



Karelia-ammattikorkeakoulu  
Tradenomi, ylempi ammattikorkeakoulututkinto  
Johtaminen ja liiketoimintaosaaminen

# Tietoturvajohdaminen osaksi organisaatiokulttuuria

Eetu Sormunen

Opinnäytetyö, Maaliskuu 2024

[www.karelia.fi](http://www.karelia.fi)



**Karelia**  
AMMATTIKORKEAKOULU

**OPINNÄYTETYÖ**

**Maaliskuu 2024**

**Johtaminen ja liiketoimintaosaaminen, ylempi  
ammattikorkeakoulututkinto**

Tikkarinne 9  
80200 JOENSUU  
+358 13 260 600 (vaihde)

Tekijä(t)  
Eetu Sormunen

Nimeke  
Tietoturvajohdaminen osaksi organisaatiokulttuuria

Toimeksiantaja  
Meidän It ja Talous Oy

Opinnäytetyön tarkoitus oli kartoittaa organisaation tietoturvajohdamisen nykytilanne tietoturvallisuuden hallintajärjestelmän ISO 27001 ja valmentavan johtamisen näkökulmasta sekä kuinka tietoturvallisuus ilmenee organisaatiokulttuurissa ja tunnistaa mahdollisia kehitystarpeita.

Tutkimus toteutettiin laadullisena tutkimuksena, tiedonhankinnan menetelmänä käytettiin teemahaastattelua ja kerätty aineisto analysoitiin sisältöanalyysiä käyttäen.

Tulokset osoittivat roolien vastuiden ja valtuuksien määrittelyn tärkeyden läpi organisaation sekä johdon esimerkkinä toimimisen merkityksen. Tietoturvan hallintajärjestelmän jalkauttamiseksi osaksi organisaatiokulttuuria vaaditaan määrätietoista kouluttamista ja uusien toimintatapojen noudattamiseen kannustamista. Tietoturvasta viestittäessä olisi hyvä pyrkiä myönteiseen sävyyn ja siihen, kuinka tietoturva toimii työntekemisen mahdollistajana sen sijaan, että keskitytään aina vain uhkakuihin ja negatiivisiin seurauksiin tietoturvan pettäessä.

Kieli  
suomi

Sivuja 70  
Liitteet 2  
Liitesivumäärä 2

Asiasanat  
tietoturva, johtaminen, organisaatiokulttuuri, tietoturvakulttuuri, ISO 27001, valmentava johtaminen



**THESIS**  
**March 2024**  
**Degree Programme in Business Management**  
**and Leadership, Master's Degree**

Tikkarinne 9  
80200 JOENSUU  
FINLAND  
+ 358 13 260 600 (switchboard)

Author (s)  
Eetu Sormunen

Title  
Integrating Information Security Management into Organizational Culture

Commissioned by  
Meidän Itä ja Talous Oy

The purpose of the thesis was to study the current state of organization's information security management from the perspective of the ISO 27001 information security management system and coaching leadership. It was also examined how information security manifests in the organizational culture and to identify possible areas for improvement.

The research was conducted as a qualitative study with thematic interviews as the method of data collection and analysing the collected data using content analysis.

The results indicated the importance of defining roles, responsibilities, and authorities across the organization, as well as the significance of leadership setting an example. Integrating the information security management system into the organizational culture requires systematic training and encouragement for adopting new practices. When communicating about information security, it is advisable to maintain a positive tone, emphasizing how security facilitates work rather than solely focusing on threats and negative outcomes in case of security breaches.

Language  
Finnish

Pages 70  
Appendices 2  
Pages of Appendices 2

Keywords  
Information security, management, organizational culture, security culture, ISO 27001, coaching leadership

# Sisältö

1	Johdanto .....	5
1.1	Tavoitteet .....	6
1.2	Aiempien opinnäytetöiden tulokset .....	8
2	Meidän IT ja Talous Oy .....	10
2.1	Yrityksen esittely .....	10
2.2	Visio, arvot ja strategia .....	12
2.3	Toimintaympäristö .....	12
3	Johtaminen, organisaatiokulttuuri ja tietoturva .....	14
3.1	Johtamisen viitekehys – valmentava johtajuus .....	14
3.2	Organisaatiokulttuuri .....	18
3.3	Tietoturvallisuuden viitekehys – ISO/IEC 27001 .....	23
3.3.1	ISO 27001 pakolliset vaatimukset .....	25
3.3.2	Tietoturvan määritelmä .....	30
3.3.3	Tietoturvallisuuden osa-alueet ja ISO 27001:2017 hallintakeinot .....	31
4	Kehittämistyön tutkimusmenetelmät ja toteutus .....	34
4.1	Teemahaastattelu .....	35
4.2	Sisällönanalyysi .....	37
4.3	Kehittämistyön luotettavuus ja eettisyys .....	40
5	Tulokset .....	41
5.1	Johtaminen .....	42
5.1.1	Valmentava johtaminen .....	43
5.1.2	Esihenkilöiden roolit ja vastuut .....	44
5.1.3	Johdon roolit ja vastuut .....	45
5.1.4	Roolien vastuut ja valtuudet .....	46
5.1.5	Johtamisen kokemus ja odotukset .....	47
5.1.6	Strategia .....	48
5.2	Organisaatiokulttuuri .....	50
5.2.1	Tietoturvakulttuuri .....	50
5.2.2	Koulutus .....	53
5.2.3	Viestintä .....	54
6	Johtopäätökset .....	57
6.1	Johtopäätökset .....	57
6.2	Kehityskohteet .....	59
6.3	Jatkotoimenpiteet .....	61
7	Pohdinta .....	62
	Lähteet .....	66

## Liitteet

- Liite 1 Teemahaastattelun kysymykset
- Liite 2 Haastattelukutsu

## 1 Johdanto

Tietoturva käsitetään monesti teknisenä ratkaisuna, jota toteutetaan muun toiminnan taustalla, jolloin se organisatorisesti sijoitetaan IT-osaston yhteyteen. Ennen lähestymistapa on voinut toimia, kun tietoturvaan liittyvät uhat olivat yksinkertaisempia ja uusien uhkien synty tapahtui hitaammin. Nykyään tietoturva pitää sisällyttää kaikkiin organisaation toimintoihin, uhkiin täytyy kyetä reagoimaan nopeammin ja on oltava hyvät suhteet kaikkiin organisaation sidosryhmiin. (Doan 2019.) Hyvän tietoturvakulttuurin, johon henkilöstö sitoutuu, muodostamiseksi organisaation täytyy ottaa huomioon henkilöstön tarpeet sekä pitää huoli, ettei tietoturvakäytänteet vaikeuta tai hidasta työntekoa tarpeettomasti. Mikäli tietoturvakäytänteet ovat kankeita on riski, että henkilöstö etsii tilalle vaihtoehtoisia tapoja toimia, jotka eivät välttämättä ole tietoturvallisia. (Traficom 2020, 24.)

Standardi ISO 27001:2017 tietoturvallisuuden hallintajärjestelmä vaatii ylimmältä johdolta johtajuutta ja sitoutumista. Tietoturvatavoitteiden on oltava yhdenmukaisia organisaation strategian kanssa ja hallintajärjestelmä tulee yhdistää organisaation prosesseihin. Lisäksi vaikuttavan hallintajärjestelmän vaatimusten noudattamisen tärkeydestä on viestittävä, on ohjattava ja tuettava henkilöstöä hallintajärjestelmän vaikuttavuuden kehittämisessä sekä tukea muiden johtoon kuuluvien johtajuutta heidän vastualueillaan. (SFS-EN ISO 27001, 2017, 7.)

Ilmonen, Kallio, Koskinen ja Rajamäki (2022) painottavat tietoturvan toteutumisen kannalta olevan tärkeää, että prosessit ja kulttuuri toimivat saumattomasti yhteistyössä teknisten ratkaisuiden kanssa eikä mitään näistä saa laiminlyödä. Tyypillisen määritelmän mukaan kyvykkyyden muodostaa teknologia, prosessit ja osaaminen, jolloin parhaaseen lopputulokseen päästään kehittämällä aktiivisesti kaikkia näitä osa-alueita. (Ilmonen, Kallio, Koskinen & Rajamäki 2022, luku 4.6.) Henkilöstön osaamisen kehittämisessä valmentavalla esimiehellä on arvokas rooli. Sen sijaan, että esimies antaa suoria ohjeita alaisilleen tai yrittää toimia esimerkillisesti toivoen alaisten ottavan hänestä mallia, valmentava esimies

pyrkii luomaan heidän kanssaan vuorovaikutussuhteen. Vuorovaikutussuhteessa he voivat yhdessä ideoida, suunnitella ja toteuttaa tapoja, kuinka alainen voi kehittää itseään ja poistaa onnistumisen tiellä olevia haasteita. (Kupias, Pelto & Pirinen 2014, 4.)

Valmentavassa johtajuudessa keskeistä on yhdessä tekeminen, jossa ulkopuolisen tarkkailijan on vaikeaa erottaa, kuka on esimies ja kuka johdettava. Olen- naista ovat toimivat prosessit eikä henkilöiden organisatorinen hierarkia ole keskiössä. Valmentavassa johtajuudessa esimies ei ole kaiken tietäjä ja tarjoa oikeita vastauksia, vaan tiimi yhdessä etsii niitä kysymällä, haastamalla ja kannustamalla toisiaan. Näin synnytetään uudenlaista ajattelua, joka mahdollistaa toiminnan muuttuvissa olosuhteissa ja ylläpitää tavoitteellista sekä osallistavaa yhteistä toimintatapaa, jossa korostuu työn merkityksellisyys ja innostavuus. (Ristikangas & Grünbaum 2014, 16.)

Johtaminen on murroksessa: vanha tapa toimia ei enää riitä, mutta uuttakaan ei vielä hallita. Polttavaksi tilanteen tekee suurten ikäluokkien siirtyminen eläkkeelle samalla kun nettisukupolvi on ottamassa näkyvämpää roolia työelämässä. Uusien johtamisotteiden omaksumisella on kiire. Siksi valmentava johtajuus on äärimmäisen ajankohtainen teema. (Ristikangas & Ristikangas 2010, 9.)

## 1.1 Tavoitteet

Tämän opinnäytetyön tarkoitus on kartoittaa organisaation tietoturvajohdamisen nykytilanne tietoturvallisuuden hallintajärjestelmän ISO 27001 ja valmentavan johtamisen näkökulmasta sekä kuinka tietoturvallisuus ilmenee organisaatiokulttuurissa ja tunnistaa mahdollisia kehitystarpeita. Opinnäytetyön lähestymistapa toteutetaan laadullisena tutkimuksena, tiedonhankinnan menetelmänä käytetään teemahaastattelua ja kerätty aineisto analysoidaan sisältöanalyysiä käyttäen. Aineisto kerätään haastatteleamalla henkilöstöä eri tasoilta johtajasta asiantuntijaan, jolloin saadaan läpileikkaus koko organisaatiosta.

Koska johtaminen ja tietoturva ovat molemmat laaja-alaisia aiheita valittiin haastattelutyypiksi teemahaastattelu. Teemahaastattelussa kysymykset ja niiden

esittäminen eivät ole kovinkaan tarkasti sidottuja tiettyyn muotoon (Kallinen & Kinnunen 2022). Teemahaastattelussa haastateltavalla on mahdollisuus vastata kysymyksiin vapaasti ja se antaa samalla haastattelijalle mahdollisuuden ohjata haastateltavaa vastaamaan haluttuihin osa-alueisiin.

Kohdeorganisaation johtamiskulttuuri nojaa vahvasti valmentavaan johtamiseen, joten opinnäytetyön johtamisen viitekehyksenä on valmentava johtaminen. Traficom kuvauksen mukaan moderni tietoturvajohdaminen painottaa avointa ja keskustelevaa johtamista (Traficom 2020, 24).

Tutkimuskysymykset ovat

- Kuinka valmentava johtajuus toteutuu tietoturvallisuuden johtamisessa?
- Kuinka tietoturvallisuus näkyy organisaatiokulttuurissa?

Aihe on kohdeorganisaatiolle ajankohtainen, sillä se sai tietoturvallisuuden hallintajärjestelmän ISO 27001 -sertifikaatin kesäkuussa 2023. Standardi on itsessään hyvin yleisluontoinen eikä tarjoa juurikaan konkreettisia tapoja, kuinka tietoturvallisuuden hallintajärjestelmää tulisi toteuttaa. Tämän vuoksi se sopiikin käytettäväksi useimmissa organisaatioissa. Koska standardi ei tarjoa tarkkaa ohjeistusta on jokaisen organisaation itse määriteltävä ja toteutettava, kuinka se täyttää standardin vaatimukset (Traficom 2019, 16).

Tässä opinnäytetyössä on hyödynnetty ChatGPT 3.5-tekoälyä vähäisissä määrin. Tekoälyn käyttö kuvataan tarkemmin kappaleessa 4.2.

## 1.2 Aiempien opinnäytetöiden tulokset

Lokakuussa 2023 Theseuksesta löytyi hakusanalla 'tietoturvajohdaminen' neljä (4) hakutulosta ylemmän ammattikorkeakoulun opinnäytetöitä, joista yksi on kunnan tietoturvajohdamisen jalkauttamista arkipäivän toimintaan (Ruonala, 2011), toinen kyberturvallisuuden hallintamallin kehittämiseen (Turunen, 2018), kolmas kyberturvallisuuskoulutuksen suunnittelun ja toteuttamisen yrityksen johdolle (Antila, 2018) ja neljäs sosiaali- ja terveydenhuoltohenkilöstön tietosuojaoosaamisen kehittämistä (Ratinen, 2021). Valmentava johtajuus taas on suosittu aihe ylemmässä ammattikorkeakoulussa. Lokakuussa 2023 Theseuksesta löytyi 'valmentava johtaminen' hakusanalla 241 hakutulosta. Tässä opinnäytetyössä tarkastellaan kahta opinnäytetyötä tietoturvajohdamisesta (Ruonala, 2011) ja (Antila, 2018) sekä yhtä valmentavasta johtamisesta (Viljamaa, 2023).

Ruonala (2011) tarkasteli opinnäytetyössään, kuinka kunnan tietoturvapoliittikka käytännössä noudatetaan. Tutkimuksessa haastateltiin kunnan osastopäälliköjä, koska he vastaavat tietoturvapoliittikan käytännön toimista. Tavoitteena oli selvittää osastopäällikköjen yleinen tietämys tietoturvasta ja sen eri osa-alueista sekä kuinka he toimivat tietoturvan johtajina. Tuloksissa esille nousi osastopäällikköjen osittain puutteelliset tiedot tietoturvan eri osa-alueitten, minkä takia tietoturvapoliittikkaan liittyviä ohjeistuksia ei voida noudattaa vaikuttavasti. Tämän vuoksi tietoturvakoulutusta olisi lisättävä kunnan osastopäälliköille. Tuloksissa ilmeni myös, ettei kaikki tietoturvaohjeistukset olleet osastopäälliköille tuttuja, minkä vuoksi heidät tulisi velvoittaa tutustumaan niihin sekä johtoryhmän tulisi nostaa ohjeistukset esille määräajoin. Säännöllisen ja suunnitelmallisen koulutuksen puute oli myös yksi kehityskohteista ja sitä tulisi tarjota kunnan koko henkilöstölle. Tutkimuksesta kävi ilmi, että vaikka tietoturvapoliittikkaan liittyvät ohjeistukset olivat asianmukaisia, niiden sisältöä ei ollut saatu viestittyä osastopäälliköille ja muulle henkilöstölle riittävän hyvin. Parannusehdotuksena on esitetty tietoturvan esillä pitämistä ja henkilöstön kouluttamista säännöllisesti. (Ruonala 2011, 46–48.)

Antilan (2018) opinnäytetyön tarkoituksena oli tuottaa kyberturvallisuusmateriaalia koulutuksen suunnitteluun ja toteuttamiseen pienten ja keskisuurten



yrittäjien johdolle. Vaikka Antilan opinnäytetyön tavoite poikkeaa omastani sekä Ruonalan aiheista, Antila esittää yhteenvedossaan samoja aihepiirejä tietoturvallisuuden johtamisen kannalta kuin Ruonala. Antila painottaa koulutuksen ja ohjeistuksen tärkeyttä kyberturvakulttuurin lisäämiseksi yrityksissä, sillä useiden tutkimusten mukaan yli 50–90 % kyberuhista organisaatiossa tulee sen sisältä joko tahattomina tai tahallisia henkilöstön tekeminä virheinä. Lisäksi Antila toteaa kyberturvallisuuden toteuttamisessa kustannusten olevan tärkeässä roolissa. On suhteutettava tietoturvallisuuden kattavuuden ja kustannusten välistä suhdetta sillä yritys ei voi koskaan täysin suojautua teknisillä tietoturvakontroleilla kaikilta tietoturvaa uhkaavilta tekijöiltä, jolloin koulutus tuottaa kustannustehokkaan ratkaisun. (Antila 2018, 82–85.)

Valmentavasta johtajuudesta Viljamaa (2023) havaitsi opinnäytetyönsä tuloksissa olevan tärkeää määritellä raamit, joiden puitteissa tiimit voivat itsenäisesti päättää asioistaan. Viljamaa esittää tuloksissaan valmentavan johtajuuden saatamiseksi osaksi päätöksentekoa luottamuksen rakentamista esihenkilön ja tiimiläisten välillä sekä luomalla yhteishenkeä ja vastuuttamalla henkilöstö pitämään kiinni yhteisesti sovitusta asioista. Tiimihenkeä ja valmentavan johtajuuden toteutumista heikentäviä tekijöitä tutkimuksessa havaittiin olevan, mikäli yhdessä sovittujen päätöksien toteuttamista ei seurata, puutteet tasa-arvoisessa kohtelussa, yhteisten pelisääntöjen noudattamattomuus sekä epätasaisesti jaakautuva työkuorma. Avoin keskustelukulttuuri, kaikkien osapuolien oikeudenmukainen ja arvostava kohtelu nähtiin henkilöstön sitouttamisen yhteisiin tavoitteisiin olennaisena osana. Lisäksi kouluttautuminen ja mahdollisuus hyödyntää omia ideoita työssään koettiin tärkeäksi. Viljamaa nostaa palautekulttuurin tärkeyden valmentavan johtajuuden osana. Tutkimustuloksista käy ilmi, että kyselyyn vastanneet kaipaavat enemmän palautetta sekä positiivista että rakentavaa. Olisi tärkeää nostaa esille onnistumisia sekä antaa kiitosta hyvin tehdystä työstä sillä nämä lisäävät henkilöstön hyvinvointia. (Viljamaa 2023, 38–43.)

## **2 Meidän IT ja Talous Oy**

### **2.1 Yrityksen esittely**

Opinnäytetyön toimeksiantajana toimii työnantajani Meidän IT ja talous Oy, eli tutummin Meita. Meita tuottaa ICT-, talous- ja henkilöstöpalveluja inhouse yhtiönä omistaja-asiakkailleen, joita ovat Etelä- ja Pohjois-Karjalan sekä Etelä-Savon kunnat, kaupungit, kuntatoimijat sekä Etelä- ja Pohjois-Karjalan hyvinvointialueet. In-house-yhtiönä toimimme tiiviisti omistaja-asiakkaidemme kanssa, joita Meitalla on 37 ja lisäksi muita asiakkaita on yli 80 kappaletta. Liikevaihtoa vuonna 2022 oli 57 miljoonaa. Meitan organisaatiorakenne kuvattu alla kuviossa 1. (Meita 2023a.)



Kuvio 1. Meitan organisaatio (Meita 2023a).

Meitan tavoitteena on olla yhden luukun kumppani, joka tarjoaa asiakkailleen helppoa, yhtenäistä ja kokonaisvaltaista palvelua. Meitan isoimmat toimipisteet sijaitsevat Lappeenrannassa, Imatralla, Mikkelissä sekä Joensuussa. (Meita 2023a.) Meita työllistää yli 450 henkilöä, joiden keski-ikä on 44 vuotta (Meita 2023b).

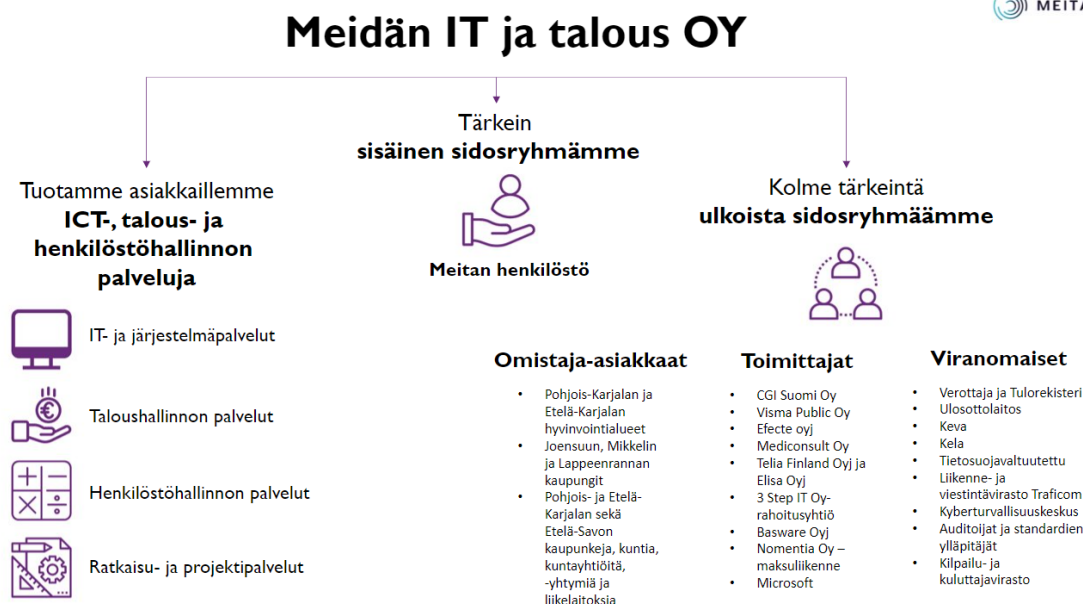
## 2.2 Visio, arvot ja strategia

Meitan visio on “Hallitsemme huomista yhdistämällä tietoa, taitoja ja tekoja!” ja tavoiteidentiteettinä on olla rohkea ja näkyvä luottokumppani. Henkilöstön osalta arvoina on olla oivaltava osaaja, rohkea vaikuttaja sekä arvostettu luottopelaaja ja toimimme ilolla yhdessä. Omistaja-arvoina ovat luotettava kumppanuus, kilpailukykyisyys sekä kuunteleminen ja sparraus. Omistaja-arvot luovat perustan yhteiselle toiminnalle, joka mahdollistaa toiminnan paremman tulevaisuuden hyväksi. (Meita 2023d; Meita 2023a.)

Meitan strategiaan kuuluu kolme pääosa-aluetta, magneettinen osaajayhteisö, yhtenäinen asiakaskokemus ja hallittu kasvu. Magneettinen osaajayhteisö tarkoittaa, että Meita pyrkii lisäämään henkilöstötyytyväisyyskyselyssä ENPS-mittarin tuloksen +30, edistämään sisäisten urapolkujen määrää, vähentämään lähtövaihtuvuutta sekä lisäämään työhakemusten määrää. Yhtenäinen asiakaskokemus pitää sisällään asiakkaiden avainhenkilöiden ja loppukäyttäjien asiointiin tyytyväisyyskyselyiden tulosten parantamista, johon pyritään tuottamalla laadukasta ja yhtenäistä asiakaskokemusta. Hallitun kasvun tavoitteena on saavuttaa toimintaedellytysten turvaamiseksi riittävä markkinaosuus julkisomisteisten TaHe- ja ICT-palvelukeskusten liikevaihdossa laskettuna. (Meita 2023e.)

## 2.3 Toimintaympäristö

Meitan toimintaympäristön sidosryhmiin kuuluu henkilöstön lisäksi omistaja-asiakkaat, asiakkaat, toimittajat ja viranomaiset. Meitan sidosryhmät kuvattu alla kuviossa 2.



Kuvio 2. Meitan sidosryhmät (Meita 2023e).

Koska inhouse-yhtiön rahoitus kerätään yhtiön omistaja-asiakkailta, taloudellisen toimintaympäristön muodostaa kuntien ja kuntayhtymien taloudellinen tilanne sekä hyvinvointialueiden rahoitus (Kortelainen 2023). Kilpailua käydään pääasiallisesti vastaavien inhouse-yhtiöiden kanssa sekä yksityisten toimijoiden, jotka tuottavat vastaavia palveluita (Meita 2023e).

Lainsäädännöllisesti toimintaa ohjaavat useat eri lait ja asetukset:

- Arkistolaki (831/1994)
- EU:n yleinen tietosuoja-asetus (679/2016)
- Laki digitaalisten palvelujen tarjoamisesta (306/2019)
- Laki julkisen hallinnon tiedonhallinnasta (Tiedonhallintalaki 906/2019)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019)
- Laki sähköisen viestinnän palveluista (917/2014)
- Laki sähköisestä lääkemääräyksestä (61/2007)
- Laki viranomaisten toiminnan julkisuudesta (Julkisuuslaki 621/1999)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Rikoslaki (39/1889)

- Tietosuojalaki (1050/2018)
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (Tietoturvallisuusasetus 681/2010) (Meita 2023f.)

Digitalisaatio laajenee asiakaskunnassa ja Meitan on pystyttävä vastaamaan nopeasti muuttuvaan teknologiseen toimintaympäristöön pysyäkseen relevanttina. Pilvisiirtymä, kyberturvallisuuden teknisten osa-alueiden sekä modernien tietoturvapalveluiden, tekoälyn, robotiikan ja automatisoinnin hyödyntäminen toiminnan tehostamiseksi ja turvaamiseksi on sekä asiakkaiden että Meitan oman toiminnan kannalta välttämätöntä. Teknologian nopea muuttuminen ja digitalisaatio muodostavat haasteen henkilöstöressurssien osalta sillä kilpailu erikoisosaajista on kiristynyt siinä määrin, että perusosaajienkin rekrytoinnissa sekä organisaatiossa pitämisessä on haasteita. (Meita 2023g).

### **3 Johtaminen, organisaatiokulttuuri ja tietoturva**

#### **3.1 Johtamisen viitekehys – valmentava johtajuus**

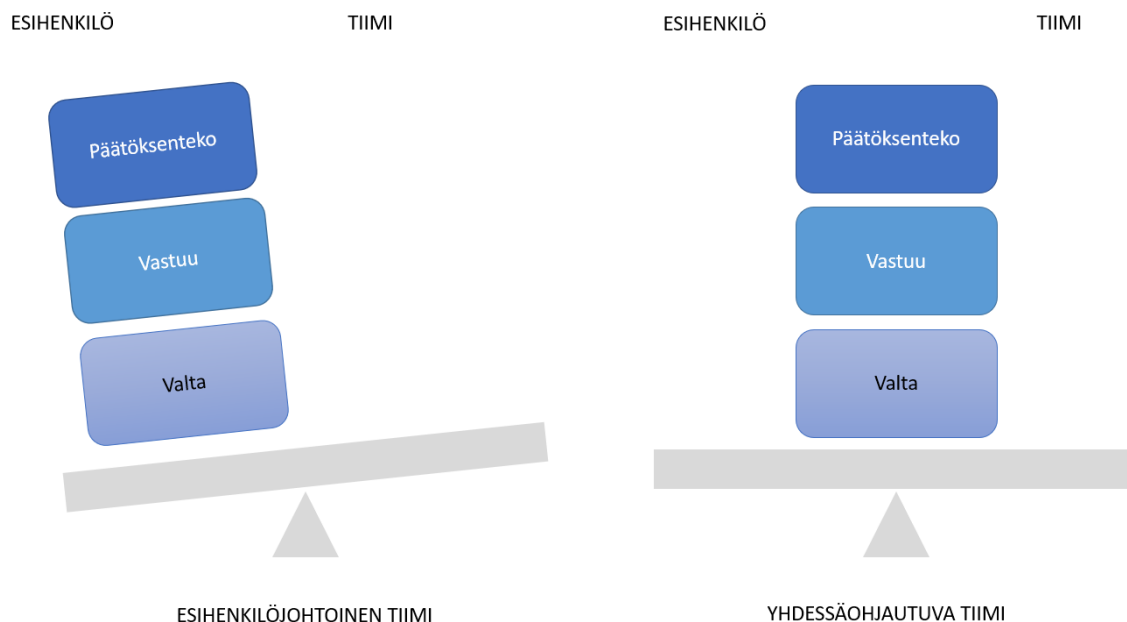
Maailman muuttuessa ja organisaatioiden kilpaillessa osaamisella ei menestyvää johtamista voida toteuttaa vanhoilla opeilla, joissa johtaja tietää, käskee, valvoo ja on muutenkin alaisiaan parempi ja ylhäisempi. Sen sijaan johtajilta vaaditaan nöyryyttä, ihmisten arvostamista, henkilöstön tukemista ja auttamista sekä mahdollistamaan heidän kasvunsa. (Räsänen 2010, 83–84.) Räsäsen mukaan valmentava johtajuus tai coaching, on nykypäivään soveltuva sillä se yhdistää yksilön kehittymisen sekä organisaation tavoitteiden saavuttamisen. Valmentavan johtajuuden tavoitteena on auttaa valmennettavaa tunnistamaan ja pysyvästi hyödyntämään omaa potentiaaliaan. (Räsänen 2010, 15–16.)

Ristikangas ja Grünbaum (2010) kuvaavat johtamisen evoluutiossa autoritäärisen kaikkietävän pomon jälkeen tulleen päinvastainen suuntaus, jossa tiiminvetäjä pyrki muodostamaan itseohjautuvia tiimejä niin, että esimiehen rooli

pyrittiin minimoimaan. Kun kokonaisvastuuta tiimin tekemisestä siirrettiin esimieheltä tiimille itselleen, aiheutui uusia ongelmia. Ilman selkeää vastuunjakoa ja esimiehen tukea perusasioista ja toimintamalleista sopiminen tiimin kesken koettiin kuluttavaksi, jolloin helposti palattiin takaisin autoritääriseen johtamiseen. Ajatus johtamisen delegoinnista ja uudenlaisesta tavasta tehdä töitä valtuuttamalla ja yhteistyössä jäi elämään. Tämän pohjalta siirryttiin seuraavaan iteraatioon johtamisessa missä jokainen tiimiläinen vastaa tavoitteiden saavuttamisessa ja valtasuhteiden merkitys väheni. Näin syntyi valmentava johtajuus, jossa yhdessä tekemällä vähän kerrallaan päästään kohti yhteistä päämäärää. (Ristikangas & Grünbaum 2010, 14–16.)

Ristikangas ja Ristikangas (2010) käsittelevät taustoja uuden johtamistavan tarpeelle tarkastelemalla työntekijöiden tulevia sukupolvia. Y-sukupolvi kyseenalaistaa hierarkiat, ei pökkuroi eikä arvota titteliä tai asemaa. Työn on oltava innostavaa, johtamisen oikeudenmukaista ja yhteistyön mukavaa. Työtä ei tehdä enää yritykselle vaan omalle tiimille. Valmentavassa johtajuudessa johtajan on tärkeää haluta ja pystyä kohtaamaan johdettavansa sekä yksilöinä että ryhmänä. On siis tärkeää pystyä olemaan läsnä ja samalla saada aikaan tuloksia. Jos ennen kvartaalitalous ajoi työnteon suorittamiseksi ja jatkuvasti ruuvin kiristämiseen, niin nyt suorittamisella ei enää ole itseisarvoa vaan tärkeintä on tehdä yhdessä päämäärätietoisesti töitä tavoitteiden saavuttamiseksi. (Ristikangas & Ristikangas 2010, 19, 40–42.)

Valmentava johtaminen on keskittynyt aiemmin pitkälti yksilöiden johtamiseen ja sen vuoksi uudemmassa kirjallisuudessa on alettu käsitellä valmentavaa tiimin johtamista. Ristikangas, Lönnroth, Ristikangas ja Ristikangas (2021) huomauttavat, että vaikka yksilön johtaminen on tärkeä ja olennainen osa valmentavan johtajuuden toteuttamista, on osattava johtaa myös tiimiä. Tiimin johtaminen eroaa yksilön johtamisesta sillä, että yksilön käytös muuttuu, kun hän toimii osana tiimiä. (Ristikangas, Lönnroth, Ristikangas & Ristikangas 2021, 13–15.)



Kuvio 3. Päätöksentekotapa yhdessäohjautuvassa tiimissä (Ristikangas ym. 2021, 78).

Ristikangas ym. (2021) kuvaavat kuviossa 3. keinulaudalla, kuinka päätösvalta jakautuu yhdessäohjautuvassa tiimissä jokseenkin tasan. Tämä ei kuitenkaan tarkoita sitä, että tiimi voisi päättää kaikista asioista itsenäisesti vaan päätöksentekoon osallistuu joukko ennalta sovittujen kriteerien perusteella. Yhdessäohjautuvuus vaatii toimiakseen selkeät pelisäännöt, milloin ja mistä asioista yksilö ja tiimi voivat tehdä päätöksiä itsenäisesti sekä milloin tarvitaan esihenkilön osallistuminen. On tärkeä muistaa, ettei esihenkilö voi välttyä päätöksenteon vastuulta ja välillä on tehtävä päätöksiä, jotka eivät miellytä kaikkia. Valmentavan tiimin johtajan vastuulla on johtaa päätöksentekoa:

1. vahvistaa yhdessä tehdyt linjaukset
2. tehdä lopullinen päätös ja ratkaista tilanteet, mikäli yhteisymmärrystä ei löydy
3. ohjata tiimiläisiä ratkaisukeskeisyyteen ja ehdotusten tekemiseen
4. päättää tärkeistä asioista, joista tiimiläiset eivät ole samaa mieltä kuten esimerkiksi budjettileikkausten kohteet ja kurinpitoprosessin mukainen menettely. (Ristikangas ym. 2021, 78–80.)



Toimiakseen tiimi tarvitsee rajat ja mikäli niitä rikotaan, on haitalliseen toimintaan puututtava. Organisaatiossa esihenkilöllä on velvollisuus johtaa ja siihen kuuluu olennaisena osana puuttuminen ei-toivottuun toimintaan. Ideaalissa tilanteessa tiimiin syntyy niin vahva kulttuuri, että ei-toivottuun toimintaan puututaan tiimin jäsenten toimesta. Tämä ei kuitenkaan poista esihenkilön puuttumisvastuuta eikä sitä, että esihenkilö on aina lopulta päävastuullinen tiimin toiminnasta. Mikäli ideaalitalanteeseen päästään ja yhteinen kulttuuri muodostuu, nopeutuu myös parempiin lopputuloksiin pääseminen ja ongelmat vähenevät. (Ristikangas ym. 2021, 315–321.)

Salminen ja Ruutu (2013) määrittelevät valmentavan esimiehen tavoitteiksi oivalluttaa, vastuuttaa ja voimaannuttaa työntekijöitä niin, että liiketoiminnan tavoitteet saavutetaan ja samalla mahdollistetaan työntekijän ammatillinen kasvu. Tavoitteena on luoda kannustava ja innovatiivinen ilmapiiri, jossa työntekijät kokevat itsensä arvostetuiksi. Valmentava johtajuus pohjautuu luottamukseen, empatiaan ja rehelliseen vuorovaikutteiseen läsnäoloon, jossa korostuu aktiivinen kuunteleminen. Valmentavaan johtajuuteen sisältyy myös ongelmanratkaisukyvykyys, vastuuttaminen sekä edistymisen seuranta. (Salminen & Ruutu 2013, luku 2.)

Vaikka Bel G. Raggad (2010) ei käytä termiä valmentava johtajuus, on hänen henkilöstöä käsittelevässä osiossaan tunnistettavissa elementtejä valmentavasta johtajuudesta. Raggad huomioi henkilöstön yhtenä tietotekniseen ympäristöön liittyvänä osa-alueena, jota tulee suojata tietoturvallisuuden näkökulmasta. Pelkkä tietoturvapolitiikan ja ohjeistuksen laatiminen ei riitä, vaan tarvitaan koulutusta ja harjoittelua. Henkilöstön tulisi olla mukana yhteistyössä parantamassa yrityksen tietoturvallisuutta jakamalla ajatuksiaan ja parannusehdotuksia. Tietoturvallisuudesta vastaavien tulisikin tehdä läheisesti yhteistyötä muun henkilöstön kanssa tiedon jakamiseksi puolin ja toisin. (Raggad 2010, 10–13.)

### 3.2 Organisaatiokulttuuri

Organisaatiokulttuuri saa henkilöstön innostumaan, turhautumaan ja lannistumaan. Kulttuuri vaikuttaa siihen, puhutaanko asioista avoimesti vai selän takana. Osallistutaanko yhdessä tekemiseen vai ollaanko itsekseen. Sitoudutaanko yhteisiin tavoitteisiin innostuneesti vai ollaanko turhautuneita ja välinpitämättömiä. Organisaatiokulttuuri ohjaa päivittäisen työntekemisen suuntaa ja keinoja, kuinka tavoitteet saavutetaan. Kulttuuri muodostaa organisaation sisäisen käsityksen, mitkä asiat ovat tärkeitä, ja mitkä eivät ja kuinka suhtaudumme muihin ihmisiin. Organisaatiokulttuuriin kuuluu näkyvä ja näkymätön osa-alue. Näkyvään kuuluu ohjeistukset, toimintamallit ja politiikat, kaikki se mikä voidaan esittää tai havaita joko kuulemalla näkemällä tai lukemalla. Näkymätön osa-alue muodostaa kulttuurista suurimman osan ja se koostuu itsestäänselvyyksistä, joita ei ole kuvattu tai välttämättä edes tiedostettu. Tämän vuoksi organisaatiokulttuuria voidaan kuvata myös jäävuorena, näemme siitä aina vain pinnalla olevan pienimmän osan. Se, minkä vuoksi organisaatiokulttuurista kannattaa olla kiinnostunut on, että ilman kulttuuria henkilöstöstä ei voi syntyä yhteisöä ja ilman toimivaa yhteisöä ei organisaatio voi tuottaa tulosta. Organisaatiokulttuurin ymmärtäminen eri organisaation tasoilla auttaa tunnistamaan, ohjaamaan ja tukemaan miten ja mihin suuntaan organisaation tulisi uudistua ja millaisia tarpeita ja mahdollisuuksia organisaatiossa on. (Kuusela 2015, 13–17.)

Korhonen ja Bergman (2019) kuvaavat kulttuurin kehittämistä elefanttimaisena tehtävänä. Organisaatiokulttuuri muuttuu vähitellen tekemisen kautta ja esihenkilöiden toimintaa tulkitaan jatkuvasti. Kaikki teot, sanat ja ilmeet vaikuttavat siihen mennäänkö kohti uutta haluttua ja tavoiteltua kulttuuria vai pysytäänkö menneissä tavoissa. Henkilöstö on hyvä ottaa mukaan organisaatiokulttuurin muutoksen suunnittelussa ja pohtia yhdessä mitkä ovat aiempien onnistumisten taustalla olevan kulttuurin tekijät, jotka kannattaa säilyttää myös tulevaisuudessa. Engelin (2018) mukaan hyväksytyt käyttäytymismallit muokkaavat organisaatiokulttuuria, mikäli huonoa käytöstä sallitaan, siitä tulee osa kulttuuria. Yrityksen johdon tulee muistaa, että muutos lähtee heistä ja vaikka johtajat tekevät loppukädessä päätökset tulisi myös henkilöstön mielipiteet huomioon. (Korhonen & Bergman 2019, 134–135; Engel 2018.)

Schein (2009) määrittelee kulttuurin olevan ryhmän omaisuutta, joka muodostuu aina, kun ryhmällä on tarpeeksi yhteistä kokemusta. Organisaatiossa kulttuurin tekee erityisen tärkeäksi se, että kulttuuri muovaa strategiaa, päämääriä ja toimintatapoja. Schein jakaa organisaatiokulttuurin kolmeen tasoon:

1. helpoiten havaittavissa oleviin artefakteihin
2. ilmastuihin arvoihin kuten dokumentaatioon
3. yhteisiin piileviin oletuksiin. (Schein 2009, 28–29, 30–36.)

Artefakteihin kuuluvat organisaation näkyvät rakenteet ja prosessit, joita voivat olla esimerkiksi tapa pukeutua (rento – muodollinen), toimistolla käyttäytyminen, jutellaanko vapaasti huoneiden ovien ollessa auki vai onko keskustelu rajautunut suljettujen ovien taakse. Tällaiset asiat voidaan havaita, mutta syytä miksi näin on ei voida tietää pelkästään sen perusteella. Kysymällä yhteisön jäseniltä miksi asiat tehdään tietyllä tavalla, voidaan selvittää ilmastuja arvoja. Ilmaistut arvot voivat olla täysin samanlaiset oli kyseessä rento matalan hierarkian organisaatio tai muodollinen käskyty- ja valvontatyyppinen organisaatio. Tämä johtuu siitä, että arvoja kuten yhteistyö, rehellisyys, asiakassuuntautuneisuus, tuotelaatu jne. voivat olla molempien organisaatioiden ilmaistuja arvoja. Esimerkiksi yhteistyön voidaan nähdä toteutuvan parhaiten yhdessä keskustelemalla vapaasti ja matalalla kynnyksellä tai niin, että yksilöt pohtivat tarkasti oman näkökulmansa itsekseen ja esittävät asiat muodollisissa tapaamisissa. Molemmilla organisaatiotyypeillä voi olla hyvin samanlaiset palkitsemis- ja kannustinmallit, jotka painottavat yksilön suoriutumista, vaikka molempien perusarvoihin kuuluu yhteistyö. Tästä ristiriitaisuudesta voidaan johtaa organisaatiokulttuurin kolmas taso yhteiset piilevät oletukset, jotka ohjaavat näkyvää käyttäytymistä. Yhteiset piilevät oletukset ovat organisaatiossa yhteisesti itsestään selvänä pidettyjä arvoja, jotka ovat muodostuneet organisaatioon ajan saatossa. Nämä arvot ovat yleensä niitä, joiden pohjalta organisaatio on menestynyt, kuten aiemmissa esimerkeissä kuvatut tavat tehdä töitä rennosti ja vapaamuotoisesti tai kurissa ja järjestyksessä muodollisesti. (Schein 2009, 30–36.)

Organisaatiokulttuurin muuttamiseksi on ymmärrettävä kulttuurin ohjaavan ihmisiä. Kulttuurin avulla yhteisön jäsenet osaavat käyttäytyä oikein omassa organisaatiossaan, jolloin työskentelystä tulee ennustettavampaa. Kulttuurin olemus pyrkii olemaan luonteeltaan pysyvää. On helpompaa toimia ennalta-arvattavassa ympäristössä missä asiat ovat vakiintuneet kuin jatkuvasti muuttuvassa kaaoksessa. Pysyvyyden vuoksi onkin tärkeää muistaa, että aina kun kulttuuria lähdetään muuttamaan, hyökätään organisaation pysyvimpien osien kimppuun. (Schein 2009, 41.)

Kulttuurin muuttaminen vaatii muutostarpeen tunnistamisen sekä löytämään motivaation muutoksen tekemiseen, sillä kulttuurin pysyvän luonteen vuoksi muutosta vastustetaan. Ei riitä, että opetellaan tekemään asioita uudella tavalla, vaan täytyy myös poisottaa vanhat tavat. Schein (2009) esittää, että lähtökohdaisesti menestyvän organisaation vakiintuneiden tapojen muuttamisen motivaatioksi tarvitaan eloonjäämistäistelun kaltaista tilaa, jolloin organisaatioon kohdistuu uhka, katastrofi tai tyytymättömyys nykyiseen toimintaan. Uhat voivat olla taloudellisia, poliittisia, teknologisia ja moraalisia tai sisäistä tyytymättömyyttä. Sisäinen tyytymättömyys tarkoittaa pelkoa, ettei organisaation sisäisiä tavoitteita tai ihanteita saavuteta, jolloin muutos on välttämätöntä. Muita uhkia yhdistää pelko siitä, ettei pärjätä kilpailijoille tai muille toimijoille joko markkinoilla tai poliittisessa toimintaympäristössä, jäädään jälkeen teknologisessa kehityksessä tai kärsitään imagollisia vahinkoja. (Schein 2009, 132–134.)

Toisena motivaation lähteenä voi olla oppimisahdistus, jolloin on tunnistettu, ettei nykyinen osaamistaso ole riittävä ja koska uutta, riittävää osaamistasoa ei ole vielä saavutettu yksilö kokee ahdistusta. Oppimisahdistus koostuu useasta pelosta, joita ovat väliaikaisen osaamattomuuden pelko, osaamattomuuden rankaisemisen pelko, henkilökohtaisen identiteetin menettämisen pelko ja ryhmän jäsenyyden menettämisen pelko. Väliaikainen osaamisen pelko on nimensä mukaisesti väliaikaista ja on yleistä muutosprosessin aikana esimerkiksi silloin, kun uutta tietojärjestelmää otetaan käyttöön eikä sen käyttö ole vielä tuttua. Yksilöt voivat myös pelätä osaamattomuudesta johtuvaa rangaistusta. Tämä ilmenee siten, että pelätään seuraamuksia, mikäli ei opita käyttämään tietojärjestelmää tarpeeksi nopeasti ja tehokkaasti, mikä puolestaan heikentää tehokkuutta.

Henkilökohtaisen identiteetin menettämisen pelko voi ilmetä henkilöillä, joilla on nykyiseen ajattelutapaan pohjautuva vahva identiteetti. Tällöin organisaation uusi tavoiteltu tapa voi muodostaa yksilölle ylitsepääsemättömän tilanteen.

Ryhmän jäsenyyden menettämisen pelkoa voidaan kokea tilanteissa, joissa yksilö olisi valmis muutosprosessiin, mutta muu ryhmä suhtautuu siihen kielteisesti. Tällaisessa tilanteessa yksilö voi pelätä joutuvansa eristetyksi pois kuulumastaan ryhmästä. (Schein 2009, 138–139.)

Oppimisahdistuksen voittamiseksi organisaation tulee luoda jäsenilleen psykologisesti turvallinen ilmapiiri, johon kuuluu

1. vastustamaton positiivinen visio – yksilön tulee uskoa, että muutos on edellytys sekä yksilön itsensä, että organisaation menestyksen kannalta. Ylimmän johdon tulee viestiä visiosta laajasti sekä noudattaa sitä itse.
2. organisaation järjestämä koulutus – muutosprosessissa vaadittavia uusia ajattelutapoja, asenteita ja taitoja tulee kouluttaa.
3. oppijan osallistuminen – erilaisille oppijoille tulee antaa mahdollisuus oppia omalla tavallaan
4. tiimien epävirallinen koulutus – organisaation sisällä ryhmillä on omat kulttuurinsa, joten on tärkeää pitää koulutusta koko ryhmälle kerrallaan, jolloin ryhmä voi muodostaa uudet normit yhdessä.
5. harjoitustilanteet, ohjaajat ja palaute – oppimiselle on varattava aikaa, resursseja ja ohjausta sekä palautetta
6. positiiviset roolimallit – mikäli uusi ajattelu- tai käyttäytymistapa on täysin uutta, voidaan tarvita esimerkkejä henkilöistä, jotka toimivat niin ja joista voidaan ottaa mallia.
7. tukiryhmät – vertaistukiryhmien avulla mahdollistetaan yhdessä oppiminen muiden samojen vaikeuksien kanssa painivien kesken
8. yhdenmukaiset järjestelmät ja rakenteet – organisaation rakenteen, palkitsemis- ja kurinpitomallin tulee olla yhteneviä tavoitteiden kanssa. Esimerkiksi mikäli tavoitteena on yhteistyön parantaminen, tulee organisaatorakenteen mahdollistaa yhteistyön tekeminen ja palkitsemismallin kannustaa yhteistyöhön yksilöiden palkitsemisen sijaan. (Schein 2009, 140–142.)

Schein johtopäätökset ovat, että muutosvastarinta on normaalia ja kuuluu muutosprosessiin. Muutosta voidaan ajaa lisäämällä eloonjäämisahdistuksen määrää, kunnes se ylittää oppimisahdistukseen liittyvät pelot ja henkilöstö pakotetaan muutokseen. Mielekkäämpänä vaihtoehtona on kuitenkin vähentää oppimisahdistusta ja luoda organisaatioon psykologisen turvallisuuden olosuhteet. (Schein 2009, 156.) Valmentava kulttuuri auttaa yksilöitä ja ryhmiä pääsemään täyteen potentiaaliinsa. Tämän mahdollistaa kulttuuri, jossa tuetaan luovuutta ja yksilö tietää saavansa tukea eikä tule tyrmätyksi uusia ajatuksia esittäessään. Yhteistyötä korostamalla ja kiinnittämällä huomiota toimintatapoihin ja arvostamiseen, osaamisen kehittämiseen sekä syventämällä vuorovaikutussuhteiden laatua voidaan saavuttaa valmentava kulttuuri. (Ristikangas & Ristikangas 2018, luku 7.)

Myönteisen tietoturvakulttuurin myötä työntekijät sisäistävät tietoturvan olevan keskeinen osa heidän työtään. Näin ollen hyvät tietoturvakäytännöt ovat osa työtapoja ja niitä on helppo noudattaa. (Paulsen & Coulson 2011, 38.) Turvallisuuskulttuuri nojaa avoimuuteen, on kannustettava henkilöstöä kertomaan havaitsemistaan huolenaiheista, uhkista ja poikkeamista ilman syyllistämistä. Näin henkilöstö uskaltaa raportoida myös tekemänsä virheet ilman pelkoa negatiivisista seuraamuksista. Keskustelun avoimuus kannustaa henkilöstöä myös kyseenalaistamaan nykyisiä toimintamalleja, jolloin voidaan yhdessä suunnitella juuri omalle organisaatiolle sopivia turvallisuuskäytänteitä. Sisäisessä viestinnässä on myös hyvä painottaa onnistumisia epäonnistumisten sijaan, esimerkiksi kuinka moni raportoi havainneensa kalasteluviestin eikä, kuinka moni lankei huijaukseen. (Traficom 2020a.)

Vaikka tekniset tietoturvakontrollit ovat olennainen osa tietoturvallisuutta, on sen toteuttamisessa enemmän kyse toimintamalleista, siitä kuinka tietoturvan toteuttaminen varmistetaan jokapäiväisessä tekemisessä. Sen sijaan, että tietoturvalisuus perustuisi yksittäisten henkilöstön jäsenten tekemiseen tulisi päästä tilanteeseen, jossa tietoturvallisuus perustuu yhteiseen toimintakulttuuriin, toimintamalleihin ja järjestelmälliseen toimintaan. (Hänninen 2020.) Raggad (2010) korostaa kestäväen turvallisuuskulttuurin merkityksen olevan keskeistä ja sen tulisi olla osa henkilöstön työskentelytapoja. Hän vertaa tietoturvallisuuteen liittyvien

toimintatapojen tärkeyttä arkipäiväiseen hygieniasta huolehtimiseen, kuten säännölliseen käsien pesemiseen. Tavoiteltuun turvallisuuskulttuuriin kuuluu tietoturvatietoisuuden ja -osaamisen jatkuva ylläpitäminen sekä henkilöstön harjoitteluun ja koulutukseen panostamisen. Näin pyritään varmistamaan, että henkilöstö toimii yrityksen tietoturvapoliitiikan mukaisesti ja noudattaa tietoturvallisia toimintamalleja kaikissa työtehtävissään. (Raggad 2010, 289–290.)

### **3.3 Tietoturvallisuuden viitekehys – ISO/IEC 27001**

ISO/IEC 27001 -standardilla voidaan osoittaa organisaation kaikille sidosryhmille organisaation sitoutumisen tietoturvallisuuden jatkuvaan parantamiseen. Standardi mahdollistaa kilpailuedun lisäksi myös organisaation sisäisesti paremman työetiikan sekä lisää tietoisuutta tietoturvallisuudesta ehkäisten tietoturvaaan liittyviä riskejä. (SGS 2023.) ISO/IEC 27001 -standardi on kansainvälinen hallinnan ja johtamisen standardi, ei tietoturvastandardi. Standardi antaa organisaatiolle riskiperusteisen viitekehysten tietoturvallisuuden kaikkien osa-alueiden johtamiseen. Onkin hyvä muistaa, ettei ISO/IEC 27001 -standardi takaa riittävää teknisen tietoturvan tasoa sillä standardi ei aseta suoria vaatimuksia esimerkiksi salasanan pituudelle vaan ainoastaan johtamisen käytäntöjä voidaan sertifioida. (Traficom 2019, 16–17.)

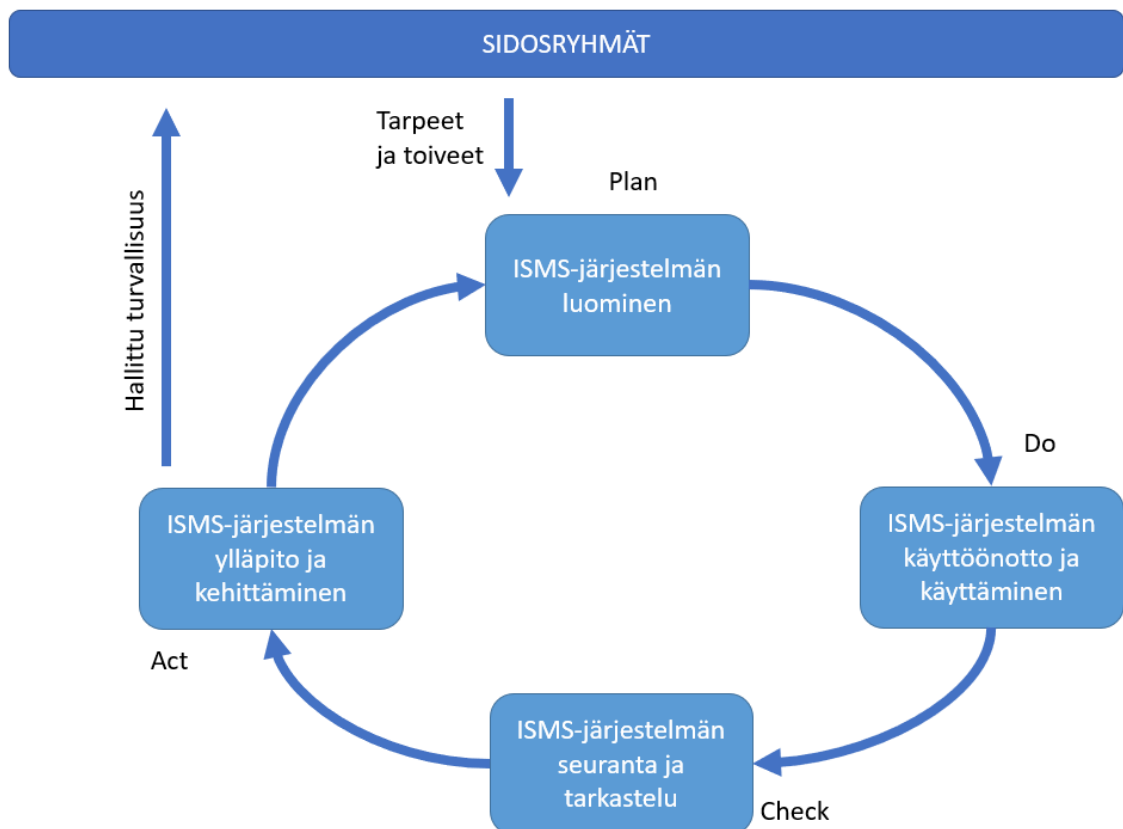
ISO/IEC 27001 -standardin tavoitteena riskienhallinnan kautta suojata tiedon luottamuksellisuutta, eheyttä ja saatavuutta sekä osoittaa sidosryhmille asianmukainen tapa hallita riskejä. Tietoturvallisuuden hallintajärjestelmä on osa organisaation prosesseja sekä hallintaa ja johtamista. Hallintajärjestelmä tulee toteuttaa organisaation omien tarpeiden mukaisesti, jolloin vaatimusten toteuttamistapaan vaikuttaa kaikki organisaation koosta, rakenteesta, tavoitteista, turvallisuusvaatimuksista ja prosesseista alkaen. Hallintajärjestelmässä on myös otettava huomioon, että nämä tekijät muuttuvat ajan kuluessa. (SFS-EN ISO 27001, 2017, 5.)

ISO 27001 -standardin tarkoituksena on määritellä tietoturvallisuuden hallinnan malli, joka perustuu jatkuvaan parantamiseen PDCA-mallin mukaisesti, kuvio 4.

Tietoturvallisuuden hallintajärjestelmä ISMS (Information Security Management System) sisältää:

1. ISMS-järjestelmän perustamisen, käyttöönoton, käyttämisen, ylläpidon, valvonnan, katselmusten sekä kehittämisen.
2. johdon vastuut ja sitoutumisen. Johdon tulee varmistaa tarvittavien resurssien saatavuus, katselmoida järjestelmän tuloksia sekä reagoida niihin ja huolehtia tietoturvatietoisuuden edistämisestä sekä jatkuvasta kehittämisestä
3. hallintajärjestelmän sisäisen auditoinnin. (Hakala, Vainio & Vuorinen 2006, 46–50.)

Myös Hakala, Vainio ja Vuorinen (2006) painottavat, ettei itse standardi aseta vaatimuksia tietoturvan tasolle tai sisällölle vaan ainoastaan, kuinka sitä suunnitellaan ja menetelmätavoille. He korostavat standardin olevan erityisen hyödyllinen tietoturvasuunnittelun näkökulmasta sillä se luo yhtenäisen ja vertailukelpoisen rakenteen hallintajärjestelmän dokumentaatiolle. (Hakala, Vainio & Vuorinen 2006, 46–50.)



Kuvio 4. PDCA-mallin mukainen prosessi (Hakala ym. 2006, 49).



### 3.3.1 ISO 27001 pakolliset vaatimukset

ISO/IEC 27001 koostuu alla esitetyistä pakollisista vaatimuksista (standardin kohdat 4–10) ja standardin liitteessä A kuvatuista hallintakeinoista. Hallintakeinoja täydentää menettelyohjeet ISO/IEC 27002:2017 jotka eivät ole pakollisia. Hallintakeinojen käyttäminen tai käyttämättä jättäminen kuvataan soveltuvuuslausunnossa. (SFS-EN ISO 27001, 2017, 9.)

#### **Organisaation toimintaympäristö**

Organisaation tulee analysoida jatkuvasti itseään ja ympäristöön sisäisiä ja ulkoisia asioita, jotka voivat vaikuttaa tietoturvallisuuden hallintaan sekä organisaation tavoitteisiin. Ulkoisiin asioihin kuuluu mm. yhteiskunnalliset ja kulttuuriset, poliittiset ja oikeudelliset, taloudelliset, teknologiset ja kilpailulliset osa-alueet. Sisäisiä osa-alueita on mm. organisaatiokulttuuri, toimintaperiaatteet, tavoitteet ja strategiat, organisaatorakenne, vastuut ja roolit sekä resurssit. Toimintaympäristön tunteminen vaatii myös sisäisten ja ulkoisten sidosryhmien tarpeiden ja odotusten ymmärtämisen sekä niiden vaikutuksen tietoturvallisuuden hallintajärjestelmään. Näiden lisäksi on määriteltävä tietoturvallisuuden hallintajärjestelmän soveltamisala kuten sovelletaanko sitä kaikkiin yrityksen tukitoimintoihin vai ainoastaan osaan. Viimeisenä osa-alueena tässä vaatimuksessa on tietoturvallisuuden hallintajärjestelmän ylläpitäminen ja jatkuva parantaminen. (SFS-EN ISO 27003, 2017, 7–12.)

#### **Johtajuus**

Ylimmän johdon tulee osoittaa johtajuutta ja sitoutumista tietoturvallisuuden hallintajärjestelmän suhteen. Tämä tarkoittaa sitä, että ylimmän johdon tulee ohjata tietoturvallisuuden hallintajärjestelmää kuin muitakin organisaation alueita. Tämä pitää sisällään ylimmän johdon laatiman tietoturvapolitiikan ja tietoturvatavoitteiden asettamisen, jotka ovat yhdenmukaisia organisaation muun strategian kanssa. (SFS-EN ISO 27003, 2017, 12–14.)

Tietoturvallisuuden hallintajärjestelmään kuuluvat vaatimukset ja hallintakeinot tulee sovittaa yhteen organisaation prosesseihin, joiden omistajien tulee viedä vaatimukset käytäntöön. Ylimmän johdon tehtävänä on varmistaa, että muutosprosessista vastaavat roolit saavat riittävästi resursseja voidakseen toteuttaa hallintajärjestelmää vaikuttavasti sekä tukea muutosprosessia muutosvastarintaa kohdatessa. Lisäksi tietoturvan näkökulmasta tärkeimmät roolit on tunnistettava ja näiden roolien vastuut sekä valtuudet on viestittävä koko organisaatiolle. Näille vastuurooleille kuuluvia toimintoja ovat esimerkiksi hallintajärjestelmän toteuttaminen, ylläpito, parantaminen ja raportointi sekä koordinointi. Tietoturvariskien arviointi ja käsittely, tietoturvaprosessien suunnittelu, tietoturvallisuuden hallintakeinojen määrittely sekä hallintajärjestelmän katselmointi, tietoturvahäiriöiden hallinta, tietojen, prosessien, riskien ja suojattavan omaisuuden omistajat. (SFS-EN ISO 27003, 2017, 14–16.)

### **Suunnittelu**

Suunnittelu kattaa riskien ja mahdollisuuksien käsittelyn, joihin kuuluvat yleiset tietoturvallisuuden hallintajärjestelmän kokonaisuuden toteuttamisen kannalta liittyvät olennaiset riskit ja mahdollisuudet sekä hallintajärjestelmään kuuluviin tietoihin liittyvät tietoturvariskit luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta sekä tietoturvatavoitteiden määrittelyn. Tietoturvariskien ja mahdollisuuksien arvioinnin ja käsittelyn tulee olla perusteellista, yksityiskohtaista ja sen vaikuttavuutta on pystyttävä arvioimaan. Riskien käsittelylle on luotava yhdenmukainen prosessi, jotta tulokset ovat päteviä ja verrattavissa olevia. Käsittelyprosessiin kuuluu riskikriteerien laatiminen, riskitason määrittely, tunnistaminen, analysointi, arviointi ja hyväksymiskriteerit. (SFS-EN ISO 27003, 2017, 16–25.)

Tietoturvatavoitteiden on tarkoitus auttaa organisaatiota saavuttamaan strategisia tavoitteita tietoturvapoliittikkansa mukaisesti. Tietoturvatavoitteiden määrittelyssä on otettava huomioon organisaation toimintaympäristö ja sidosryhmät, riskien arvioinnin ja käsittelyn lopputulokset, jotka ohjaavat tavoitteiden tarkoituksenmukaisuutta. Tavoitteet tulisi mahdollisuuksien mukaan olla mitattavissa, jotta tiedetään, päästiinkö tavoitteisiin. Tavoitteiden saavuttamiseksi vaaditut

tekijät tulee myös määritellä kuten kuka on vastuussa, mitä resursseja tarvitaan, mitä ja miten tehdään ja milloin työ saadaan valmiiksi ja kuinka lopputuloksia arvioidaan. (SFS-EN ISO 27003, 2017, 25–27.)

### **Tukitoiminnot**

Organisaation on määriteltävä ja annettava resurssit tietoturvallisuuden hallintajärjestelmän perustamiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen. Resurssit voivat esimerkiksi olla henkilöitä, toimenpiteisiin tarvittavaa aikaa, taloudellisia resursseja ja tietoa. Henkilöstöresurssien pätevyysvaatimukset tulee määritellä, minkä perusteella voidaan esimerkiksi päättää, kouluttaanko organisaation nykyistä henkilöstöä vai palkataanko tarvittava osaaminen ulkopuolelta. (SFS-EN ISO 27003, 2017, 27–29.)

Tukitoiminnot pitävät sisällään myös vaatimuksen varmistaa henkilöstön tietoisuuden tietoturvapoliitikasta sekä omasta osuudestaan tietoturvallisuuden hallintajärjestelmän vaikuttavuuteen. Lisäksi henkilöstön tulee ymmärtää ja hyväksyä mahdolliset kielteiset seuraamukset, jotka kohdistuvat joko tietoturvallisuuteen tai henkilöön itseensä, mikäli tietoturvallisuuden hallintajärjestelmän vaatimuksia ei noudateta. (SFS-EN ISO 27003, 2017, 29–30.)

Organisaatio määrittelee itse, kuinka se viestii tietoturvallisuuden hallintajärjestelmään liittyvistä asioista. Viestinnän tarkoitus on varmistaa, että kaikki tasot niin sisäisissä kuin ulkoisissa sidosryhmissä ovat tietoisia tietoturvallisuuden hallintajärjestelmän tavoitteista ja vaatimuksista, sillä tarkkuudella kuin se viestittävälle kohderyhmälle on tarpeellista. SFS-EN ISO 27003, 2017, 30–32.)

Tietoturvallisuuden hallintajärjestelmään liittyvä tieto on dokumentoitava niiltä osin kuin organisaatio pitää itse tarpeellisena hallintajärjestelmän vaikuttavuuden kannalta. Tieto on jaettava valtuutetuille sidosryhmille ja sen on oltava saatavilla tarvittaessa. Dokumentoitu tieto tulee luokitella, merkitä ja käsitellä asianmukaisesti sekä pitää huoli siitä koko tiedon elinkaaren ajan. Organisaation on myös määriteltävä mitä tiedolle tehdään, kun sen säilyttämiselle ei ole enää perusteita. (SFS-EN ISO 27003, 2017, 32–35.)

## **Toiminta**

Tietoturvavaatimusten ja -tavoitteiden saavuttamiseksi on suunniteltava, toteutettava ja ohjattava prosesseja, joihin kuuluu esimerkiksi johdon katselmointi, sisäinen auditointi, tietoturvariskien käsittely kokonaisuudessaan sekä ulkoisten prosessien kuten ulkoistettujen palveluiden hallinta. Toiminnassa on otettava huomioon esimerkiksi dokumentoidun tiedon kerääminen tietoturvariskien käsittelysuunnitelman mukaisesti tehdystä arvioinnista, käsittelystä ja tulosten läpikäynnistä syntyvien dokumenttien säilyttäminen, jotta voidaan arvioida toiminnan vaikuttavuutta ja jatkuvaa parantamista. (SFS-EN ISO 27003, 2017, 35–38.)

## **Suorituskyvyn arviointi**

Tietoturvallisuuden tasoa ja tietoturvallisuuden hallintajärjestelmän vaikuttavuutta tulee seurata, mitata, analysoida ja arvioida. Seurannalla ja mittaamisella varmistetaan, että organisaatio on päässyt asettamiinsa tietoturvatavoitteisiin. Seurannan ja mittaamisen lähtökohtana on organisaation määrittelemän tietotarpeen täyttäminen. Mitattavat attribuutit on hyvä suunnitella ja rajata tarkasti, ettei mitata epäollennaista tai jopa vääriä asioita eikä lisätä työmäärää tarpeettomasti, joka voisi johtaa kasvaviin kustannuksiin ja väärin tuloksiin. Mittareina voidaan käyttää esimerkiksi suorituskykymittareita tai vaikuttavuusmittareita. Suorituskykymittareina voidaan käyttää esimerkiksi henkilömäärää, välitavoitteiden saavuttamista tai tietoturvallisuuden hallintakeinojen toteuttamistasoa. Vaikuttavuusmittareilla ilmaistaan kuinka suunnitellut toimet ovat vaikuttaneet organisaation tietoturvatavoitteisiin. (SFS-EN ISO 27003, 2017, 38–39.)

Suorituskykyä arvioidaan myös suorittamalla sisäistä auditointia sekä johdon katselmointeja. Sisäisessä auditoinnissa organisaatio toteuttaa itse suunnittelemansa auditointiohjelman mukaisesti, kuinka tietoturvallisuuden hallintajärjestelmän sekä organisaation omia vaatimuksia noudatetaan. Organisaation omia vaatimuksia ovat esimerkiksi lakien ja sopimuksien vaatimukset sekä samoin kaikki organisaation omat ohjeistukset, vaikka ne olisivat tietoturvallisuuden hallintajärjestelmään kuulumattomia. Sisäisen auditoinnin suorittajille on

määriteltävä ja varmistettava pätevyys. Sisäisessä auditoinnissa voidaan havaita poikkeamia, riskejä sekä mahdollisuuksia. Poikkeamat tulee kuvata syineen ja korjaussuunnitelmineen, että korjaajineen. Auditointien raportit ja tulokset tulee toimittaa ylimmälle johdolle. (SFS-EN ISO 27003, 2017, 40–42.)

Johdon katselmuksessa ylimmän johdon on tarkoitus varmistaa tietoturvallisuuden hallintajärjestelmän jatkuva soveltuvuus, tarkoituksenmukaisuus ja vaikuttavuus. Tärkeimpiä tietolähteitä johdon katselmointiin ovat aiemmin mainitut mittarit, riskien arviointien tulokset sekä sisäisten auditointien tulokset. Johdon katselmointi kaikkiin tietoturvallisuuden hallintajärjestelmän osa-alueisiin tulee tehdä vähintään kerran vuodessa ja useammin mikäli hallintajärjestelmä on vasta luotu tai ollut vain vähän aikaa käytössä. Tuloksista tulisi käydä ilmi päätökset jatkuvan parantamisen mahdollisuuksista sekä mahdollisista muutostarpeista tietoturvallisuuden hallintajärjestelmään. (SFS-EN ISO 27003, 2017, 42–44.)

### **Parantaminen**

Parantamiseen kuuluu poikkeamiin reagointi, arviointi sekä tarvittavien korjaavien toimenpiteiden suorittaminen. Poikkeama muodostuu, mikäli tietoturvallisuuden hallintajärjestelmän vaatimuksia ei täytetä. Vaatimuksia voi asettaa ISO/IEC 27001 -standardi, lait ja sopimukset sekä organisaation omat tietoturvallisuuden hallintajärjestelmässä esitetyn vaatimukset ja hallintakeinot. Poikkeama voi olla esimerkiksi, että henkilöstö toimii tietoturvapoliitiikan vastaisesti tai ettei toimittaja noudata sopimuksessa sovittuja asioita. Jatkuva parantaminen on ISO/IEC 27001 -standardin kantava ajatus. Tietoturvallisuuden hallintajärjestelmä ei ole koskaan täydellinen, joten sitä voidaan aina parantaa. Jatkuvan parantamisen tavoitteena on pitää organisaatio tietoisena toimintaympäristön ja sidosryhmien muutoksista ja vaatimuksista, minkä perusteella voidaan arvioida tietoturvallisuuden hallintajärjestelmän soveltuvuutta, vaikuttavuutta, yhteensopivuutta ja ajantasaisuutta organisaation tavoitteisiin nähden. (SFS-EN ISO 27003, 2017, 44–48.)

### 3.3.2 Tietoturvan määritelmä

Tietoturvalla on kolme tavoitetta, jota yleisesti kuvataan CIA-mallilla tai suomeksi LES-mallilla. Kirjainlyhenne muodostuu sanoista Confidentiality (Luotettavuus), Integrity (Eheys) ja Availability (Saatavuus). Tiedon luottamuksellisuu-  
della tarkoitetaan sitä, että tiedot tulee suojata niin ettei niihin pääse käsiksi ulkopuoliset henkilöt eli vain ne henkilöt, joilla on oikeus päästä tietoon saavat käsitellä niitä. Tiedon eheyden varmistamisella taataan, ettei tietoihin kohdistu oikeudettomia muutoksia. Oikeudettomia muutoksia ovat esimerkiksi tilanne, jossa työntekijällä on pääsy omiin palkanmaksutietoihin, jolloin hän voisi muuttaa hänelle maksettavaa palkkaa, hakkerien pääsy muokkaamaan verkkosivujen sisältöä tai tietojärjestelmän sisällä tapahtuva ohjelmistovirhe, joka muokkaa tietoja virheellisesti. Tiedon saatavuus takaa sen, että tietoja päästään käsittelemään tarvittaessa. Saatavuuteen liittyvät ongelmat ovat yleensä teknisiä ja täydellisen saatavuuden saavuttaminen voi olla jopa mahdotonta. Esimerkiksi pankit panostavat verkkopankkijärjestelmien toimintaan ja vikasietoisuuteen suuria summia rahaa, mutta siitä huolimatta palvelut eivät aina toimi. (Järvinen 2022, 13–15.)

Hakala, ym. (2006) sekä Raggad (2010) kuvaavat CIA-mallin klassiseksi tiedon arvoon perustuvaksi määrittelyksi, joka on nykyään riittämätön sillä se ei huomioi tiedon tuottajan tai omistajan identiteettiä eikä huomioi laitteistojen tai tietojen tietoliikennejärjestelmän arvoa. Tämän vuoksi kolmen klassisen määritelmän osa-alueen luottamuksellisuus, saatavuus/käytettävyys ja eheys lisäksi tulee käyttää myös kiistämättömyyttä (non-repudiation) sekä pääsynvalvontaa (authentication). Kiistämättömyydellä pyritään takaamaan tietojärjestelmän tietoja käyttävän ja tallentavan käyttäjän henkilöllisyys, niin että tietojen alkuperä tai tietojen käyttäminen voidaan todentaa. Kiistämättömyydellä on tärkeä rooli esimerkiksi oikeustapauksissa, joissa käyttäjän tekemät toimet tulee pystyä todentamaan luotettavasti. Pääsynvalvonnalla tarkoitetaan menetelmiä, kuten käyttäjän tunnistamista käyttäjätunnuksen ja salasanan avulla. Pääsynvalvonnalla on tarkoitus rajata pääsy esimerkiksi organisaation tietojenkäsittelyinfrastruktuuriin, johon kuuluu muun muassa organisaation tietoliikenneyhteydet ja laitteet.

Tietojenkäsittelyinfrastruktuurin käytön rajoittaminen on olennaista sillä, mikäli käyttäjät suorittavat omia henkilökohtaisia toimintojaan organisaation verkossa se voi aiheuttaa ongelmia niin käytettävyyden kuin eheyden ja luottamuksellisuuden suhteen. (Hakala, ym. 2006, 5–6; Raggad 2010, 22–23.)

### 3.3.3 Tietoturvallisuuden osa-alueet ja ISO 27001:2017 hallintakeinot

Hakala, ym. (2006) jaottelevat tietoturvallisuuden useampaan paremmin hallittavaan osa-alueeseen. Ensimmäinen osa-alue on **hallinnollinen turvallisuus**, joka varmistaa tietoturvan kehittämisen ja johtamisen. Tähän sisältyy yhteydenpito sekä sisäisiin ja ulkoisiin sidosryhmiin kuten organisaation omien turvallisuudesta vastaavien elimien sekä viranomaisten kanssa. Yhteydenpidon lisäksi hallinnolliseen turvallisuuteen kuuluu vaikutustenarviointi erilaisten sopimusten ja lainsäädännön vaikutuksista organisaation tietoturvakäytäntöihin. Toinen osa-alue on **fyysinen turvallisuus**, joka suojaa tiloja, kuten toimistoja ja palvelinsaleja, erilaisilta fyysisiltä uhilta. Näihin uhkiin kuuluu muun muassa suojautuminen vesivahingoilta, tulipaloilta, tiloihin murtautumiselta, ilkivallalta sekä sähkö- ja lämmitysjärjestelmien toimintahäiriöihin varautuminen. Kolmantena osa-alueena on **henkilöturvallisuus**, joka kattaa laajasti kaikki ne toimet, joilla varmistetaan tietojärjestelmien käyttäjien toimintakyky. Tämä sisältää käyttäjien kouluttamisen, käyttäjien oikeuksien ja vastuiden määrittelyn sekä taustatietojen tarkistamisen. (Hakala, ym. 2006, 10–12.)

Neljäs osa-alue, **tietoaineistoturvallisuus**, käsittää tiedon elinkaaren hallintaan kuuluvat toimenpiteet, kuten tietojen säilyttämisen, varmuuskopioinnin, palauttamisen sekä tuhoamisen, kun tietoja ei enää ole tarpeellista säilyttää. Viidennen osa-alueen muodostaa **ohjelmistoturvallisuus**, joka pitää sisällään ohjelmistoversioiden ja lisenssien hallinnan sekä ohjelmistojen testaamisen ja varmistamisen. Tavoitteena on taata, että ohjelmistot ovat käyttötärpeeseensa soveltuvia, luotettavia ja virheettömiä sekä yhteensopivat muiden tietojärjestelmien kanssa. Kuudes osa-alue, **laitteistoturvallisuus**, vastaa organisaation tietojärjestelmiin

kytkettävien laitteiden turvallisuudesta, elinkaarenhallinnasta sekä yhteensopivuudesta. Lopuksi **tietoliikenneturvallisuus** turvaa organisaation tietoliikennetarkaisut, kuten sisä- ja ulkoverkot ja viestintäjärjestelmät. (Hakala, ym. 2006, 10–12.)

Alla kuvattu, kuinka ISO 27001:2017 käsittelee pakollisten vaatimusten lisäksi edellä mainittuja Hakalan ym. (2006) kuvaamia osa-alueita hallintatavoitteiden ja -keinojen viiteluettelossa liitteessä A. Liite A on yhtenevä ISO/IEC 27002:2017 menettelyohjeiden kanssa (ISO 27001, 2017, 15).

**Hallinnollinen turvallisuus:** A.5-A.6 Tietoturvapoliittikat ja Tietoturvallisuuden organisointi. Näihin kuuluu tietoturvapoliittikat ja niiden katselmointi, sisäisen organisaation tietoturvaroolien ja -vastuiden määrittely, tehtävien eriyttäminen, yhteydet viranomaisiin ja osaamisyhteisöihin sekä tietoturvallisuuden projektinhallinnassa. (ISO 27001, 2017, 15.)

**Fyysinen turvallisuus:** A.11 Fyysinen turvallisuus ja ympäristön turvallisuus, johon kuuluu turva-alueiden määrittely, kulunvalvonta, toimistojen, tilojen ja laitteistojen suojaus ulkoisia ja ympäristön aiheuttamia uhkia vastaan, turva-alueilla työskentelyn sekä toimitus- ja kuormausalueet. (ISO 27001, 2017, 19–20).

**Henkilöturvallisuus:** A.7 Henkilöstöturvallisuus, johon kuuluu ennen työsuhteen alkua taustatarkistus, työsuhteen ehdot, joissa on otettu huomioon ja eritelty työntekijöiden ja organisaation vastuut tietoturvallisuudesta. Johdon vastuut työsuhteen aikana, tietoturvatietoisuuden ylläpitäminen ja siihen liittyvän opastuksen ja koulutuksen järjestäminen sekä muodollisen kurinpitoprosessin ylläpitäminen. Työsuhteen päättyessä on määriteltävä millaiset vastuut ja velvollisuudet työntekijälle jäävät voimaan. (ISO 27001, 2017, 16.)

**Tietoaineistoturvallisuus:** A.8. Suojattavan omaisuuden hallinta, sisältää tietojen luokittelun sekä tietovälineiden käsittelyn. Suojattava omaisuus on



luetteloitava ja luetteloa on ylläpidettävä. Suojattavalla omaisuudella on oltava omistaja, joka määrittelee suojattavan omaisuuden hyväksyttävän käytön ja huolehdittava prosessi kuinka suojattava omaisuus palautetaan esimerkiksi työsuhteen päättyessä. Tiedot on luokiteltava, merkittävä ja suojattavan omaisuuden käsittelystä on oltava ohjeistus, joka ottaa kantaan onko ja miten siirrettäviä tietovälineitä hallitaan sekä kuinka ne hävitetään. Tietoaineistoturvallisuuteen kuuluu myös A.12.3. varmuuskopiointi. (ISO 27001, 2017, 17,21.)

**Ohjelmistoturvallisuus:** Ohjelmistoturvallisuuteen ISO 27001:2017 ottaa kantaa useammassa kohdassa kuten A.8. suojattavan omaisuuden hallinta, joka kattaa myös lisenssit, A.12.5. tuotantokäytössä olevien ohjelmistojen hallinta ja A.14 järjestelmien hankkiminen, kehittäminen ja ylläpito. (ISO 27001, 2017, 17,22–24).

**Laitteistoturvallisuus:** A.11.2 laitteet, joka sisältää laitteiden sijoittamisen ja suojaamisen tunkeutumista ja ympäristöuhkia vastaan, peruspalveluiden varmistamisen kuten sähkökatkoilta ja muilta vioilta suojautumisen, kaapeloinnin turvallisuuden, laitteiden huollon sekä poistamisen, määriteltävä ohjeistus kuinka varmistetaan toimitilojen ulkopuolelle vietävien laitteiden turvallisuus ja kuinka ilman valvontaa jäävät laitteet suojataan. (ISO 27001, 2017, 20).

**Tietoliikenneturvallisuus:** Sisältyy A.13 viestintäturvallisuuteen, joka sisältää verkon hallinnan ja verkkopalvelujen turvaamisen ja verkkosegmentoinnin sekä tietojen siirtämisen periaatteet. (SFS-EN ISO 27001, 2017, 22–23).

ISO 27001 -standardin tämän hetken uusin versio 2022 jaottelee liitteen A hallintakeinot tiiviimmin neljän pääotsikon alle:

1. organisaatioon liittyviin hallintakeinoin
2. henkilöstöön liittyviin hallintakeinoin
3. fyysisiin hallintakeinoin
4. teknologisiin hallintakeinoin. (SFS-EN ISO 27002:2022, 2–4).

Vanhempi versio vuodelta 2017 sisältää neljätoista pääkohtaa:

1. tietoturvapoliitikat
2. tietoturvallisuuden organisointi
3. henkilöstöturvallisuus
4. suojattavan omaisuuden hallinta
5. pääsynhallinta
6. salaus
7. fyysinen turvallisuus ja ympäristön turvallisuus
8. käyttöturvallisuus
9. viestintäturvallisuus
10. järjestelmien hankkiminen, kehittäminen ja ylläpito
11. suhteet toimittajiin
12. tietoturvahäiriöiden hallinta
13. liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia
14. vaatimustenmukaisuus. (SFS-EN ISO 27002:2017, 2–3.)

## **4 Kehittämistyön tutkimusmenetelmät ja toteutus**

Ihmistieteissä tutkimusmenetelmät määritellään tyypillisesti laadulliseen eli kvalitatiiviseen tutkimukseen ja kvantitatiiviseen eli määrälliseen tutkimukseen (Kallinen & Kinnunen, 2023). Hirsjärvi, Remes ja Sajavaara (2009) kuvaavat laadullista tutkimusta todellista elämää heijastavana. Siihen kuuluu moninaisia toisiinsa liittyviä tapahtumia, jotka vaikuttavat toisiinsa muodostaen perusteet, joiden avulla tutkimuksen kohdetta tarkastellaan kokonaisvaltaisesti. Lopputuloksesta ei voida tehdä yleistystä vaan se on tutkittavaan aikaan ja paikkaan sidottua tietoa, jota värittää tutkijan arvot sekä tutkijan oma tietämys. Tämän vuoksi perinteisessä mielessä tutkimus ei ole täysin objektiivista, sillä tutkija ei voi täysin poissulkea omia arvojaan, minkä lisäksi tutkimuksen lähtökohtiin vaikuttaa tutkijan oma tietämys aiheesta. (Hirsjärvi, Remes & Sajavaara 2009, 161.)

Laadullisessa tutkimuksessa pyritään kuvaamaan ja ymmärtämään tutkittavaa ilmiötä sekä antamaan sille mielekäs teoreettinen tulkinta, eikä tuottamaan tilastollista tietoa, josta voidaan tehdä yleistyksiä. Tämän vuoksi on tärkeää kerätä tietoa henkilöiltä, jotka tietävät aiheesta paljon tai heillä on siitä muuten kokemusta. Onkin tärkeää, että tutkija perustelee syyt, miksi haastatteluun valitut tiedonantajat ovat tarkoituksenmukaisia ja harkittuja tutkimuksen onnistumisen kannalta. (Tuomi & Sarajärvi 2018, 98.)

Tässä opinnäytetyössä aiheen määrittämisen jälkeen perehdyttiin valmentavaan johtajuuteen, tietoturvallisuuden hallintaan ja organisaatiokulttuuriin liittyvään kirjallisuuteen teoreettisen viitekehyksen muodostamiseksi. Teorian ja tutkimuskysymysten pohjalta muodostettiin teemahaastatteluun teemat sekä apukysymykset. Teemahaastatteluun valittujen haastateltavien valinta pyrittiin toteuttamaan, niin että saatiin hyvä läpileikkaus koko organisaatiosta ja ettei aineisto paisu liian suureksi. Haastattelut toteutettiin Microsoft Teams-tapaamisina, jotka nauhoitettiin litterointia varten. Vastaajien anonymiteetin suojaamiseksi aineistoissa ei käsitellä haastateltavien nimiä missään kohdassa vaan heidät on nimetty haastattelujärjestyksen mukaan H1, H2, H3, H4, H5 ja H6. Haastattelut litteroitiin ja aineistolle tehtiin sisällönanalyysi, minkä perusteella saatiin tulokset sekä kehitysehdotukset jatkolle.

#### **4.1 Teemahaastattelu**

Yksi laadullisen tutkimuksen käytetyimmistä tiedonkeruumenetelmistä on teemahaastattelu, siinä haastateltava keskustelutetaan tutkittavaan ilmiöön liittyvistä asioista. Haastattelu etenee haastateltavan ehdoilla ja hän saa vapaasti kertoa aiheeseen liittyen tutkittavasta ilmiöstä. Tutkijan roolina on tehdä tarkentavia kysymyksiä ja pitää keskustelu tutkittavassa aiheessa. Tutkijalla tulee olla riittävät ennakkotiedot tutkittavasta aiheesta pystyäkseen laatimaan teemat haastattelun rungoksi. Teemahaastattelu etenee yleisestä yksityiskohtaiseen, jolloin haastattelu aloitetaan yleisemmällä kysymyksellä ja keskustelun edetessä edetään kohti yksityiskohtaisempia tietoja, kuin kuorisi sipulia kerros kerrallaan, kunnes lopulta päästään ytimeen. (Kananen 2014, 76–77.)

Teemahaastattelun aiheet koostetaan teemoista, joilla pyritään kuvaamaan tutkittavan aihe niin, että tutkija ymmärtää, millaisesta ilmiöstä on kyse. Teemahaastattelussa tutkija keskustelee tutkittavan kohteen kanssa valitusta aiheesta, niin, että kohde saa vastata aiheeseen mahdollisimman vapaasti. (Kallinen & Kinnunen 2022.) Haastattelun etu verrattuna kyselylomakkeeseen on joustavuus. Haastattelussa kysymyksiä voidaan tarvittaessa toistaa ja selventää sekä tarkentaa niiden sisältöä keskustelemalla haastateltavan kanssa. Teemahaastattelussa kysymysten teemat perustuvat tutkimuksen viitekehykseen eli tutkittavasta tiedosta etukäteen tiedettyihin tietoihin. (Tuomi & Sarajärvi 2018, 85–88.)

Tässä opinnäytetyössä haastatteluiden teemat muodostettiin tutkimuskysymysten pohjalta liite 1. Haastateltaville lähetettiin kutsu sähköpostitse liite 2, jossa kuvattiin haastattelun tarkoitus. Kutsussa kerrottiin myös, kuinka haastattelussa kerättyä aineistoa käsitellään, pyydettiin lupa haastattelun tallentamiseen ja annettiin mahdollisuus esittää lisäkysymyksiä haastatteluun liittyen. Haastatteluun valikoitui kuusi henkilöä, joista kaksi toimii esihenkilöasemassa. Ensimmäinen haastattelu oli harjoitushaastattelu. Harjoitushaastattelu sujui hyvin eikä sen perusteella haastattelurunkoon tai kysymyksiin tarvinnut tehdä kuin pieniä tarkennuksia, joten myös harjoitushaastattelun aineistoa hyödynnettiin opinnäytetyössä. Haastattelut pidettiin Microsoft Teams -etätapaamisina ja ne nauhoitettiin, niin että haastateltava ja haastattelija pitivät kameran päällä.

Haastattelut toteutettiin kahden työviikon aikana ja litteroinnit tehtiin seuraavina viikonloppuina. Aikaa litterointiin kului noin kuusi tuntia per haastattelu. Videotalenteet katsottiin ensin puolitetulla nopeudella, jolloin haastattelua pystyi litteroimaan suurimmaksi osaksi puhuttua nopeutta. Litteroinnin ensimmäisen version jälkeen videotallenne katsottiin puolitoistakertaisella nopeudella kaksi kertaa peräkkäin, jonka yhteydessä korjattiin kirjoitusvirheet. Litteroinnin tarkkuudeksi valikoitui sanatarkkaa litterointia yleisempi taso, niin että osa ilmaisun sisällön kanalta turhista ja tarpeettomista fraaseista jätettiin pois.

## 4.2 Sisällönanalyysi

Aineistolähtöisen sisällönanalyysin eteneminen jaetaan kolmeen osaan: aineiston pelkistäminen (redusointi), aineiston ryhmittely (klusterointi) ja teoreettisten käsitteiden luominen (abstrahointi). Ennen analysoinnin aloittamista on määriteltävä analyysiyksikkö, joka voi olla yksittäisestä sanasta useamman lauseen sisältämään ajatuskokonaisuuteen. Analyysiyksikön määrittelyyn vaikuttaa tutkimustehtävä sekä tutkittava aineisto. Aineiston pelkistämisen tarkoituksena on poistaa aineistosta kaikki tutkimuksen kannalta epäolennainen tieto. Aineistoa pelkistäessä sitä voidaan myös tiivistää yhdistämällä samaa tarkoittavia ilmaisuja toisiinsa, jolloin alkuperäisilmauksista muodostetaan pelkistettyjä ilmauksia. Lista pelkistetyistä ilmauksista luo pohjaa seuraavalle vaiheelle eli aineiston ryhmittelylle. (Tuomi & Sarajärvi 2018, 122–123.)

Aineistojen ryhmittelyssä aineistoa tiivistetään käymällä alkuperäisilmaukset läpi etsimällä niistä samankaltaisuuksia sekä eroavaisuuksia kuvaavia käsitteitä, jotka ryhmitellään ja yhdistetään omiksi luokikseen, joista muodostuu alaluokkia. Alaluokat luokitellaan tutkittavan ilmiön ominaisuuden, piirteen tai käsityksen mukaan ja nimetään sisältöä kuvaavasti. Yhdistelmällä ja ryhmittelemällä aineistoa sen sisällön mukaan alaluokista johdetaan yläluokkia, yläluokista pääluokkia ja pääluokista yhdistäviä luokkia, jolloin aineisto tiivistyy sillä jokainen, yksittäinen tekijä sisältyy yleisempiin käsitteisiin. (Tuomi & Sarajärvi 2018, 123–125.)

Aineiston ryhmittelyn jälkeen se käsitteellistetään eli abstrahoidaan. Tässä vaiheessa aineistosta erotetaan tutkimuksen kannalta olennainen tieto, jonka perusteella voidaan muodostaa teoreettisia käsitteitä. Käsitteellistämisessä edetään alkuperäisilmauksista kohti teoreettisia käsitteitä ja johtopäätöksiä. Luokkia yhdistetään mahdollisimman pitkälle ottaen huomioon aineiston sisältö. Käsitteellistämisen avulla muodostetaan kuvaus tutkimuskohteesta, jossa teoriaa ja johtopäätöksiä vertaillaan alkuperäisaineistoon. Tämän pohjalta syntyy uutta teoriaa. (Tuomi & Sarajärvi 2018, 125–127.)

Tässä opinnäytetyössä litteroitu aineisto käytiin läpi siten, että Microsoft Word -tekstitiedostoon luotiin kahden sarakkeen taulukko, jonka vasempaan sarakkeeseen syötettiin alkuperäisilmaukset ja oikeanpuoleiseen sarakkeeseen lisättiin koodi kuten 'roolit' mikäli haastateltava kertoi organisaation roolitukseen liittyvistä asioista. Tällä tavalla käytiin ensimmäiset kolme haastatteluaineistoa läpi. Kolmen haastatteluaineiston koodit kopioitiin uuteen tekstitiedostoon ja niistä alettiin etsiä yhdenmukaisuuksia ja eroavaisuuksia sekä samanlaisia koodeja yhdistettiin toisiinsa. Työn edetessä tarkennettiin koodauksen tasoa esimerkiksi 'Roolit:Vastuut' sekä lisättiin käytössä olevat koodit Microsoft Excel -laskentataulukon muistilistaksi. Seuraavaksi käytiin loput kolme haastatteluaineistoa läpi ja lisättiin niistä ilmenneet uudet koodit taulukkoon. Yksilöllisiä koodeja muodostui lopulta 54 kappaletta.

Koodien avulla alkuperäistekstistä pystyttiin hakemaan kohdat, joissa aihealuetta käsiteltiin ja josta muodostettiin pelkistetyt ilmaukset. Osassa pelkistettyjen ilmausten käsittelyä käytin apuna ChatGPT 3.5-tekoälyä. Tekoälylle annettiin tehtäväksi tiivistää ja selkeyttää alkuperäisilmausta antamalla syötteeksi kysymys ja alkuperäisilmaus. Tekoälyä käytettiin helpottamaan laajempien vastausten sisällön jäsentelyä ja siinä käyttötapauksessa se toimi hyvin. Tekoälyn vastauksia verrattiin itse muodostettuun pelkistettyyn ilmaukseen, jonka perusteella pelkistettyä ilmausta tarkennettiin. Tekoälylle ei missään vaiheessa annettu yksilöivää tietoa tai muuta salassa pidettävää tietoa. Kuvassa 1. esitetty esimerkki tekoälyn käytöstä:

**You**

Tiivistä ja selkeytä tätä ajatusta joka on vastaus organisaation tapaan viestiä tietoturvasta: puhuminen tietoturvakulttuurista näin yleisemmin, että mitä me vaaditaan ja miksi nämä ovat tärkeitä meidän asiakkaille tai semmoiselle että meidän oma palvelutuotanto ei vaarannu tai tässä ei vaarantuisi vaikka meidän maine tai tietosuoja ja sitä kautta niin kuin tulisi vaikutuksia vaikka meihin niin ehkä semmoinen keskustelu on jäänyt pikkuisen taka-alalle. Tietoturvasta keskustelu on paljon sitä niin kuin sitä teknologia vetoista vielä. Puhutaan virustorjunnasta ja roskapostisuodattimista ja teknologioista MFA ja kaiken näköiset valvontatyökalut ja ne mutta sitten taas hallinnollisempi näkemys tietoturvaan on jäänyt vähän taka-alalle.

**ChatGPT**

Organisaation tapa viestiä tietoturvasta on ollut pääasiassa teknologiapainotteista, keskittyen virustorjuntaan ja teknisiin työkaluihin kuten MFA:han ja valvontajärjestelmiin. Keskustelu tietoturvasta yleisemmin ja sen merkityksestä organisaatiolle ja asiakkaille on jäänyt taka-alalle. Olisi tärkeää korostaa myös hallinnollista näkökulmaa ja keskustella siitä, mitä tietoturva vaatii ja miksi se on tärkeää organisaation toiminnalle ja maineelle.

Kuva 1. Esimerkki tekoälyn hyödyntämisestä pelkistetyn ilmaisun muodostamiseen.

Tekoälyn vastauksen pohjalta muodostettu pelkistetty ilmaisu:

*Tietoturvaan liittyvä keskustelu on pitkälti teknologiapainotteista. Yleinen keskustelu tietoturvasta ja sen merkityksestä organisaatiolle sekä asiakkaille ovat jääneet taka-alalle. Olisi hyvä keskustella myös hallinnollisen tietoturvan roolista ja miksi se on tärkeää organisaation toiminnalle ja maineelle.*

Tekoälyn käyttäminen helpotti ja nopeutti työtä huomattavasti, kun ryhmiteltyyn aineistoon pelkistettyjä ilmauksia muodostui 36 sivua. Ryhmittelyn aikana aineistoa käytiin läpi ja luotiin taulukko, johon täytettiin yhdistävä luokka 'Tietoturvallisuus organisaatiokulttuurissa ja sen johtaminen' sekä pääluokat 'Johtaminen' ja 'Organisaatiokulttuuri'. Pääluokkien alle pelkistetyistä ilmauksista muodostettiin asiasisältöjä yhdistäviä alaluokkia. Jossain tapauksissa koodi oli sama kuin siitä muodostunut alaluokka, esimerkkinä koodista 'Viestinnän sävy' muodostui alaluokka. Tässä vaiheessa koodeja edelleen yhdenmukaistettiin ja niitä sulautettiin yhteen. Aineiston käsittelyn edetessä kävi ilmi, että osa koodauksista olivat päällekkäisiä ja asian sisältö oli jo poimittu käyttöön toisen koodauksen käsittelyn yhteydessä. Näissä tilanteissa varmistettiin asiayhteys käytetyn

koodin, pelkistetyn ilmaisun ja sille valitun alaluokan välillä, ettei mitään olennaista jäänyt käsittelemättä. Aineistoa käytiin läpi useita kertoja ja varmistettiin alkuperäisilmaisun sisällön välittyvän pelkistettyyn ilmaisuun ja että luokat tiivistyivät loogisesti. Alaluokista muodostettiin yläluokkia, jotka yhdistyivät aiemmin määriteltyihin pääluokkiin ja lopulta yhdistävään luokkaan. Taulukossa 1 esitetään esimerkki kokonaisuuden muodostumisesta.

Alkuperäisilmaus	Pelkistetty ilmaisu	Alaluokka	Yläluokka	Pääluokka	Yhdistävä luokka
Väittäisin että aina on autettu, mikäli näihin liittyen (tietoturvaan) on tullut tai tulee kysymyksiä, aina on vastaus saatu. En ole jäänyt yksin asian kanssa miettimään miten tämän kuuluisi mennä, on saatu menemään sitten kuten kuuluu.	Tietoturvaan liittyvissä asioissa ja kysymyksissä esihenkilö auttaa eikä jätä yksin.	Esihenkilön tuki tietoturvaan liittyvissä kysymyksissä.	Valmentava johtaminen	Johtaminen	Tietoturvallisuus organisaatiokulttuurissa ja sen johtamien
Mutta esimerkiksi edellisessä tiimissä niin kyllä varmistin asioita esihenkilön puolelta ja jos hän ei tiennyt tai osannut sanoa, niin sitten yleensä käännettiin tietoturvatimiin puoleen.	Esihenkilön kanssa tietoturvaan liittyviä asioita käytiin läpi ja tarvittaessa konsultoitin tietoturvatimiä.				
ehkä oma esimies ei oo sillä lailla ollut se tiedonlähde noissa tietoturvaan liittyvissä vaan kyllä sitä aika pitkälti tietoturvaorganisaation puoleen on käännetty aina näissä tietoturva-asioissa ja aika paljon sieltä varmaan ohjataan myös, jos omalta esihenkilöltä lähtee kyselemään, että se ohjautuu sinne tietoturvaorganisaation puoleen sitten.	Esihenkilö ohjaa tietoturvaan liittyvissä asioissa olemaan yhteydessä tietoturvatimiin.				
hän niin kuin kannattaa semmoisia asioita, että sillä tavalla kannustaa esihenkilöt ja kirjaavat muistioon, että näin on sovittu... ne on yhdessä tehtyjä ne sovitut asiat. Se on minusta tärkeää, että niitä yhdessä tehdään.	Asioista on tärkeä sopia yhdessä tiimin kanssa.	Esihenkilön kanssa sovitaan yhteisistä toimintatavoista.			

Taulukko 1. Esimerkki aineiston ryhmittelystä.

### 4.3 Kehittämistyön luotettavuus ja eettisyys

Laadullisen tutkimuksen luotettavuuden arviointiin ei ole yksiselitteisiä ohjeita. Luotettavuutta on kuitenkin mahdollista arvioida tarkastelemalla tutkimuksen kokonaisuuden johdonmukaisuutta sekä kuinka tutkija on perustellut ja kuvannut tutkimusaineiston keräämisen ja analysoinnin lukijalle. Voidakseen antaa lukijalle riittävästi tietoa olisi tutkimuksen raportissa vastattava seuraaviin kysymyksiin. On perusteltava mitä tutkitaan ja miksi. Miksi tutkittava aihe on tutkijan mielestä tärkeä, omat alkuolettamat tutkittavasta aiheesta sekä ovatko ajatukset



muuttuneet tutkimuksen aikana? Aineiston keräämisen kuvaaminen ja perustelu sekä tiedonantajien valinnan perustelu ja määrä. Kuvaus kuinka suhde tutkijan ja tiedonantajan välillä toteutui. Tutkimuksen aikataulun kuvaaminen. Aineiston analysoinnin kuvaaminen ja johtopäätöksiä muodostaminen. Perusteltava miksi tutkimusraportti on luotettava ja eettisesti korkeatasoinen. (Tuomi & Sarajärvi 2018, 163–165.)

Tässä opinnäytetyössä noudatetaan Karelian opinnäytetyön raportoinnin ohjeistusta, EU:n tietosuojasetusta henkilötietojen käsittelyssä ja Tutkimuseettisen neuvottelukunnan ohjeistusta (2019). Tulosten luottamuksellisuutta voi osaltaan heikentää tutkijan rooli organisaation tietoturvapäällikkönä. Haastatteluiden alussa haastateltaville korostettiin, että haastattelijaan kannattaa pyrkiä suhtautumaan kuin organisaation ulkopuoliseen henkilöön. Toisaalta tietoturvapäällikkönä toimiminen on antanut hyvän kuvan organisaation toiminnasta ja sen vastuuvuudesta ISO 27001 -standardin vaatimuksiin. Tutkimuksen luotettavuutta on pyritty vahvistamaan, niin että opinnäytetyön aiheen valinta on perusteltu sekä lopputulokseen pääsyä on pyritty kuvaamaan siten, että lukija saa käsityksen, kuinka aineisto on kerätty, käsitelty, analysoitu ja kuinka johtopäätökset muodostettiin. Toimintatapoja on pyritty kuvaamaan avoimesti ja tarvittavalla tarkkuudella.

## 5 Tulokset

Opinnäytetyön tutkimuskysymykset olivat:

- Kuinka valmentava johtajuus toteutuu tietoturvallisuuden johtamisessa?
- Kuinka tietoturvallisuus näkyy organisaatiokulttuurissa?

Haastattelujen kaksi teemaa olivat 'Valmentava johtaminen tietoturvan johtamisessa' ja 'Organisaation tietoturvakulttuuri'. Teemojen tukena oli apukysymyksiä, jotka on esitetty liitteessä 1. Aineistoista muodostui kahden pääluokan alle yhteensä yhdeksän (9) yläluokkaa ja kolmekymmentäviisi (35) alaluokkaa. Pelkistettyjä ilmauksia oli 129 kappaletta.

Pääluokan 'Johtaminen' alle muodostui kuusi yläluokkaa. Yläluokan nimen perässä siihen kuuluvien alaluokkien ja pelkistettyjen ilmausten lukumäärä.

Valmentava johtaminen, 8, 16  
 Esihenkilöiden roolit ja vastuut, 2, 8  
 Johdon roolit ja vastuut 2, 8  
 Roolien vastuut ja valtuudet 1, 5  
 Johtamisen kokemus ja odotukset 3, 11  
 Strategia 2, 11

ja 'Organisaatiokulttuuri' alle kolme:

Tietoturvakulttuuri 7, 30  
 Koulutus 6, 19  
 Viestintä 4, 21

Yleisesti ottaen haastateltavien suhtautuminen organisaation tietoturvakulttuurin nykytilaan oli positiivinen ja tietoturvan johtamisen kehittymiseen tulevaisuudessa uskottiin.

*Mutta sitten kaikki on vähän alkutekijöissään meillä, mutta minä tiedän, että se kehittyy tässä lähiaikoina ja tulevaisuudessa, mutta aika alkutekijöissään.*

*Minun mielestä koko ajan kehitystä tapahtuu ja meillä on semmoinen aktiivinen ote siihen kuitenkin. Että ei vaan tuota, ei niin kuin pelkästään seisota paikallaan ja olla tyytyväisiä itseemme vaan on lähetty kehittämään asioita. Siinä on varmaan tuo ISO-sertifiointi esimerkiksi on pistänyt kyllä liikettä tuota firmaan, että siinä mielessä mielestäni ihan semmoinen positiivinen kehitysasenne.*

## 5.1 Johtaminen

Tiivistettynä haastatteluissa johtamisesta keskusteltaessa korostui eri roolien vastuiden ja valtuuksien kuvaamisen tärkeys. Tietoturvastrategian ja -tavoitteiden selkeyttäminen. Tapoja motivoida ja kannustaa tietoturvallisiin toimintamalleihin ei juurikaan tunnistettu eikä niitä toisaalta ollut osattu kaivata. Valmentavan johtajuuden käsite ei ollut kaikille haastateltaville tuttu, mutta siihen liittyviä

elementtejä tunnistettiin keskusteluissa. Lähiesihenkilöiden tuki koettiin hyvänä ja ote valmentavana sekä asioista sovitaan yhdessä.

### 5.1.1 Valmentava johtaminen

Aineiston perusteella valmentavan johtajuuden periaatteet toteutuvat organisaatiossa siten, että asiantuntijoita osallistetaan työn suunnitteluun ja päätöksien tekemiseen. Oman työn sisällön suunnittelu on mahdollista ja yhteiset pelisäännöt sovitaan esihenkilön ja tiimin kesken.

*Koen, että tällä hetkellä pääsee vaikuttamaan asioihin ja otetaan keskusteluihin mukaan, niin se on mielestäni sitä, koetetaan hyödyntää, että olisi mukana, ettei välttämättä jäisi se ylätaso pelkästään pyörittelemään asioita vaan omalla porukalla.*

*kysellään mitä voisi tehdä toisin, onko jotain juttuja mitä tekisin toisin, ettei ole pelkästään sitä, että kerrotaan mitä pitää tehdä toisin vaan ihan kyselemälläkin viedään sitä asiaa eteenpäin.*

*Ei minua hirveästi käsketä suoranaisesti mitä tehdään, vaan pystyy itse etsimään omaa hommaa ja mitä sitten haluaakaan tehdä. Tietysti on tehtäviä mitä pitää tehdä se on kaikille selvää, ettei voi tehdä pelkästään sitä mitä itseä huvittaa.*

*Hän niin kuin kannattaa semmoisia asioita, että sillä tavalla kannustaa esihenkilöt ja kirjaavat muistioon, että näin on sovittu... ne on yhdessä tehtyjä ne sovitut asiat. Se on minusta tärkeää, että niitä yhdessä tehdään.*

Esihenkilöt auttavat tietoturvaan liittyvissä asioissa ja kysymyksissä tai ohjaavat kysymään tietoturvatiimiltä.

*Väittäisin että aina on autettu, mikäli näihin liittyen (tietoturvaan) on tullut tai tulee kysymyksiä, aina on vastaus saatu. En ole jäänyt yksin asian kanssa miettimään miten tämän kuuluisi mennä, on saatu moneen sitten kuten kuuluu.*

*...esimerkiksi edellisessä tiimissä niin kyllä varmistin asioita esihenkilön puolelta ja jos hän ei tiennyt tai osannut sanoa, niin sitten yleensä käännettiin tietoturvatiimin puoleen.*

*ehkä oma esimies ei oo sillä lailla ollut se tiedonlähde noissa tietoturvaan liittyvissä vaan kyllä sitä aika pitkälti tietoturvaorganisaation puoleen on käännetty aina näissä tietoturva-asioissa ja aika paljon sieltä varmaan*

*ohjataan myös, jos omalta esihenkilöltä lähtee kyselemään, että se ohjautuu sinne tietoturvaorganisaation puoleen sitten.*

Tärkeitä tietoturvaan liittyviä dokumentaatiota katselmoidaan laajasti sisäisten sidosryhmien kanssa ja mikäli kysymykseen liittyvää dokumentaatiota on saatavilla, kannustetaan tietoa hakemaan sieltä.

*...keskustelussa on ollut mukana, ainakin kutsuttuna, arkkitehtejä, tietoturvaa ja siinä katsotaan sitä läpi.*

*Tietoturvaorganin puolelta on jotain asioita kysytty niin, siellä on saatettu vastata niin että ”tässä on dokumentaatiota tutustukaapa tähän näin.” Ettei ole suoraan välttämättä annettu vastausta vaan on katsottu, että tässä se tieto on olemassa ja tuota sitten laitettu siihen tien alkuun ja ohjattu... Silloinhan se oppiminen tulee syvemmäksi, kun joutuu itse vähän vaivaakin näkemään siinä. Tulee tietolähteet ja nämä tutuksi samalla mistä voi tietoa sitten itse myös hakea.*

### 5.1.2 Esihenkilöiden roolit ja vastuut

Esihenkilöiden rooliin haastatteluissa nähtiin kuuluvan tukeminen hallintajärjestelmän jalkauttaminen, kuten tiimipalavereissa tietoturvaohjeistusten ja dokumentaation esittely ja valvoa niiden noudattamista.

*He ovat tietysti tukena siinä (ISMS jalkauttamisessa), että heidän vastuulla on tuoda sitten se tieto sinne työntekijöille ja järjestää omille asiantuntijoille se aika, että he pystyvät kouluttautumaan. Näkisin, että se on sellainen tukirooli tietoturvan johtamisessa*

*Mutta sitten se varsinainen jalkautus, ne on ne intra, tiimipalaverit, nämä möiset asiat niissä pitää sitten esimiesten ja muiden pitää huoli, että ne jalkautuu.*

Esihenkilöiden roolissa haasteiksi koettiin vastuiden jakaantuminen ja epätietoisuus, kuinka tulisi edetä hallintajärjestelmän jalkauttamisessa, minkä vuoksi esihenkilöille kasaantuu paljon itsenäisesti ratkaistavia asioita.

*Se (tietoturvan johtaminen) on kuitenkin niin laaja osa-alue ja kuuluu käytännössä vähän niin kuin jokaiselle, mutta sitten se johtaminen on jokaisen päällikön tehtävä varmasti, mutta minkä verran se sitten kuuluu kenellekin niin se ei nyt ole ihan täysin päivän selvää itsellekään. Kyllä sitä voisi ehkä tarkentaa mikä kuuluu kenellekin sen osalta.*

*omasta mielessä esihenkilöillä on aika hurja rooli siinä tällä hetkellä, että se ei tällä hetkellä ihan hirveästi ylimmältä johdolta tule se niin kuin roolimalli siihen, miten siinä pitäisi edetä, joten tuntuu että esihenkilöille kasaantuu aika paljon, että miten sitä pitäisikään tehdä ja se on vähän myös ongelmallinen myös, kun koko vyyhti on aika iso ja ne alueet on esihenkilöillä mahdollisesti isoja ja paljon alaisia*

### 5.1.3 Johdon roolit ja vastuut

Johdon rooli tietoturvallisuuden johtamisessa koettiin keskittyvän enemmän yksittäisiin työkaluihin ja teknologiavalintoihin kuin tietoturvallisuuden kokonaiskonseptin ymmärtämiseen, tilaturvallisuuteen ja tietoturvasta ylätasolla keskittyvään viestintään. Haastatteluaineistosta ilmeni, ettei johdon roolien sisältöä ja sitä, millä tasolla heidän tulisi ottaa asioissa kantaa, ole määritelty selkeästi tai sitä tietoa ei ole henkilöstöllä. Tietoturvan ohjaamisen ja tavoitteellisuuden osalta koettiin johdon tahtotilana olevan tietoturvan toteutuminen yleisesti, mutta johdon omaa vahvaa näkemystä tietoturvan suunnasta ei ole.

*jos mietin että minkälaisia asioita ylimmältä johdolta tulee, niin ehkä enemmän tällaisiin tilaturvallisuusasioihin ja sitten ehkä tällaiseen niin kuin teknologioihin työkalujuttuihin sellaisiin saattaa tulla niin kuin sitä ylhäältä päättämistä minkälaisia otetaan käyttöön tai minkälaisia tulee niin kuin vähän konsulttinäkökulmista mun mielestä sitä, mutta sellaista niin kuin ehkä arkityöhön liittyviä juttuja ei ihan niin paljoa sieltä*

*ihan johto, ylin johto niin en ole kuullut sellaisia tietoturvallisuuteen varsinaisia asioita esim. forensiikka on sellainen mistä en ole kuullut mitään kommentteja. Ja se on mielestäni aika tärkeä asia kuitenkin, huomioida se asia. Se on minusta enemmän sellaista pistemäistä hommaa kuten otetaan vaikka E5 käyttöön tai jotain muuta.*

*kyllähän se pitäisi ylemmällä tasolla kuvata se rooli johtajien osalta... Mutta en minä tiedä niitten rooleja oikein mitä johdon roolit on niin kuin seuraavan tason mukaan ottaa kantaa niin kuin tietoturva-asioissa.*

*Ehkä johdon tahtotila on enemmän se, että nämä asiat toteutuu. Se on vähän semmoinen, toteutuuko vai eikö toteudu toteaminen, mutta semmoista, niin kuin hirmu vahvaa ajuria siihen tai jos pitäis tehdä, vaikka päätöksiä siitä, että mikä nyt on näistä oikein, niin en oo ihan varma löytyykö sieltä taas hirveästi syvällisempää ajatusta.*

#### 5.1.4 Roolien vastuut ja valtuudet

Vastauksissa tietoturvaan liittyvien roolien vastuisiin ja valtuuksiin korostui tarve selkeyttää niitä läpi organisaation. Osassa rooleja koettiin roolin sisällön muodostuneen kyseisessä roolissa työskennelleen henkilön oman harrastuneisuuden pohjalta. Henkilövaihdoksen myötä rooleja ei ole arvioitu uudelleen, jolloin uusi henkilö ei välttämättä vastaa aiemmin käytännössä muodostuneen roolin odotuksia. Itseohjautuvan asiantuntijuuden tukemiseksi ja byrokratiaa vähentäväksi toimeksi koettiin valtuuksien parempi määrittely. Työtä roolien selkeyttämiseksi on jo tehty ja tarve sen jatkokehittämiselle on myös tunnistettu.

*Nimenomaan siitähän siinä on kysymys eli valtuutetaan just se, että silloinhan ihmiset, kun heidät on valtuutettu, jotain juttuja niin ei tarvii pyörittää kaikkia asioita johdon kautta eikä johdon tarvii kaikkea määrätä. Sen takia se just nämä roolikuvaukset, joita parhaillaan tehdään on osa tätä just nimenomaan ratkaiseva valtuutusväline sitten.*

*sanotaan että X tiimillä on tietoturvaavoittuvuus jossain, niin se on vähän sitten, että mitkä vastuut ovat sillä tiimillä sen hoitamisessa niin se on vähän kanssa. Ja sitten sieltä, että mitä se esihenkilö tekee sen, että minkä verran se kuuluu sille, on ollut ehkä vähän epäselvää itselle*

*paljonhan tässä on tätä henkilöstön vaihtuvuutta viime vuosina ollut, että siinä on niin kuin huomattu sitä, että semmoinen yleinen dokumentaatio jotta miten me tietoturvaa tehdään tai mitä vastuuta ja rooleja on. Niin ne on vähän ollut epäselviä. Ja sitten niissä rooleissa on paljon sitä, että tietyt ihmiset ovat olleet tietynlaisia ja heidän vahvuutena on ollut tietyt jutut niin heille on ajautunut tietyt asiat ettei niitä rooleja ole välttämättä kuvattu sinänsä järkevästi*

*Kyllä se varmasti vaatii vielä meiltä sitä kehittämistä, että ne roolit täsmentyvät entisestään. Ja vastuut kirkastuvat kaikille ja se että kaikista haastavintahan se on tietysti, että ne saadaan ihan sinne asiantuntijatasolle saakka se tietotaito mitä kaikkea on osattava huomioida.*

*kyllähän meillä on niitä rooleissa on jo täsmennetty sitä työryhmän roolia ja ohjausryhmän roolia, mutta se edelleen vaatii yhteistä keskustelua siitä, että miten niin kuin reunaehdoja ja linjauksia ynnä muita, että se työryhmälläkin on varmuus toimia sitten niin kuin niitten mukaisesti.*

### 5.1.5 Johtamisen kokemus ja odotukset

Johtamiseen kuuluvat henkilöstön motivointi ja kannustaminen. Haastateltavat kokivat, ettei tietoturvaohjeistusten noudattamiseen ole kannustettu tai motivoitu varsinaisesti. Yksi esihenkilönä toimiva henkilö koki, että organisaatiossa motivoidaan ja kannustetaan tietoturvaohjeistusten noudattamiseen. Moni piti tietoturvaohjeistusten noudattamista niin itsestään selvänä, ettei erillistä motivointia tai kannustusta ollut osattu edes kaivata. Osa koki olemassa olevat ohjeet ja koulutukset motivointina, vaikka niihin perehtyminen ja kaikkien työntekijöiden pakollinen tietoturva- ja tietosuojakoulutus vaadittiin autoritäärisesti. Aiheesta keskusteltaessa esiin nousi ajatuksia tietoturvaan liittyvistä tavoitepalkkiomittareista ja palkitsemisesta, mikäli tekee organisaation ylläpitämään tietoturvallisuuteen liittyen korjaukseen johtavan havainnon. Esille nousi myös sisäisen motivaation lähde, monen oletetaan kokevan ammatillista tyytyväisyyttä havaitessaan tietoturvaan liittyviä puutteita ja pystyessään niistä ilmoittamaan niistä.

*Tuo on itse asiassa hyvä kysymys. Se on käytännössä kannustuksen puolelta, nyt kun mietin. En oikein osaa suoraan sanoa, tuokin on vähän itsestäänselvyys loppujen lopuksi itselle. Nyt lyö kyllä ihan tyhjää... En osaa oikeastaan sanoa mikä kannustaisi. Kyllä se ohjeistukset on ja tuolle, että niitä noudatetaan on itselle riittävä.*

*koulutukset on periaatteessa kannustusta. Mutta en tiedä mitä sitä pitäisi odottaa, ... , että en nyt kuitenkaan näe että tietoturvapääällikkö tosiaan oisit jossain taputtamassa selkään*

*Minusta se on vähän tässä ICT-maailmassa, ei meillä motivoida siihen varsinaisesti sen niin kuin mitenkä sen sanoisin. Tuohon on vähän vaikea vastata. Mutta en minä nyt ole nähnyt sellaista motivointia siihen kyllä varsinaisesti. Ei ole jäänyt mieleen, että olisi motivoitu. On sitä voitu tehdä, mutta en ole niin kuin havainnut sitä. Ehkä tuo tts-koulutus niin perustasolla niin sehän on sellaista motivoivaa vähän, että vaaditaan se koulutus. Mutta sinäkin on se vaatimus mukana*

*Niin kyllä siitä ehkä vaan ilmoitetaan, että näin se kuuluisi tehdä, että alkää tehkö toisin. En tiedä onko siinä mitään sellaista selkeää motivointikeinoja. Kyllä siitä ehkä vähän se motivointi puuttuu. Suurin motivointi mitä siihen on käytännössä, on se, että esimies tulee sanomaan, että tämän piti olla tehtynä ja luettuna tuohon ja tuohon päivämäärään mennessä. Käytännössä ilmoitetaan siitä, se on vaan pakollinen paha tehdä niitä ei siinä sellaista motivointia ole.*

*No ei oikeastaan suoranaisesti. Että semmoista mitään palkitsemisjärjestelmää tietoturvaan liittyen tai kannustimia siihen, niin kuin aktiiviseen toimintaan, niin ei suoranaisesti kyllä ole. Että se on enemmänkin semmoista että ihmiset varmaan kokee sitä jonkinlaista ammatillista pätevyyttä siitä että voi reagoida.*

Roolien selkeyttämisen lisäksi organisaation johdolta odotettiin tietoturvan johtamiseen vahvempaa auktoriteettiä pohjautuvaa julkilausumaa tietoturvaohjeistusten ja dokumentaation hierarkian noudattamiseen.

*Minusta johdon pitäisi nyt ensinnäkin, ensin määritellä ihan yksiselitteisesti se asia... että meillä pitää noudattaa meidän niin kuin suunnittelun, arkkitehtuurin, tietoturvan ohjeistuksia... niihin pitäisi oikeasti olla sellainen vaatimus, että niitä noudatetaan, johdolta tulla se.*

*Mutta siihen ei riitä minun natsat tai alemman johdon natsat näköjään yhtään vaan siihen pitäisi olla johdon yksiselitteinen vähän niin kuin ”määräys” tai tällainen, että näin meillä toimitaan.*

### 5.1.6 Strategia

Strategian alaisiin aiheisiin sisältyi tietoturvan suunnittelu ja kehittäminen sekä tietoisuus organisaation tietoturvatavoitteista ja -strategiasta. Tietoturvallisuuden kehittämisen nähtiin tapahtuvan pitkälti asiakastarpeiden pohjalta ja tietoturvan johtamisen isojen linjojen puuttumisena. Kuten aiemmin kappaleessa 5.1.3 johdon roolit ja vastuut todettiin johdon roolin olevan teknologiavalinnoissa, niin niitä valintoja ohjaavat asiakastarpeet. Painopisteet ovat työkalujen ympärillä, joita asiakkaat haluavat eikä organisaatiolla ole välttämättä omaa selkeää näkemystä siitä mitä ja milloin olisi syytä ottaa käyttöön. Tämän vuoksi erilaisten konsulttien antamat suositukset ohjaavat tekemistä eikä parantamista ja kehittämistä suunnitella tiekarttamaisesti toimintaympäristöön peilaten.

*Paljon meidän tekeminen nojautuu asiakastarpeiden täyttämiseen. Mielestäni se ajaa jopa ohi oman organisaation kehittämisen tarpeen tai sen että, pohdittaisiin miettimään, miten voitaisiin tehdä tehokkaammin ja järkevämmiin. Vähän sellainen klassinen esimerkki, että on niin kiire, ettei ehditä nousta mopon kyytiin vaan juostaan siinä mopon vieressä.*

*Vähän sellainen tunne siitä tulee, että asiakas haluaa tällaisia juttuja tänä vuonna tai jopa tälle neljännekselle ja sitten muutetaan fokusta*



*siinä. Että semmoinen niin kuin, mikä on vaikka mikä tietoturvan fokus tänä vuonna, niin paljon se taas tulee niitten kautta, no tämmöisiä työkaluja ja tälle asiakkaalle tätä ja tämmöistä pitäisi kehittää*

*Toisaalta meiltä vaatii asiakkaat meiltä aikamoisia ratkaisuja aina välillä. Sitten niitä niin kuin vanha käytäntö on tehdä niitä asiakasratkaisuja. Tämä on vähän joka asiassa muussakin kuin tietoturvassa näkyy, ...noudatetaan sitä asiakkaan toiveita hyvin herkästi ja se on minusta se ongelma tässä tietoturvassakin ehkä vähäsen.*

*Tällä hetkellä minusta puuttuu ne isot linjat tai minulla ei ole niitä tiedossa ainakaan... niin tämä ylemmän tason maailma, kun meiltä puuttuu, niin meillä, niin johtamistaso, niin meillä mennään vähän yksittäisiin asioihin sitten. Ja se ei ole mielestäni hyvä. Se on vähän niin kuin, johtaminen on vielä alkutekijöissään, sanoisinko.*

*tämmöiset teknologiahankkeet on monesti ne mitkä ajaa sitä muutosta... meillä ei ole tämmöiset asiat omassa roadmapissa, että me haluttaisiin itse niitä vaan ne yleensä tulee teknologian pakottamana tai sitten meillä käy joku konsultti tekemässä ... ja sitten juostaan korjaamaan sitä. Että ne ei välttämättä ole sellaisia mitä itse oltaisiin tunnistettu tai havaittu ...että nyt tämä pitäisi korjata. Enemmän tarvittaisiin omaa aktiivisuutta ja ymmärrystä missä mennään... ja sitten priorisointi olisi hyvä siinä ... että nyt niin kuin tänä vuonna tämä ja tällä hetkellä näyttää, että ens vuodelle voisi tämän jättää, mutta arvioidaan vaikka loppuvuonna onko maailma muuttunut. Me ei mielestäni tarpeeksi peilata siihen maailman tilanteeseen vielä.*

Organisaation tietoturvatavoitteet ja niiden liittyminen strategiaan koettiin haastaviksi kuvata. Osalle tavoitteet itsesään olivat tuttuja, vaikka niitä ei ulkoa muistettu.

*En muista mikä se tietoturvatavoite olikaan tai tavoitteen jotenkin, mutta miten se siihen strategiaan uppoutuu niin sitä en muista.*

*Tähän en kyllä osaa vastata suoraan, en osaa suoraan sanoa tietoturvatavoitteita. Että yritetään pitää se ISO-sertifikaatin mukainen taso. En osaa enempää lähteä tuohon ainakaan omalla tiedolla.*

*jaa-a, En varmasti pysty lausumaan jotain tiettyä slogania mikä siellä mahdollisesti on, mutta tietoturvahan nyt sinällään on tavoite itsessään. En nyt oikein osaa tuohon tuota sanoa. Strategia itsessään sehän taitaa justinsa siis nämä dataeheydet ja kaikki saatavuudet ja näin edelleen.*

*On, mutta en muista sanasta sanaan. Pitkiä tavoitteita on, mutta kyllä meillä on tietoturvatavoitteet.*

## 5.2 Organisaatiokulttuuri

Organisaatiokulttuurista keskusteltaessa esille nousi esimerkkejä tietoturvakulttuurin näkymisestä työpäivässä. Organisaation tavasta suhtautua tietoturvaan, kuinka se oppii ja kehittää toimintaansa. Dokumentoidun tiedon ja ohjeistusten noudattamisen tärkeydestä. Koulutuksen riittävydestä, vaikuttavuudesta, sisällystöstä ja kehittämisestä sekä organisaation viestinnästä.

### 5.2.1 Tietoturvakulttuuri

Organisaatiokulttuuri koettiin turvalliseksi eikä ongelmatilanteissa syyllisen löytäminen ole tärkeintä vaan ongelmat ratkotaan asiakeskeisesti. Henkilöstön koettiin olevan aktiivinen toimija tietoturvaan liittyvien epäkohtien ilmoittamisessa sekä seuraavan organisaation omia että median tietoturvan ajankohtaisia uutisointeja. Tietoturvan koettiin oleva osa työntekoa. Tietoturvallisuus ilmenee työpäivän aikana sen aktiivisena tiedostamisena, tietojenkäsittelyohjeistusten noudattamisena ja tietosuojan huomioimisena, varovaisuutena sähköpostien käsittelyssä, fyysisen tietoturvallisuuden noudattamisessa ja organisaation tietoturvaohjeistuksen hyödyntämisenä.

*miten itse olen kokenut, niin on se pääosin ongelman ratkaisuun keskittyvää. En ole kokenut, että se olisi syyllinen tärkeä, toki syy miksi on tapahtunut niin se varmasti kiinnostaa.*

*Koen että ilmoittavat, se kynnys on ehkä myös madaltunut koska siitä puhutaan sen verran paljon. Tällöinen mielikuva minulla on*

*Varmaan joku on lukenut ehkä teidänkin tuottamia dokumentteja mistä on jäänyt mieleen asioita. Sittenhän meillä on näitä tiedottamisia, että tulee joku phishing-site -viesti tai -posti ihmisille, niin siitä ihmiset yhdistää. Sitten on tietämystä ihan mediasta, kun jotain tapahtuu, niin silloinhan keskustellaan meilläkin asiasta ja siinä tietämys lisääntyy ja ihmiset oivaltaa asioita.*

*Siihenhän minä itse just firman linjauksien puolesta käytän Intran tietoturvan käsikirjaa, niin sieltä käyn tarkistamassa, jos on jotain sellaista. Esimerkkinä kun vaihdoin tiimiä, niin kävin tarkistamassa läpi etätyöohjeistukset.*

*No se on sellainen taustavarjo, joka kulkee koko ajan mukana, kun pitää miettiä, että tekee oikein. Väittäisin, että se näkyy meillä jokaisen työssä jollain tavalla, ellei joka päivä, niin lähes joka päivä. Meidän pitää miettiä aina mihin me kirjaudutaan, mitä sähköposteja me avataan, olla koko ajan skarppina mitä syötteitä meille tulee, onko nämä tietoturvasia tai muita. Kyllä se on aika olennainen osa meidän jokapäiväistä työtä.*

*Sitten tietenkin ei levitetä ylimääräistä tietoa kuulumattomiin paikkoihin, jota jokainen varmaan joutuu miettimään mihin mikäkin asia kuuluu, saako sen laittaa tänne vai ei.*

*no kyllä siis miten se (tietoturvaohjeistusten noudattaminen) vaikuttaa niin toimistolla varsinkin se ehkä sen verran että pitää olla katsele-massa, että pitää olla katselemassa ketä siellä liikkuu, jos tulee joku tuntematon vastaan, on asia, johon tulee kiinnittää huomiota. Ei juuri vaikuta kuin sen tosiaan, että sitten joutuu vähän ylimääräistä aivotyötä tekemään ennen kuin toimii.*

*...Ja sitten näitä mitä dataa voit yleensä käsitellä niin sekin pitää huomioida tekemisessä. Sieltähän voi tulla joltakin sellaista dataa, joka on GDPR:n mukaista, vaikka ei olisi tarkoitus, että minä saan sellaista dataa.*

Organisaation koettiin oppivan tekemistään virheistä ja toimintatapojen kehittämisen nähtiin olevan aktiivista. ISO 27001 -sertifioinnin nähtiin positiivisena ajurina toiminnan kehittämiseksi.

*Kyllä niistä saadaan opit talteen omasta mielestäni. Prosessia koitetaan korjata sen mukaan, ettei uudestaan samalla tavalla tapahtuisi, jos siellä joku selkeä poikkeama on ollut jossakin.*

*Oma näkemys on, että opitaan. Käytännössä juuri poikkeamat ja häiriöt ja kaikki näistä pyritään ottamaan mitä siellä, jos on jotain tehty väärin, miten se jatkossa vältetään ja miten parannetaan. Minun mielestä oma näkemys on, että opitaan siitä.*

*minun mielestä koko ajan kehitystä tapahtuu ja meillä on semmoinen aktiivinen ote siihen kuitenkin. Että ei vaan tuota, ei niin kuin pelkästään seisota paikallaan ja olla tyytyväisiä itseemme vaan on lähetty kehittämään asioita. Siinä varmaan tuo ISO-sertifiointi esimerkiksi on pistänyt kyllä liikettä tuota firmaan, että siinä mielessä mielestäni ihan semmoinen positiivinen kehitysasenne.*

Haastatteluissa ilmeni, ettei organisaatiossa hyödynnetä vielä vertaisoppimista palvelualueiden tiimien välillä sekä epäselvyyttä oli, onko kaikissa tapauksissa ongelmanratkaisun jälkeen päivitetty siihen liittyviä työohjeita.

*meillä vielä puuttuu sellainen kulttuuri, että jos jokin tällöinen virhe löytyy, niin siitä saataisiin kaikille se tieto selkeästi niin kuin, että tällöinen oli voitteko katsoa omanne, löytyykö teiltä vastaavaa tai tässä oli tullut tällöinen ajatusvirhe, että tämä mahdollisesti tällöisen... Ehkä semmoinen niin kuin tiedon jakaminen, että se saavuttaisi kaikki tiimit tai että tulisi niitä kokemuksia, että muillekin sattuu tai muut havainnoi, niin tällä hetkellä puuttuu semmoinen.*

*Oisko se esimerkin voima semmoinen hyvä, että sieltä olisi niitä tarinoita, vaikka siitä, että joku osasto joka ois vaikka tehnyt esittelisi koko henkilöstölle me ollaan tehty tällaisia juttuja ja me dokumentointiin meidän järjestelmä näin*

*Onko se sitten noiden ongelmatilanteiden jälkiselvittely, onko se ollut riittävä siten, että niistä on tieto valunut eteenpäin. Melkein väittäisin, että kyllä yleensä tieto on valunut eteenpäin. Mutta onko se esimerkiksi johtanut siihen, että ne on sitten kirjattu ne ohjeistukset pysyviin ohjeistuksiin. Että onko se sinne vaikuttanut, siitä en ole ihan varma. Saattaa olla, että jos jossain akuutin tilanteen jälkeen on tiedotettu, että tällöinen ja tällöinen ongelma ja näin, mutta onko se jäänyt sitten pysyviin ohjeistuksiin aina jotain korjausta, en varmaksi osaa sanoa kaikissa tilanteissa ainakaan.*

Dokumentaatio ja ohjeistusten noudattaminen koettiin erittäin tärkeiksi kehityskohteiksi. Dokumentaation tulee olla sisällöltään kohderyhmälle ymmärrettävässä muodossa ja asioita tulisi yleisesti ottaen dokumentoida enemmän ja laadukkaammin.

*Dokumentointi on helskutin tärkeää, että ne on kuvattu ymmärrettävässä muodossa.*

*olen ehkä itse sitä mieltä, että kaikki pitäisi dokumentoida mahdollisimman laajasti, ettei se jää tietäjät tietää tyyliin, niin siinä ehkä on parannettavaa.*

Dokumentaatio itsessään ei tee autuaaksi vaan niiden sisältö täytyy saada niitä tarvitseville tiedoksi ja niiden ohjeistuksia tulee noudattaa. Ohjeistusten noudattamisen haasteeksi koettiin vuonna 2019 tapahtunut kahden eri maakunnan organisaation fuusioituminen yhdeksi, jonka vuoksi molempien organisaatioiden vanhat työtavat ovat vielä olemassa.

*Itse koen, että meillä on tietoturvaohjeistus olemassa, mutta se käytäntö mitä ihmiset taas tekee, niin onko ne yksi yhteen, ei välttämättä. Voi olla, että on, se voi olla, että taas monesti sitä mitä ollaan vuosikautia tehty ja mikä on muovautunut tietoturvakulttuuriksi joko nykyisessä yrityksessä tai niissä missä on aiemmin fuusioitunut tai mistä ihmiset tuleekaan ja millainen kokemustausta kelläkin on.*

*Niin tuota jos tuota niistä on, moni niistä arkkitehtuurikuvista on niin kuin läpi käyty eri suunnittelijan tai asiantuntijan kanssa keskustelua ja niihin hyväksynät saatu. Mutta sitten taas joku muu saattaa katsoa, että ei näin tehdäänpäs toisella tavalla, sitä minä haen, että johdon pitäisi määrätä se, että meillä noudatetaan näin näitä, eri roolien mukaisia dokumentaatiotasoja.*

## 5.2.2 Koulutus

Teknologiaan ja työkaluihin liittyvää koulutusta koettiin olevan tarpeeksi ja organisaation nykyinen tietoturva ja -suojakoulutus perusasioiden osalta hyvänä. Haastatteluissa ilmeni TTS-koulutuksen vaikuttavuuden todentamisen puuttuminen sekä epäiltiin ettei kerran suoritettavan koulutuksen sisältö jää muistiin ilman säännöllistä kouluttamista. TTS-koulutuksen toivottiin myös olevan sisällöllisesti lähempänä koulutusta suorittavan henkilön työtehtäviä, kun se nykymuodossaan on kaikille sama roolista riippumatta.

*Ne koulutukset mitä yleisesti meidän talossa on käyty, on paljon sitä teknisen tietoturvan jonkun työkalun toteuttamisen nyansseja tai miten joku tietty valmistaja näkee, vaikka miten kannattaa tehdä. Niitä asioita meillä on saatavilla paljon, mutta sitten taas sellainen yleisempi ymmärrys tietoturvasta ja mitä me tehdään, niin se on paljon sen yhden tts-koulutusmateriaalin varassa*

*Kyllä koen, koska on oma historiakin näistä asioista taustalla, että olen ollut niin paljon tietoturva ja tietosuoja asioiden kanssa tekemisissä. Niin tuota omassa roolissani koen, että on riittävästi.*

*Ja sitten tämä tietoturvakoulutuksen vaikuttavuus, niin sitähan ei seurata ollenkaan, että me seurataan lähinnä sellaisena 0 1 tyyppisenä onko koulutus käyty vai eikö ole ja onko se tähän päivämäärään mennessä käyty. Ja sitten viimeisenä päivänä ihmiset käy naputtamassa sen kiireellä läpi ja huokaistaan nyt tämä on taas vuodeksi tässä. Että sitä, että miten ihmiset oikeasti osaa, niin se on paljon just sen yksittäisen tentin varassa mikä tts-koulutuksen lopussa on, joka ei ole kovin kompleksinen tai vaikea mun mielestä.*

*Periaatteessa se ei ehkä tarpeeksi ole enemmän uusia koulutuksia, mutta esimerkiksi se tts-koulutus olisi hyvä uusia jossain vaiheessa. Käytäisiin läpi uudelleen se mitä on opittu, onko se vielä hanskassa. Tällä hetkellä se taitaa olla niin, että tehdään tämä ja sitten olet tehnyt sen, hyvä jatka samaan malliin. Ja sitten käytännössä unohdat ne asiat, jos et joudu niitä aktiivisesti käyttämään. Se voisi olla ehkä ihan hyvä*

*jossain vaiheessa käydä läpi uudelleen, ihan muistin virkistykseksi, että onko tämä vielä hallussa ja tiedät varmasti mistä on kyse.*

### 5.2.3 Viestintä

Tietoturvaviestintään liittyen esiin nousi viestinnän tavoitavuus, sisältö, ketkä viestivät tietoturvasta ja viestinnän sävy. Haastatteluissa tunnistetut tietoturvan viestintäkanavat ovat organisaation intra, kuukausittain järjestettävä henkilöstöinfo, sähköposti akuutisti tiedotettavissa asioissa, esihenkilöiden säännöllinen tapaaminen, johtoryhmä, tietoturvan ohjaus- ja työryhmien tapaamiset sekä Teams-keskustelut. Lähtökohtaisesti tavoitavuus koettiin hyvänä intran ja henkilöstöinfon osalta. Toisaalta koettiin myös, että riippuu henkilön omista sisäisistä sidosryhmistä, kuinka paljon on mukana tietoturvaviestinnässä. Sähköpostin todettiin tavoittavan koko henkilöstön, mutta sitä luetaanko niitä vai hukkuvatko ne muiden viestien joukkoon epäiltiin.

*Meidän intrassa on ajankohtaiset tietoturva-asiat nostettu ylös. Jos jostain on käytännössä tietoturvapuolelta mielenpäällä, niin kyllä se sieltä ja käytännössä tarvittaessa henkilöstöinfoissa tulee esille.*

*Henkilöstöinfossa ja on ollut intrassa ja niitä luetaan tosi hyvin. Kyllä ne mielestäni ovat todella hyviä kanavia.*

*Kyllä siitä kommunikoidaan, se on käytännössä, jos ajatellaan firmaa koskevia tietoturva juttuja, niin intra on se mistä itse lähtisin etsimään. Sitten tietysti henkilöstöinfossa on tietysti ollut tarvittaessa tietoiskuja, jos on sellaista kerrottavaa... tietysti sähköposti, jos on tietysti sellaista akuuttia.*

*Minun kokemuksen mukaan siitä puhutaan ja kommunikoidaan suht hyvin, jos olet oikeissa kanavissa mukana... näkisin ne mitä menee sähköpostilla tietysti tavoittaa varmaan suurimman osan, en usko, että kaikki niitäkään lukee vaan ne hukkuvat sähköpostiin kuitenkin. Osa saadaan kiinni intrasta ja jos ajatellaan vaikka talouspuolta, niin Teams-keskusteluiden tietoturvapuhe ei heitä tavoita.*

Henkilöstöinfoihin viestinnän sisältöön toivottiin monipuolisempia ja vähemmän toistuvia aiheita, kuten varoittelua kalasteluviesteistä. Myös yleistä keskustelua tietoturvallisuudesta ja sen merkityksestä organisaatiolle toivottiin olevan

enemmän. Kehitysehdotuksena oli Kyberturvallisuuskeskuksen kybersään läpikäymistä organisaatiossa.

*Henkilöstöinfoissa voisi olla vähän enemmän sitä niin kuin ja monipuolisempia sisältöjä ja vähän niin kuin tämmöisiä vaihtuviakin juttuja... että jos aina tietoturvatiimikin tulee vain puhumaan kalastelusta ja niistä samoista aiheista, niin jaksaako ihmiset kuunnella, jos ne ei ole tarpeeksi mielenkiintoisia tai uusia pointteja.*

*Se on vähän hankala koska, jos se on tyyliin henkilöstöinfo, niin sitten kun on kuitenkin erilaisia rooleja ja osalla on tekniset roolit ja sitten siellä on tämmöisiä rooleja, joilla ei ole it-taustaa... moni noista tapahtumista voidaan pureskella silleensä, että niistä saa hyvin arkipäiväisiä esimerkkejä. Että muutaman kerran, kun kysyy miksi, sieltä lopulta paljastuu mahdollisesti kiire tai dokumentaation, resurssin tai koulutuksen puute. Ne on aika universaaleja asioita.*

*Puhuminen tietoturvakulttuurista näin yleisemmin, että mitä me vaaditaan ja miksi nämä ovat tärkeitä meidän asiakkaille tai semmoiselle että meidän oma palvelutuotanto ei vaarannu tai tässä ei vaarantuisi vaikka meidän maine tai tietosuoja ja sitä kautta niin kuin tulisi vaikutuksia vaikka meihin, niin ehkä semmoinen keskustelu on jäänyt pikkuisen taka-alalle. Tietoturvasta keskustelu on paljon sitä niin kuin sitä teknologia vetoista vielä. Puhutaan virustorjunnasta ja roskapostisuodattimista ja teknologioista MFA ja kaiken näköiset valvontatyökalut ja ne, mutta sitten taas hallinnollisempi näkemys tietoturvaan on jäänyt vähän taka-alalle.*

Tietoturvasta viestiviksi rooleiksi tunnistettiin tietoturvatiimin tietoturvapäällikkö ja tietoturvasuunnittelija, tuotantopäällikkö ja service deskin palvelukoordinaattori. Haastateltavien kokemus johtajien osallisuudesta tietoturvaviestinnässä oli, ettei johto osallistu viestintään merkittävästi.

*Meillä on sellainen tietoturvapäällikkö, joka on tuossa toisella puolella, joka saattaa ilmoitella intrassa. Meidän tiedottajat saattaa myös niitä viestejä laitella, mikäli on jotain havaittu, johon pitäisi kiinnittää huomiota... Sanoisin ettei ainakaan ylätason johto ole siinä mukana.*

*No tietoturvapäällikkö, ennen tietoturvasuunnittelija, tuotantopäällikkö myös lähinnä ketjuviestien osalta, siinä ne melkein on ne tärkeimmät... Tietysti jos on jotain tiedotettavaa, niin service deskin koordinaattorin puolelta tulee myös häiriötiedote puolelle eli sinne SD:n palstalle intraan tai sitten tekstiviesteillä ja sähköpostilla.*

*Kun näistä viestitään henkilöstöinfoissa niin sieltähän ne aika vahvasti tulee sieltä suunnalta. Niitä ei yleensä ole kertomassa kukaan johtaja vaan yleensä tietoturvapäällikkö.*

*Jos puhutaan siitä viestinnästä niin ehkä siinä tietoturva-asiassa viestimässä on meidän tuotantopäällikkö jonkin verran. Sieltähän on jonkun verran näitä asioita käsitelty. Ehkä se johtuu siitä, että siellä aktiivisesti selvittelään niitä ongelmia niin siellä hanakammin tartutaan mahdollisiin ongelmakohtiin ja niitä nostellaan esille ja niistä tiedotetaan ja näin.*

*Kun mietin niin mielestäni ei ihan älyttömästi kyllä, kyllä se mielestäni vähän itsestäni sinällään on vähän hassua. Se ei ehkä sieltä, niin kuin sanottu se aina henkilöityy sinne tietoturvayksikön puoleen mielestäni. Että sieltä se aika paljon tulee viestintä. Siinä mielessä se on vähän erikoista, kyllä sitä varmaan tulee muualtakin mutta ei se ehkä muualla se ei ole niin näkyvää, että olisi esimerkiksi osa jotain palvelualueen palaveria, että siellä käsiteltäisiin... esimerkiksi johtaja, kun pitää omaa osuuttaan niin siinä ei ole erikseen ollut tietoturva-asiat esillä, ehkä, sellainen mielikuva ainakin itsellä on.*

Pääosin haastateltavat kokivat yleisesti ottaen tietoturvasta viestinnän ja siihen liittyvän keskustelun sävyn myönteisenä. Mielikuva tietoturvan luonteesta koettiin kuitenkin ongelmiin keskittyvänä ja työntekoa hankaloittavaksi, jolloin viestinnän sisältö keskittyy luonnollisesti ongelmien ja uhkakuvien käsittelyyn. Unohtamatta uhkakuvia olisi tärkeää pystyä esittämään tietoturvan positiivisessa valossa ja tuoda esille, kuinka se mahdollistaa työntekemisen.

*Kyllähän siitä yritetään positiivisesti puhua, mutta kun se on valitettava totuus, että tietoturva on sellainen ala, että se herkästi menee siihen ikäväksi asiaksi käyttäjille tavallaan, kun estetään työntekoa.*

*Kyllähän tietoturva on vähän sellainen, joka keskittyy pitkälti ongelmiin, sehän on ihan selvä. Kyllähän se siinä viestinnässä näkyy sitten, kyllä se varmasti on jotain sellaista, että kun tietoturvasta puhutaan niin joku yrittää jotain, ei niin kivaa, ja jotakin vähän ikävillä konsteilla, niin paljon negatiivisia asioita siihen liittyy... Kyllä se enemmän lähtee sieltä uhkakuvien kautta tämä homma kuitenkin. Jos ihan totta puhutaan, niin aika paljonhan sitä maalaillaan niitä ongelmia ja mahdollisia seurauksia mitä siitä seuraa, jos ei noudateta ohjeita. Ehkä positiivinen kulma ei ehkä ole silleen hirveän hallitseva.*

*Tietoturvaa pitäisi pyrkiä vähän kannustavasti puhumaan siitä asiasta, että tietoturva toimisi mahdollistajana. Ettei se olisi aina sitä pelottelua, että älkää tehkö mitään, että kädet pois näppäimistöltä, ettei käy mitään. Vaan enemmän sitä, että tietoturvankin tehtävä niin työkalujen kuin hallinnollisen on löytää se keino, miten sitä työtä voidaan tehdä turvallisesti.*



## 6 Johtopäätökset

### 6.1 Johtopäätökset

Tiivistettynä tuloksista ilmenee, että organisaatiossa on tärkeää määritellä roolien vastuut ja valtuudet selkeästi. Henkilöstölle johdon esimerkillinen toiminta, aktiivinen osallistuminen ja suunnan näyttäminen koetaan merkityksellisenä. Dokumentaation laadukkuus ja riittävyys nousi myös esille, minkä lisäksi ohjeistukset on pystyttävä kouluttamaan henkilöstölle ymmärrettävästi. Viestinnässä on huomioitava koko organisaatio ja tietoturvan eri aihealueita on hyvä käydä läpi vaihtelevasti mielenkiinnon ylläpitämiseksi.

Valmentavan johtajuuden toteutumista erityisesti tietoturvan johtamisessa oli hankala todentaa, sillä tietoturvan johtaminen koettiin uutena asiana ja tietoturvaaan liittyvien roolien vastuiden ja valtuutuksien määrittelyt ovat puutteellisia tai niitä ei ole kommunikoitu selvästi. Valmentavan johtajuuden elementtejä esihenkilötyössä toteutui haastatteluiden perusteella ja esihenkilöiden työskentelyyn oltiin tyytyväisiä.

Johtamisen osa-alueella merkittävimmät kehityskohteet ovat roolien vastuiden ja valtuuksien sekä tietoturvastrategian ja -suunnitelmien määrittely. Ristikangas & Grünbaum (2010) määritelmiä valmentavan johtajuuden toteutumiselle esiteltiin kappaleessa 3.1 Johtamisen viitekehys – valmentava johtajuus. Edellytyksiin kuuluu yhteisten pelisääntöjen sopiminen, kuten mistä ja milloin yksilö tai tiimi voi päättää itsenäisesti ja milloin tarvitaan esihenkilön osallistumista päätöksentekoon. Roolien vastuiden ja valtuuksien määrittely tulee myös ISO 27001 vaatimuksista, kuten sivulla 25 johtajuuden määrittelyssä esitettiin. Tämän opinnäytetyön tulokset tukevat sivulla 9 esiteltyjä aiempien opinnäytetöiden tuloksia valmentavasta johtajuudesta. Viljamaan (2023) tutkimuksen tuloksissa todettiin olevan tärkeää määritellä raamit, joiden puitteissa tiimit voivat itsenäisesti päättää asioistaan. Viljamaa esitti myös valmentavaa johtajuutta heikentäviksi tekijöiksi esimerkiksi, ettei yhdessä sovittujen päätösten toteutumista

seurata, puutteet tasa-arvoisessa kohtelussa, yhteisten pelisääntöjen noudattamattomuus ja epätasaisesti jakautuva työkuorma.

Haastatteluiden pohjalta korostui johdon merkitys tietoturvallisten toimintamallien vaikuttavasta jalkauttamisesta toimimalla esimerkillisesti ja viestimällä tietoturvan tärkeydestä. Johdon viestintä on myös yksi ISO 27001 -standardin vaatimuksista, 5.1 Johtajuus ja sitoutuminen. Johdon rooli esihenkilöiden tukemisessa tietoturvallisuuden hallintajärjestelmän jalkauttamisessa koettiin tärkeänä ja johtajien toivottiin pystyvän ohjaamaan esihenkilöitä siinä.

Johdolta odotetaan myös tietoturvaan liittyvien isojen linjausten määrittelyä ja vähemmän yksittäisiin teknologioihin puuttumista. Asiakasnäkökulma on vahva ja se varmasti tulee olemaan, koska kyseessä on in-house-yhtiö. Tietoturvan strategia ja suunnitelmat tulisi mahdollisuuksien mukaan yhdistää asiakkaiden ja organisaation yhteisiksi tavoitteiksi tiekarttoineen, jolloin kaikki olisivat saman sateenvarjon alla.

Varsinaista tietoturvallisuuteen kannustamista ja motivointia ei aineiston perusteella tunnistettu ja siihen liittyen keskusteluissa nousikin kehitysehdotuksia ottaa tietoturva mukaan tavoitepalkkiomalliin sekä henkilöstön ilmoittamista korjaustoimenpiteisiin johtaneista tietoturvapoikkeamista palkitsemiseen. Havaituista tieturvapoikkeamista olisi hyvä jakaa kultajyvät organisaation sisällä, ettei kaikkien tarvitse tehdä samoja virheitä itse vaan opittaisiin muiden kokemuksista.

Organisaatiokulttuurissa tunnistettiin myönteisiä elementtejä sekä kehitystarpeita. Tietoturvaan lähtökohtaisesti suhtaudutaan aineiston perusteella myönteisesti. Aineistosta kävi ilmi, että asioita tehdään vielä paljon vanhoilla totutulla tavalla eikä ohjeistuksia välttämättä noudateta läpi organisaation. Tämä on ymmärrettävää ottaen huomioon organisaation fuusioituneen kahdesta samantyylisestä organisaatiosta vuonna 2019 sekä tuoreen tietoturvallisuuden hallintajärjestelmän käyttöönottamisen vuoksi. Sivuilla 20–22 käsiteltiin Scheinin (2009) määritelmää oppimisahdistuksesta ja mitä organisaatio voi tehdä voittaakseen sen. Se, että organisaatiossa on tuotettu dokumentaatiota ja ohjeistuksia ei

vielä itsessään muuta henkilöstön toimintamalleja vaan ne tulee kouluttaa kaikille. Myös aiemmissa opinnäytetöissä, joita tarkastelimme sivulla 8–9 Ruonala (2011) ja Antila (2018) esittivät omissa tuloksissaan ohjeistusten aktiivisen koulutuksen olevan tärkeää, Ruonalan parannusehdotus oli säännöllinen henkilöstön koulutus ja tietoturvan esillä pitäminen. Onkin tärkeää tunnistaa kehityskohteet ja suunnitella kuinka tieto saadaan jaettua vaikuttavasti henkilöstölle. Yksittäinen henkilö oli se sitten toimitusjohtaja tai joku muu, ei pysty käskemällä muuttamaan totuttua kulttuuria, vaan sen eteen on tehtävä johdonmukaisesti työtä. Johdon on toki ilmaistava ohjeistusten noudattamisen tärkeys ja perusteltava ohjeistusten merkitys sekä organisaation että asiakkaiden toiminnan kannalta ja toimittava itse esimerkillisesti.

## 6.2 Kehityskohteet

Vaikka parannettavaa on, antaa organisaatiokulttuurin positiiviset löydökset hyvän pohjan toiminnan kehittämiseksi. Henkilöstö koettiin aktiivisena ja organisaatio kehittymishaluisena sekä ilmapiiriltään turvallisena, jossa tunnustetaan tietoturvallisuuden olevan inhimillistä toimintaa ja virheitä sattuessaa asioita käsitellään asioina ilman syylistämistä.

Merkittävimmät kehityskohteet ovat roolien vastuiden ja valtuuksien selkeyttäminen läpi organisaation ja tietoturvakoulutusten kehittämisen ja vaikuttavuuden varmistaminen. Myös tietoturvasta viestintää olisi hyvä monipuolistaa ja reflektoida esimerkiksi ehdotettua Kybersäätä organisaation omaan toimintaan ja käydä sitä henkilöstön kanssa läpi. Alla taulukossa 2. on tiivistetty aineistosta ilmenneet kehityskohteet.

<b>Roolit</b>	Roolien vastuiden ja valtuuksien selkeyttäminen läpi organisaation
	Johdon roolien avaaminen
	Esihenkilöiden kouluttaminen mitä ISMS tarkoittaa heidän näkökulmastaan.

	Tehtäväkuvan läpikäynti avainroolien henkilöstövaihdosten yhteydessä. Muutoksista viestintä henkilöstölle.
<b>Johtaminen ja strategia</b>	Johdon aktiivinen osallistuminen tietoturvasta viestintään ja esimerkkinä toimiminen.
	Tietoturvastrategia ja -suunnitelmat tulisi soveltuvilta osin yhdistää asiakkaiden ja organisaation yhteisiksi
	Tietoturvan sisällyttäminen tavoitepalkkiomalliin.
	Korjaukseen johtaneista tietoturvaan liittyvistä parannusehdotuksista palkitseminen.
<b>Oppiminen ja viestintä</b>	Vertaisoppimisen lisääminen, kaikkien ei tarvitse tehdä samoja virheitä
	Varmistaa ohjeistusten päivittäminen ongelmatilanteiden selvittämisen jälkeen.
	Dokumentaation tulee olla kohderyhmälle ymmärrettävää ja sisältö kouluttaa
	Organisaation tietoturvaohjeistuksien ja dokumentaation aktiivinen kouluttaminen henkilöstölle tietoisuuden parantamiseksi.
	Koulutuksen sovittaminen paremmin sitä suorittavan henkilön työtehtävään
	Henkilöstöinfoihin monipuolisempia aiheita kuten tietoturvan hallinnollisia osa-alueita teknisten näkökulmien lisäksi

	Kyberturvallisuuskeskuksen kyber- sään läpikäynti suhteessa oman or- ganisaation toimintaan
	Viestinnässä pyrittävä positiivisem- paan sävyyn, uhkakuvia unohtamatta olisi hyvä kertoa kuinka tietoturva mahdollistaa työntekemisen eikä aina vain hidasta sitä

Taulukko 2. Kehityskohteet tiivistetysti.

### 6.3 Jatkotoimenpiteet

Organisaatiossa kuluvan vuoden yhdeksi tavoitteeksi on jo otettu roolien läpi-  
käynti. Lisäksi opinnäytetyötä viimeisteltäessä organisaatiossa aloitti uusi ICT-  
ja ratkaisupalveluiden liiketoimintajohtaja ja tavoitteena on lähteä yhdenmukais-  
tamaan asiakasratkaisuja, joihin myös tietoturva kuuluu. Opinnäytetyön tulokset  
tukevat siis organisaatiossa valittuja kehitystoimenpiteitä. Loppujen kehityskoh-  
teiden osalta tulee organisaatiossa käydä keskustelu mitä niistä lähdetään edis-  
tämään.

Jatkotoimenpiteinä voisi olla henkilöstökyselyjen toteuttaminen merkittävien  
muutosten jälkeen, kuten menossa olevan roolien muutostyön. Lomakekyselyn  
voisi suunnitella tämän opinnäytetyön tulosten pohjalta ja selvittää onko tilanne  
muuttunut. Vaikka organisaatiolla on ISO 27001 -sertifiointi, minkä myötä tieto-  
turvallisuuden hallintajärjestelmää arvioidaan säännöllisesti ulkoisten ja sisäis-  
ten auditoijien toimesta, voisi tämän opinnäytetyön kaltaiselle, mutta kevyem-  
mälle haastatteleamalla kerättävälle tilannekatsaukselle olla käyttöä myös jat-  
kossa. Tätä puoltaa myös sivulla 22 esitetty Raggadin (2010) toteamus ”Tieto-  
turvallisuudesta vastaavien tulisivin tehdä läheisesti yhteistyötä muun henkilös-  
tön kanssa tiedon jakamiseksi puolin ja toisin”.

Organisaation tietoturvakulttuurin muuttamisessa voidaan hyödyntää sivulla 20  
esitettyjä Scheinin (2009) kahdeksaa tapaa oppimisahdistuksen voittamiseksi.

Organisaatiossa on löydettävä oma tapansa viestiä ja kouluttaa tietoturvaa henkilöstölle vaikuttavasti. Koulutuksia suunniteltaessa on hyvä varmistaa, että erilaiset oppijat saavat mahdollisuuden oppia omalla tavallaan. Tiimit voidaan vastuuttaa järjestämään itse omia epävirallisia koulutuksia, jotka sopivat tiimin omaan kulttuuriin paremmin kuin yleiset virallisemmat koulutukset. Opittuja asioita on harjoiteltava sekä uusien toimintamallien noudattamista tulisi kannustaa esimerkiksi palkitsemisjärjestelmän muodossa. Tiivistetysti tietoturvan tulee tukea ja olla sidottu tavoitteisiin, jotka mahdollistavat organisaation menestymisen.

## 7 Pohdinta

Ennen opinnäytetyötä ISO 27001 -standardi ja siihen liittyvät ohjeistukset olivat jo tuttuja. Valmentavan johtajuuden käsite oli tuttu koulun opintojaksoilta ja organisaation tarjoamien koulutusten myötä. Organisaatiokulttuurin teoria tuli tutuksi vasta opinnäytetyötä tehdessä. Teoriaan syvempi tutustuminen oli mielenkiintoista ja se on auttanut hahmottamaan, millaista johtamis- ja organisaatiokulttuuria haluan itse olla edistämässä. Alkuun arvelutti, onko opinnäytetyön aiheen laajuus liikaa käsiteltäessä sekä valmentavaa johtajuutta että organisaatiokulttuuria. Jälkikäteen voidaan todeta olleen hyödyllistä käsitellä molempia aiheita, sillä ilman valmentavaa otettava tukevaa organisaatiokulttuuria on valmentavaa johtajuutta hankala toteuttaa.

Opinnäytetyöprosessi oli aikaa vievä projekti, joka viivästyi puolella vuodella työnantajan vaihtuessa syyskuussa 2022. Työnantajan vaihtuminen ei itsessään johtanut opinnäytetyön edistämisen lykkäämiseen. Itse asiassa tilanne olisi ollut jopa edullisempi tutkijalle, sillä uutena työntekijänä haastattelut olisi voitu tehdä lähestulkoon ulkopuolisena henkilönä. Uudessa organisaatiossa oli kuitenkin tilanne, jossa organisaatio oli ollut puolen vuoden ajan ilman tietoturvapäällikköä, minkä lisäksi tavoitteena oli saada ISO 27001 -sertifiointi vuoden 2023 aikana. Punnitsin tilannetta kahdesta näkökulmasta. Ensimmäinen näkökulma oli kuinka luotettavia tuloksia sen hetkisen tilanteen tutkiminen antaisi,

kun organisaatiosta on puuttunut yksi tietoturvan avainhenkilö pidemmän aikaa sekä samalla on menossa merkittävä projekti tietoturvallisuuden hallintajärjestelmän uudistamiseksi. Toinen näkökulma oli, mitä pidempään toimin itse tietoturvapääällikkönä sitä enemmän omat näkemykseni muovaavat organisaatiota sekä omia ennakko-oletuksia tutkimuksen suhteen. Päädyin tulokseen, että on pienempi paha vaikuttaa organisaation toimintaan kuin tehdä johtopäätöksiä merkittävien muutosten keskellä olevasta organisaatiosta.

Tämän opinnäytetyön tarkoituksena oli kartoittaa, kuinka valmentava johtajuus toteutuu organisaation tietoturvan johtamisessa ja kuinka tietoturva ilmenee organisaatiokulttuurissa. Vaikka valmentavan johtajuuden näkökulmaa juuri tietoturvan johtamisessa oli hankala todentaa, oli valmentavan johtajuuden olemassaolo havaittavissa organisaatiokulttuurissa enkä näe yhtään syytä miksi se ei toteutuisi myös tietoturvan johtamisessa tulevaisuudessa. Opinnäytetyön aihe oli ja on organisaatiolle ajankohtainen ja uskon tuloksista olevan hyötyä sekä organisaatiolle että itselleni tietoturvan johtamisen kehittämisessä. Haastateltavien määrää lisäämällä aineistoa olisi saatu enemmän. Toisaalta tietoturvallisuuden johtamisen ja ISO 27001 -sertifiointin vaatimusten ollessa uusia asioita organisaatiossa ei laajempi haastatteluaineisto välttämättä olisi antanut merkittävästi sisällöllisesti enempää. Työelämän kehittämisen projektina koen opinnäytetyön vastanneen tavoitteita ja olen lopputulokseen tyytyväinen. Opinnäytetyön tulokset olivat käytännönläheisiä näkökulmia organisaation toiminnasta, jotka vahvistivat organisaation aloittamien parannustoimenpiteiden olevan oikeansuuntaisia. Vaikka tuloksissa painotetaan paljon johdon vastuuta ja johdolta odotetaan paljon, on hyvä muistaa, ettei johto saa yksin tuloksia aikaiseksi vaan siihen tarvitaan aktiivista henkilöstön osallistumista sekä tietoturvasta käytännön tasolla vastaavia henkilöitä. Näiden sidosryhmien välillä tulee olla mahdollisuus käydä avointa ja rakentavaa dialogia toiminnan kehittämisestä.

Vaikka jokainen organisaation on omanlaisensa, niin omakohtaisen kokemuksen ja teoriaosuudessa esitettyjen kirjallisten lähteiden perusteella näkisin opinnäytetyössä havaittujen kehityskohteiden olevan universaaleja, eivätkä ne rajoitu ainoastaan tämän opinnäytetyön organisaatioon. Tämän vuoksi tämän opinnäytetyön tuloksia voidaan hyödyntää myös muissa organisaatioissa, jotka

ovat ottamassa tai ovat vasta ottaneet ISO 27001 -standardin käyttöön. Näille organisaatioille suosittelen nimeämään johdosta vastuuhenkilön, joka toimii keulakuvana tietoturvallisuuden johtamisessa. Tämän henkilön tulee sisäistää standardin vaatimukset, jotta hän voi ohjata hallintajärjestelmän käytännön ylläpidosta ja kehittämisestä vastuussa olevia henkilöitä. Kyseessä on tietoturvallisuuden hallintajärjestelmän johtamisen standardi, joten johdon edustajan on pystyttävä perustelemaan, miksi uusia toimintamalleja vaaditaan. Lisäksi standardin noudattaminen voi vaatia isoja hallinnollisia muutoksia koko organisaation tasolla, joita johdon on hyvä ohjata. Hallintamallin jalkauttamiseksi kannattaa jo heti alusta alkaen miettiä, kuinka nämä asiat viedään käytäntöön. Huomioitavia asioita ovat esimerkiksi, millaista koulutusta tarvitaan, kuka kouluttaa, kuinka opittuja asioita harjoitellaan ja oppiminen todennetaan. Jalkauttamista miettiessä on hyvä muistaa, että organisaatiossa tiimin toimintatavat tuntee parhaiten tiimi itse, minkä vuoksi henkilöstö tulee ottaa mukaan tietoturvallisten toimintatapojen suunnitteluun. Tämä ei tarkoita sitä, että jokainen tiimi tekee omanlaisensa ohjeistuksen vaan sitä, että tiimien on tunnettava organisaation yleiset tietoturvaohjeistukset sekä tunnistaa omissa työtehtävissään ne käyttötapa-  
paukset joihin ohjeistus ei ota kantaa ja joihin tiimikohtaiset ohjeistukset tarvitaan.

Opinnäytetyön aiheena oli tietoturvajohtaminen osaksi organisaatiokulttuuria. Onko tietoturvan johtaminen sitten lopulta sen erikoisempaa kuin minkään muunkaan asian johtaminen? Kun muistetaan, että tietoturva on teknisten kontrollien lisäksi myös oikeanlaisten toimintatapojen noudattamista, niin väittäisin ettei se ole. Tietoturvaa tulisi johtaa kuten mitä tahansa muutakin organisaation liiketoiminta-aluetta. Syy siihen, miksi aihe voidaan kokea haastavaksi, voi johtua siitä, että tietoturvasta huolehtiminen kuuluu kaikille ja sen varmistamiseksi tarvitaan koko organisaatiota. Tietoturva ei ole sitä, että organisaation tietoturvasta vastaavat henkilöt koittavat lisätä kerroksen tietoturvaa kaiken muun toiminnan päälle, vaan se olisi saatava sisäänrakennetuksi ominaisuudeksi. Pidän erityisesti sivulla 22 esitetystä Raggadin (2010) vertauksesta tietoturvan ja arkipäivän hygienian välillä. Hän vertaa tietoturvallisuuteen liittyvien toimintatapojen tärkeyttä arkipäiväiseen hygieniasta huolehtimiseen, kuten säännölliseen käsien pesemiseen. Tietoturvan toimintaympäristö muuttuu nopeasti, ja sen



vaatimukset edellyttävät jatkuvaa tietoisuutta ja aktiivista lähestymistapaa sekä henkilökohtaisessa elämässä kuin työssäkin. Ilman motivaatiota, harjoittelua ja jatkuvaa ylläpitoa siitä ei tule vakiintunutta toimintatapaa, kuten käsien pesemisestä. Siksi on tärkeää luoda yhteinen, vastustamaton positiivinen visio tietoturvasta, johon kaikki organisaatiossa sitoutuvat. Helppoa se ei ehkä ole, mutta se on olennaista kestävästä tietoturvakulttuurin rakentamisessa.

## Lähteet

- Antila, K. 2018. Kyberturvallisuuskoulutuksen suunnittelu ja toteuttaminen yrityksen johdolle. Tampereen ammattikorkeakoulu. Yrittäjyyden koulu-tus (YAMK). <https://urn.fi/URN:NBN:fi:amk-2018120420123>. 6.10.2023.
- Doan, M. 2019. Companies Need to Rethink What Cybersecurity Leadership Is. <https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is>. 29.9.2023
- Engel, J. 2018. Why Does Culture 'Eat Strategy For Breakfast'?. <https://www.forbes.com/sites/forbescoachescouncil/2018/11/20/why-does-culture-eat-strategy-for-breakfast/>. 13.10.2023.
- Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.
- Hirsjärvi, S. & Hurme, H. 2022. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Ellibs-ekirjat. Helsinki: Gaudeamus. 11.11.2023.
- Hirsjärvi, S., Remes, P. & Sajavaara, P. Tutki ja kirjoita. 2009. Helsinki: Kustannusosakeyhtiö Tammi.
- Hänninen, A. 2020. Tietoturva nousee toimintakulttuurista. <https://sfs.fi/tietoturva-nousee-toimintakulttuurista/>. 8.10.2023.
- Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2022. Johda riskejä – käytännön opas yrityksen riskienhallintaan. Turenki: Hansaprint Oy. Ellibs-ekirjat. 13.10.2023.
- Järvinen, P. 2022. Yrityksen tietoturvaopas. Helsinki: Helsingin seudun kauppa-kamari.
- Kallinen, T. & Kinnunen, T. 2022. Laadullisen tutkimuksen verkkokäsikirja. Yhteiskuntatieteellinen tietoarkisto. <https://www.fsd.tuni.fi/fi/palvelut/metelmaopetus/kvali/laadullisen-tutkimuksen-aineistot/haastattelu/>. 10.12.2022.
- Kallinen, T. & Kinnunen, T. 2023 Etnografia. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. <https://www.fsd.tuni.fi/fi/palvelut/metelmaopetus/kvali/mita-on-laadullinen-tutkimus/johdatus-laadulliseen-tutkimukseen-ja-verkkokasikirjaan/>. 19.11.2023.
- Kananen, J. 2014 Laadullinen tutkimus opinnäytetyönä. Miten kirjoitan kvalitatiivisen opinnäytetyön vaihe vaiheelta. Jyväskylä: Jyväskylän ammattikorkeakoulu.
- Korhonen, H. & Bergman, T. 2019. Johtaja muutoksen ytimessä, käsikirja uudistumismatkalle. Helsinki: Alma Talent Oy. Alma Talent Oy Verkkokirjahylly. 13.10.2023.
- Kortelainen, S. 2019. Meita on inhouse-yhtiö – mitä se oikein tarkoittaa?. Meitan Blogi. 28.5.2019. Blogi. <https://www.meita.fi/2021/05/meita-on-inhouse-yhtio-mita-se-oikein-tarkoittaa/>. 27.10.2023.
- Kupias, P., Peltola, R. & Pirinen, J. 2014. Esimies osaamisen kehittäjänä. Helsinki: Alma Talent Oy. Alma Talent Oy Verkkokirjahylly. 13.10.2023.
- Kuusela, S. 2015. Organisaatioelämää Kulttuurin voima ja vaikutus. Helsinki: Alma Talent Oy. Alma Talent Oy Verkkokirjahylly. 14.10.2023
- Meita. 2023a. Yhtiömme. <https://www.meita.fi/yhtiomme/>. 7.10.2023.

- Meita. 2023b. Meita yhtiön esittely. Meidän It ja Talous oy:n intra. 7.10.2023.
- Meita. 2023c. Me olemme Työpäiväsi taustavoima. [https://www.meita.fi/tyopai-  
kat/](https://www.meita.fi/tyopai-<br/>kat/). 7.10.2023.
- Meita. 2023d. Meitan ja Efettan arvot. Meidän It ja Talous oy:n intra. 7.10.2023.
- Meita. 2023e. Strategia ja toimintasuunnitelma 2023. Meidän It ja Talous oy:n intra. 7.10.2023.
- Meita. 2023f. Tietoturva- ja tietosuojakäsikirja – Lainsäädäntö. Meidän It ja Talous oy:n intra. 27.10.2023
- Meita. 2023g. Toimintaympäristön tilannekuva. Meidän It ja Talous oy:n intra. 27.10.2023.
- Paulsen, C. & Coulson, T. 2011. Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security. Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security (csusb.edu). 6.10.2023.
- Raggad, B. 2010. Information Security Management. Concepts and Practice. Milton Park: Taylor & Francis Group.
- Ristikangas, M-R. & Grünbaum, L. 2014. Valmentava esimies - Onnistumista palvelevat positiot. Helsinki: Talentum.
- Ristikangas, M-R., Lönnroth, A., Ristikangas, V. & Ristikangas, V. 2021. Valmentava tiimin johtaminen – yhdessäohjautuvuus ja systeeminen ajattelu onnistumistekijöinä. Helsinki: Alma Talent Oy. Alma Talent Oy Verkkokirjahylly. 14.10.2023.
- Ristikangas, M-R. & Ristikangas, V. 2010. Valmentava johtajuus. Helsinki: WSOYPro.
- Ristikangas, M-R. & Ristikangas, V. 2018. Valmentava johtajuus. Helsinki: Alma Talent. Ellibs-ekirjat. 7.1.2024.
- Ruonala, K. 2011. Kunnan tietoturvajohtaminen: Tietoturvan jalkauttaminen osaksi arkipäivän toimintaa. Rovaniemen ammattikorkeakoulu. Teknologiaosaaminen ja johtaminen (YAMK). <https://urn.fi/URN:NBN:fi:amk-201105249399>. 6.10.2023
- Räsänen, M. 2010. Coaching ja johtajuus, valmentava ote esimiestyössä. Helsinki: Edita Publishing Oy.
- Salmimies, R. & Ruutu, S. 2013. Ratkaisuja esimiestyön haasteisiin. Alma Talent Oy Verkkokirjahylly. 5.1.2024.
- Schein, E. 2009. Yrityskulttuuri – selviytymisopas. Espoo: Suomen Laatukeskus Oy.
- SFS-EN ISO/IEC 27001:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS.
- SFS-EN ISO/IEC 27002:2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Helsinki: Suomen Standardisoimisliitto SFS.
- SFS-EN ISO/IEC 27003:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Ohjeistusta. Helsinki: Suomen Standardisoimisliitto SFS.
- SFS-EN ISO/IEC 27002:2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. Helsinki: Suomen Standardisoimisliitto SFS.
- SGS. 2023. ISO/IEC 27001:2013 – tietoturvallisuuden hallintajärjestelmät. ISO/IEC 27001:2013 – tietoturvallisuuden hallintajärjestelmät | SGS Finland. 15.10.2023.

- Traficom. 2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. [https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T\\_KyberHV\\_digiAUK\\_220120.pdf](https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf). 10.12.2022.
- Traficom. 2019. Luottamuksen lähteillä, näkökulmia tietoturvan standardointiin ja sertifiointiin. Luottamuksen\_lahteilla.pdf (kyberturvallisuuskeskus.fi). 15.10.2023.
- Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Kustannusosakeyhtiö Tammi.
- Tutkimuseettinen neuvottelukunta. 2019. Ihmiseen kohdistuvan tutkimuksen eettiset periaatteet ja ihmistieteiden eettinen ennakkoarviointi Suomessa. Tutkimuseettisen neuvottelukunnan ohje 2019. Tutkimuseettisen neuvottelukunnan julkaisuja 3/2019. Ihmiseen kohdistuvan tutkimuksen eettiset periaatteet ja ihmistieteiden eettinen ennakkoarviointi Suomessa (tenk.fi). 4.1.2024.
- Viljamaa, K. 2023. Työssäjaksamisen tukeminen johtamisen keinoin. Oulun ammattikorkeakoulu. Liiketalouden kehittäminen (YAMK). Opinnäytetyö. <https://urn.fi/URN:NBN:fi:amk-2023080724664>. 6.10.2023.

## Teemahaastattelurunko

Teemat:

1. Valmentava johtajuus tietoturvallisuuden johtamisessa
2. Organisaation tietoturvakulttuuri

Apukysymykset teemoittain:

1. Kuinka valmentava johtajuus toteutuu tietoturvallisuuden johtamisessa?
  - a. Voitko antaa esimerkin tilanteesta, jossa valmentava johtajuus on ollut nähtävissä?
  - b. Miten esihenkilöt tukevat tietoturvallisuuteen liittyvissä kysymyksissä ja asioissa?
  - c. Millaisia tietoturvakoulutuksia ja/tai -valmennuksia yrityksessä on järjestetty?
  - d. Millaisia haasteita tietoturvallisuuden johtamisessa on ollut tai on?
  - e. Kuinka valmentava johtajuus näkyy tietoturvaan liittyvien päätösten ja strategian kehittämisessä?
2. Kuinka tietoturvallisuus näkyy organisaatiokulttuurissa?
  - a. Miten yrityksen arvot ja tavoitteet tukevat tietoturvallisuutta?
  - b. Kuinka tietoturvallisuudesta kommunikoidaan?
    - i. Missä foorumissa?
    - ii. Kuka kommunikoi?
    - iii. Sävy, kannustava/syyllystävä, positiivista/negatiivista?
  - c. Millä tavoin tietoturvallisuus on osa jokapäiväistä työskentelyä?
    - i. kuinka se ilmenee?
    - ii. kuinka työntekijöitä kannustetaan ja motivoidaan noudattamaan tietoturvaohjeita?
    - iii. kuinka tietoturvaohjeistusten noudattaminen näkyy tai vaikuttaa työtehtävien suorittamisessa?
  - d. Millä tavoin tietoturvaan liittyviin ongelmiin reagoidaan?
    - i. Opitaanko niistä?
    - ii. Jaetaanko tietämystä?

## Haastattelukutsu

Hei,

opiskelen johtamisen ja liiketoimintaosaamisen koulutusohjelmaa Karelia ammattikorkeakoulussa (YAMK). Opinnäytetyöni aiheena on tietoturvajohdaminen osaksi organisaatiokulttuuria. Tavoitteena on selvittää, kuinka valmentava johtajuus näkyy yrityksemme tietoturvallisuuden johtamisessa ja kuinka tietoturvallisuus ilmenee organisaatiokulttuurissamme. Tutkimusaineisto kerätään haastatteleamalla eri työtehtävissä olevia henkilöitä, joiden vastausten perusteella karotetaan tietoturvallisuuden johtamisen ja tietoturvakulttuurin nykytilaa sekä kehitystarpeita. Haastateltavien nimeä, tarkkaa työnimikettä tai mitään muitakaan tunnistetietoja ei esitetä opinnäytetyössä. Haastattelu pidetään Teams-tapaamisessa ja se tallennetaan. Haastattelutallenteet litteroidaan ja analysoidaan. Haastattelutallenteet tuhoetaan heti, kun aineisto on saatu käsiteltyä. Haastattelutallenteet ovat ainoastaan opinnäytetyöntekijän käytössä. Haastattelu kestää noin 60–90 minuuttia.

Osallistumalla haastatteluun annat suostumuksen haastattelussa antamiesi tietojen käsittelyyn opinnäytetyön tekemisessä. Voit perua osallistumisesi ja kieltää tietojesi käyttämisen missä tahansa opinnäytetyön tekemisen kohtaa.

Lisätietoja haastattelusta voit kysyä joko sähköpostitse tai Teamsin kautta.

Eetu Sormunen