg/2016/679/oj

LIITE 1 KYSELYLOMAKE



1. Voin osallistua haastatteluun *

- (•) Kyllä ja nimeäni saa käyttää pro gradun lähteenä.
- ( ) Kyllä, mutta nimeäni ei saa käyttää pro gradun lähteenä.
- ( ) Ei kiitos.

2. Tehtävänimike Kelassa *

3. Ehdota haastateltavia (vapaaehtoinen)

Complete

LIITE 2 TEEMAHAASTATTELURUNKO

1 Johdon tuki

- Strategisiin tavoitteisiin vastaaminen
- Esimerkillä johtamisen toteutuminen
- Odotukset jatkuvaan ja näkyvään viestintään

2 Projektin ja tiimin perustaminen (resursointi)

- Vaatimukset monipuolisesta asiantuntijuudesta
- Poikkihallinnollisen tiimin muodostamisen edellytykset
- Vaatimukset raportoinnista ylimmälle johdolle

3 Toimintasuunnitelman laatiminen

- Vaatimukset tietoisuusohjelman tavoitteista
- Budjetti, ulkoiset ja sisäiset resurssit
- Nykytila-analyysi ja sen toteuttaminen
- Kohderyhmien ja pätevyystasojen tunnistaminen

4 Sisältö

- Velvollisuuksien ja vastuiden määrittely
- Politiikat ja periaatteet organisaatiossa
- Uhkaskenaarioiden hyödyntäminen harjoittelussa
- Seuraamus ja palkitsemiskäytännöt
- Toivotun käyttäytymisen luonnolliset ajurit

5 Toteuttaminen

- Viestintäkanavia koskevat havainnot ja odotukset
- Käytännönläheisten oppimistehtävien toteuttaminen
- Yksilöllisten oppimistyylien huomiointi
- Jatkuvan oppimisen mahdollistaminen

6 Jatkuva parantaminen

- PDCA-syklin toteuttaminen organisaatiossa
- Sisäisen auditoinnin toteuttaminen
- Muuttuvien strategisten tavoitteiden huomiointi

LIITE 3 VAATIMUSTEN TAULUKOINTI

1 Johdon tuki	1.1 Jatkuva ja näkyvä viestintä	1.1.1 Viestintä tuo esille strategisia tavoitteita selkeässä ja ymmärrettävässä muodossa
		1.1.2 Viestintä on aktiivista ja oma-aloitteista
		1.1.3 Viestintä toteutuu kaikilla johtamisen tasoilla
		1.1.4 Viestinnällä jaetaan tietoa sidosryhmille
	1.2 Esimerkillä johtaminen	1.2.1 Johto noudattaa vastuitaan ja velvollisuuksiaan
		1.2.2 Tietoturvatietoisuus on kiinteä osa työviikkoa
2 Resursointi	2.1 Tarvittava asiantuntijuus ja osaaminen	2.1.1 Tietoturvan viestintä- ja koulutusosaaminen
		2.1.2 Riskienhallintaosaaminen
		2.1.3 Psykologinen osaaminen
		2.1.4 Liiketoimintaosaaminen
	2.2 Organisointi	2.2.1 Tietoturvatietoisuuden kehittämiseen on muodostettu poikkihallinnollinen virtuaalitiimi
		2.2.2 Tiimillä on nimetty vastuuasiantuntija, jolla on riittävä osaaminen. Lisäksi useampi yhteyshenkilö, jotta toiminta ei ole yhden henkilön varassa
		2.2.3 Osallistujilla on lähtökohtainen motivaatio tietoturvatietoisuuden kehittämiseen
	2.3 Budjetti ja ajankäyttö	2.3.1 Tietoturvatietoisuuden kehittämiseen on budjetoitu riittävästi rahaa
		2.3.2 Henkilöstöltä on varattu riittävästi työaikaa tietoisuusohjelmalle
3 Suunnittelu	3.1 Tavoitteiden määrittely	3.1.1 Tavoitteet noudattavat strategisia tavoitteita
		3.1.2 Yksikön tavoitteet, joiden saavuttamista tietoisuuden kehittämisellä voidaan tukea, on tunnistettu
		3.1.3 Tavoitteissa huomioidaan tulevaisuuden osaamistarpeet
	3.2 Kohderyhmien tunnistaminen	3.2.1 ECSF- ja NICE-viitekehyksiä käytetään sekä hallinnollisen että operatiivisen tietoturvan osa-alueilla
		3.2.2 Kohderyhmät dokumentoidaan roolikorteiksi/-profiileiksi tietoturvan hallintajärjestelmään
	3.3 Pätevyystasojen määrittely	3.3.1 Pätevyysprofiilit perustuvat roolikortteihin
		3.3.2 Sovelletaan ECSF- ja NICE-viitekehyksiä
		3.3.3 Huomioidaan lainsäädäntö ja määräykset
		3.3.4 Osaamisalueet on priorisoitu liiketoimintatarpeiden mukaan
		3.3.5 Osaamisen tavoitetasot on määritelty
	3.4 Asiakaspolkujen laatiminen	3.4.1 Tunnistetaan osaamisen kehittämisen edellytykset työsuhteen elinkaaren aikana
		3.4.2 Kohderyhmille on laadittu tarvittaessa omat koulutussuunnitelmansa

	3.5 Nykytilan analyysi	3.5.1 Perustuu riskienarviointiin
		3.5.2 Osaamista ja osaamistarpeita tunnistetaan yhteisissä työpajoissa sekä henkilökohtaisissa osaamiskeskusteluissa
		3.5.3 Hyödynnetään ECSF-viitekehystä
4 Sisältö	4.1 Politiikat ja periaatteet	4.1.1 Tuo esille johdon sitoutumisen tietoturvaan
		4.1.2 Kytkee Kelan tavoitteet tietoturvan tavoitteisiin ja kuvaa strategian toteuttamista arjessa
		4.1.3 Riittävä painoarvo koko organisaatiossa
		4.1.4 Dokumentoituna osaksi hallintajärjestelmää
	4.2 Uhkaskenaariot	4.2.1 On olemassa uhkaskenaariopankki, jonka ylläpitäminen on joukkoistettua
		4.2.2 Uhkaskenaarioille on prioriteettijärjestys
	4.3 Velvollisuudet ja vastuut	4.3.1 Asiantuntija vastaa oman osaamisen ylläpitämisestä. Osaamisen ylläpitäminen on itseohjautuvaa
		4.3.2 Esihenkilö varmistaa asiantuntijan riittävän osaamisen ja mahdollistaa sen kehittämiseen työsuhteen aikana
		4.3.3 Esihenkilö huolehtii, että työn kuorma pysyy kohtuullisena ja mielekkäänä siten, että motivaatio osaamisen kehittämiseen säilyy
	4.4 Seuraamus- ja palkitsemiskäytännöt	4.4.1 Virheitä saa tehdä, eikä niistä tule seuraamuksia
		4.4.2 Palkitseminen on säännöllistä ja avointa
		4.4.3 Kiitetään hyvin tehdystä työstä
		4.4.4 Palkitaan siten, että se ohjaa kohti tavoitteita
		4.4.5 Noudatetaan positiivista asiakaspalveluasennetta
	4.5 Käytännön toimintamallit	4.5.1 On olemassa yleiset ohjeet, joissa on kuvattuna tiedon suojaaminen ja asiakirjojen turvallinen käsittely, etä- ja hybridityön tietoturvallisuus, yhteydenotto ja neuvontakanavat sekä tietoturvapoikkeamista raportointi
		4.5.2 On laadittu yhteisesti hyväksytyt pelisäännöt yhteisiin tilaisuuksiin
		4.5.3 Valitut toimenpiteet ja toimintamallit perustellaan huolellisesti
		4.5.4 Tehdyt toimenpiteet kirjataan ylös ja toteuttamista seurataan
5 Toteutus	5.1 Viestintä	5.1.1 Viestintä on monikanavaista ja jatkuvaa
		5.1.2 Saavuttaa kohderyhmän ilman erillistä tiedon hakemista
		5.1.3 Viestintää tehdään sähköpostitse, viikkopalavereissa sekä pikaviestintävälineissä
		5.1.4 Mahdollisuuksia työvälineenä käytettävissä sovelluksissa tapahtuvaan tiedonjakoon kehitetään

	5.2 Koulutus	5.2.1 Perustason kyberturvallisuuskoulutus kaikille
		5.2.2 On tarjolla roolikohtaisia koulutuksia, joissa periaatteiden hyödyntämistä omassa työssä
		5.2.3 Oppimistehtävissä korostuu käytännönläheisyys ja säännöllisyys
		5.2.4 Koulutus keskittyy tunnistettuihin osaamispuutteisiin
		5.2.5 Huomioi käytettävissä olevan ajan
	5.3 Harjoittelu	5.3.1 Perustuu laadittuihin uhkaskenaarioihin
		5.3.2 Harjoittelua tehdään tiimin sisällä sekä sidosryhmien kanssa
		5.3.3 Asiantuntijoilla on käytössään tekniset harjoitteluympäristöt
	5.4 Infotilaisuudet	5.4.1 Tilaisuudet tallennetaan
		5.4.2 Mahdollistetaan vuorovaikutuksellisuus
	5.5 Yksilöllisten oppimistyylien huomiointi	5.5.1 Suositaan videomuodossa olevaa materiaalia
		5.5.2 Kaikille on olemassa henkilökohtaiset oppimissuunnitelmat
6 Jatkuva parantaminen	6.1 Jatkuvuus	6.1.1 Tietoisuusohjelma sisältää toisteisuutta
		6.1.2 Järjestetään säännöllisiä osaamisen kehittämisen työpajoja ryhmän tai tiimin kesken
	6.2 Seuranta	6.2.1 Mittaaminen perustuu tietoisuusohjelman tavoitteisiin
		6.2.2 Kehitystoimenpiteistä kerätään välitön palaute
		6.2.3 Koulutuksista ja seminaareista pidetään kirjaa
		6.2.4 Seurataan linjauksiin ja päätöksiin liittyviä kysymyksiä
		6.2.5 Henkilökohtaisten oppimistavoitteiden toteutumista seurataan kehityskeskusteluissa
	6.3 Muutokset	6.3.1 Tavoitteet tarkistetaan säännöllisesti ja strategian muutosten yhteydessä ja niitä päivitetään tarvittaessa
		6.3.2 Muuttuvista politiikoista, periaatteista sekä ohjeista viestitään asianosaisille
		6.3.3 Tavoitteiden muuttuessa mittareita arvioidaan uudelleen